Information Security for Digital Researchers

Jonathan Martin
Welcome to DHSI 2019!

Thanks for joining the DHSI community!

In this booklet, you will find essential course materials prefaced by some useful information about getting settled initially at UVic, finding your way around, getting logged in to our network (after you’ve registered the day before our courses begin), and so on.

Given our community’s focus on things computational, it will be a surprise to no one that we might expect additional information online for some of the classes - your instructors will let you know - or that the most current version of all DHSI-related information may be found on our website at dhsi.org.

Do check in there first if you need anything that’s not in this coursepak.

To access the DHSI wifi network, simply go into your wireless settings and connect to the “DHSI” network and enter the password “dhsi2019”.

And please don’t hesitate to be in touch with us at institut@uvic.ca or via Twitter at @AlyssaA_DHSI or @DHInstitute if we can be of any help ....
DHSI Wi-Fi

Network name: DHSI
Passkey: dhsi2019
The 2019 schedule is just taking shape nicely! A very few things to confirm, add, etc, still but this is the place to be to find out what is happening when / where ...

Psst: Some Suggested Outings

If you're here a day or two before we begin, or staying a day or two afterwards, here are a few ideas of things you might consider doing ....

Suggested Outing 1, Botanical Beach (self-organised; car needed)

A self-guided visit to the wet, wild west coast tidal shelf (and historically-significant former research site) at Botanical Beach: we recommend departing early (around 8.00 am) to catch low tide for a better view of the wonderful undersea life! Consider bringing a packed lunch to nibble-on while looking at the crashing waves when there, and then have an afternoon drink enjoying the view from the deck of the Port Renfrew Hotel.

Suggested Outing 2, Butchart Gardens (self-organised)

A shorter journey to the resplendently beautiful Butchart Gardens and, if you like, followed by (ahem) a few minutes at the nearby Church and State Winery, in the Saanich Penninsula. About an hour there by public bus from UVic, or 30 minutes by car.

Suggested Outing 3, SaltSpring Island (self-organised; a full day, car/bus + ferry combo)

Why not take a day to explore and celebrate the funky, laid back, Canadian gulf island lifestyle on SaltSpring Island. Ferry departs regularly from the Schwartz Bay ferry terminal, which is about one hour by bus / 30 minutes by car from UVic. You may decide to stay on forever ....

Suggested Outing 4, Paddling Victoria's Inner Harbour (self-organised)

A shorter time, seeing Victoria's beautiful city centre from the waterways that initially inspired its foundation. A great choice if the day is sunny and warm. Canoes, kayaks, and paddle boards are readily rented from Ocean River Adventures and conveniently launched from right behind the store. Very chill.

And more!

Self-organised High Tea at the Empress Hotel, scooter rentals, visit to the Royal BC Museum, darts at Christies Carriage House, a hangry breakfast at a local diner, whale watching, kayaking, brew pub sampling (at Spinnaker's, Swans, Moon Under Water, and beyond!), paddle-boarding, a tour of used bookstores, and more have also been suggested!

Sunday, 2 June 2019 [DHSI Registration + Suggested Outings]

9:00 to 4:00

Early Class Meeting: 4. [Foundations] DH For Department Chairs and Deans (David Strong Building C124, Classroom)

Further details are available from instructors in mid May to those registered in the class. Registration materials will be available in the classroom.

3:00 to 5:00

DHSI Registration (MacLaurin Building, Room A100)

After registration, many will wander to Cadboro Bay and the pub at Smuggler's Cove OR the other direction to Shelbourne Plaza and Maude Hunter's Pub OR even into the city for a nice meal.

Monday, 3 June 2019

Your hosts for the week are Alyssa Arbuckle, Ray Siemens, and Jannaya Friggstad Jensen.

7:45 to 8:15

Last-minute Registration (MacLaurin Building, Room A100)
Welcome, Orientation, and Instructor Overview (MacLaurin A144)
- Welcome to the Territory
- Welcome to DHSI: Ray Siemens, Alyssa Arbuckle
- Welcome from UVic: Jonathan Bengtson (University Librarian), Alexandra D'Arcy (Associate Dean Research, Humanities)

8:30 to 10:00

Classes in Session (click for details and locations)
- 1. [Foundations] Digitisation Fundamentals and their Application (Clearihue A103, Lab)
- 2. [Foundations] Introduction to Computation for Literary Criticism (Clearihue A102, Lab)
- 4. [Foundations] DH For Department Chairs and Deans (David Strong Building C124, Classroom)
- 5. [Foundations] Developing a Digital Project (With Omeka) (Clearihue A031, Lab)
- 9. Out-of-the-Box Text Analysis for the Digital Humanities (Human and Social Development A160, Lab)
- 10. Sound and Digital Humanities (Cornett A120, Classroom)
- 11. Critical Pedagogy and Digital Praxis in the Humanities (Clearihue D132, Classroom)
- 12. Digital Humanities for Japanese Culture: Resources and Methods (McPherson Library A003, Classroom)
- 14. Retro Machines & Media (McPherson Library 120, Classroom)
- 15. Geographical Information Systems in the Digital Humanities (Clearihue A105, Lab)
- 16. Introduction to IIIF: Sharing, Consuming, and Annotating the World’s Images (Cornett A121, Classroom)
- 17. Web APIs with Python (Human and Social Development A170, Lab)
- 18. Ethical Data Visualization: Taming Treacherous Data (Cornett A128, Classroom)
- 19. Linked Open Data and the Semantic Web (Cornett A132, Classroom)
- 21. Information Security for Digital Researchers (David Strong Building C114, Classroom)

10:15 to Noon

12:15 to 1:15

Lunch break / Unconference Coordination Session (MacLaurin A144)
(Grab a sandwich and come on down!)
Discussion topics, scheduling, and room assignments from among all DHSI rooms will be handled at this meeting.

1:30 to 4:00

Classes in Session

Institute Lecture: Jacqueline Wernimont (Dartmouth C): “Sex and Numbers: Pleasure, Reproduction, and Digital Biopower”
Chair: Anne Cong-Huyen (U Michigan)
(MacLaurin A144)

4:10 to 5:00

Abstract: Drawing from Numbered Lives (MIT 2018), this talk will consider a long history of sex-number entanglement in Anglo-American Cultures. Drawing on historical and contemporary objects and practices, Wernimont will ask “in what ways do theories of biopower, critical gender and critical race studies, and media studies” suggest that we can understand this set of entanglements and their impacts. NB: While relevant, this talk will not include discussions of sexual trauma or violence. It will include frank discussion of sex acts and various ways of translating sexual behavior into numbers.

5:00 to 6:00

Opening Reception (University Club)

Tuesday, 4 June 2019

9:00 to Noon

Classes in Session

12:15 to 1:15

Lunch break / Unconference

"Mystery" Lunches

1:30 to 4:00

Classes in Session

DHSI Conference and Colloquium Lightning Talk Session 1 (MacLaurin A144)
Wednesday, 5 June 2019

9:00 to Noon Classes in Session

Lunch break / Unconference

"Mystery" Lunches

Presentation: An Introduction to Scholarly Publishing with Manifold (MacLaurin A144)
Lunch included for those who [register here]

This presentation introduces Manifold Scholarship, a Mellon-funded digital publishing platform developed by the CUNY Graduate Center, The University of Minnesota Press, and Cast Iron Coding. Manifold allows you to create beautiful, dynamic open access projects that can include text, images, video, embedded resources, and social annotation. We will provide an overview of Manifold and demonstrate how faculty, students and staff in the digital humanities can use Manifold to publish open access scholarly works, conduct and participate in peer review, and create custom edited versions of public domain course texts and OER.

12:15 to 1:15 Classes in Session

DHSI Conference and Colloquium Lightning Talk Session 2 (MacLaurin A144)
Chair: Kim O'Donnell (Simon Fraser U)

- Catherine Ryu (Michigan State U), "Tone Perfect: Developing a Multimodal Audio Database for Mandarin Chinese as an Open Source"
- Kenzie Burchell (U Toronto Scarborough), "Making Responsible Reporting Practices Visible: Comparing newswire coverage of humanitarian crises in Syria"
- Jessica Linzel (Brock U), "The Shopkeeper Aristocracy: Mapping Trade Networks in Colonial Niagara"
- Kirsten Painter (U Washington), "From Bogatyr to Bread: Digitization & Online Exhibition of Rare Russian Children's Books at the U Washington"
- John Barber (Washington State U), "A Mighty Span"

6:00 to 7:00 "Half Way There!" [An Informal, Self-Organized Birds of a Feather Get-Together] (Felicitas, Student Union Building)
Bring your DHSI nametag and enjoy your first tipple on us! [A great opportunity for an interest group meet-up ....]

Thursday, 6 June 2019

9:00 to Noon Classes in Session

Lunch break / Unconference

"Mystery" Lunches

[Instructor lunch meeting]

4:15 to 5:15 Classes in Session

DHSI Conference and Colloquium Lightning Talk Session 3 (MacLaurin A144)
Chair: Kim O'Donnell (Simon Fraser U)

- Colleen Kolba (U South Florida), "What Comics can Teach our Students about Multimodal Literacy"
- Trish Baer (ETCL; U Victoria), "Preserving Digital Legacies: Archived Websites and Digital Discoverability"
- Suchismita Dutta (U Miami), "The Importance of Archival Transcription for Genre Building"
- Jeffrey Lawler (California State U, Long Beach), "Twining our way through the Past: Video Game Authoring as History Pedagogy"
Sean Smith (California State U, Long Beach), “Gaming the History Curriculum, Games Writing as History Pedagogy in College Classroom”

Friday, 7 June 2019 [DHSI; ADHO Pedagogy SIG Conference Opening]

9:00 to Noon
Classes in Session

12:15 to 1:15
Lunch Reception / Course E-Exhibits (MacLaurin A100)

1:30 to 1:50
Remarks, A Week in Review (MacLaurin A144)

2:00 to 3:00
Joint Institute Lecture (DHSI and ADHO Pedagogy SIG Conference):
Matt Gold (CUNY Graduate Center and Association for Computers and the Humanities): “Thinking Through DH: Proposals for Digital Humanities Pedagogy”
Chair: Diane Jakacki (Bucknell U)

Abstract: How do we teach digital humanities, and how should DH be taught? What, indeed, should we teach when we teach DH? This talk will present a proposal for grounding digital humanities pedagogical practice in the research interests of our students and the epistemological foundations of our methods rather than through an approach grounded more central in data and methods.

Joint Reception: DHSI and ADHO Pedagogy SIG Conference (University Club)
E-Poetry Event (Chris Tanasescu)
Watch this space for details, including how to participate!

DHSI Conference and Colloquium Poster/Demo Session
- Pia Russel (U Victoria); Emily Stremel (U Victoria), “British Columbia’s Historical Textbooks Digital Library”
- Cody Hennesy (U Minnesota); Rachael Samberg (U California, Berkeley); Stacy Reardon (U California, Berkeley), “Finding the Haystack: Literacies for Accessing and Using Text as Data”
- Paula Johanson (ETCL; Independent Scholar), “Proving Seahorses and Juan de Fuca’s Travels in The Curve of Time”
- Tara Baillargeon (Marquette U); Elizabeth Wawrzyniak (Marquette U), “FellowsHub: J. R. R. Tolkien Fanzine Portal”
- Caterina Agostini (Rutgers U), “Art at the Time of Syphilis: A First-Person Medical Narrative in Benvenuto Cellini’s Vita”
- Lauren Elle DeGaine (ETCL; U Victoria), “Women at the Front: A Digital Exhibit of Victorian Frontpiece Illustrations”
- Adam Griggs (Mercer U); Kathryn Wright (Mercer U); Christian Pham (Mercer U); Gail Morton (Mercer U); Stephanie Miranda (Mercer U), “Digitizing Middle Georgia’s History of Slavery”

Saturday, 8 June 2019 [Conference, Colloquium, and Workshop Sessions]

8:00 to 9:00
Conference / Workshop Registration (MacLaurin A100)
The day’s events are included with your DHSI registration. If you’re not registered in DHSI, you’re very welcome to join us by registering here as a Conference / Colloquium / Workshop participant. We’ll have a nametag waiting for you!

Coffee, Tea, &c?
Looking for some morning coffee or tea, or a small nibble? Options and hours of operation for weekend campus catering are available here. Mystic Market usually opens around 10.00.

9:00 to 4:00
DHSI Conference and Colloquium Sessions
ADHO Pedagogy SIG Conference Sessions
Right2Left Workshop Sessions

9:00 to 4:00
All Day DHSI Workshop Session (click for workshop details and free registration for DHSI participants)
- 55. Introduction to Machine Learning in the Digital Humanities [8-9 June; All day, each day] (David Strong Building C124, Classroom)

9:00 to 9:10
Informal Greetings, Room Set-up (Lobby, outside Hickman 105)

Session 1
DHSI Colloquium and Conference (Hickman 105)
Digital Humanities & Literature, Chair: Kim O’Donnell (Simon Fraser U)
- Youngmin Kim (Dongguk U), “Transdiscursivity in the Convergence of Digital Humanities and World Literature”
- Caroline Winter (U Victoria), “Digitizing Adam Smith’s Literary Library”
- Kaitlyn Fralick (U Victoria); Kailey Fukushima (U Victoria); Sarah Karlson (U Victoria), “Victorian Poetry
<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
</table>
| 9:10 to 10:30| **ADHO Pedagogy SIG Conference** (Hickman 110)<br>Chair: Katherine Faull (Bucknell U)<br>Aaron Tucker and Nada Savicevic (Ryerson U), "Write Here, Right Now: An Open Source eTextbook for the Flipped Classroom"
Heather McAlpine (U Fraser Valley), "Digital Meters: Using Text Encoding to Teach Literature in the Undergraduate Classroom"
Tiina H. Airaksinen (U Helsinki), "Digital Humanities in Cultural Studies: Creating a MOOC course for University Students and A-Level Students"
| Right2Left Workshop (Hickman 116)<br>Keynote - Nathan P. Gibson (Ludwig Maximilians U, München): "Thinking in #JTR: Reorienting the Directional Assumptions of Global Digital Scholarship" |
| 10:30 to 10:40| Break                                                                                         |
| 10:40 to Noon| **Session 2**<br>DHSI Colloquium and Conference (Hickman 105)<br>Digital Humanities & Society, Chair: Eleanor Reed (Hastings C)<br>- Joel Zapata (Southern Methodist U), "Uncovering the Southern Plains’ Mexican American Civil Rights Movement"
- Ayo Oisainwo (U Ibadan), "Online Newspaper Construction of Agitation for the Sovereign State of Biafra in Nigeria"
- Joseph Jones (U British Columbia), "Testbed for an Approach to Distant Reading: Fictions That Represent Vietnam War Resisters in Canada"
- Brendan Mackie (U California, Berkeley), "Visualizing Long-Term Cultural Change: An Example From The Birth of Civil Society"
| ADHO Pedagogy SIG Conference (Hickman 110)<br>Chair: Laura Estill (St Francis Xavier U)<br>Jane Jackson (Chinese U of Hong Kong), "Interrogating digital spaces for intercultural meaning-making"
Ryan Ikeda (UC Berkeley), "Disrupting Digital Literacy: Situating Electronic Literature Among Public Education Initiatives"
Christopher Church, Katherine Hepworth (U Nevada, Reno), "We’re STEAMed! A call for balancing technical instruction and disciplinary content in the digital humanities"
Chelsea Milbourne (Cal Poly, San Luis Obispo), "Finding the Right Fit between Technology and Class Content: Reflections on Including Web Development in a Digital Storytelling Course"
| Right2Left Workshop (Hickman 116)<br>- Edward "Eddie" Surman (Claremont Graduate U), "Qualitative Digital Text Analysis and #Right2Left Languages: A Demonstration of Atlas.ti using the Hebrew Bible"
| Noon to 1:10 | Lunch (We recommend Mystic Market on weekends!)                                                |
| 1:10 to 2:30 | **Session 3**<br>DHSI Colloquium and Conference (Hickman 105)<br>Digital Humanities & Community, Chair: Claire Carlin (U Victoria)<br>- Pia Russel (U Victoria); Emily Stremel (U Victoria), "Mentorship and disability: Supporting disabled employees in digital humanities"
- Amy Lueck (Santa Clara U), "Virtually Emplacing Indigenous Memory"
- Md. Shehabul Alam (National U Bangladesh), "Integrating Library Service with Union Information and Service Center: A Joint Initiative towards Digital Bangladesh"
- Veronica Gomez (Instituto de Humanidades y Ciencias Sociales (HuCoSo) - UNL-CONICET), "Latin American E-literature and Location: The Nation Revisited in Electronic Literature Organization (ELO)"
| ADHO Pedagogy SIG Conference (Hickman 110)<br>Chair: Chris Tănăsescu (UC Louvain)<br>Laura Estill (St Francis Xavier U), "One Assignment, Three Ways: Assessing DH Projects in a Literature Course"
Felix Bayode Oke, Stella N. Kpolugbo (Anchor U Lagos), "The Multimodal Technique as a Pedagogical Tool in Pelu Awofeso’s White Lagos: A Definitive and Visual Guide to the Eyo Festival"
Shu Wan (U Iowa), "A digital "historical gaze" of Chinese students in Iowa, 1911-1930"
Francesca Giannetti (Rutgers U, New Brunswick), "So near while apart: Correspondence Editions as Critical Library Pedagogy and Digital Humanities Methodology"
| Right2Left Workshop (Hickman 116)<br>- Najla Jarkas (American U Beirut) and David Joseph Wrisley (NYU Abu Dhabi), "RTL Software Localization and Digital Humanities: the Case Study of Translating Voyant Tools into Arabic"
Sunday, 9 June 2019 [Workshop Sessions]

DHSI Registration (MacLaurin Building, Room A100)

8:00 to 5:00
The day’s events are included with your DHSI registration. If you're not registered in DHSI, you're very welcome to join us by registering here as a Conference / Colloquium / Workshop participant. We'll have a nametag waiting for you!

Coffee, Tea, &c?
Looking for some morning coffee or tea, or a small nibble? Options and hours of operation for weekend campus catering are available here. Mystic Market usually opens around 10.00.

9:00 to 4:00
All Day Workshop Sessions (click for workshop details and free registration for DHSI participants)
- 55. Introduction to Machine Learning in the Digital Humanities [8-9 June; All day, each day] (David Strong Building C124, Classroom)
- 56. Pedagogy of the Digitally Oppressed: Anti-Colonial DH Methods and Praxis [9 June; All Day] (Hickman 116, Classroom)
- 57. Natural Language Processing and Network Coding Apps for Text & Textual Corpus Analysis in the Humanities [9 June; All Day] (David Strong Building C114, Classroom)

AM Workshop Sessions (click for workshop details and free registration for DHSI participants)
- 59. 3D Visualization for the Humanities [9 June; AM] (Cornett A229, Classroom)
- 60. It’s All Relational: AbTeC’s Indigenous Video Game Workshops as Storytelling Praxis [9 June; AM] (Cornett A121, Classroom)
- 61. Spatial DH: De-Colonizing Cultural Territories Online [9 June; AM] (Clearihue D130, Classroom)
- 63. Creating a CV for Digital Humanities Makers [9 June; AM] (David Strong Building C108, Classroom)

Noon to 1:00
Lunch (We recommend Mystic Market on weekends!)

PM Workshop Sessions (click for workshop details and free registration for DHSI participants)
- 65. Indigenous Futures in the Classroom and Beyond [9 June; PM] (Cornett A121, Classroom)
- 66. DHSI Knits: History of Textiles and Technology [9 June; PM] (Fine Arts 109, Classroom)
- 68. Linked Open Datafication for Humanities Scholars [9 June; PM] (McPherson Library A003, Classroom)
- 69. Stylo - WYSIWYM Text Editor for Humanities Scholars [9 June; PM] (McPherson Library A025, Classroom)

After the day, many will wander to Cadboro Bay and the pub at Smuggler's Cove OR the other direction to Shelbourne Plaza and Maude Hunter's Pub OR even into the city for a bite to eat.
### Tuesday, 11 June 2019

<table>
<thead>
<tr>
<th>7:45 to 8:15</th>
<th>DHSI Last-minute Registration (<a href="#">MacLaurin A100</a>)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30 to 10:00</td>
<td>Welcome, Orientation, and Instructor Overview (<a href="#">MacLaurin A144</a>)</td>
</tr>
</tbody>
</table>

#### Classes in Session (click for details and locations)

- 33. Digital Storytelling ([Cornett A120](#), Classroom)
- 34. Text Mapping as Modelling ([Clearihue D131](#), Classroom)
- 35. Stylometry with R: Computer-Assisted Analysis of Literary Texts ([Clearihue A102](#), Lab)
- 36. Open Access and Open Social Scholarship ([Clearihue D130](#), Classroom)
- 37. Digital Games as Tools for Scholarly Research, Communication and Pedagogy ([Cornett A229](#), Classroom)
- 38. Queer Digital Humanities ([David Strong Building C114](#), Classroom)
- 39. Parsing and Writing XML with Python ([Clearihue A108](#), Lab)
- 40. Introduction to Electronic Literature in DH: Research and Practice ([Cornett A128](#), Classroom)
- 41. Surveillance and the Critical Digital Humanities ([David Strong Building C108](#), Classroom)
- 42. Text Analysis with Python and the Natural Language ToolKit ([Clearihue A103](#), Lab)
- 43. Creating LAMP Infrastructure for Digital Humanities Projects ([Human and Social Development A170](#), Lab)
- 44. Processing Humanities Multimedia ([Human and Social Development A150](#), Lab)
- 45. Digital Humanities Pedagogy: Integration in the Curriculum ([Cornett A121](#), Classroom)
- 46. Accessibility & Digital Environments ([Priestly Law Library 265](#), Classroom)
- 47. Agile Project Management ([Cornett A132](#), Classroom/Lab)
- 48. XPath for Processing XML and Managing Projects ([Clearihue A105](#), Lab)
- 49. Endings: How to End (and Archive) your Digital Project ([Priestly Law Library 192](#), Classroom)
- 50. Text Processing - Techniques & Traditions ([McPherson Library A025](#), Classroom)
- 51. Introduction to Humanities Data Analysis & Visualization in R ([Human and Social Development A160](#), Lab)
- 52. Introduction to Network Analysis in the Digital Humanities ([Clearihue D132](#), Classroom)

#### 12:15 to 1:15

Lunch break / Unconference Coordination Session ([MacLaurin A144](#))

Grab a sandwich and come on down!

"Mystery" Lunches

### 1:30 to 4:00

Classes in Session

### 4:10 to 5:00

Institute Lecture: Angel David Nieves (San Diego State U): "3D Mapping and Forensic Traces of Testimony: Documenting Apartheid-Era Crimes Through the Digital Humanities"

Chair: Constante Crompton (U Ottawa)

([MacLaurin A144](#))

Abstract: In 1989 the killing of a queer, 14-year-old youth in Winnie Mandela's house named Stompie Seipei (an event that few in South Africa are willing to recall, let alone discuss, in any detail) -- is perhaps one of the most glaring examples where the queer and activist community was suppressed or erased from anti-apartheid/liberation histories. Digital humanities may actually help both reconstruct and uncover a history that is still very early in the telling, despite what is commonly believed about the liberation struggle and the contributions of queer activists in the dismantling of apartheid. Perhaps it could explain why a youth such as Seipei was killed -- or at the very least, provide a more complex and messy narrative that permits one to know more how the history of queer anti-apartheid activists was suppressed. This talk outlines a methodology for "messy thinking and writing" in the digital humanities that -- through a queer and feminist intersectional framework -- permits a more complex layering of oral histories and 3D historical reconstructions.

### 5:00 to 6:00

Reception ([University Club](#))

### 9:00 to Noon

Classes in Session

### 10:15 to Noon

Lunch break / Unconference Coordination Session ([MacLaurin A144](#))

### 12:15 to 1:15

"Mystery" Lunches
Wednesday, 12 June 2019

1:30 to 4:00
Classes in Session

4:15 to 5:15
DHSI Conference and Colloquium Lightning Talk Session 4
Chair: Lindsey Seatter (U Victoria)
- Ashley Caranto Morford (U Toronto); Kush Patel (U Michigan); Arun Jacob (McMaster U), "Our DHs anti-colonial: Questions and challenges in dismantling colonial influences in digital humanities pedagogy"
- Julia King (U Bergen), "Developing Network Visualizations of Syon Abbey's Books, 1415-1539"
- Luis Meneses (ETCL; U Victoria), "Identifying Changes in the Political Environment in Ecuador"
- Alicia Brown (Texas Christian U), "Digital Cartography of the Ancient World"
- Laura Horak (Carleton U), "Building the Transgender Media Portal"
- Andrew Boyles Peterson (Michigan State U), "Last Mile Tracking: Implications of Rental Scooter Surveillance"

6:00 to 8:00
DHSI Newcomer's Gathering (Grad House Restaurant, Graduate Student Centre)
Come down, buy meal and a beverage, and make some new friends!

9:00 to Noon
Classes in Session

12:15 to 1:15
Lunch break / Unconference

"Mystery" Lunches

12:15 to 1:15
Presentation: An Introduction Jupyter Notebooks for Researchers
Chair: Lindsey Seatter (U Victoria)
- Calin Murgu (New College of Florida), "Putting local metadata to strategic use: A Dashboard for visualizing 60 years of theses metadata"
- Jason Lajoie (U Waterloo), "Queer Critical Making and the Logic of Control"
- John Barber (Washington State U), "Zambezi River Bridge"
- Kent Emerson (U Wisconsin-Madison), "Digital Mappa and the George Moses Horton Project"

1:30 to 4:00
Classes in Session

4:15 to 5:00
Institute Lecture: Karina van Dalen-Oskam (Huygens Institute and U Amsterdam; Alliance of Digital Humanities Organizations): "The Riddle of Literary Quality: Some Answers"
Chair: Aaron Mauro (Penn State, Behrend C)
Abstract: What is literature, and can you measure it? That is the key question of the project The Riddle of Literary Quality. "The Riddle" is a research project of the Huygens Institute for the History of the Netherlands (Amsterdam) in collaboration with the Fryeke Akademy (Leeuwarden) and the Institute for Logic, Language and Computation (University of Amsterdam). The Riddle combines computational analysis of writing style with the results of a large online survey of readers, completed by almost 14,000 participants. In my talk, I will go into...

Thursday, 13 June 2019

9:00 to Noon
Classes in Session

12:15 to 1:15
Lunch break / Unconference

"Mystery" Lunches

1:30 to 4:00
Classes in Session

4:10 to 5:00
Institute Lecture: Karina van Dalen-Oskam (Huygens Institute and U Amsterdam; Alliance of Digital Humanities Organizations): "The Riddle of Literary Quality: Some Answers"
Chair: Aaron Mauro (Penn State, Behrend C)
Abstract: What is literature, and can you measure it? That is the key question of the project The Riddle of Literary Quality. "The Riddle" is a research project of the Huygens Institute for the History of the Netherlands (Amsterdam) in collaboration with the Fryeke Akademy (Leeuwarden) and the Institute for Logic, Language and Computation (University of Amsterdam). The Riddle combines computational analysis of writing style with the results of a large online survey of readers, completed by almost 14,000 participants. In my talk, I will go into...
some of the main results of the project.

Friday, 14 June 2019

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:00 to Noon</td>
<td>Classes in Session</td>
</tr>
<tr>
<td>12:15 to 1:15</td>
<td>Lunch Reception / Course E-Exhibits (MacLaurin A100)</td>
</tr>
<tr>
<td>1:30 to 2:00</td>
<td>Closing, DHSI in Review (MacLaurin A144)</td>
</tr>
</tbody>
</table>

Contact info:
institut@uvic.ca  P: 250-472-5401  F: 250-472-5681
Information Security for Digital Researchers - DHSI 2019

**Instructor:** Jonathan Martin (jonathan.martin79@icloud.com & @songsthatsaved)

**Suggested Course Hashtag:** #HackingDH

**Extended Course Materials and Schedule (in-progress):**
Hello, everyone!

Welcome to the course! In our time together at DHSI, we’re going to learn how to protect our digital lives, how to protect our data, and how to ensure that our data outlives us.

This will involve some hacking.

It will also involve some reading.

(These often go together.)

On the website above, you’ll find some helpful contextual materials that I would encourage you to dig through. You don’t have to become an expert, but it may be helpful to survey the territory that we’re going to be exploring.

Below, you will find some general reading material that covers personal security issues. Don’t obsess too much over this, as we will cover most of it in class. I’ve provided it as a reference for the work ahead.

So, then, let me just say that I’m thrilled to embark on this journey with all of you, and I hope you will find the course helpful. Please don’t hesitate to get in touch (during, or out of, class) with any questions or concerns.

Cheers,

Jon
## Draft Course Schedule (Implementation May Vary)\(^1\)

<table>
<thead>
<tr>
<th></th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Morning</strong></td>
<td>Intro to Information Security</td>
<td>Intro to Data Security (Encryption, Communication, And Storage)</td>
<td>Intro to Data Preservation (Censorship, Archiving, And Eternity)</td>
<td>Putting it all together, Hands-on projects and practice</td>
<td>Discussion about next steps, (Hands-on)</td>
</tr>
<tr>
<td><strong>Afternoon</strong></td>
<td>Intro Continued, (Hands-on)</td>
<td>Intro Continued, (Hands-on)</td>
<td>Intro Continued, (Hands-on)</td>
<td>Hands-on projects and practice</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### Useful Resources:

Our Course Website: [https://hackingdh.com/dhsi2019.html](https://hackingdh.com/dhsi2019.html)

---

\(^1\) The hope is that this will be an organic course that adapts to the particular interests and needs of its participants. As such, this schedule is only a proposed template, and, it is not intended to be the final word. (If we’re doing it right, we’ll probably blow the whole thing up by day two… ;)

Seven Steps To Digital Security

Here are some basic tips to consider when thinking about your own digital security.

Knowledge is Power

Good security decisions can't be made without good information. Your security tradeoffs are only as good as the information you have about the value of your assets, the severity of the threats from different adversaries to those assets, and the risk of those attacks actually happening. This guide should help you gain the knowledge you need to identify the threats to your computer and communications security, and judge the risk against possible security measures. And some of this knowledge you already have: knowledge of your own situation, who might want to target you, and what resources they have. You already have more power than you think!
The Weakest Link

Think about assets as components of the system in which they are used. The security of the asset depends on the strength of all the components in the system. The old adage that "a chain is only as strong as its weakest link" applies to security too: The system as a whole is only as strong as the weakest component. For example, the best door lock is of no use if you have cheap window latches. Encrypting your email so it won't get intercepted in transit won't protect the confidentiality of that email if you store an unencrypted copy on your laptop and your laptop is stolen. That doesn't mean you have to do everything simultaneously, but it does mean that you should spend time thinking about every part of your information and computer use.

Simpler is Safer and Easier

It is generally most cost-effective and most important to protect the weakest component of the system in which an asset is used. Since the weak components are much easier to identify and understand in simple systems, you should strive to reduce the number and complexity of components in your information systems. A small number of components will also serve to reduce the number of interactions between components, which is another source of complexity, cost, and risk. That also means that the safest solution may be the least technical solution. Computers may be great for many things, but sometimes the security issues of a simple pen and notepaper can be easier to understand, and therefore easier to manage.

More Expensive Doesn't Mean More Secure
Don't assume that the most expensive security solution is the best; especially if it takes away resources needed elsewhere. Low-cost measures like shredding trash before leaving it on the curb can give you lots of bang for your security buck.

It's Okay To Trust *Someone* (But Always Know Who You're Trusting)

Computer security advice can end up sounding like you should trust absolutely no one but yourself. In the real world, you almost certainly trust plenty of people with at least *some* of your information, from your close family or companion to your doctor or lawyer. What's tricky in the digital space is understanding who you are trusting, and with what. You might deposit a list of passwords with your lawyers: but you should think about what power that might give them—or how easily they might be maliciously attacked. You might write documents in a cloud service like Dropbox or Microsoft OneDrive that are only for you: but you're also letting Dropbox and Microsoft access them, too. Online or offline, the fewer people you share a secret with, the better chance you have of keeping it secret.

There is No Perfect Security—There’s Always a Trade-Off

Set security policies that are reasonable for your lifestyle, for the risks you face, and for the implementation steps you and your colleagues will take. A perfect security policy on paper won't work if it's too difficult to follow day-to-day.

What's Secure Today May Not Be Secure Tomorrow
It is also crucially important to continually re-evaluate your security practices. Just because they were secure last year or last week doesn't mean they're still secure! Keep checking sites like SSD, because we will update our advice to reflect changes in our understanding and the realities of digital security. Security is never a one-off act: it's a process.

Last reviewed: 2015-05-21
Assessing Your Risks

Trying to protect all your data from everyone all the time is impractical and exhausting. But, do not fear! Security is a process, and through thoughtful planning, you can assess what’s right for you. Security isn’t about the tools you use or the software you download. It begins with understanding the unique threats you face and how you can counter those threats.

In computer security, a threat is a potential event that could undermine your efforts to defend your data. You can counter the threats you face by determining what you need to protect and from whom you need to protect it. This process is called “threat modeling.”

This guide will teach you how to threat model, or how to assess your risks for your digital information and how to determine what solutions are best for you.

What might threat modeling look like? Let’s say you want to keep your house and possessions safe, here are a few questions you might ask:

What do I have inside my home that is worth protecting?
- **Assets** could include: jewelry, electronics, financial documents, passports, or photos

**Who do I want to protect it from?**

- Adversaries could include: burglars, roommates, or guests

**How likely is it that I will need to protect it?**

- Does my neighborhood have a history of burglaries? How trustworthy are my roommates/guests? What are the capabilities of my adversaries? What are the risks I should consider?

**How bad are the consequences if I fail?**

- Do I have anything in my house that I cannot replace? Do I have the time or money to replace these things? Do I have insurance that covers goods stolen from my home?

**How much trouble am I willing to go through to prevent these consequences?**

- Am I willing to buy a safe for sensitive documents? Can I afford to buy a high-quality lock? Do I have time to open a security box at my local bank and keep my valuables there?

Once you have asked yourself these questions, you are in a position to assess what measures to take. If your possessions are valuable, but the risk of a break-in is low, then you may not want to invest too much money in a lock. But, if the risk is high, you’ll want to get the best lock on the market, and consider adding a security system.

Building a threat model will help you to understand threats that are unique to you and to evaluate your assets, your adversaries, and your adversaries' capabilities, along with the likelihood of risks you face.
What is threat modeling and where do I start?

Threat modeling helps you identify threats to the things you value and determine from whom you need to protect them. When building a threat model, answer these five questions:

1. What do I want to protect?
2. Who do I want to protect it from?
3. How bad are the consequences if I fail?
4. How likely is it that I will need to protect it?
5. How much trouble am I willing to go through to try to prevent potential consequences?

Let’s take a closer look at each of these questions.

What do I want to protect?

An “asset” is something you value and want to protect. In the context of digital security, an asset is usually some kind of information. For example, your emails, contact lists, instant messages, location, and files are all possible assets. Your devices may also be assets.

Make a list of your assets: data that you keep, where it’s kept, who has access to it, and what stops others from accessing it.

Who do I want to protect it from?

To answer this question, it’s important to identify who might want to target you or your information. A person or entity that poses a threat to your assets is an “adversary.” Examples of potential adversaries are your boss, your former partner, your business competition, your government, or a hacker on a public network.

Make a list of your adversaries, or those who might want to get ahold of your assets. Your list may include individuals, a government agency, or corporations.
How bad are the consequences if I fail?

There are many ways that an adversary can threaten your data. For example, an adversary can read your private communications as they pass through the network, or they can delete or corrupt your data.

The motives of adversaries differ widely, as do their attacks. A government trying to prevent the spread of a video showing police violence may be content to simply delete or reduce the availability of that video. In contrast, a political opponent may wish to gain access to secret content and publish that content without you knowing.

Threat modeling involves understanding how bad the consequences could be if an adversary successfully attacks one of your assets. To determine this, you should consider the capability of your adversary. For example, your mobile phone provider has access to all your phone records and thus has the capability to use that data against you. A hacker on an open Wi-Fi network can access your unencrypted communications. Your government might have stronger capabilities.

Write down what your adversary might want to do with your private data.

How likely is it that I will need to protect it?

Risk is the likelihood that a particular threat against a particular asset will actually occur. It goes hand-in-hand with capability. While your mobile phone provider has the capability to access all of your data, the risk of them posting your private data online to harm your reputation is low.
It is important to distinguish between threats and risks. While a threat is a bad thing that can happen, risk is the likelihood that the threat will occur. For instance, there is a threat that your building might collapse, but the risk of this happening is far greater in San Francisco (where earthquakes are common) than in Stockholm (where they are not).

Conducting a [risk analysis](/en/glossary/risk-analysis) is both a personal and a subjective process; not everyone has the same priorities or views threats in the same way. Many people find certain threats unacceptable no matter what the risk, because the mere presence of the threat at any likelihood is not worth the cost. In other cases, people disregard high risks because they don't view the threat as a problem.

Write down which threats you are going to take seriously, and which may be too rare or too harmless (or too difficult to combat) to worry about.

**How much trouble am I willing to go through to try to prevent potential consequences?**

Answering this question requires conducting the risk analysis. Not everyone has the same priorities or views threats in the same way.

For example, an attorney representing a client in a national security case would probably be willing to go to greater lengths to protect communications about that case, such as using encrypted email, than a mother who regularly emails her daughter funny cat videos.

Write down what options you have available to you to help mitigate your unique threats. Note if you have any financial constraints, technical constraints, or social constraints.

**Threat modeling as a regular practice**

Keep in mind your [threat model](/en/glossary/threat-model) can change as your situation changes. Thus, conducting frequent threat modeling assessments is good practice.
Create your own threat model based on your own unique situation. Then mark your calendar for a date in the future. This will prompt you to review your threat model and check back in to assess whether it’s still relevant to your situation.

**Last reviewed:** 2017-09-07
CHAPTER 1

KEEP YOUR IDENTITY SAFE

Identity thieves can buy, sell, or capture your identity and use the information to get money and services—or use your name, credit rating, or insurance to take out a loan or get free medical care.

There are myriad ways for the bad guys to get your information and use it for all sorts of nefarious purposes—mainly, stealing your money, although occasionally for other kinds of fraud or to cover their tracks when committing additional crimes. That’s one of the big reasons identity theft can be so devastating. If a criminal steals your credit card information, your bank will likely refund you the money that was lost. If the same criminal impersonates you to run an international child pornography ring, however, then your problems just got a whole lot worse... especially since many law enforcement folks aren’t up on the latest types of cybercrime, so “that wasn’t me” might not go over well.

How does it happen? We’ll examine the many methods of identity theft in the pages that follow, and we’ll also show you how you can protect yourself from being a victim or fight back if you already are. The methods of ID theft range from the seriously low tech (such as digging through your trash for unshredded financial documents or stealing those new credit cards that the bank sends you unexpectedly) to sophisticated database breaches and other hacks staged half the world away by large crime syndicates to fund cyberterrorism operations.

AMERICA’S FIRST IDENTITY FRAUD

Philip Hendrik Nering Bögel had some financial problems, and he was a creative thinker. So in 1793, when things got too hot for the Dutchman (who was wanted for embezzlement at the time), he did what any forward-thinking identity thief would do today: He hot-footed it out of the Netherlands, setting forth on this continent a new city, conceived in parsimony, and dedicated to the proposition that Bögel deserved better. Calling himself “Felipe Enrique Neri, Baron de Bastrop,” Bögel started being awfully helpful to early Texas leaders Moses and Stephen F. Austin in obtaining land grants. After being named Texas land commissioner, Bögel came to settle a Texas city that he named after himself. Today, visitors to Bastrop, Texas, population 5,340, can celebrate how America’s earliest successful ID fraud operation netted one guy a whole city.
**T/F**

**"MY IDENTITY ISN'T WORTH STEALING!"**

FALSE Attacker are smart, and they seek the easiest path to their ultimate target. Often, that easiest path runs through your computer is you. You may say, "I just have photos of my grandkids on my hard drive." But your machine is connected to the internet, making it a target. Hackers can hijack your computer and join it into a secret global network for spam, attacks on other computers, and more nefarious activities. While they're at it, they might just steal your banking information as well. It is also not unknown for hackers to destroy a computer, so that even those family photos that are priceless to you, while worthless to others, end up lost with the dead computer.

**MANY TYPES OF IDENTITY THEFT** Criminals impersonate you online for a range of different reasons and in a variety of ways. For cyberstalkers (see pages 50-51 for Amanda Nickerson's story), the impersonation is usually part of a larger cyberbullying effort. But in most cases, the motivations are financial. Whether it's designed to get bank cards or bank loans in your name, obtain credit in your name, or impersonate you to use your existing credit, identity theft is usually a gateway cybercrime—an initial act, atop which lie other criminal schemes. So really, "identity theft" should be thought of as a family, or a category, of cybercrime.

Even though it's common for victims to be reimbursed by banks or credit card companies, the damage done by ID theft can affect you for years. Your credit score and history are the main ways that banks, car dealers, and other lenders determine the risk of extending you credit, and the black marks can be hard to erase.

**A Taxing Scheme** One of the fastest growing crimes in America is tax return fraud, which can net identity thieves thousands of dollars for each successful impersonation they make to the IRS. The criminals get hold of your Social Security number and personal information, and then create a tax return in your name that shows a modest overpayment on your part. The return is filed online using software, and within days, the IRS sends out a refund to "you"—at the address given by the thief. The refund is typically made using prepaid Visa cards, which can be easily exchanged for cash or property.

**FORMS OF IDENTITY THEFT**

Fraudsters don't just steal your driver's license or credit card. They'll take your whole identity and make use of any part they can.

- Attempted Fraud
- Credit Card
- Medical Fraud
- Phone & Utilities
- Bank Fraud
- Employment Fraud
- Gov't Benefits Fraud
- Loan Fraud
Strangers with Candy

In 2004, some InfoSec folks did a little experiment in which they offered passersby on the street a candy bar if they would tell them their work logins and passwords. To their surprise, some 70 percent were willing to part with the information—half of them did so even without the chocolatey bribe. You'd think that would have been a wake-up call. And indeed, governmental agencies and private-sector companies spend millions of dollars on training to make employees aware of proper security procedures and how important it is to follow them. How's that going? Well, when the experiment was repeated in London in 2008, there was no difference.

Whether the reasons are cultural or technical, the fact is, people are just really bad at keeping their passwords secret. They just don't take it seriously. What's even more galling to those who work with companies and individuals to improve security comprehension is that "your password" is still taken literally. By which I mean that most people to this day use just one password for many or all of their accounts—and a weak one, at that (see page 28 for more on creating a secure password).

You might think that this problem would have already been solved with the creation of password manager apps, which significantly reduce the toil and trouble of thinking up (let alone remembering) strong new passwords, such as the ever-popular 98cLkD2rh29#@36kaggl!. Plus, the programs are easy to use and can automatically change the passwords for all your online accounts.

So in 2016, when a security consultant decided to try the chocolate bar trick again, this time staging it as a contest in which the person with the "best" login and password would win prizes ranging from candy to a bottle of Champagne, he finally got different results. They were even worse than before.
TINFOIL HATS It's a common joke that some people are so paranoid, they line their hats in tinfoil. Funny thing? That might not always be such a bad idea.

There are many ways to conduct data theft, and some of them do rely on secret transmissions. The best (or, at least, one of the coolest) examples of this was the Soviet hack against IBM Selectric II and III typewriters in the 1970s. About fifteen of these were used in the U.S. Embassy in Moscow and the consulate in Leningrad, and were modified by Soviet spies to contain a device that measured the magnetic disturbances generated when the little Selectric ball swiveled. Each letter, it turned out, had its own signature. By implanting a receiver in the walls (the buildings were, of course, built by Soviet contractors), the government could see the very pages of documents as they were typed up.

HOW THEY DO IT Criminals engage in obtaining identities to exploit in a range of ways, from low-tech to Secret Squirrel. Once the most common method of identity theft, paper or wallet theft is still popular, but now it's a small-time operation. Still, someone lifting your wallet and using your ID and credit cards can do a fair bit of damage. Similarly, ID theft can occur when people rifle through your trash and find bank statements and other bills with account numbers, balances, and dates. These specifics allow thieves to call those vendors and report your cards as lost, change your address, and have replacements mailed to them.

Other schemes to separate you from your identity run the gamut from physical theft of personal documents from service providers to breaking into a computer network specifically for the purpose of stealing data. Another popular method is phishing (see page 24).

But of course, the most common method of stealing identities is to do so en masse in a large-scale breach of a retailer, bank, insurance provider, or government agency. This gives criminals the biggest bang for their buck and the largest number of targets. See the chart on the facing page for more information about how this works.

One Step Ahead of the Law It is very difficult for authorities to prevent or successfully prosecute identity thieves. Because much of the fraud can be done at a distance and by using online tools, catching the criminals in the act is difficult. What's more, with the global nature of the internet, the criminals don't even have to be in the United States to commit these crimes. And, finally, ID theft can go on for some time before a victim is even aware that it has happened.
HOW MIGHT YOU BE VULNERABLE? The vast multibillion-dollar cybercrime industry can be divided into three basic categories, each with its own objectives, although at the end of the day, the result is the same: You've been had. Understanding the differences, and what happens at each stage of the game, can help you stay safe. Here's how these crimes roll out.

IF YOU ARE

THE TARGET

THAT MEANS

an adversary has targeted you on a highly personalized basis.

IN THIS CASE, THE HACKER MIGHT WANT TO

extort money from your small online business.

So he or she

crafts an email to you personally, using specific details to convince you he works for your website's registrar.

AND THEN

believing you're speaking to your own provider, you reveal the log-in information for your account.

ONCE THAT'S DONE

the hacker logs in, takes your site down, and changes your password.

AND IN THE END

the hacker demands a $5,000 USD wire transfer to restore your site.

IN THE TARGET POOL

THAT MEANS

you are part of a group being targeted by a broad-based or general attack.

IN THIS CASE, THE HACKER MIGHT WANT TO

access PayPal accounts.

So he or she

buys or builds a spamming list of ten million email addresses, one of which is yours.

AND THEN

the hacker sends a fake but realistic and compelling phishing email that tricks you and other users into revealing PayPal account log-in information.

ONCE THAT'S DONE

the hacker harvests logins from anyone who fell for the phishing email.

AND IN THE END

the hacker logs into your account and sends himself a fraudulent payment.

THE VICTIM BUT NOT THE TARGET

THAT MEANS

you are a bystander caught up in someone else's mistake.

IN THIS CASE, THE HACKER MIGHT WANT TO

access health records at a major insurer.

So he or she

registers a look-alike domain resembling the real one, say One-Health.com, instead of OneHealth.com.

AND THEN

the hacker crafts believable emails using a company executive's name, role, and title to convince users to open a malicious attachment.

ONCE THAT'S DONE

the hacker accesses the network, in this case gaining access to millions of private medical records.

AND IN THE END

your records are stolen even though you're not the one who clicked on the malware.
CHAPTER 1

TEACH A MAN TO PHISH Phishing isn't one specific thing. Rather, the term is used for a wide range of methods designed to gain access to your information. Understanding what those methods are, along with the basics of how they work, is central to both recognizing and avoiding many of the risks you face online. So before we go any further, let's do a quick overview of the many types of phish in the sea and the ways they can bite. Here are three common methods that these criminals will try when going after your data.

Voluntary Disclosure The first method is diabolically simple: Attackers use a rich mix of psychological techniques, known collectively as social engineering, to get you to give up the goods, essentially conning you into giving away the information that they want. People are generally trusting, and it's amazing how much information the average person will give up simply because someone happened to ask them in the right way.

Malicious Attachments In these cases, computer users are tricked by some compelling message into opening a poisoned email attachment, which then installs malicious malware on their machine, thus giving the hacker access to their computer or network. These masquerade as documents that the users "requested," photos they "just have to see to believe," and the like.

Malicious Links Because many email systems can now block out malicious email attachments, some attacks will use malicious links to drive the user to an infectious web page instead. Most people are so accustomed to clicking on links almost automatically that this technique is highly effective. Most of these links are disguised to boot—an image in the email with a logo or a line of text displaying an address or site to visit that is actually a cover for a malicious web address which a hacker has set up for just this purpose.

KEY CONCEPT

WHY IS IT CALLED PHISHING? Phishing is a term used to describe some of the most widespread and effective methods for obtaining information online. The term itself is a mash-up of two words—"fishing" and "phreak." The fishing part is just what you'd imagine: to fish for victims or data by using electronic bait, hooking victims, and reeling them in—an obvious and accurate metaphor for the act itself. The alternate spelling is a nod to the pre-internet practice of telephone-system hacking known as phone "phreaking," done by "phreaks." This is related to another hacker practice, called "feet speak," which substitutes numbers for letters and some letters for others to create an often goofy insider jargon. It's quaint today, but you will still see versions in chat rooms, as hackers somewhat jokingly refer to one another as "1337 H4x0r5," or "elite hackers."
TYPES OF PHISH There are a lot of phishing schemes in the
sea. You've probably been exposed to at least a couple of the
examples listed below—and hopefully you didn't fall for them,
although if you did, you're one of millions of people who have.
Using the information below, you'll be better able to spot
these scams and steer clear.

<table>
<thead>
<tr>
<th>TYPE OF SCAM</th>
<th>HOW IT WORKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLASSIC PHISHING</td>
<td>A fake website &quot;spoofs&quot; or closely resembles a real one, into which users enter their access credentials, identity data, or other sensitive information.</td>
</tr>
<tr>
<td>SPEARPHISHING</td>
<td>As the name would imply, this is a highly targeted attack, often designed to victimize a small, specific group or even one individual, using highly personalized messages that may be the result of hours or even weeks of online reconnaissance on the target.</td>
</tr>
<tr>
<td>WHALE PHISHING</td>
<td>The spear phishing of a high-profile or high-value individual, such as a CEO or celebrity, that is, a &quot;big fish&quot; or whale.</td>
</tr>
<tr>
<td>CATPHISHING</td>
<td>The use of fake online personas or profiles to create a phony emotional or romantic relationship, either for financial gain or access to sensitive information.</td>
</tr>
<tr>
<td>VISHING/SMISHING</td>
<td>Scams or data thefts that leverage phishing-like techniques but target phone users over voice lines or SMS.</td>
</tr>
</tbody>
</table>
DEFEND YOURSELF AGAINST PHISHING

So if the thieves are smart, and not even the rich and famous can protect themselves, does that mean you’re hosed? Not at all. That’s because in most cases, victims fall for these attacks not out of a lack of resources but a lack of awareness. An astute and informed user with a zero-dollar budget is harder to victimize than an oblivious and untrained one with all the money in the world. Here are five simple steps you can take, starting right now, that will make you a significantly tougher target for phishers.

Be Aware Simple awareness is the first line of defense. Be suspicious. Understand and believe that you are a target. Treat any message in any electronic medium from someone you don’t know as highly suspect.

Use the Hover Test Any modern email program will show you the destination of a hyperlink if you mouse over it without clicking. This “hover test” can help you spot suspicious links in any email you’ve received. If the visible link and the underlying destination don’t match exactly, don’t click!

Check the URL Learn how to properly read a web address. The name of the site you’re visiting is the last thing to the left of the first single slash, not the first thing to the right of the double slash. Phishers constantly use this lack of knowledge to trick people.

SAFE: https://www.amazon.com/
UNSAFE: http://www.amazon.phishingforyou.com/

Be Attachment Phobic Malicious attachments are the number one way to let password stealers, Trojan horse viruses, and other nasties
get onto your computer. You should only open attachments from people you know, and even then limit yourself to messages you're expecting, such as an invoice for services you actually have received.

**Confirm Out-of-Band** If you happen to receive a suspicious message or a request for information that seems too personal, even from individuals or companies you trust, confirm the request via a different medium. For example, if they email you asking for your information or requesting that you click the link to their website to correct an issue, try visiting their website or calling them by phone. And remember, type the web address out manually or find the phone number yourself. Never rely on the link or phone number in the suspicious message. Those could both be fakes run by the phisher!

**HACKER HISTORY**

**PHONING IT IN** The first known online mention of the term “phishing” was in the online group alt.2600, a discussion forum for phone hackers, in early 1996. The “2600” refers to the frequency in hertz that early phone phreakers discovered they could play into a phone handset to take over the phone company’s switches and make free calls to anywhere in the world. That this hack was so simple to execute, and so fundamental to the system that it was simply too expensive to fix, led to an entire subculture around building “blue boxes,” or tone generators that would play the 2600 Hz whistle tone. Even Steve Jobs and Steve Wozniak, of Apple fame, sold them in the early days. One intrepid phreaker, John Draper, worked with some blind phreakers who were, as you'd imagine, particularly sensitive to tone. He learned that a plastic whistle offered as a free prize in boxes of Cap'n Crunch cereal blew at, yes, 2600 Hz. Draper used the whistle widely and became known in hacking circles as Crunchman. He's still around, too: You can find him on Twitter @jdcrunchnman, or look for John "Captain Crunch" Draper on Facebook.

**GOOD TO KNOW**

**YOU'RE NOT ALONE** Millions of ordinary citizens have been victimized by one type of hack or another. Even the smart, powerful, and rich have been victims. For example, real-life rocket scientists at NASA have had their computers taken over by Chinese hackers. The U.S. government has concluded that Russians hacked the DNC and that Anonymous hacked Donald Trump during the 2016 election. In 2008, vice presidential candidate Sarah Palin's email was stolen by a hacker who figured out the Alaska governor's email password. Other notable victims have included Attorney General Eric Holder, FBI Director Robert Mueller, Jay Z and Beyoncé, Paris Hilton, Mel Gibson, Kim Kardashian—and Nick Selby, one of the authors of this book. This isn't even taking into account the massive amounts of top-secret government information released by WikiLeaks, Edward Snowden, and others.
CREATE A POWERFUL PASSWORD Now that you know what to avoid in emails, what's the next step? Well, every online account requires an account name (often derived from your own name or email address) and a password. The following guidelines can help you come up with passwords that are as unbreakable as possible.

One Size Does Not Fit All Look at the keys on a key ring. Each is a different design and cut. Just as each key is made to fit a specific lock, each password should be unique to the account it's used for. Otherwise, if you're a victim of ID theft, whoever stole your information will have access to every single account of yours that the criminal can think to try.

Bigger Is Better Some sites limit how long your password can be. While a long password may be hard to remember, it's harder for a hacker to break, even with brute-force methods (that is, using programs that try every single possible combination of characters).

Get Complicated Passphrases like "correcthorsebatterystaple" are easy to remember, but anything that uses dictionary words is easily hackable. Avoid simple substitutions, too, such as "p4ssw0rd" instead of "password." Use every single type of character you can: lowercase and capital letters, numbers, punctuation, and anything else available. Finding a number between 0 and 9 is easy for a hacker or ID thief; finding the right character in a total of sixty-two numbers and lowercase and capital letters is massively more challenging, especially the longer the string gets. If you have to write down a password to help remember it, keep said document hidden and safe from prying eyes or theft, or consider using a password manager.

Change Is Good Don't just come up with a password and then leave it be. Change your passwords frequently and, if at all possible, never reuse one. If hackers steal older data, they may score a hit if you're using that old password for a new account.
security

Basic

just don't The top ten most common—and thus worst—passwords have stayed largely the same since passwords became a thing, only changing in order from year to year. Right now the top contenders are:

1. 123456
2. 123456789
3. 111111
4. qwerty
5. 12345678
6. password
7. 123123
8. 000000
9. 1234567
10. 1234567890

who wants to know? Sometimes an extra layer of protection, called “knowledge-based authentication,” or KBA, is added to your password, either in addition to your basic login and password or to verify your identity if you’ve forgotten your password. Of course, like many other defenses, this tool can also be turned against you.

Static KBA Also known as “shared secret questions,” these are questions along the lines of your mother’s maiden name, town where you were born, and so forth—often matters of public record. In addition, this information is stored somewhere, so it can be stolen which means that even the weirder questions, like “Who’s your favorite poet?” aren’t secure.

Dynamic KBA Here, questions are generated in real time from a range of public and private records. You don’t know what questions will be asked, but, hopefully, you’ll remember the answer. Examples might include “What color was your Honda Accord?” or “Which of these streets have you never lived on?” You only have a short time to answer; the odds of someone guessing correctly on the fly are lower.

Unfortunately, you may not have the luxury of only patronizing sites with excellent dynamic KBA, although if you have the choice, take it. The simple workaround? Lie. It’s relatively easy to figure out where someone went to high school. But if the “correct” answer is Narnia, Petticoat Junction, or Westeros, that’s less likely to show up in old yearbooks. More’s the pity.
90% of victims report they weren't even aware that their personal data had been compromised before thieves tried to use it fraudulently.

HISTORIC COST OF FRAUD IN THE U.S.

GROWTH IN CASES OF ID FRAUD

THE MOST TARGETED GROUPS

PEOPLE AGED 18 TO 24

ANYONE WITH A WEAK PASSWORD

PEOPLE MAKING OVER $75,000

COUNTRIES WITH HIGHEST INCIDENCE OF IDENTITY THEFT PER CAPITA

1. MEXICO
2. THE USA
3. INDIA
4. THE UNITED ARAB EMIRATES
5. CHINA
6. THE UNITED KINGDOM
7. BRAZIL
8. AUSTRALIA
9. SINGAPORE
10. SOUTH AFRICA
11. CANADA

32% of victims do not notify the police

64% Credit cards that showed attempted or successful use by thieves.
Signs Your Identity Has Been Stolen

- Your credit cards rates go up
- Your credit rating drops
- Mystery bills show up
- Car insurance goes up
- Bank statements stop coming
- Tax refund denied
- Can't renew drivers license
- Check-up reminders for medical conditions you don't have
- Calls from collection agencies
- Turned down for loan
- Fail to pass background check for job

If your personal information is stolen, how long does it take to resolve?

- 48% 1 day or less
- 16% 2 to 7 days
- 18% 8 days to a month
- 6% 1 to 3 months
- 3% 3 to 6 months
- 9% 6 months or more

Most Common Forms of Identity Theft

- 49.2% Attempt to access government documents*
- 15.8% Credit card fraud
- 9.9% Phone of utilities fraud
- 5.9% Non-credit card bank fraud
- 3.5% Loan fraud
- 3.3% Employment-related fraud
- 22.9% Misc other forms

30 Days

Average time needed to handle identity theft crime.

30 Hours

Average time to handle and settle a disputed charge with a credit company.
**GOOD TO KNOW**

**SECURITY BASICS**
Your wallet often has all of your identification and bank cards (and more). If that wallet gets stolen, your entire life's identity and finances will literally be in someone else's hands. Should that happen, the best plan is to have culled its contents well beforehand so that you're only carrying the minimum number of IDs and credit cards—nothing more than is absolutely necessary. This will limit your losses in case of theft. And, it means that the only calls you will have to make will be to your credit card company, your local DMV office, and your employer to report the losses. Your credit card and driver's license will be replaced, and your employer can deactivate your work ID card, thus preventing whoever stole your wallet from using the card to break into your office and clean you out of paper clips and printer ink cartridges.

**THE SEVEN-POINT ID THEFT RECOVERY PLAN**
If you have been the victim of identity theft, it is very important that you take steps to safeguard your good credit, warn the appropriate agencies of the event, and protect your good name. Often, you'll want to talk to the police. That's a good idea, but don't be surprised if you learn that there's not a lot they can do. The rest of this chapter explains how you can help yourself when you are the victim of identity theft. If you don't, it can cost you dearly when applying for a car loan, mortgage, or credit card. It could also make it harder for you to find a job, rent an apartment, or buy insurance.

The first thing you must do when you are a victim of identity theft is to get organized. The seven-step checklist here is just a suggested series of steps; customize it as necessary to your needs.

**STEP 1**
**FILE A POLICE REPORT**

If you discover you have been victimized, contact the non-emergency number of your local police department and ask to speak to a detective.

**STEP 2**
**GATHER DOCUMENTS AND EVIDENCE**

Contact your nation's consumer protection agencies, as well as stores and creditors to gain copies of the documents used to open accounts in your name.

**STEP 3**
**CREATE AN AFFIDAVIT AND ID THEFT REPORT**

Your local consumer protection agency should be able to provide documents you will need and demonstrate how to present them. They also provide sample forms for an identity theft report, which, along with your police report, will help speed up the process with creditors, banks, and other agencies.
PLAN if you have been notified that you take steps appropriate agencies of the law. You'll want to talk to the police if you learn that you've been contacted by the investigator of identity theft. If you're applying for a car loan, mortgage, or a job, rent an apartment, or open a new account, a victim of identity theft should be notified as a suggested step for your needs.

INFORM THE CREDIT AGENCIES AND CREATE AN EXTENDED ALERT

To establish a fraud alert with the credit agencies, contact them directly. You will need to reissue the alert every ninety days.

INFORM YOUR BANK, CREDITORS, AND MERCHANTS

With the package you've created, contact your bank and other creditors and merchants with whom you have accounts and inform them of the issues you have faced.

PROTECT YOUR SOCIAL SECURITY NUMBER

If your number was misused, inform the national agency and request information on an ID Theft Affidavit. You may also wish to contact your agency if your Social Security number is being continually abused or if your credit card number is being used without your knowledge.

MONITOR YOUR CREDIT

You are entitled to at least one free credit report per year, but that is often insufficient for monitoring. There are several commercial companies offering these services, and we recommend that you seek professional advice on which to choose. Several nonprofit organizations are out there to help victims, offering assistance to victims of identity theft by internet or phone.
CHAPTER 1

SYNTHETIC ID THEFT This chapter deals with the theft of someone’s actual identity, but here’s a new twist: synthetic identity theft. That’s when an identity that has never before existed is created by scammers. Identity thieves typically seek to obtain names, national identity numbers and dates of birth, medical account numbers, addresses, birth certificates, death certificates, passport numbers, bank account or credit card numbers, passwords (like your mother’s maiden name or children’s or pet’s names), telephone numbers, and even biometric data (such as fingerprints or iris scans). With synthetic ID theft, thieves only need some of this information to create a whole new fake person.

Thieves then create a credit file—the closest thing in the digital domain to conjuring up a human. This exploits a weakness in the authentication scheme used by credit reporting agencies: If an identity doesn’t exist when it is checked, a new file is created. And a file? That’s gold.

Credit Where No Credit Is Due The best thing to do with a synthetic ID is build its credit over time. This can be done in the traditional way—almost anyone can get a high-interest, low-limit, unsecured credit card at a hardware store, so the idea is to get one, then buy a hammer and pay it off over time. To get fancier about it, they might join up with a “data furnisher” who works at a business and will write up a phantom credit account for our spooky friend, showing scheduled payments made over time to speed things up. There’s an entire industry around this, because the stakes are very high.

The most common way is to conjure up children. This is because, for the eighteen years or so after most kids are born, they don’t do anything with their credit. During that time, anyone who establishes a credit file for the young one in question would likely be free from...
any interference until someone notices—that’s typically at just about the worst time: when the kid applies for a college loan. The best way to protect against misuse of your child’s credit is the same as it is for yours: Check it regularly, and check on it as often as you can. Should you happen to see fraudulent accounts, yell early, often, and loudly.

If you are on active duty in the military, it is recommended that you put an active duty alert on your own credit files by contacting any one of the three major credit agencies. Credit agencies all share active duty alerts. Each alert will stay in your files for at least twelve months. If someone applies for credit in your name, creditors will take extra precautions to make sure that the applicant is really you.

**THE TAKEAWAY**

Here’s how to apply the lessons of this chapter, whether you’re looking for basic safeguards, enhanced security, or super-spy measures to safeguard your privacy.

<table>
<thead>
<tr>
<th>BASIC SECURITY</th>
<th>ADVANCED MEASURES</th>
<th>TINFOIL-HAT BRIGADE</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Use strong passwords.</td>
<td>• Always use two-factor authentication.</td>
<td>• If any service provider’s site uses weak KBA, take your business elsewhere.</td>
</tr>
<tr>
<td>• Use different passwords for every site.</td>
<td>• Don’t get kids social security cards unless necessary.</td>
<td>• File your taxes the old-fashioned way, on paper.</td>
</tr>
<tr>
<td>• Use a password vault program.</td>
<td>• Check your kids’ credit at least quarterly.</td>
<td>• Escueh electronic information wherever possible.</td>
</tr>
<tr>
<td>• Never share your login information with anyone.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Don’t click on suspicious links or download unexpected files.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**GOOD TO KNOW**

**WHAT LAWS PROTECT YOU?** In virtually every place you care to look, identity theft is considered a federal crime. But it can still be next to impossible to actually get a federal office to investigate your individual case of identity theft—well, unless you are famous, or rich, or there is something larger at stake connected to the theft itself. Most states have their own laws against identity theft as well, and your local police department may have a program that can help you—ask them what resources are available in your area. Ultimately, however, you may simply be on your own, as it can be difficult to track down a specific perpetrator of identity theft (especially given that you may just be one of many victims caught in the same sweep). Usually, the best you can do at the local level is work to limit the damage done and clear your name.
Aside from their rather evocative (and nearly meaningless) monikers, few people actually know what the "deep web" and "darknet" are—or understand the differences between the two. In this chapter, we'll look at what happens when you venture away from the brightly lit thoroughfares of the information superhighway and explore some of its shadier back alleyways. While in reality it's neither as glamorous nor as murderous as various crime shows on TV make it out to be, the fact remains that this aspect of the internet is a significant contributor to the world's economy—and to global criminal activity as well.

Although we can assume that a large number of transactions on the darknet are relatively benign (although that depends on whether you consider stolen Netflix logins or off-brand Viagra to be harmless), many are not. As with any lawless wild frontier, you can find some real bad guys profiting off humanity's darker side. In this case, those bad guys might be dealing child pornography or heroin, selling hacked credit card accounts, or even involved in human trafficking. That said, some of the good guys out there can benefit from the same anonymity as well, particularly if they happen to be whistleblowers or individuals fighting oppressive regimes.

**SHADY DEALINGS** How much money is changing hands out there on the so-called darknet? More than you might think, although by their very nature, these sorts of transactions are obviously difficult to track and quantify. Reliable experts estimate that black-market transactions account for about 23 percent of the world's total goods and services. Think about that. If the global world product is almost $78 trillion USD, that means almost $18 trillion more is traded through the black market. In other words, almost a quarter of the world's transactions occur outside of the legitimate global exchanges. What are those transactions? Anyone who wants to make or receive untraceable (and untaxed) payments for anything, including illegal goods and services—from guns and drugs to hacking and stolen data—can find what they are looking for on the digital black market.
GOING DEEPER The first thing to know in getting your head around this topic is that the web is not the internet. While they may seem synonymous in daily life, the internet is far more than the World Wide Web. The internet is the entire global set of computers connected to a giant public network that shares certain rules for communicating various types of information. The most familiar of these are web pages and emails, but there are in fact many other things you’d never notice or care about that run over this same global network. Here’s the basic breakdown.

The Surface Web Most of what you see online, from Facebook to eBay to Amazon to Twitter, is the surface web. It’s made up of all the various public websites that share content, sell goods, or otherwise want to be easily found. They allow any guest to visit, and they invite search engines to index them so that users can find them through Google, Yahoo, and the like.

The Deep Web Millions of sites out there don’t appear in search engines, often because they don’t want to be found easily. These sites have no inbound links from any other site, and they block search engines. You can still visit them using a standard browser, but only if you have some other way of knowing the address, for example, if a link is sent in private email to a specific list of recipients. This type of arrangement is often used to share content, such as hacked data or child pornography, with a closed community that wants no outsiders.

The Darknet Simply put, the “darknet” is anything that cannot be accessed via a standard browser because it requires special software, and often special knowledge, to access. The darknet typically refers to sites on the Tor network (more on that on page 170) that look and feel just like regular sites but require a special Tor browser to view. The darknet, more broadly, includes other protocols and environments common users don’t know about, such as IRC (internet relay chat) channels and I2P (Invisible Internet Project) networks. In addition, the darknet isn’t indexed the way surface web sites are; virtually all of its sites’ addresses must be shared instead of searched for, and not everyone out there will be keen on sharing.

The bottom line is that, for average users, the deep and dark web may seem alluring or sexy thanks to television. In reality, what you’ll find there is malware, viruses, illegal content, and criminals ready to take advantage of the uninformed. Unless you really know what you’re doing, keep out.
SHOPPING IN THE DARK While it offers many legitimate uses to activists, whistleblowers, law enforcement, and political refugees, the darknet also supports an underground black-market economy that follows its own set of rules. Buyers and sellers have many reasons to trade outside normal open markets. These can include the following.

Illegal Goods Anyone looking for products or services that can’t be sold in the open, such as drugs, stolen identity data, or weapons.

Anonymity These transactions can be done without records, allowing the buyer and seller to remain anonymous, with (theoretically) no paper trail or electronic footprint.

Price Controls Products that are subject to taxation, import duties, price controls, and other constraints—such as cigarettes or alcohol—are attractive to black-market profiteers. So are products such as Tide laundry detergent, Gillette Mach3 razors, Crest whitening strips, and other huge-markup common necessities.

Technology has made it easier for black-market buyers and sellers to safely connect and do business. In the constant back-and-forth between authorities and black markets, one black market is shut down, but another takes its place.

T/F YOU CAN HIRE A HITMAN ON THE INTERNET

TRUE The most notorious online black market was Silk Road, operated by a hacker known as the Dread Pirate Roberts in 2011. It was an online marketplace functioning much like eBay or Amazon, except the offerings included guns, illegal drugs, hacking services, and even murder for hire. Silk Road was shut down by the FBI in November 2013, and Ross William Ulbricht, the Dread Pirate Roberts, is now serving a lifetime prison sentence. Not surprisingly, countless other illicit marketplaces have sprung up in its place. It’s not entirely clear whether the many “hit for hire” services are pure fantasy or con men preying on the gullible. On the other hand, if they were as good as they say, how would we know?
CHAPTER 12

PEELING AWAY THE ONION The largest and best-known element of the darknet is the Tor network. Tor, which stands for "The Onion Router," was originally a project started by the U.S. Navy but has long since been turned over to a private nonprofit organization. The details are extremely technical, but, as an average user, you can think of the Tor network as three related technologies.

A Web Browser The Tor browser works like a normal web browser, but it routes users requests for web pages through the Tor network.

Safe Passage Tor anonymizes users' activity by stripping identifying data from page requests, then sending the requests through multiple encrypted transfers between volunteer-run computers all over the world that run special Tor software, letting them act as transit points. When a user with a Tor browser types in a standard web address, that request goes from the "normal" web into Tor, gets bounced through various intermediate relays, then reenters the normal web via a Tor "exit node" and arrives at the destination website. The site responds to the page request, and the content is sent back to the user by the Tor network through a similar process.

Hidden Websites Computers equipped with the right Tor software can also run websites (and other services, including IRC chat channels) accessible a via Tor browser. So users with a Tor browser are able to not only anonymize their browsing of the standard web but can see a whole second "web" (albeit relatively small) made up of sites ending in .ONION that can't be reached by a standard browser.

Software for browsing acting as a node or hosting a Tor website can be found at TORproject.org.

UNDERCOVER ON THE DARKNET

One of the darknet's most notorious traits is its ability to hide. A colleague's home was burglarized, knives and drugs were stolen, and the Tor browser was discovered. Instead of exchanging the Tor browser for a wire, he had been surfing Tor sites from distributor to distributor, from web to exchange.

Shopping for Tor

Krebs on Security

The darknet's most visible aspect to the public is its anonymity. Krebs has taken various calls to report a Tor-based website that was hacked and has been alerted by darknet users who have converged several times with the same vendor, all to send heroin to him and keep an eye on him. The site, search his mail. They've told him, "If you're going to tell on us, you do.

"The darknet doesn't like us as we belong to a low percentage of the kinds of conversations, looks for leads and stops practices.

Reputation Management

In a world of anonymity, trustworthiness and interests are subjects to trustworthiness.

Of course, reputation management can arrange to meet with criminals and criminal groups in helping law enforcement develop new trends, and it has the power to attract darknet trading with Tor to help out the good

Check It Out—Curious

Curious—those who don't think they have speed (you can have a look (and warez, aka "loot") how the rest of the world uses the darknet, not just to find have bitcoin (or

PEELING THE ONION

Using Tor means that internet traffic on the browser is routed through multiple layers of Tor user relays, like an onion—hence its name.

TOR CLIENT

ENTRY GUARD

MIDDLE RELAY

DESTINATION

TOR NETWORK

ENCRYPTED BY TOR

NOT ENCRYPTED BY TOR
UNDERCOVER OOPS While criminals lurk in the shadowy recesses of the darknet, so too do law enforcement officers from around the world. A colleague in the UK complained that he'd bought too many knives and drugs to know what to do with. I spend countless hours surfing Tor sites looking for child pornography producers (distinct from distributors, who are often careless enough to use the surface web to exchange their unforgivable goods).

Shopping for Trouble The intrepid cyber security reporter Brian Krebs has taken on so many darknet criminals that his local police department had to come up with a special procedure when someone calls to report a violent crime at Krebs's house after SWAT teams, alerted by darknet thugs that there was a "hostage situation," had converged several times on his house. Krebs has also had criminals send heroin to his house, and then call authorities with the tip to search his mail.

"The darknet is where the bad guys are," a high-ranking federal agent told me. "We've got to get good at being there and looking like we belong there, because that's the only way we get into the kinds of conversations and relationships that will enable us to get leads and stop plots."

Reputation Matters This raises an important non-obvious point: In a world of anonymous users, reputation—based on common interests and sustained, consistent activity—is the only measure of trustworthiness. That's something that keeps academics busy.

Of course, reputation is how good reporters and journalists arrange to meet with sources to safely learn of corruption schemes and criminal gangs. The work done by these journalists is important in helping law enforcement and academic researchers understand new trends, and reporters can sometimes break stories based on darknet trading patterns. Brian Krebs, for example, broke the Target hack. Steve Ragan, another cyber reporter, has for years reported on criminal malware and hacktivist groups.

Check It Out—Carefully Who else is on the darknet? The morbidly curious—those who want to see whether you really can buy heroin and speed (you can) or hire a hit man (you can). The authors recommend you have a look around, if only to see for yourself the kinds of wares (and warez, aka pirated software) for sale, to educate yourselves about how the rest of this book isn't a bunch of people making stuff up. On the darknet, no one knows if you're a dog, but they do know if you have bitcoin (more on this digital currency in a bit).
144,000
TOTAL AMOUNT OF BITCOINS THE FBI SEIZED FROM ROSS ULBRICHT, THE ORIGINAL “DREAD PIRATE ROBERTS,” FOUNDERS OF SILK ROAD.

$12 MILLION
ESTIMATED VALUE OF BITCOINS LOST IN A “HEIST” WHEN EVOLUTION MARKET DISAPPEARED FROM THE DARKNET OVERNIGHT.

$820K
VALUE OF BITCOINS LOST WHEN SHEEP MARKETPLACE SHUT DOWN IN 2013, SCAMMING ITS MEMBERS.

$100 MILLION
VALUE OF BITCOINS THAT A FORMER SECRET SERVICE AGENT ADMITTED TO STEALING DURING THE SILK ROAD INVESTIGATION.

HERE’S A TIMELINE OF BITCOIN VALUE AT THE START OF EACH YEAR

<table>
<thead>
<tr>
<th>Year</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>$0.07</td>
</tr>
<tr>
<td>2011</td>
<td>$0.30</td>
</tr>
<tr>
<td>2012</td>
<td>$5.10</td>
</tr>
<tr>
<td>2013</td>
<td>$13.66</td>
</tr>
<tr>
<td>2014</td>
<td>$273.98</td>
</tr>
<tr>
<td>2015</td>
<td>$839.62</td>
</tr>
<tr>
<td>2016</td>
<td>$914.68</td>
</tr>
<tr>
<td>2017</td>
<td>$433.38</td>
</tr>
</tbody>
</table>

BITCOIN VALUES HAVE FLUCTUATED BETWEEN $0.0001 AND $1,250.99 IN ITS LIFETIME THUS FAR.

$1.2 BILLION
DREAD PIRATE ROBERTS AND SILK ROAD
BITCOIN + EBAY-LIKE BLACK MARKETPLACE + AMATEUR TECHIE + VISIONS OF CHALLENGING THE U.S. GOVERNMENT = SILK ROAD. A STORY AS SHADY AS THE DARK MARKET.

The internet has enabled new business models that connect buyers and sellers from around the world for illegal transactions as well as legal ones. eBay was one of the first big online marketplaces, and it has carefully policed sellers to be sure no one is breaking the law. So where’s an online shopper looking for something a little less conventional to go? It was only a matter of time before something arose to serve those interests.

The breakthrough for illicit online marketplaces came when bitcoin, a decentralized digital currency that works a lot like cash, was introduced. Word on the street was that bitcoin allowed you to make purchases online with perfect anonymity. This turned out not to be the case, but it’s still a more stealthy way to operate than, say, using PayPal to purchase that shoulder-mounted grenade launcher you’ve had your eye on.

The first of the darknet markets, Silk Road was started in February 2011 by an anonymous self-taught administrator who later became known as the Dread Pirate Roberts, aka DPR. At the peak of Silk Road’s popularity, it was estimated that the operation was bringing in $10K–$13K USD a month.

Silk Road emerged at a perfect time. It was like eBay but for black-market goods—mostly drugs, both illicit and pharmaceutical. As with eBay listings, sellers were rated, and there was an escrow to increase trust in the transactions.

There were certain illicit goods that were prohibited. DPR’s philosophy was to hurt no one—thus child porn, for example, was not allowed. (Silk Road as a new black market challenge the government status quo.)

In June 2011, major press outlets such as tech blogs. This users—and also law enforcement. Task forces formed, and the DEA was tasked with unmasking and taking down the site. One DEA agent, Force IV, donned identity—that of a drug cartel player in the Dominican Rep.

“IT WAS BUT FOR MARKET

reached out to a genuine friend, was complicated as a member of the Silk Road Task Force trying to bring DPR to justice. At one point, Force to help him murder with federal employee who was convincing fak
thus child porn and stolen data were not allowed. DPR saw Silk Road as a new brand that would challenge the government status quo.

In June 2011, Silk Road got major press on a number of tech blogs. This attracted more users—and also the attention of law enforcement agencies.

Task forces from the FBI and the DEA were formed to unmask and take down DPR. One DEA agent, Carl Mark Force IV, donned an alternate identity—that of a mid-level drug cartel player from the Dominican Republic—and reached out to DPR. They struck up a genuine friendship, but it was complicated because Force, as a member of the Baltimore Silk Road Task Force, was still trying to bring DPR in.

At one point, DPR asked Force to help him arrange the murder with DPR of a Silk Road employee who was cooperating with federal authorities. The task force managed to stage a convincing fake murder for hire.

The Silk Road bust came after months of chasing IP addresses and confirming site logins to DPR’s account.

Chris Tarbell was the agent who eventually found Silk Road’s IP address and traced it to a data center in Iceland. With a letter from the U.S. attorney, he walked out of the data center with a mirror of the drive, which was used to trace an IP address to Café Luna in San Francisco.

Ross William Ulbricht was the man arrested in October 2013 in San Francisco’s Glen Park Public Library. All the bitcoins that were held on Silk Road servers were seized by the U.S. government and later sold in a series of auctions. Ulbricht was convicted of money laundering, computer hacking, and procuring murder. He is serving a life sentence without parole.

In a strange twist to the story, the undercover DEA agent Carl Force went rogue and was convicted of embezzling a small fortune of the seized bitcoins. He was sentenced to six and a half years in June 2015, including counts on money laundering and obstruction of justice. His colleague, Shaun Bridges, a former secret service agent, was also charged.

The Silk Road brand lives on, but it isn’t controlled by Ulbricht. As of this printing, they’re on Silk Road 3.0.

“IT WAS LIKE EBAY BUT FOR BLACK-MARKET GOODS.”

LESSON LEARNED

DARKNETS ALL THE WAY DOWN There have always been black markets, and they will never go away. Silk Road and the many sites that sprung up after its fall made buying illegal goods easy. As these sites became more popular, they also drew the eye of government. These black markets are lucrative, but most operators know they will eventually be busted. Buyers and sellers know this too and therefore keep minimal funds on the sites, in case they are seized. Criminals are both clever and greedy, and it seems like every new technology can be bent to nefarious uses. More tech-savvy criminals arise all the time, competing with laws and law enforcement—both sides aided by technology, which is itself value-agnostic. But how bad might it be, really, to have a clean, well-lit place for illicit transactions? For knowing the quality of the products sold? Some might say “Better the devil you know . . .”
**Security Basics**

**Keep Your Identity Off the Darknet**

With the increasing numbers of site hacks, it’s just a matter of time before your personal data is sold on the black market. There’s not much you can do to protect yourself from someone else’s site getting hacked—that’s up to the site’s security technology. But you can use good account password hygiene. Never reuse the same username/password combination on different sites. One of the first things hackers will do with freshly hacked data is automatically check the hacked username/password combos on numerous banking, social, and email websites. If you use the same username and password combination at other sites, hackers could get into your accounts on those sites, even though those sites were not hacked. Use a complex but easy to remember password combination.

**Let the Buyer Beware**

Until recently, the U.S. dollar, in cash, was the preferred currency for black-market transactions. Cash is untraceable and anonymous, but it’s difficult to use cash for online commerce. Credit cards and other common payment methods leave a paper trail. That’s why bitcoin is so ideal for shady shoppers. While as noted above they’re not entirely anonymous, the use of bitcoin “tumblers” and anonymizing sites can obscure ones trail pretty well. Should you do this? There are legitimate reason to keep a light financial footprint, particularly if you subscribe to any number of concerns (or conspiracy theories, to unbelievers) about your government and its nosy ways.

**Give It a (Careful) Go**

There are some reasons why a noncriminal user might consider these underground markets. For example, you might wish to rent access to the internet via another user’s computer elsewhere in the world where, for example, Netflix shows first-run films not available to U.S. users, or you reside in a part of the world where freedom of expression is limited and you want to be able to communicate with others about civil rights or human rights issues.

**Approach with Caution**

Small mistakes in your “operational security” can have massive consequences. It’s not enough to be careful. You must be very careful and follow a strict set of procedures every time you enter and leave the darknet and even the deep web.

First off, don’t use your own computer for this kind of exploration. In fact, you shouldn’t even use a real-world one. Instead, download a bootable Linux image and always be sure to load your Tor sessions through that path. You should also load tools such as PGP (Pretty Good Privacy) encryption onto that bootable drive.

This setup will allow you to load your entire browsing session in the host computer’s memory so that, when you finish, you restart the computer and there are no traces of the activity on your hard drive.

We don’t recommend doing any shopping of course, but if you do get curious, don’t just use Tor to access darknet sites. For extra an (virtual private network) sites. All these techniques are used, but they’re really the degree of security for illicit gets caught by banking—and thus. You can’t really know how your adventures. You could be exploring, not doing anything wrong.
sites. For extra anonymity, you'll want to use an additional VPN (virtual private network) to completely anonymize your traffic.

All these techno-stealth measures may seem like a lot of work, but they're really the only way to access the darknet with any degree of security. And that's important once you think about the fact that almost everyone who gets caught doing something illicit gets caught because of security lapses. We will even go so far as to recommend using a clean laptop—completely devoid of any personal data or links to legitimate online accounts such as banking—and thus dedicated only to your deep web and darknet adventures. You certainly don't want to be playing around in these neighborhoods with a computer that, if breached, would reveal a lot about your activities.

THE TAKEAWAY
The darknet is a fascinating place to spend a little time exploring, but dangers lurk everywhere, even if you're not doing anything illicit. Take reasonable precautions.

**BASIC SECURITY**
- Don't engage in any kind of illegal or questionable activity on the Internet.
- If you do any transactions on darknet sites, even perfectly legal ones, use encryption for everything.
- Disable all scripts ion your browser before logging on to Tor.

**ADVANCED MEASURES**
- Only use cryptocurrency for darknet transactions, and employ a tumbler to ensure optimal anonymity.
- Change usernames and passwords frequently.

**TINFL-HAT BRIGADE**
- Minimize coin kept in escrow to avoid losing it in a bust or heist.
- Use both Tor and a VPN to completely anonymize your traffic.
- Keep your data on a thumb drive so that you can erase all traces from your regular machine.
We close this book by taking a look at cybersecurity on a global scale. Know who’s already doing that? Every government on Earth, and each has been at it for a very long time. Nation-states consider “cyber” to be a key area of operations. It’s where they communicate, spy, command, and control—and sometimes, where they attack.

Cyberspying against the United States became so problematic by 2011 that the military changed its policy on cyberattacks to “equivalency”—essentially, online attacks are now viewed just like physical ones. An unnamed military source told the Wall Street Journal that “if you shut down our power grid, maybe we will put a missile down one of your smokestacks.” It was as a clear warning to Chinese and Russian hackers, the latter of whom had recently used cyber attacks to turn off the lights in Estonia, and then again in Georgia, as precursors to invasion.

Nations have a number of ways to rattle their cyber sabers. At the low end of aggression is intellectual-property theft and piracy. At the high end is the notion of crashing another nation’s infrastructure or hacking its military. And what about non-nation-states doing such things? Could a teenage hacker really start a world war?

CUCKOO FOR CYBER SPIES Although cyberterrorism has been fairly big news as of late, it’s actually far from a new concept. The contemporary cyber espionage era started up pretty much as soon as computers were first connected to public networks. For a real thriller of a hacker story, try reading Clifford Stoll’s 1989 classic The Cuckoo’s Egg. This nonfiction page-turner tells the incredible but true-to-life tale of how a systems administrator doggedly chased down a 75-cent UNIX-system accounting error, which unfolded into ultimately taking down a complex, KGB-funded cyber operation in 1986 that was seeking to steal U.S. military secrets through the fledgling internet. Stoll solved the case himself in spite of a series of infuriatingly dense FBI agents straight out of Central Casting, along with a cast of dozens of square-jawed spooks, each one of them more impossibly unhelpful than the last.
STEALING OUR GOOD STUFF So, what is intellectual property (IP) anyway? The legal definition is “creations of the mind, such as inventions; literary and artistic works; designs; and symbols, names, and images used in commerce.” The term covers everything from art and music to apps and code. Theft of IP isn’t super glamorous, so most cases, even multibillion-dollar ones, don’t make the news outside of the business pages. The U.S. government recently estimated that cybertheft of intellectual property costs the economy $300 billion USD a year. If you find yourself wondering why cyber espionage is so prevalent, it’s simple: It is substantially cheaper and faster to steal stuff than it is to build it from scratch.

“The only adversary one needs to worry about,” says David Etue, from cyber security firm Rapid7, “is the one who figures out that he can steal for $2 million what it takes you $2 billion to research and develop.” Etue is right. It’s much easier for foreign government-controlled companies to simply steal their way to success than it is to build it through R&D.

Industrial Espionage It’s not just commercial IP that gets ripped off. Drug trials, oil and fuel formulations, and other industrial secrets are in great demand. And it’s not just the Chinese and the Russians doing the dirty work. Industrial espionage is top of the pops in France, as well as in many other nations. What a lot of people may not realize is that, to China and Russia, commercial adversaries count as targets for government espionage. Chinese and Russian companies are often owned by the government, so interference

THE COST OF CYBER THEFT The thing about IP is that it frequently forms the core of a company’s identity. A stolen computer can be replaced, stolen money can be recouped. A cyber breach of this kind is more like identity theft on a grand scale, and the real and intangible costs can be staggering.

Visible Costs of IP Theft
- Investigations
- Need to Notify Customers
- Monitoring Customer Security Post-Breach
- Regulatory Compliance Issues
- PR to Combat Negative Publicity
- Upgrade Cyber Security & Training
- Lawyers’ Fees, Other Legal Costs

Hidden Costs of IP Theft
- High Insurance Premiums
- Lower Credit Rating
- Lost Productivity & Low Morale
- Lost Customers
- Loss of Potential Future Business
- Reputation and Value of Brand Suffer
- R&D Time and Investment Wasted

HOW TO GET AWAY WITH IT... Supercomputer hacking is just the tip of the iceberg. From the Russian backdoor in the Ukrainian power grid, to the hack of the Denver Broncos in 2015, Henry—the former Black Hat hacker who now works for the intelligence service and has offered insights into the press about how to escape without detection—told The Wall Street Journal that commercial secrets are a tool of legitimate nations.
from government or military hacking groups against American competitors is seen not as a business chicanery but a matter of national security. It's not just the money, per se. It's about securing the future—especially in the realms of critical infrastructure, energy, medicine, and finance. It's business as usual.

**National Security** That's why, when the United States began shouting its protestations about Russian involvement in the 2016 hack of the Democratic National Committee, none other than Shawn Henry—the former assistant executive director of the FBI, for which he had largely established its cyber practice, and the man who led the investigation into the DNC hack for CrowdStrike—spoke out in the press about it in no uncertain terms: "It's the job of every foreign intelligence service to collect intelligence against their adversaries," he told the *Washington Post.* For the Chinese and Russians, commercial secrets and commercial organizations are considered legitimate nation-state adversaries.

**BORDER SECURITY** A relatively new concern in 2017 was searches of electronic devices by U.S. Customs and Border Protection. The law allows these searches, but they are still rare—in 2016, there were 390 million crossings and 24,000 searches. Still, if you don't want Uncle Sam plowing through your hard drive, power down devices fully before crossing borders (cold boot security is often stronger than when merely suspended or locked) and minimize the amount and sensitivity of data and equipment you transport across borders. Be aware that citizens cannot be denied entry but can be detained briefly for questioning. Under no circumstances should you lie to CBP officials. If they request or demand a password, it is your right to refuse to comply, but equipment can still be detained for weeks or months. If this happens, you should consider legal assistance—Ryan Lackey, Founder, Reset Security
KEY CONCEPT

ZERO-DAY Security researchers seek out vulnerabilities in code. When they find one, they have several courses of action. If they work for a government spy agency or a criminal gang, they may choose to create code that can exploit the vulnerability they have found—this weaponized code, before it is disclosed to anyone else, is called a "zero-day." It comes from the amount of time, in days, once the vulnerability is known until the maker of the software can fix the problem. On day zero (which is actually the first day—as computers always count everything starting from zero), the weapon is active. The ethics of selling zero-days is debatable. Companies that sell them to governments argue that, so long as the transaction is legal, the ethics are beside the point. Critics say that governments can use zero-days to attack and monitor dissidents. It's a tough call.

Chapter 14

INFRASTRUCTURE ATTACKS In March of 2007, researchers at Idaho National Laboratory sent a test cyberattack to breakers that protected a 2.25-megawatt diesel-powered generator. Within a minute, the generator, weighing tons, literally jumped in the air, began to smoke, and was destroyed. Official video of this attack—considered the first public demonstration of a successful cyberattack on critical infrastructure—was leaked to CNN. The "Aurora Vulnerability," as it was called, was shocking for its simplicity, and cyber security experts began pointing out that America's supervisory control and data acquisition (SCADA) networks and industrial control system (ICS) networks are aged, fragile, overwhelmingly small, and privately owned—so this problem is not something that the U.S. government can simply order fixed. Ultimately, if a local power department decides not to invest $3,000 USD in patch management, that's a private business decision that the government can't overrule, absent clear threat and a court order.

The media became fascinated by attacks on SCADA and ICS, seeing every shutdown as a potential hack. Several attacks on critical infrastructure have happened, and each has been denied vocally by some. In 2009, widespread power outages in Brazil were reportedly caused by hackers; experts reported that it was soot, not hackers. Senior U.S. officials countered "nuh-uh," and it's never been settled.

Russian Aggressions No such uncertainty exists when it comes to Russian tactics: Russian government-mounted cyber attacks in the form of website takeovers, DNS attacks, and ultimately the complete blackout of Georgian internet traffic, which served as a precursor to invasion in 2008. This tactic has become a standard by Russia, which rather openly cyber-attacked the Ukrainian power grid in 2016, shutting down more than fifty power substations.

ATTACK DISTRIBUTION

No matter the time of year, criminals, activists, and others are busy with cyber attacks and other operations.

What's at Risk? The U.S. government relies on nearly 80% of the nation's electrical grid, telecommunications systems, food and fuel supply networks, and water, oil, and gas. The good news is that the U.S. government, along with industrial and communication companies, and corporations and the ICS community have been more effective than in the past. Cyber attacks on SCADA and ICS in the U.S. are in marginally clear danger, and those who believe the worst (and there are many) say attacks have been as brazen and wide-ranging as they should not, and as they shouldn't be, so there is no cause for alarm.

PAGING YOUR ATTENTION

As we discussed in our recent articles on cyber war, cyber espionage, and economic warfare, wireless paging systems are a valuable commodity in the market. They are valuable as a foundation to the reporting and distribution of valuable information. Whether it's in the form of a message or connected to a specific location, cyber attacks or cyber espionage can be made as easy as paging a group of people with the term "cyber espionage." But as we've also seen, this isn't our reality. What we need to do is look at cyber pages more carefully and take the time to ensure that the information we give them is worth the effort.
What's at Risk? The scary news is that the SCADA systems in control of the nation's power are no any worse off than the systems that protect water, sewage, or other critical infrastructure, such as oil and gas. The good news is that, over the past few years, the federal government, along with the North American Electric Reliability Corporation and other groups, has been focusing intensely on SCADA and ICS issues. The problems are not yet solved, but we are in marginally more aware than we were a few years ago. That said, attacks have indeed been weaponized, and more things are connected to the internet than ever before (even though they shouldn't be), so it all may be a wash.

PAGING YOUR INFRASTRUCTURE Does anyone use pagers anymore? Funny thing—apparently, a large number of critical infrastructure players, including chemical manufacturers, nuclear and electric plants, defense contractors, and others rely on unsecured wireless pagers to automate their industrial control systems. According to a 2016 report, this practice opens them to malicious hacks and espionage. In the report, researchers from security firm Trend Micro collected more than fifty-four million pages during a four-month span using low-cost hardware. In some cases, the messages alerted recipients to unsafe conditions affecting mission-critical infrastructure as they were detected. According to the report, "These unencrypted pager messages are a valuable source of passive intelligence, the gathering of information that is unintentionally leaked by networked or connected organizations. . . . Taken together, threat actors can do heavy reconnaissance on targets by making sense of the acquired information through paging messages. Though we are not well versed with the terms and information used in some of the sectors in our research, we were able to determine what the pages mean, including how attackers would make use of them in an elaborate targeted attack or how industry competitors would take advantage of such information."

T/F

AMERICA'S NUCLEAR LAUNCH CODES ARE KEPT ON FLOPPIES

TRUE Currently, if you want to launch a nuclear strike, you need technology from the 1970s in order to do so—an 8-inch floppy disk of the kind most modern adults have never even seen. It's not unreasonable to assume that this is on purpose—sort of a Battlestar Galactica scenario, where our most sensitive data is kept in such a way that our enemies (or teenage hackers) can't get at it. In fact, the truth is much more mundane—the U.S. government's cyber systems are woefully out of date, and we spend some $60 billion USD annually on maintaining those outdated systems.
**MOBILE PHONE HACKS** From sometime before 2004 (during the run up to the Olympic games in Greece) until January of 2005, either a criminal-based or nation-state-sponsored hacking gang engaged in a mass mobile phone network hacking operation. This group was tapping into Vodafone’s switches in Greece, and targeting a range of calls to specific phones. Targets of this hacking incident included the mobile phones belonging to ministers of Greek national defense, foreign affairs, and justice departments; the mayor of Athens; the European Union commissioner for Greece; a variety of individuals engaged in civil rights, anti-globalization, and peace activism; and diplomats carrying mobile phones belonging to the U.S. embassy at Athens. Since that time, security experts have pointed out similar cases around the world in which the mobile networks in various countries have been compromised.

**A History of Vulnerability** None of these issues are particularly new—mobile networks, just like any other network, are susceptible to security issues. Nonetheless, occasionally this sort of thing becomes big news. In 2016, we learned of vulnerabilities in a digital signaling protocol that mobile phone carriers such as AT&T, T-Mobile, and Sprint use to track their users’ identity, location, and more. A 60 Minutes segment highlighted a hacker using that vulnerability to access phone data. That episode scared the pants off of seemingly everyone who saw it—and a bunch who just heard about it second-hand. Mobile networks are being patched as fast as they can, but SS7 (Signaling System No. 7, a common network protocol for handling phone calls and SMS messages) is only one of many vulnerabilities in how mobile operators handle the complex task of routing more and more voice and data calls each day.

**MOBILE PRIVACY**
Your mobile device's signal and data could be intercepted mid-transmission, and you might never know it.

[Diagram of mobile privacy setup with cell tower, van, and mobile users]
Mobile Privacy Today  During the past handful of years, the privacy community has begun to seriously question how good law enforcement really is at intercepting cellular signals and harvesting mobile phone data. The equipment for doing this sort of thing has been available to federal agencies and to some larger law enforcement agencies for several years by now. Technical advances have brought the costs down, while increased reliance on smartphones by individuals has increased the bang for the buck these products can provide, so more agencies are using them. These include tools called IMSI-catchers, which we’ve discussed briefly earlier in this book. IMSI stands for “international mobile subscriber identity” — that is, the unique identification number tagged to each mobile phone, which then allows a cellular network to distinguish each user from another. This device works as a man-in-the-middle platform for eavesdropping on phones on the GSM (global system for mobile) network.

Essentially, IMSI-catchers are portable base stations that can simulate a powerful cellular phone signal tower so that your phone, which always seeks out the most powerful signal within range, associates itself with it. Once that happens, the IMSI-catcher will intercept your signal before passing it on to a real tower (so that your call still does go through), but it captures everything that both sides say all the while — and you probably won’t even notice.

Spying on the Airwaves  Think IMSI-catchers are the thing you need to worry about if you want to avoid being eavesdropped on? Unfortunately, that’s far from the case. The emergence of 4G LTE (long-term evolution) networking, also known as LTE, addressed some of these privacy issues, but, in 2015 researchers released information about kits that run about $1,200 USD and allow anyone who has a laptop and a universal radio software peripheral (USRP) and the proper software to intercept and locate 4G LTE traffic.

Another thing to consider is the advent of open platforms for mobile telephone operators. What Linux is to operating systems such as OpenBTS and OpenLTE are to mobile telephony: a set of freely available tools that can enable highly sophisticated mobile operations. David Burgess, one of the creators of OpenBTS, set up a mobile network at the Burning Man festival using his OpenBTS platform — and it worked just fine for everyone using it. As these tools to interact with increasingly smarter phones become less expensive and more commonly available, and as we rely more on our mobile devices for everything, we can expect even more attacks on cellular phones and mobile networks using this vector.
WHAT’S THE BUZZ? After 9/11, one of the most commonly heard terms from the intelligence community in the public domain was “chatter.” It’s a brilliant term because it sounds highly specific, but it’s really quite generic, encompassing signals intelligence and publicly overheard sentiment on radio, television, internet forums and chatrooms, newspaper editorials, and gossip. Basically, chatter can mean just about anything.

We won’t hear anything useful about SIGINT being gathered today (unless it’s being proffered as a justification for military actions or economic sanctions), because our intelligence agencies focusing on that (mainly the National Security Agency) are incredibly good at not saying things. But we do understand from a few peeks inside how chatter is used by professionals to track terror groups.

Taking Responsibility If 9/11 resulted from a breakdown of intelligence upon a national scale, at the New York Police Department it was seen as a failure to take responsibility for the city’s destiny. New York doesn’t stay on the wrong side of a problem very long; at about 9 a.m. on September 11, 2001, senior officials at the NYPD surveyed the smoldering wreckage of the World Trade Center and said, “Yeah, this is not going to happen ever again.” They began to create an intelligence capability that has become an extraordinary agency in its own right, combining tradecraft and procedures imported from agencies like the CIA (David Cohen, the NYPD’s first commissioner for intelligence, is ex-CIA) and a hodgepodge of methods that other agencies practiced. The result was uniquely New York, because the NYPD got to do something few ever get to do: start from scratch and create a culture.
Doing It Right Like many other intelligence agencies, the NYPD created a cadre of incredibly capable young officers to be stationed around the world to provide continuous, on-the-ground intelligence. And one thing that the NYPD Intelligence Bureau had done very well was to establish it early on. Uniquely, for its cyber capability, the bureau used NYPD detectives to focus on looking for threats, capabilities, and intent, while also relying on civilian analysts to provide the language expertise (everything from Arabic to Pashto to Urdu) and for their cyber-fu. Meanwhile, the bureau also allowed the detective-investigators to remain professionals in their highly significant areas of expertise.

Typically, the IB Cyber Unit focuses on detection and investigation of radicalization and various threats as they pertain to New York City. In a nutshell, the team focuses on the enormous pile of people saying stuff that sounds radical, separating out people who are just spouting off or exercising free speech from those truly thinking about radicalization, then investigating and separating the curious from those with true intent.

WHO’S BEING ATTACKED?

As one might expect, the vast majority of cyberattacks are launched at the USA, but many other nations fall victim as well.

- U.S.A.
- China
- Germany
- Britain
- Brazil
- Spain
- Italy
- France
- Turkey
- Poland
- India
- Canada
- South Korea
- Taiwan
- Japan
- Mexico
- Argentina
- Australia
- Israel
- All Other Countries
Chapter 14

ONE SILVER LINING TO THINK OF REGARDING CYBER WAR... AT LEAST IT'S EASIER TO REBOOT A NETWORK THAN REBUILD A CITY.

Cyber Terrorism In the last five years, many of the cyber-attack tools that were once used exclusively by nation-states have become more easy to obtain, meaning that they can now also be used by criminal gangs and—at least in theory—terror groups as well. But buying a great piano really cheap doesn't mean you can suddenly play Chopin. The money and training that go in to a cyber operation is the true barrier to entry.

During the 2016 election, hacking by Russia caused tremendous disruption in the United States. We now know that during the six-to nine-month gestation period after the Russians gained entry to the network of the Democratic National Committee, but before they began to release email publicly, their activities consisted mainly of lateral movement within the network. During that time, the attackers engaged in rather routine but essential activities of a long-term network reconnaissance operation, including data classification and location. The hackers were answering the questions: What does the DNC have? Where do they keep it? How do they use it? How do they access it? Basically, they were learning the answer to “What does normal look like in this organization?” All this showed one important difference between a nation-state attack and those mounted by terror groups: tradecraft.

Art and Craft Tradecraft is the techniques, methods, and tools that together form the art of spying, and it's not something that comes easily. It takes years of experience, lots of money, and great leadership and training. Mostly, when we look at terror groups, we see them spending what money and leadership and training resources they have not on tradecraft but on materiel and logistics for attack: moving men, guns, and bombs across distances; getting them training; smuggling them across borders; and mounting attacks.
Hackers Are Everywhere The barriers terrorists being able to launch a cyber attack are getting lower. When we look at the troubles that groups like Anonymous and LulzSec have caused law enforcement and other government groups, the disruption was significant. Their success was based on a commonly agreed-upon mission, a decentralized command and control, and the availability of free, easy-to-use, and easy-to-learn hacking and attack tools. This sounds like the basis of a classic terrorist attack, and it can be used by groups such as ISIS once the cyberweaponry they would need has been simplified to the point that it’s easily adopted by groups with minimal resources. It just takes a small group of radicalized, computer-literate believers to tip these scales.

THE TAKEAWAY
Protecting your data when you travel is fairly easy. Stopping a global cyber war—not so much. Still, there are always ways to be prepared.

**BASIC SECURITY**
- Protect your IP online and when traveling.
- Encrypt all products and IP-related communications.

**ADVANCED MEASURES**
- Use purpose-built devices for cross-border travel.
- Maintain minimal mobile mail settings (no one needs more than thirty days of email on their phone at this point).
- Encrypt everything.
- Minimize data sets provided to business partners.
- Audit partners’ security as you would your own.

**TINFOIL-HAT BRIGADE**
- Prepare for an infrastructure attack.
- Get off the electric grid with solar power.
- Prepare to have an interruption in your water supply.
- Practice self-sufficiency.

SHALL WE PLAY A GAME? In 1983, a movie called *WarGames* captured the world’s imagination with the plotline in which a teenage hacker almost starts World War III when he hacks into a Defense Department computer. One major unexpected consequence of that film was that then-president Ronald Reagan saw it and was subsequently moved to devote resources into what we now call cyber security. A great number of young hackers were also inspired by the movie, perhaps most the famous being a group of Milwaukee-area high-school students who went by the collective name The 414s (for their area code in Wisconsin). The 414s breached a number of big corporate networks for fun, simply as a prank rather than to steal or damage anything. Since hacking was more difficult to prosecute at the time, they were finally charged with making illegal phone calls.
Throughout this book, we’ve ended each chapter with a summary of what we’ve called “the takeaways”—some hands-on action items you can apply in your everyday life to avoid the dangers highlighted in that chapter. Avid readers have no doubt noticed that some of these measures are repeated multiple times, because some safety measures are widely applicable. Some other suggestions may only show up once, if they pertain to a very specialized area (such as online education, or international affairs). This chart is the “if you remember nothing else, remember these things” summary to clip out and hang on that smart, Wi-Fi-enabled refrigerator that for all you know is sharing scandalous tidbits about your snacking habits with foreign spies right now.

**BASIC SECURITY**

- Use different strong passwords for every login (website, desktop programs, phone apps).
- Use a password vault program.
- Password-protect and disable remote management on your modem, router, and any other Internet-connected devices using unique passwords.
- Password-protect home Wi-Fi and encrypt with WPA-2 PSK at a minimum—never WEP.
- Never share your login information with anyone.
- Don’t click on suspicious links or download unexpected files.
- If anything you’re offered online seems too good to be true, it is.
- Never give private information out over email or text. Always call the bank, utility, or service that’s ostensibly asking for your information.
- If you lose your wallet, report missing cards immediately. Carry the minimum set of cards, and never your Social Security card.
- Set all social media privacy settings as high (private) as possible.
- Monitor kids’ social media usage, and talk to them about online sharing and safety.
- Use a minimum of 8-digit screen lock codes (not fingerprint or face recognition) on all mobile devices.
- Encrypt your phone.
ADVANCED MEASURES

- Always use two-factor authentication (2FA) when possible.
- Don’t get your children Social Security cards if possible.
- Check your credit report regularly; do so for all family members including kids.
- File a police report after fraud of any amount.
- Only use CHIP-and-signature cards (or CHIP+PIN where available).
- Only use the internet in incognito mode.
- Encrypt everything.
- Never use public Wi-Fi without a VPN or SSH tunnel.
- Restrict and lock down your home network, starting with DNS.
- Install GPS tracking apps on kids’ phones.
- Limit location services and Wi-Fi use on your phone.
- Ensure the minimum metadata is saved with all photos.
- Only use credit cards that offer fraud and identity protection.
- Maintain minimal mobile mail settings.

TINFOIL HAT BRIGADE

- Eschew electronic communication wherever possible.
- File your taxes the old-fashioned way; on paper.
- Don’t use banking apps on your phone.
- Don’t shop online except through guest accounts and one-time credit cards.
- Don’t shop at stores with older, swipe-only (non-Chip) POS terminals.
- Post online only under anonymous usernames; change them frequently.
- Lock down all social media accounts to private; ensure your children have done the same.
- Cover all computer webcams and microphones with electrical tape; remove cameras and microphones from mobile devices if you can.
- Use spyware to track all of your children’s online activity.
- Use a private LAN for kids’ computers, IoT devices, and TVs, and aggressively blacklist sites at the router.
- Use encrypted DNS.
- Regularly reflash your phone to factory settings.
- Prepare for an infrastructure attack with off-the-grid self-sufficiency measures.
GLOSSARY

BITCOIN: The first of the difficult-to-trace digital currencies. It uses cryptographic techniques for peer-to-peer transactions that are not linked to traditional banking institutions, allowing users to keep their identities separate from their online wallets.

BURNER PHONE: A disposable phone, bought for cash, to avoid tying identity to a number. Related, a burner number is a temporary phone number generated by an app that lets users keep their main number private, adding an extra layer of privacy to smartphones.

CRYPTOGRAPHY: The enciphering and deciphering of messages as well as the storing and transmission of data in such a way that only those for whom the data is intended can read and process it.

CYBERCRIME: Generally, crime involving a computer or network; specifically, illegal activity committed through or leveraging an electronic-based medium or targeting a computer-based platform.

CAMMING: The use of a webcam to communicate with someone through the Internet, usually refers to sexual performance done for fun or money.

CATPHISHING: The practice of creating a false online profile for the purpose of deceiving people who are looking for genuine relationships.

CRYPTOME: Created in 1996 by privacy advocate John Young, this site collects information about freedom of speech, privacy, cryptography, dual-use technologies, national security, intelligence, and government surveillance.

BLACK HAT HACKER: A hacker who breaks into systems and networks for malicious intent. The black hat hacker might steal data, install malicious code, or otherwise exploit the penetration.

CRYPTOCURRENCY: Operating independently of a central bank or much government regulation, cryptocurrency is a medium of exchange that uses encryption techniques to transfer funds anonymously and to regulate the creation of "new" currency.

BIOMETRIC DATA: Mathematical representations of measurable physical characteristics, such as irises, fingerprints, facial structure, voice, etc., utilized to verify identification.

BLACK HAT HACKER: A non-obvious entryway built into a computer system or software program for remote administration; also refers to a method of bypassing authentication security to enable an unauthorized person to gain access.

CATPHISHING: The practice of creating a false online profile for the purpose of deceiving people who are looking for genuine relationships.

CRYPTOCURRENCY: Operating independently of a central bank or much government regulation, cryptocurrency is a medium of exchange that uses encryption techniques to transfer funds anonymously and to regulate the creation of "new" currency.

DARKNET: An underground network. It is only accessible through advanced access techniques. Elements include anonymizing technologies and careful movements. This is the "cyber underworld."
APPENDIX

CYBERWARFARE: The use of computer technology to attack or sabotage vulnerable information systems of a state or a nation for strategic or military purposes. Attacks encompass introducing viruses, disabling websites and networks, denying or disrupting essential services, stealing or altering classified data, among other nefarious possibilities.

DARKNET: An intentionally hidden, small segment of the deep web that is only accessible through special software and cannot be reached through standard web browsing techniques. Encryption and anonymizing software hide users’ movements. The darknet is often used for accessing illicit content and illegal peer-to-peer file sharing, although whistle-blowers and political dissidents, among others, have valid reasons for utilizing it.

DEEP WEB: Making up 90 percent of the Internet, the deep web is essentially anything a search engine can’t find, consisting of vast amounts of unindexed information. Examples include anything that is password protected, I.R.S. and Social Security information, members-only databases or emails, bank statements, etc.

DIGITAL NATIVES: The generation of kids born after the mass adoption of the Internet.

DISTRIBUTED DENIAL OF SERVICE (DDOS): A cyberattack whereby an online service is rendered unavailable by overwhelming it with traffic from multiple sources.

DOXXING: The practice of researching and broadcasting online private or identifiable information (especially personal information such as a home address) about an individual or organization.

DUMP: A credit card dump is when cyber thieves copy the information in the magnetic strip of an active credit card to make a fake credit card that can be used by cybercriminals to make purchases.
EXIF DATA: Short for Exchangeable Image File, this is the data your smartphone or digital camera collects when you take a photo, which, in addition to camera settings, can reveal when and where your image was taken, enabling stalkers to track you.

FIREWALL: The first line of defense in network security, firewalls monitor incoming and outgoing computer traffic and, based on predefined security rules, determine which traffic should be allowed or blocked.

FRAUDULENT DATA FURNISHING: Done by a complicit business insider, this scheme involves reporting fake financial data for a synthetic ID to credit bureaus. In more sophisticated schemes, the business doing the reporting may also be fictitious.

GRAY MARKET: The trade of legal non-counterfeit goods that are sold outside of the manufacturer’s chosen distribution channels; gray-market goods, also known as “parallel imports,” are usually much cheaper when purchased this way, but do not come with warranties.

HACKTIVISM: A portmanteau of “hacking” and “activism,” hacktivism is the act of breaking into a computer system to promote social or political change.

HASH: Used to create signatures to authenticate messages and files, a hash is an algorithm that turns the contents of a file (such as text or an image) into a fixed-length value called a “hash value” or “hash code.”

KNOWLEDGE-BASED AUTHENTICATION (KBA): A method some websites use for account verification. With static KBA, also known as “shared secret questions,” users answer previously defined questions; with dynamic KBA, questions are generated based on what the site knows about the visitor, culled from public and private data. An example might be, “What was your street address when you were ten years old?”

KOMPROMAT: A portmanteau of the Russian words for “compromising” and “information”, and a mainstay of espionage, this term refers to compromising materials about a politician or other public figure used to create negative publicity, or to use for blackmail or for ensuring loyalty.

EXPLOIT: An attack on a computer system, taking advantage of a vulnerability that allows unauthorized access.

IMSI-CATCHER: An eavesdropping device that impersonates cell-towers and intercepts cell phone traffic tracking the movement of the user.

INFOSEC: The term refers to “information security,” or the protection of information (both electronic and physical) from unauthorized access, use, destruction, etc.

INTERNET OF THINGS (IOT): A network of interconnected objects that send and receive data via the Internet using Bluetooth or Wi-Fi.

’LEET (1337) SPEAK: An informal language used by hackers to conceal their sites from search engines that usually consists of replacing letters with numbers or symbols.

LULZ: Derived from the plural of lol (laughing out loud), this term primarily means “laughs” or “laughing,” but the Internet term has come to mean laughing at someone else’s expense.

MALWARE: Malware stands for “malicious software,” programs that can damage or compromise those who unwittingly download it.

MMOG: A massively multiplayer online game.

MT. GOX: A Tokyo-based bitcoin exchange, which was launched in 2010 and filed for bankruptcy in 2014 after hackers apparently stole the equivalent of $460 million from its online "virtual bank." The origin of the names comes from Magic: The Gathering Online eXchange, the site’s original use (exchanging Magic: The Gathering cards.)
such as a bank, designed to lure unsuspecting victims into giving out personal information online that will compromise their security.

**PHREAKING:** The act of illegally breaking into telecommunications systems (hacking), especially to obtain free calls.

**RANSOMWARE:** Malicious software designed to encrypt files and backups, holding them hostage until the victim pays for the decryption key. Often uses the same techniques as phishing in order to trick the recipient into opening the attached program that initiates the encryption process.

**RED MARKET:** Economic activities banned by the state, such as drug dealing, arms trade, human trafficking, and the buying and selling of human flesh such as blood, bones, and organs.

**SHODAN:** A search engine that indexes and points to Internet-connected devices; Shodan's crawlers search the internet seeking connected servers, webcams, printers, routers, and other devices.

**SIGNALS INTELLIGENCE (SIGINT):** Intelligence gathering by intercepting electronic signals and communications. This can include all forms of video, voice and data communications.
SILK ROAD: A darknet market, described as “the eBay for drugs” (and other contraband and nefarious services), it was started by Ross Ulbricht in 2011 before being shut down in 2014. The market used TOR and bitcoin to avoid detection. The site’s buyer feedback system lent a sense of security to illegal transactions, and some merchandise offered was considered to be of high quality. Ulbricht was convicted of money laundering, computer hacking, and conspiracy to traffic narcotics and sentenced to life without parole.

SKIMMING: The practice of collecting data from the magnetic strip on a credit card (or debit card) with a camouflaged counterfeit card reader, usually affixed over the card slot on Automated Teller Machines, gas pumps and other point of sale systems. The information harvested is then sold, and ultimately transferred onto a blank card.

SOCIAL ENGINEERING: The use of deceptive means to manipulate individuals into revealing all kinds of personal information. Similar to confidence games.

SPEARPHISHING: Unlike phishing, which involves mass-emailing, spearphishing generally targets users within a single organization and appears to be from an individual or business known to the recipient.

STEGANOGRAPHY: From the Greek word meaning “covered writing,” this refers to the practice of concealing messages within other seemingly innocuous messages, often used to supplement encryption.

SWATTING: Making a prank call to emergency services in an attempt to bring about the dispatch of a large number of armed police officers to a particular address.

SURFACE WEB: Anything that can be indexed by a typical search engine like Google.

SURVEILLANCE MARKETING: The practice whereby companies observe and exploit the information you generate while using their service.

SYNTHETIC IDENTITY: An identity created from real and fabricated information, which is then used to establish a credit profile and secure an easy-to-get, low-limit credit card.

TOR: An acronym for “The Onion Router,” Tor is a protocol that encrypts data and sends it through a network of volunteer relays set up around the world, creating layers that conceal users’ source IP address.
The anonymous network, which was originally developed by the U.S. Department of Defense, can only be accessed with special software and a properly configured web browser.

**TRUECRYPT:** Shut down by its developers, TrueCrypt was once the go-to full- and partial disk encryption software, creating what amounts to a cryptographically hidden, password-protected section of your hard disk.

**TWO-FACTOR AUTHENTICATION (2FA):** Also known as two-step verification, this is a method of verifying login identity by utilizing two (or more) authentication factors. There are three types of authentication factors: something you know (such as a password, PIN, or user name); something you have (such as a bank card or a one-time password token); and the something you are (typically a physical characteristic such as a fingerprint or retina sample). It is possible to have multiple element but single-factor authentication a good example is a website that uses a password (something you know) and a knowledge-based authentication question (something you know).

**TUMBLERS:** Programs or sites that mix identifiable or "tainted" cryptocurrency funds with others to obscure the fund’s original source. The tumbler can also rapidly mingle fractions of transactions without revealing who the transaction is coming out.

**USER-MANAGED ACCESS MANAGEMENT (UMA):** This is an access management model that defines how users log in and receive selective sets of rights for a given security business or entity, and gives them them back over their life.

**VIRTUALIZATION:** The process of virtualizing computing resources on an operating system or application. Virtualization allows multiple operating systems to run inside multiple virtual machines simultaneously.

**VIRTUALIZATION MANAGEMENT:** The process of enabling virtualization on a computing system or network. It enables the creation of virtual machines or virtual networked systems, and can allow management of these resources.

**VIRTUALIZATION MANAGEMENT (VMware):** The process of enabling virtualization on a computing system or network. It enables the creation of virtual machines or virtual networked systems, and can allow management of these resources.
fractions of bitcoins in multiple transactions, after which the bitcoins come out squeaky clean.

**USER-MANAGED ACCESS (UMA):** This OAuth-based access management protocol standard defines how developers enable selective secure data sharing of a smart object. UMA removes the security burden from a manufacturer and gives the consumer/owner power over their own data.

**VIRTUALBOX:** A software virtualization package that installs on an operating system as an application, enabling you to run multiple operating systems, inside multiple virtual machines, simultaneously.

**VIRTUAL MACHINE (VM):** An emulation of a computer system. A virtual machine is an operating system installed atop software that imitates the presence of hardware, providing the same functionality of a physical computer. The end user has the same experience as they would have on their dedicated hardware.

**VIRTUAL SESSION:** A period of use on a computer, when a hypervisor (a piece of software running on top of either an operating system or bare metal) fools the operating system into thinking it is running on hardware, when in fact it is running in memory.

**VOICE OVER INTERNET PROTOCOL (VOIP):** Hardware and software that enables phone service over the Internet.

**VIRTUAL PRIVATE NETWORK (VPN):** An encrypted connection between a user’s computer resident in an untrusted Internet location and a point behind the firewall and within a private network. A VPN allows users to safely traverse public networks (such as a guest Wi-Fi hotspot) by protecting all communications within an encrypted “tunnel.” This is termed virtual because the encrypted tunnel mimics the connectivity provided by an actual network a user would access via, for example, a dedicated fiber connection.

**VULNERABILITY:** A weakness in a software application, computer system, or a network that can be taken advantage of by attackers.

**WARDRIVING:** Also called “access point mapping,” this is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer or smartphone. Also used to describe the act of gaining access to Wi-Fi networks that are unprotected or poorly protected.

**WAREZ:** Pirated, or illegally copied, software that is distributed through the Internet; offering warez is illegal in the United States, as it is considered a form of copyright infringement.

**WHITE HAT HACKER:** This term refers to an ethical computer hacker or a computer security expert who breaks into protected systems and networks to test and assess their security before malicious (or black hat) hackers can detect and exploit them.

**ZERO-DAY OR 0-DAY EXPLOIT:** An action that takes advantage of a software vulnerability that is previously unknown to the software’s author. “Day zero” is the first day in the count of days between the time the vulnerability becomes known until the day it is patched. Security researchers who create 0-days can, depending on their motivations, collaborate with the software publisher to coordinate a patch and then announce, or, commonly in the criminal or nation-state world, never report the vulnerability and simply use or stockpile the exploit until such a time as it is considered appropriate to use it. There is a small but lucrative legal and illegal global industry in creating, trading, and selling exploits.
HOW TO BE A DIGITAL REVOLUTIONARY
BY VIOLET BLUE

RESIST FIGHT CENSORSHIP
BE HEARD STAY SANE
DEFY SURVEILLANCE GEAR UP
The amount of surveillance we're under from corporations and authorities alike should be worrying to anyone, regardless of your politics. Spying on us is big business.

Internet companies have reshaped the world into an economic system dependent on monetizing the ways they can track and surveil us. Then they try to smooth it over with doublespeak about "improving our experience" or "keeping our communities safer." In just one example, smart TV company Vizio had to pay $2.2 million in 2017 to the FTC for its unprecedented spying on customers. Facebook has been an arrogant foe of privacy advocates since it launched, and its data coffers fuel surveillance by authorities. In 2016 the company announced its plans to track which physical stores people shop at and report that information to advertisers. Where do you think that information ends up? Everywhere developers want it to be.

We're out of bounds with spying on each other, as well. Surveilling each other with the use of apps has been happening for as long as consumers have had tech in their homes. In 2017 two commercial cellphone surveillance products, FlexiSpy and Retina-X, were hacked revealing that everyone was spying on someone; parents, construction workers, lawyers, jealous lovers, and more.

Authorities are routinely overreaching with surveillance too, regardless of the law. In a 2016 oversight report, we found out that warrantless spying on Americans had more than doubled since the NSA disclosures of 2013. In 2015, New York police were caught lying about the use of Stingrays to intercept citizens' phone signals, doing so without court oversight.

Politicians see it as their duty to actively help those they think matter most—the wealthy and powerful people, corporations, and countries. Coming full circle back to 2017, this is the year the White House made it free and legal for our internet service providers (ISPs) to track, record and sell all the information they can grab about our online habits.

Defying surveillance isn't about being a liberal, conservative, socialist, or anarchist. It's about standing up for our rights to keep our personal information and our secrets private, and to insist on consent. You need to communicate safely and learn how to defy surveillance every day, whether you're gearing up for a rally, keeping your parents out of your personal life, or angry as hell about corporations and cops stepping all over your rights.

If you skipped Chapter 3 ("Hack-proof your life") and Chapter 4 ("Your phone is a tracking device") then skip right back and read those first. Then you'll be ready for the next level: Anonymity and encryption.
When you want to message friends and family but want to make sure your communication isn't being spied on, you'll want to avoid regular SMS (text messages) and apps like WeChat or Snapchat. That's because neither of these messaging methods use what's called "end-to-end encryption."

Think of end-to-end encryption as if you're sending your messages in a sealed canister, where only the outside of the container is seen by anyone except your recipient. At various points in its journey, the canister is checked to make sure it's sealed, and it verifies its identity. The only person that can open it is the person you send it to. The companies handling your message can't see it or open it.

**Encrypted apps**

Encryption is complicated to set up and maintain if you're not technical, so it's not the kind of thing you can necessarily do yourself. Fortunately more apps are using it than ever before, so you just need to pick the right one.

For most people, apps like WhatsApp, Facebook Messenger, and Signal (Open Whisper Systems) will do the job nicely. They each have drawbacks. Both WhatsApp and Messenger are owned by Facebook. The company has been pretty obvious about the fact that it scans the content of communications in Messenger, and have been facing some legal heat over it. If you use Messenger, be sure to turn on "Secret Conversations" to activate encryption.

As of this book's publication, a German consumer group is suing Facebook over its decision to link and track users’ profiles between the two services (it matches your WhatsApp account with your Facebook profile) to gather more data for its advertisers.

Signal, which comes in phone and desktop versions, is seen as safer and more secure than the Facebook owned alternatives. Yet Signal has a few drawbacks, too. At this time, there is no way to hide your phone number within the service—so anyone you communicate with on Signal will see your phone number. In one instance, it led to the unmasking of a once-anonymous source that insisted on communicating with journalists over Signal. The press outlet found out who the source was by Googling their phone number.

Signal notifies your contacts when you install (join) the service by sending Signal messages to your contacts announcing your arrival—only if those contacts use Signal. You can't turn off that message being sent, you don't get a notification that it was sent, and you aren't told whom it goes to. So if you don't know who uses Signal in your address book, you may want to hold off until Signal (hopefully) creates the ability to make it anonymous.

One app that gets it all right is Threema. With this app, you can be as anonymous as you like, and it gives you fine-grain control over who knows you're on the service, or not. You don't have to let it scan your contacts, and you can create a random profile username, among many other great details. Telegram is another popular encrypted app, but many hackers and security professionals don't trust it. If you use it, be sure to turn on encryption and know that it doesn't work on group messages.
VPNs and online anonymity

Websites and their advertisers are continually making a record of your unique IP address and tracking what computer or cell phone you’re coming from. This means they have a very good idea of your physical location. They could also stitch together information about your online activity. In worst-case scenarios, authorities can contact your Internet Service Provider (ISP) and obtain your identity.

If all that is something you want to keep private, you should know that you can’t trust these businesses (and probably not their employees) with that information. You’ll need to decide if it is important for you to hide your IP address when you visit certain websites or during certain activities or time periods.

Most people prefer to only protect their IP address when they’re using Wi-Fi or Internet access they don’t know or trust. Some people are careful to hide their IP address when they use their laptops in public, like at a café (it helps safeguard against malicious hackers), but they don’t bother to hide their IP at home on their own network. Some people don’t mind if their IP address/location is known to websites and their partner businesses. Others find that trying to keep their IP address private is such a pain in the ass that they make peace with taking the risk.

If there was a show on Netflix about stealing candy from babies, it would look a lot like using public Wi-Fi without a VPN. All advice about attending (or getting anywhere near) a hacker conference begins with “Get a good VPN for all your devices and use it at all times.” Turns out there are some scary-good reasons for that.

A VPN, or virtual private network, masks your computer’s IP address. You can use a VPN to secure access to your own network as well as to public Wi-Fi or Internet access spots. It’s a great way to keep your browsing private, your IP secret, and you attack-proof. A VPN is also a handy way to protect your identity if you want to leave a comment or browse secretly without the website you’re visiting knowing your location.

In companies, a VPN is typically used to connect employees who aren’t at the workplace to a computer at work; they connect remote employees to central work servers. Many companies have VPNs so workers can access files and other resources over the Internet. Outside of company use, VPNs are being used more and more by people who just want to make their Internet use more secure from attackers.

Using a VPN might feel like insider InfoSec knowledge at this point, but so was making complex passwords not too long ago. When you use a VPN, the only thing an attacker sees is your computer talking to it—they can’t see the connection to the sites you’re visiting. Your Internet connection travels encrypted from computer to VPN server; from there the user’s connection travels unencrypted to their final destination (a website). This way, websites only see the VPN’s IP address and not yours. The ability of anyone to spy, intercept, attack, or steal information stops at the VPN.

When you use public Wi-Fi in a café, plane, or airport without turning on a VPN first, you can
be hacked by anyone who's downloaded any of the many, excellent, free, open-source network traffic analysis tools (like Wireshark or TCPDump). The risk of being scanned like this is typically low in private networks, and extremely high in public ones.

Without a VPN, someone with one of these tools who is on the same network as you can see the URLs you're looking at, metadata, and any information transmitted between you and the sites you're visiting. They can also maliciously inject traffic, where you visit a trusted web page that's spiked with code to infect you with malware, which typically steals your banking and identity credentials.

Even if the connection is encrypted (yet you're sans VPN), the attacker is limited to the URL you're visiting and any leaking metadata. But if it's not an "https" site, they'll be able to see and capture plain-text passwords.

If you turn off your VPN to watch Netflix, and leave browser tabs or online apps with active sessions running in the background, you're handing over to malicious hackers anything that's being transmitted while you're watching Netflix.

How to install a VPN:

1. Choose a reputable service
2. Sign up/subscribe
3. Install it on all your devices
4. Adjust your settings
5. Open and surf!

Once installed, a VPN is simple to use: just turn it on before you go online (before you open your email, open a browser window, and so on), and you're all set. In a public Wi-Fi environment like a café or airport, you'll need to log in to the Wi-Fi first and then open your VPN before making another move.

I love how much better I feel using a VPN when I'm at hacker conferences! I can't imagine life without using a VPN, and I can't recommend VPN use strongly enough.

Find a safe VPN

Selecting a VPN you can trust already took research and consideration, weighing connection speeds and pricing, learning about who keeps records and for how long and more. VPN services are also like any other in that they change their record-keeping policies and privacy practices over time, so that's another thing to keep up with.

In addition, these services can accidentally be misconfigured by the VPN itself. Just over a year ago, VPN provider Perfect Privacy found a massive security hole in many services called "Port Fail." It was a bug that de-anonymized users, and most VPN services ignored the problem until the press made noise about it. Many took weeks to put in a fix. One of those was a service
endorsed by Lifehacker, which just shows that anyone can have problems finding a reputable VPN.

It can be overwhelming. It's not as simple as using whatever VPN the security cool kids say is "the one," because even popular services have been behaving badly. For example, popular service Hola VPN recently got caught selling user traffic to a botnet.

Fortunately like most InfoSec topics, VPNs are a bit of a fetish unto themselves for people who are into them. If you want to know what the hallmarks of a trustworthy VPN service are, I have a controversial suggestion for you: the website Torrent Freak. Every year the site writes a post asking, "Which VPN Services Take Your Anonymity Seriously?"

In these extensive posts, TF talks to dozens of top VPN services and asks them what their record keeping policies are, as well as "various other privacy related issues." If a VPN gets a great review one year, has a less great review the next, and then drops off the list completely (like TigerVPN did), then definitely take that as a "buyer beware."

So if a VPN is recommended somewhere, do a little homework before you fork over your data (and your cash). Names that come up as trusted include Perfect Privacy, Freedome, TorGuard, Tunnelbear, FoxyProxy, Black VPN and others. It's generally considered best to use a paid (rather than free) VPN service, and there are a lot of great inexpensive ones to choose from. Your home Internet service provider might even offer a reputable one for free.

Should you have one for your phone? Absolutely, and most VPNs have mobile apps—though look out for the bad ones. Google's Project Fi (the company's phone service provider) automatically secures users on a Google VPN in every public Wi-Fi situation.

The drawbacks? They can slow your connection down, and they may not work with services like Netflix that want to know where you're physically located. Some public places block the use of VPNs, which should be your sign that the network isn't safe to use anyway.

Once you're all set up with your new VPN, use the steps in this post on Lifehacker (lifehacker.com/how-to-see-if-your-vpn-is-leaking-your-ip-address-and-1685180082) to test your VPN to make sure the outside world can only see your VPN's IP address, and make sure you're not leaking your actual IP. Another recommended (and reputable) tool to try is Cocoon. Cocoon hides your IP address when you access the Internet with a Cocoon account, and the Cocoon client can be installed on your browser or on your mobile device.

**Tor is one option**

One way to protect your identity as you cruise around the Internet is to use the free Tor ("The Onion Router") tool or apps that use Tor, like Orbot for Android. Tor is software that allows users to browse the Internet anonymously—most of the time.

Tor is often recommended for dealing with totalitarian regimes and targeted surveillance, rather than people who want to prevent getting hacked or surveilled on public Wi-Fi, want to use torrents, or want to hide their IP address. When it's time to undertake sensitive tasks online, it's best to have several privacy and security options at your disposal rather than automatically
turning to Tor.

You certainly wouldn't want to use Tor for everyday browsing. Bouncing traffic between relays will considerably slow down your internetting. If you're uploading or downloading media for an event or are in the middle of developing news (like a protest), you'll need to be very patient.

It is not easy to set up (or troubleshoot) if you're not particularly tech-savvy. As the Tor Project notes, it "does not protect all of your computer's Internet traffic when you run it. Tor only protects your applications that are properly configured to send their Internet traffic through Tor." They add, "To avoid problems with Tor configuration, we strongly recommend you use the Tor Browser."

How to install Tor:

- Download the Tor Browser Bundle (torproject.org/projects/torbrowser.html.en)
- Double-click to extract the folder
- Open it and click “Start Tor Browser”
- Decide where to keep it
- Click "Install"

When Tor sends your traffic bouncing around through different relays, it eventually comes out through a single one before sending you to your final destination. The last relay is called the "exit node." Because Tor doesn't encrypt your traffic between an exit node and the destination server, any exit node is in a position to intercept any traffic passing through it.

An example of what this can mean happened in 2007 when a security researcher intercepted thousands of emails sent by human rights groups by surveilling the connections coming out of an exit node he was running.

This problem can be solved by using end-to-end encryption on everything while you're using Tor.

Take extra care opening files downloaded via Tor, as they may access the Internet behind the scenes and give away your true IP address. Digital Rights Management (DRM)-protected media files can be used to reveal Tor Browser users’ actual IP address and therefore possibly reveal their identity. If your situation is truly dire, do your research to ensure that you’re not vulnerable to threats like DNS leaks and attacks designed to cross-reference your Tor activities with your non-Tor activities to track you down.

If you only want to stop websites and advertisers tracking you online then hardening your browser with plugins like Privacy Badger or NoScript will do the trick without drawing attention to yourself. If you're not concerned about anonymity but simply want to stop people eavesdropping on sensitive information, then secure HTTPS connections and/or a VPN should keep your secrets safe.

Likewise, if you’re primarily concerned about the metadata retention scheme but have nothing
significant to hide, then Tor is overkill. A correctly configured VPN should be enough to mask your IP address, so efforts to track online activities back to you come to a dead end.

**What if I'm paranoid?**

The most complete way to go to blocked sites and avoid Internet surveillance is to use an operating system called "Tails" (or The Amnesic Incognito Live System). Like the Apple, Windows, or Android operating systems, Tails is an environment within your computer that you switch to using instead of your computer's regular operating system. It forces all outgoing connections through Tor, and non-anonymous connections are blocked.

The Tails website (tails.boum.org) explains you can:

- Use the Internet anonymously and circumvent censorship;
- All connections to the Internet are forced to go through the Tor network;
- Leave no trace on the computer you are using unless you ask it explicitly;
- Use state-of-the-art cryptographic tools to encrypt your files, emails and instant messaging.

Like Tor, Tails is not a "silver bullet" against spying or getting around censorship. A "Warning" page on the Tails website explains what Tails doesn't protect you from, including user missteps and certain kinds of targeted attacks. For instance, it won't protect you from compromised hardware, firmware exploits, man-in-the-middle (MiTM) attacks, or being targeted by a global adversary.

Your Internet Service Provider (ISP) or your local network will see that you're connecting to a Tor relay, so be cautious about drawing attention by using Tails. It also doesn't protect you form yourself, meaning that it won't remove metadata in documents or photos, nor will it separate your identities. To keep identities separate while using Tails, only use one identity at a time and shut down/restart Tails when you switch identities.

Tails can be installed and run on a DVD, USB stick, external drive, or SD card. Once you turn off your computer (or in case of danger, just unplug the USB stick), your Internet activity and disappears without leaving a trace, not even on the external drive. Conveniently, Tails has a great setup assistant on its website that walks you through the installation process (tails.boum.org/install/index.en.html).

**Encryption and PGP**

When the U.S. government's widespread surveillance by the National Security Agency (NSA) was revealed through leaks in 2013, most people learned that governments can spy on anything they want to. And when government authorities fail at spying on us, they make private companies hand over information about users.

It's no longer a matter of finding a microphone in a lampshade; we seldom know we're being
tracked. In fact, companies like Facebook, Yahoo!, Microsoft, and others have been pretty up front about the fact that this happens every day.

Company employees and agencies like the NSA also do bad things for their own purposes all the time. In 2013, U.S. officials confirmed to the Wall Street Journal that NSA officers and employees used the agency’s eavesdropping tools to spy on their love interests. The practice has a typical NSA spy-ops name: LOVEINT, short for love interest.

It’s enough to make anyone want to have truly private communication, regardless of whether or not you want to join a protest. You can protect your email, instant messaging, texting, and Internet browsing from attacks like these, and more, when you start adding encryption to your digital life.

Without encryption, anyone with a few minutes of access to your computer, tablet, or smartphone can spy on, copy, or steal your files.

Encrypting your computer lets you protect your files with a virtually uncrackable password, and Windows, Mac, iOS, and Android all offer ways to encrypt your local storage. Search online to find out how to turn encryption on for your system. Look for Apple’s built-in encryption program FileVault and BitLocker on Windows.

That takes care of your startup drive, but what if you have other drives or files? Locking a folder is a simple barrier that puts a basic level of protection on your files, but encrypting the folder is much better if you really want to keep it private—this process uses a cipher to make the data contained within completely unreadable, so it can’t be circumvented as easily. Multiple internal drives, partitions on a single drive, external drives or thumb drives are not included in FileVault or BitLocker, so if you want to encrypt those you have to do it manually.

When it comes to email, there are a range of ways to secure what you send and receive. When selecting an email provider, choose a major company that offers web-based email, and make sure it uses Secure Sockets Layer (SSL) to send email securely. SSL establishes an encrypted link between a web server and a browser, creating a secure connection. You can tell when a website uses SSL because the address bar (where the URL appears) will show https instead of http.

If an email service (or website in general) doesn’t use SSL, it’s not taking your security seriously at all. So if you fill out a form, press Submit, and the website doesn’t have the s, it means that attackers could read all the information you just submitted to the website. If instead the website is using https, the information being sent over the Internet is encrypted, and it can’t be read by anyone snooping on Wi-Fi—or any network—traffic. Needless to say, you should never ever enter your credit card number into a website that only uses http.

I recommend installing the plug-ins and extension HTTPS Everywhere, which turns your browser into a privacy shield by enabling encryption automatically on sites that support it.

You can take it further. The only way to truly, 100 percent keep your email private is to use something called OpenPGP. This is email encryption, which protects your email so that the only person who can read it is the one you’re sending it to. (PGP stands for “pretty good privacy.”)
There are a couple of free options that aren’t prohibitively technical, such as Mailvelope and GPG Suite.

GPG Suite is an open source (Mac only) plugin for Apple Mail that’s incredibly easy to install and use. With a few simple clicks, you can encrypt, decrypt, sign and verify email.

You can purchase commercial PGP software or use free plugins like Mailvelope. If you’re more technically inclined, download the open source version that uses the OpenPGP protocol, such as GPG (GNU Privacy Guard). No matter what, if you want to send an encrypted email, you need your recipient’s public key (if they have one).

Many PGP implementations have plug-ins for different email clients, such as Outlook on PCs or Mail on Apple computers. As with all software, this can be problematic when system updates and PGP implementation updates don’t come at the same time. Also, it’s important to note that you might be restricted from using PGP at work or on your employer’s network.

With free services such as Mailvelope, any recipient you send an encrypted message to will have to enter a password to read it—and without the password, your message will just look like a bunch of garbage. Gmail/Google Apps, Outlook, Yahoo!, and GMX are all supported, and the app can be configured to support others.

Mailvelope is a browser extension for Google, Chrome, and Firefox that allows secure email communication based on the OpenPGP encryption standard. The framework of Mailvelope and products like it is relatively straightforward. First, install the plug-in. Next, you’ll generate a key pair, which means you’ll use the plug-in to make two sets of code. One set is called your public key, and this is the one you’ll publish. Each contact in your address book who uses PGP or products like Mailvelope will have their own public key, too.

The next time you open Gmail, Yahoo!, or whichever email brand you use, you should notice a lock icon in the compose area when you begin an email. When you’re done writing and ready to send, just click on the lock icon, and Mailvelope should encrypt the message with the recipient’s public key (if they have one) when you hit send.

When you get an email that’s encrypted, the process goes in reverse. You should see the encrypted message with a lock on it, so just click it to enter your key as a password to open it. Mailvelope will then search your saved keys to find the right one and decrypt the message for you.

You have a few options when it comes to encrypted chat apps. Signal is considered the best choice by far, with iPhone, Android, and desktop versions. With Signal you can also make encrypted phone calls. iMessage is for Apple iOS only, but it’s a great choice.

WhatsApp is another popular choice, and it runs on Signal’s secure protocol—though it is owned by Facebook. WhatsApp updated its terms of service in August 2016 to begin sharing names and phone numbers with its parent company, Facebook—which is under investigation for lying about automatically matching WhatsApp users to their Facebook profiles when it acquired WhatsApp in 2014. One app to flat-out avoid is Telegram, which has a laundry list of security problems.
There's another way keep your online messaging secure: A tool called Off-the-Record (OTR) messaging. OTR encrypts your instant messages when you use services like Google Hangouts and Facebook Chat.

Chat/IM software clients like Adium and Xabber all come with OTR messaging, and there are OTR plug-ins you can get if you use clients like Pidgin. OTR encrypts your messages so they can't be read if someone intercepts them, but it doesn't let you save your chats—which might be a desirable thing, depending on how private you want to make your communication. Using OTR means that even the service sending and receiving your IMs and chat can't read the content.

Although it's the best tool we have today, PGP encryption (and OTR) isn't bulletproof. If the NSA really wants to spy on you, it has the resources to figure out a way to break OTR (if it hasn't already). But that takes money, time, staff and a really good reason. Unless you're hiding state secrets or doing something really nefarious that will make the authorities hunt you down, PGP and OTR should do the job for you, because you probably care more about keeping your messages confidential than about evading authorities.

It's important to also consider that there are ways for people interested in digging up dirt on you to use information that PGP doesn't encrypt. Like the recipient of your message, when you messaged them, their IP address, and so on. That said, if you're an activist (or journalist, blogger, or writer) in a country where you're a government target, use encrypted communications with caution. Reports of activists “flagged” for targeting because they use encryption (or privacy tools such as Tor) are not uncommon.

Like everything in privacy and security, it pays to be cautious and slightly paranoid. Still, it's easy to get caught up in surveillance hysteria, or feel like an outsider when limelight-addicted activists one-up each other about who knows more, or has better "OPSEC" (shorthand for "operational security"). Ignore the hype and posturing, and listen to your gut. Fighting surveillance is a very personal experience, and unique to each person's situation and needs. Take what you've learned in this chapter, its tools and information, and assess what's best for you.
CHAPTER 7
FIGHT CENSORSHIP

The control and suppression of opinions, ideas, words, images, and information is the hallmark of oppression. Whether it's done by a despotic government regime, a company, an algorithm, or an individual, it's censorship. This is the imposing of political or moral values on others, and it comes in different forms.

They ways you'll encounter censorship will vary. Considering how conservative and easily-abused social networks are, you've probably already dealt with censorship in one way or another already.

This is especially true if you speak up about controversial topics, or have anything to do with human sexuality in life or art. You might be censored by a social network for posting a photo or video, or even for criticizing the network itself. It's possible that your meme, posts, or other media gets censored by other people, who attempt to silence you by unfairly reporting your post or account for Terms of Service violations.

Or, you've encountered censorship when you've tried to access controversial or non-conservative information online—from content filters. Like when a government pressures an Internet provider to filter or shut off access to users.

When you're censored online, no one can find you—and you can't tell anyone you're being silenced. Censorship happens in secret. This chapter shines a light on what's going on with online censorship and how it directly affects you—and gives you tools to fight with.

How they censor you
The Open Net Initiative (opennet.net) identifies four different kinds of Internet censorship: Technical methods, search request removals, takedowns, and induced self-censorship.

Technical methods include IP blocking, DNS tampering, and URL blocking using a proxy. According to Open Net, these techniques block specific pages, URLs, or IP addresses. "These methods are most frequently used where direct jurisdiction or control over websites are beyond the reach of authorities," they explain. Further, "keyword blocking, which blocks access to websites based on the words found in URLs or blocks searches involving blacklisted terms, is a more advanced technique that a growing number of countries are employing."

Search request removals are exactly what it sounds like. A government asks or pressures a search company like Google to exclude websites and terms from search results.

This can also be done in developer circles with a search that's done in apps and on specific sites, for reasons either moral, political or personal. In 2015, someone found my name in a list of banned search terms that was used as the basis for a large commercial photo website. The list
had been copied and used in hundreds of other projects. It took considerable work to fix the issue, and the originator of the "banned words" list ignored everyone's requests for an explanation. Most people assumed his ambivalence to these inquiries indicated that he disliked me or my work. The end result in any situation with banned, blocked, or removed search terms is that the topic, term, and websites can't be found. The person or the thing is simply erased.

Takedown censorship is when an entity legally demands the removal of websites. Open Net explains that in many countries, "a cease and desist notice sent from one private party to another, with the threat of subsequent legal action, is enough to convince web hosts to take down websites ... Where authorities have control of domain name servers, officials can deregister a domain that is hosting restricted content, making the website invisible to the browsers of users seeking to access the site."

Induced self-censorship is something we've seen a lot of with the various election propaganda wars on social media, and with harassment and bullying of people in movements such as Black Lives Matter. People are pressured to self-censor both in browsing habits, for fear of surveillance, and in choosing what they do (or don't) post online. Self-censorship is an enormous tool leveraged on social networks, whose methods of preventing abuse (and its resulting intimidation and silencing) are all quite broken. Additionally, ONI tells us "the threat of legal action, the promotion of social norms, or informal methods of intimidation" are also used to censor our voices online.

Finally, there's algorithmic censorship. Keyword censoring largely fuels this, yet some social networks have been taking it a step further. Facebook scans and tracks the private messages and posts of its users, censoring out content at its discretion (and without explanation or recourse).

Many LGBT users of the site who have written posts asking about being targeted for "real names" or alleged content infractions have reported having these messages and posts deleted. In the case of a public post takedown where a drag queen was inquiring if her friends were having the same issues, she immediately got an automated message saying post violated "safety" rules on the site. Censorship is now automated, for the safety of corporate interests.

When governments censor

Governments, Internet service providers, Wi-Fi apps, airline Wi-Fi, and public networks all censor web content from users. Most people don't know it's happening. It can starve legitimate businesses from traffic and revenue, and keep people from learning about democracy or life outside their country. It can prevent the public from finding out about state-sanctioned violence, and oppress ideas by "disappearing" art, film, writing, or people. It can make online work impossible in airplanes or at cafes, or prevent someone from finding a resource they desperately need.

A government might force providers to keep websites and news topics from its citizens—or a government might force an Internet blackout on its citizens during times of protest. So-called
"family friendly" filters used by public Wi-Fi providers and companies like Open DNS seek to prevent access to pornography, gambling, and hate speech. But they always get it wrong, and their automation invariably prevents people from accessing things like breast cancer sites, LGBT news, and violence prevention resources.

When we talk about Internet censorship, most people think of what's called the "Great Firewall of China." This refers to laws and technologies implemented by the Chinese government to closely monitor the activity of Internet users within the country, and block access to information and websites the government doesn't like. If you're curious, the site greatfirewallofchina.org can tell you if a website is blocked or not.

For instance, people in China searching for Amnesty International won't be able to find or access anything about the organization. The New York Times was blocked in China until 2001; an article the Chinese government didn't like got the Times re-blocked in 2012. In March 2017 the Times wrote, "Our Android app was never accepted in Chinese Android stores and recently Apple removed our iOS app from their Chinese app store, most certainly because of Chinese government pressure." The paper's censorship in China is aided by Apple and Android stores, who bend to the will of the government.

In 2011, all traffic from the country of Syria to the rest of the Internet simply stopped. The Syrian Minister of Information told press that the government did not "turn off" the Internet, but the U.S. State Department believed otherwise. Syria shut down its Internet just in time for the largest anti-government protest of the country's uprising. While the Internet was off, terrible things happened. During the blackout, Syrian authorities opened fire into crowds of protesters, killing over 72 people, while government forces assaulted towns seen as key to the demonstrations, killing even more. It wasn't the only time.

Other Internet censorship feels softer, but it's no less insidious. In the UK, government-driven filters are implemented at the ISP level. Internet customers in the UK have their Internet access filtered "by default," meaning that users have to "opt out" if they want an unfiltered Internet experience. The filtering program began in 2013, after the government basically strong-armed ISP's into complying under the guise of protecting children from online pornography—a frequent line from censors.

The UK's filtering program has been so uneven and defiantly un-transparent that it has censored a wide range of websites. The "Great British Firewall's" website overblocking has included sex education, suicide prevention, drug advice, child protection services, rape and domestic violence services, and more. The Open Rights Group became so frustrated and appalled, they created blocked.org.uk so people can find out whether or not their site is being blocked.

Filters, shutdowns, and company collusion with governments all happen behind closed doors. Their targets, reasoning, and lists are never disclosed, and any excuses given to press can seldom be trusted. Amnesty International, the ACLU, and Human Rights Watch all monitor Internet censorship and have calls to action worth keeping an eye on. The Open Net Initiative
has complete documentation and an index on global Internet filtering, as well as interactive maps.

Circumvention tools
While you'd need advanced technical help in a country where the Internet has been shut off, getting around blocks and filters in most locations can be done with a few simple circumvention tools. The primary ways to get around filters and Internet censorship are with the same things most recommended to protect against hacking and surveillance: Tor ("The Onion Router") and VPNs (Virtual Private Networks).

Avoid censorship:

- Turn off "quality filters" on social media accounts
- Turn off "safe search"
- Use a VPN, Tor or Tails (blocks and blacklists)

There are a few ways to bypass the technical aspects of Internet censorship, namely web blocks and filtering. In general, techniques include cached (copied and saved) web pages, website mirrors and archives (duplicates of websites on different URLs), alternate DNS servers, SSH tunneling, proxy websites, virtual private networks (VPNs), and other circumvention software tools like Tor or the Tails operating system.

RSS aggregators like Feedly can let you receive RSS feeds that might be on sites that are blocked directly. Half of those techniques require having access to the unfiltered Internet in the first place. For most people, a VPN is the answer.

Why is everyone saying I should use Tor?
Countries that tightly censor their Internet also surveil it, and monitor traffic for threats to their censorship. This can include looking for unusual activity, and the installation of popular circumvention tools like Tor ("The Onion Router"). This is unfortunate, because helping at-risk people circumvent filters and surveillance is exactly what Tor was made for. Read more about installing and using Tor to fight spying (and what Tor does and doesn’t do for you) in Chapter 5, "Defy Surveillance."

Tor is an oft-recommended tool for dissidents and whistleblowers that want to avoid censorship or being tracked online. The Tor Project is the nonprofit organization behind the software. Its culture is one of anti-surveillance activists with strong beliefs and the rabid fans (and detractors) that come with it. Its proponents like to recommend it as an all-purpose anti-surveillance, anti-censorship remedy.

This is pretty problematic. The software has its limitations and has gone for significant amounts of time in the past with security holes in it—ones that have been exploited by the U.S.
government. While it is true that Tor can be used with the legitimate goal of anonymity on the Internet, it is also used for accessing sites on the ‘darknet’ or ‘dark web’ the underground network of .onion websites that aren’t exposed to the wider Internet. So, naturally, Tor is of enormous interest to law enforcement, and government hackers spend a lot of effort figuring out ways to break it.

Tor is also a well-known circumvention tool that can make you look suspicious if authorities are watching for such activity. So if you're in a heated situation and suddenly start using Tor (or any form of encrypted communications), you will draw the unwanted attention of the authorities, which is of particular concern to activists. You are using a new technology, and this will make you stand out, which can raise flags and potentially see you subjected to closer surveillance. Some places ban the use of Tor on their network or Wi-Fi. Setting up a Tor node inside a network runs a risk of an organization’s IP being added to an Internet blacklist, notably if the node is involved in suspicious activities.

Tor is great for some things. Generally, it is excellent for covering your tracks. Tor routes your Internet traffic through what’s called an overlay network, which makes it difficult for nosy people to follow the path your data takes and trace it back to you. Along the way multiple layers of encryption are used to hide your true IP address, thus the onion metaphor. Another option is the Tails operating system, which you should read more about in Chapter 5, "Defy Surveillance."

Unfortunately, Tor is not always great for getting around blocks and filters, because you may not be able to access some websites. Most services that protect websites from DDoS will stop Tor users from accessing the site. (A Distributed Denial of Service is an attack that overloads a site with traffic, and Tor is often used in the attack.) In addition, Tor's default security settings will break some websites or make them unusable altogether by blocking scripts and other features. Unless you really know what you're doing, changing these settings can affect your privacy.

A VPN is a better choice for many people in most situations. There's no need to resort to Tor to bypass web filtering unless there's a real risk of being dragged away in the middle of the night due to your web browsing habits.

**Everyone should have a VPN**

Connecting to a VPN (Virtual Private Network) server that's outside your own country will also let you bypass censorship. These services and apps make it incredibly easy with their simple interfaces. Plus, a VPN is a lot less conspicuous. You're more likely to blend in by using a VPN because they're everywhere, marketed to regular people who want to be safe from hacking. According to GlobalWebIndex, over 400 million people use virtual private networks to circumvent censorship or for an increased level of privacy. You should always use one when you travel, regardless any censorship concerns, for your own safety.

Where Tor bounces your traffic through a bunch of servers to make your IP random, with a VPN you pick a server in the country you want your traffic to look like it's coming from. Most VPN
services have around a dozen countries you can choose from at any time, and all the reputable ones have mobile and tablet versions, too.

It's important to choose a safe a reputable VPN. Flip over to Chapter 5, "Defy Surveillance," to read in detail everything you need to know about selecting and using a VPN.

**Social network censorship**

No one censors its users better than Facebook. The social media monopoly takes down videos, photos, posts, accounts, pages, and even your private messages if it doesn't like them. It has removed one of the world's most important war photos, images of culturally essential (and classical) artwork, and videos of human rights abuses. It has allowed videos of child abuse, rapes, and murders stay online. Its censorship is harmful to society, and there is no doubt that it has helped erode our free speech and capacity for empathy—for this is what art and free speech does, along with keep us free as a society.

We can't trust the company's excuses or explanations, nor can we guess as to why this is. The company offers no proof or verification of its claims when evading accountability. We can only judge its actions in censorship, which aid conservatism and repressive regimes, and fly in the face of art and free expression as values intrinsic to human rights.

Keep this in mind when you upload and share anything to Facebook. It doesn't care about following its own rules, for it makes exceptions for celebrities, politicians, and governments all the time. It doesn't care about you, or the social importance of your media—unless the press makes a stink about it. Luckily for Facebook, few people have access to this kind of leverage. Facebook is a tool for distribution but it cannot be trusted with anything important. It's the lowest bar, and it gives you an example of what to expect when you're dealing with the worst practices in fairness and censorship.

Like Facebook, Twitter facilitates censorship by those who maliciously use reporting tools. This has been an issue since the Internet's beginning: The "report abuse" function has been used on almost every social media site to silence and censor other users. It's a problem you'd think would be solved by now, but in my opinion it's an issue that won't be until we get more decision makers behind the scenes who from groups likely to be silenced by such censorship. As in, not the people who are currently making and running our social networks.

Companies are beyond terrible at protecting their users from this; it is literally not a real concern for them. That's because the people at these companies can't imagine it happening to them. And for us, it feels incredibly personal.

Google censors too, and so does Instagram (they're as bad as their parent company, Facebook). YouTube has similar issues with abuse of their reporting systems, and they only recently stopped censoring LGBT videos as "adult content."

**Fight censorship:**
- Make copies of everything
- Document attackers
- Document your censorship ordeal (screencaps)
- Know the site's redress policy
- Find others with the same experience
- Find others not being censored
- Share everything with followers and press

Unfortunately for us, this censorship is both part of the problem and a fact of life. When you speak up about injustice, people will try to report you for anything they can. You will be censored, and unfairly. To expect it is to be prepared. Always make backup copies of everything, and screencap anything you think might get taken down.

When this happens to you, make noise. Lots of it.

**How to use SecureDrop**

There may come a time when you want to share or send something to a journalist or news outlet securely and anonymously. Or, you may face censorship so egregious that you are compelled to share your message or information with the press. These are high-risk situations. That's when you'll see if the media outlet you'd like to share it with has SecureDrop on their website.

SecureDrop is an open-source software platform created to facilitate secure communication between journalists and their sources (or whistleblowers). It was originally conceived and built under the name DeadDrop by hackers Aaron Swartz and Kevin Poulsen.


Using it is done in steps. SecureDrop uses Tor, and each media outlet's SecureDrop website is only accessible on the Tor network.

Download and install the Tor browser. Take your security a step further and install the Tails operating system to use while you engage with SecureDrop. Tails has a great setup assistant on its website that walks you through the installation process (tails.boum.org/install/index.en.html). Tor and the Tails operating system have their limits, so be sure read up about them Chapter 5. Make sure you're accessing the Internet safely; don't use your home or work network. *The Guardian* recommends:

"You should avoid using the platform on small networks where Tor usage may be monitored or restricted, or in public places where your screen may be viewed by CCTV. We recommend that you don't jump straight from this landing page to the SecureDrop site when uploading, especially on business networks that may be monitored. Best practice
would be to make a note of the Tor url and upload your content from a different machine at a later time."

Then copy and paste the unique Tor address provided by your media outlet of choice into the address bar. When the page loads, you will find specific instructions on how to submit files and messages to the outlet.

After this, you'll be assigned a random "code name." If a reporter or editor from the press outlet wants to contact you, they'll do so in the SecureDrop platform. Those messages are the only way they'll contact you, so don't lose or forget your code name.

Getting our messages out and having access to information is becoming critical for our survival. The fight against censorship in all its forms may feel like an uphill battle, but the more of us who know how to fight it, the better we can beat it back into the Dark Ages where it belongs.
## Hacker's Manifesto

### Current issue: #7

- **Release date:** 1986-09-25
- **Editor:** Taran King

<table>
<thead>
<tr>
<th>Title</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacker's Manifesto</td>
<td>The Mentor</td>
</tr>
<tr>
<td>Phrack Pro-Phile of Scan Man</td>
<td>Taran King</td>
</tr>
<tr>
<td>Hacker's Manifesto</td>
<td>The Mentor</td>
</tr>
<tr>
<td>Hacking Chilton's Credimatic</td>
<td>Ryche</td>
</tr>
<tr>
<td>Hacking RSTS Part 1</td>
<td>The Seker</td>
</tr>
<tr>
<td>How to Make TNT</td>
<td>The Radical Rocker</td>
</tr>
<tr>
<td>Trojan Horses in Unix</td>
<td>Shooting Shark</td>
</tr>
<tr>
<td>Phrack World News VI Part 1</td>
<td>Knight Lightning</td>
</tr>
<tr>
<td>Phrack World News VI Part 2</td>
<td>Knight Lightning</td>
</tr>
<tr>
<td>Phrack World News VI Part 3</td>
<td>Knight Lightning</td>
</tr>
</tbody>
</table>

**Get tar.gz**

---

**Volume One, Issue 7, Phile 3 of 10**
The following was written shortly after my arrest...

\\The Conscience of a Hacker/\\

by

+++The Mentor+++  

Written on January 8, 1986

Another one got caught today, it's all over the papers.  "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...

Damn kids.  They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker?  Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a hacker, enter my world...

Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...

Damn underachiever.  They're all alike.

I'm in junior high or high school.  I've listened to teachers explain for the fifteenth time how to reduce a fraction.  I understand it.  "No, Ms. Smith, I didn't show my work.  I did it in my head..."

Damn kid.  Probably copied it.  They're all alike.

I made a discovery today.  I found a computer.  Wait a second, this is cool.  It does what I want it to.  If it makes a mistake, it's because I screwed it up.  Not because it doesn't like me...

Or feels threatened by me...

Or thinks I'm a smart ass...

Or doesn't like teaching and shouldn't be here...

Damn kid.  All he does is play games.  They're all alike.

And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found.

"This is it... this is where I belong..."

I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...

Damn kid.  Tying up the phone line again.  They're all alike...

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless.  We've been dominated by sadists, or ignored by the apathetic.  The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud.  We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals.  We explore... and you call us criminals.  We seek after knowledge... and you call us criminals.  We exist without skin color, without nationality, without religious bias... and you call us criminals.  You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal.  My crime is that of curiosity.  My crime is that of judging people by what they say and think, not what they look like.  My crime is that of outsmarting you, something that you will never forgive me
for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

+++The Mentor+++