

LIS 510

Digital Privacy, Safety, and Security

Information School
University of Wisconsin-Madison
Spring 2019

Instructor: Dorothea Salo (please call me “Dorothea”)
Office hours: M T 8-9 am or by appointment
Special course attributes: Digital Studies P

salo@wisc.edu, 4261 Helen C. White Hall
Course URL: <https://canvas.wisc.edu/courses/142682>
Course modality: Face-to-face

Introduction

Course description

Students completing this course will earn three credit hours. One credit is the learning that takes place in at least 45 hours of learning activities, which include time in lectures or class meetings, in person or online, labs, exams, presentations, tutorials, reading, writing, studying, preparation for any of these activities, and any other learning activities.

This course has no prerequisites or co-requisites. No prior technology or computer-science experience is assumed.

This course introduces you to personal, social, organizational, and basic technical concepts and skills related to the digital privacy, safety, and security of individuals and organizations. It also helps individuals and organizations enhance their online privacy, safety, and security. Phenomena to be examined include:

- individual and societal need for digital privacy, safety, and security
- user behavior with regard to digital privacy, safety and security; usability of security measures, and impact of (lack of) usability on security; incentives (and lack thereof) for good security practices
- Internet of Things security; workplace bring-your-own-device security
- social engineering attacks; insider attacks; contractor attacks; supply-chain attacks
- person-on-person attacks: doxing, cyberbullying, etc.
- risk assessment and mitigation; threat assessment; attack surfaces
- authentication, authorization, access control, identity, and attacks against them
- security technologies and practices: log analysis, network and storage monitoring, digital forensics
- vulnerabilities, vulnerability disclosure; ethical hacking

Assignments in this course offer repeated practice in *communicating* about privacy, safety, and security. Why? Because communication skills (such as incident reporting, composing training materials, communicating with people in power, and technical communication aimed at layfolk) are commonly noted as *absolutely required* in job contexts involving online security—as well as commonly noted as lacking in too many digital-security professionals.

Course Policies

I aim to make this course as accessible as possible to all students. Students seeking accommodations for lecture or assignments must obtain a McBurney Center VISA. For more information, see <https://mcburney.wisc.edu/apply-for-accommodations/>.

Preferred name/pronouns: It is sometimes the case that a student’s legal name or gender assigned at birth are reported to me on official documents in a form not in keeping with that student’s preferred name or gender expression. Please let me know, as you are comfortable, about your preferences. My pronouns are she/her/hers. UW-Madison also permits students to indicate a preferred name: https://registrar.wisc.edu/preferred_name.htm

Contacting me

READ THE SYLLABUS before asking a question, please; the syllabus may answer it! For any difficulty with the course that is not private or confidential, please speak up in class; *I will not answer such questions by email*. Please also do your best to assist your classmates.

Should you see dead links (it does happen, usually with no notice), weird due dates, or other syllabus problems, please bring them up in class.

Textbooks and software

REQUIRED: Schneier, Bruce. *Secrets and Lies*. Wiley, 2000 (updated edition 2015).

REQUIRED: “The Equifax Data Breach.” House Oversight Committee, 2018. Available from <https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf> (see me if the government shutdown is still breaking this link). You will want to highlight/annotate this! Print it if you prefer to annotate a physical copy.

The library has print and electronic copies of *Secrets and Lies*, but I encourage you to purchase your own; though its examples are admittedly dated, its explanations are classic. Either the original edition or the 2015 15th-anniversary edition is fine; we will generally be reading whole chapters, not page-specific segments.

We will be using various pieces of command-line software in the course. I will make detailed installation and use instructions available for anything we do not actually handle in class. Note: If you are using any Windows version older than Windows 10 on your own computer(s), *please let me know immediately!*

Assignments

Grading scale

All final grades will be based on this scale:

A: 93.5-100, AB: 89.5-93.4, B: 83.5-89.4, BC: 79.5-83.4, C: 73.5-79.4, D: 64-73.4, F: anything below 64.

Due dates below are specified by module. For most assignments, this means “at class time,” but Week 14 assignments are due the final day of term.

	Final-grade %	Due date
Book review(s)	15%	Week 7; Week 14 for graduates' second review
Lab activities	20%	(various; see below)
Explain a vulnerability	15%	(various; see below)
Incident report		
Individual components	16%	Weeks 4 through 11
Peer review	9%	(one week after each individual-component due date)
Final report	15%	Week 14
Final presentation	10%	Week 14

Late assignment policy

Late assignments will be penalized one final-grade percentage point per day or fraction thereof late. I will allow revision and resubmission at my sole discretion and on my schedule only; any student resistance will remove the opportunity.

Book review(s)

Read and review a book! A good book review is no more (ideally much less) than 1000 words long (I am giving you a breather here; many review venues insist on half that or less, and *shorter does not mean easier to write*) and engagingly written. It often includes (but need not be limited to!) a BRIEF summary of the book's argument(s), a summary of the book's strengths and weaknesses, and a recommendation (or not) for reading or purchase along with a statement of appropriate audiences for the book.

For more reviewing advice, I strongly suggest perusing the “First-Time Reviewer” suggestions at the *LSE Review* website: <http://blogs.lse.ac.uk/lsereviewofbooks/guidelines-and-examples/> I would specifically like you to evaluate *how well the book communicates* its content: for whom is it written? is it clear to that audience? understandable to them? persuasive? dismissive or otherwise offputting? scaremongering? How might it improve its approach?

Post your review to the Canvas book-review forum by the due date.

UNDERGRADUATES: One book review, written as for a newspaper, magazine, or online reviewing outlet. You may, if you wish, specify the targeted publication (I strongly suggest Cybersecurity Canon for any book they have not already reviewed; instructions at <https://cybercanon.paloaltonetworks.com/nominate-a-book/>).

GRADUATES: Two book reviews, each book from a different category in the categorized list below, written as for a scholarly or professional journal. You may, if you wish, specify the targeted publication, and I encourage you to contact journals that carry relevant reviews to volunteer to review one of the more recent publications on the list.

BOOK LIST:

Individual privacy online

- Julia Angwin, *Dragnet Nation*
- Bruce Schneier, *Beyond Fear*
- Violet Blue, *Smart Girl's Guide to Privacy*
- Marvin Waschke, *Personal Cybersecurity*
- Jacqueline Ryan Vickery, *Worried about the Wrong Things*
- Kevin Mitnick, *The Art of Invisibility*

Society, privacy, and security

- Cathy O'Neil, *Weapons of Math Destruction*
- Bruce Schneier, *Data and Goliath* or *Click Here to Kill Everyone* or *Liars and Outliers*
- Susan Athey, *The Digital Privacy Paradox*
- Shoshana Zuboff, *Surveillance Capitalism*

Digital security how-tos

Word to the wise: The technical content of books in this category varies widely. I recommend skimming a book before you choose it to review.

- Shancang Li, *Securing the Internet of Things*
- Anne Kohnke, *Implementing Cybersecurity*
- Jeremy Wittkop, *Building a Comprehensive IT Security Program*
- Brian Kernighan, *Understanding the Digital World*
- John Bandler, *Cybersecurity for the Home and Office*

Many books on the list are available electronically: on the open web, via UW-Madison library subscription, or for relatively-inexpensive purchase. Several others are on print reserve in the iSchool Library. You should be able to find some in local public libraries. Please use discretion in checking out books! If you would like to review a relevant book I haven't listed (one good source is Cybersecurity Canon at <https://cybercanon.paloaltonetworks.com/>), tell me about it by the end of the second week of class, so that I can decide whether to allow it. (Usually I say yes, but one constraint: I do not want you reviewing tool-specific books, e.g. *Metasploit Unleashed*. It's a terrific book and I recommend it highly—but I want you to review books that take a broader view of privacy and/or security.)

Post your review to the Book Reviews forum on Canvas by the day it is due. The forum is open all semester long; you are welcome and encouraged to post reviews early. **Do NOT attach your review as a Word file or PDF**, please; *this will mean an automatic zero!* You are not required to read all posted reviews, but I do recommend that you read reviews for as many of the different books/collections as possible.

Grading criteria: Writing suitable for the specified outlet (use the Writing Center if you need it!), appropriate structure, depth of analysis and critique of the book's arguments, savvy reading/purchase recommendations.

Lab activities

Several modules come with graded lab activities attached; we will go over how to do them in class. Typically you will turn in a screenshot or text file showing that you did the activity. Completion is worth the full point total!

- Module 1: Command-line software installation and testing (ungraded)
- Module 2: Hashing (3 points)
- Module 4: Basic password cracking (3 points)
- Module 8: Reconnaissance tools (3 points)
- Module 10: Sniffing network traffic with Wireshark (4 points)
- Module 12: Recovering "deleted" files (3 points)
- Module 13: NIST Greg Schardt/"Mr. Evil" forensic investigation (4 points)

Explain a vulnerability or attack

Clearly and engagingly explain a vulnerability or attack type to your classmates (who enter the course, please remember, with widely varying levels of technology knowledge) in your choice of:

- an infographic
- a short (five minutes maximum!) in-class presentation
- a short (five minutes maximum!) well-produced podcast
- a short (three minutes maximum!) well-produced video or screencast
- a blog-post-length written explanation, with images/diagrams if you wish

You may choose the week your explanation is due; weeks 3 through 13 are available. In-class presentations will take place at class start, right after announcements. They are strongly recommended for aspiring academic librarians, aspiring book talkers or other public speakers, and aspiring supervisors/managers. Other forms of explanation are to be posted (as attachments or links, as necessary) to the designated Canvas discussion forum.

Glance at a few of Bruce Schneier's analogies/explanations in *Secrets & Lies*, or posts on Troy Hunt's blog (e.g. <https://www.troyhunt.com/fixing-data-breaches-part-2-data-ownership-minimisation/>), for excellent examples of written explanations.

Your explanation should ideally include:

- what kind(s) of digital devices, software, and/or infrastructure are subject to the vulnerability/attack
- what kind(s) of damage the vulnerability/attack can do, or allow bad actors to do
- a real-life example of the vulnerability/attack and/or its exploitation
- in broadly-understandable terms, how the vulnerability/attack works
- in broadly-understandable terms, how to defend against the vulnerability/attack

You may choose a vulnerability/attack type from any of the most current OWASP Top Ten lists (see <https://www.owasp.org/>), or from the list following (honor system, computer science and software engineering students especially: please choose one you do not already know a lot about):

- SQL injection (or other-language injection e.g. Javascript injection)
- Man-in-the-middle attack
- Buffer overflow
- Hardcoded/default password
- Unvalidated/unescaped user input
- Race condition
- Privilege escalation (see also "rootkit")
- Distributed denial-of-service attack
- Memory corruption
- Cross-site scripting attack
- Cross-site request forgery
- HTTP response splitting
- DNS rewriting
- Remote file inclusion
- Username enumeration attack
- Reidentification
- Format string attack

You may also choose one of the following specific vulnerabilities or attacks, explaining its nature, history, damage done, and significance:

- the ILOVEYOU virus
- Heartbleed and Shellshock
- Petya (you are allowed to be a little vague here; there are a LOT of named variants on this one!)
- Meltdown and Spectre
- LoJax
- the Conficker worm

If you would like to explain a different vulnerability/attack or vulnerability/attack type, please clear it with me first.

Incident report

Over the course of the class, you will build up an incident report explaining as clearly as possible what happened before, during, and after a major security, privacy, or safety failure (or series of failures). Your major deliverables will be an **incident report** (such as a security professional would write for an organization's leadership) and a short (no longer than five minutes) **pre-recorded presentation** explaining the most important material in the report (as though you were speaking to that leadership).

The House Oversight Committee report on Equifax is the most thorough, exhaustive, clear incident report I've ever seen—which means you cannot match it and should not try! (That said, its structure is worth consideration as a model for yours.) A more feasible (though probably too-short) example you can draw on is Brian Krebs's blog post on the National Bank of Blacksburg: <https://krebsonsecurity.com/2018/07/hackers-breached-virginia-bank-twice-in-eight-months-stole-2-4m/> Several templates for incident reports also exist that you can draw inspiration from, though most will be more detailed than you can manage, and not all they contain will be relevant. Consider:

- US Department of Justice guidance on incident reporting, section II, and consider evaluating your incident against the Preparedness Checklist at the end: <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf>
- the PCI Security Standards Council template for incident reporting at https://www.pcisecuritystandards.org/documents/Final_PFI_Report_v2.1.pdf
- Section 3 "Handling an Incident" (especially 3.4.1) of NIST's "Computer Security Incident Handling Guide" <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
- Lenny Zeltser's Report Template for Threat Intelligence and Incident Response <https://zeltser.com/cyber-threat-intel-and-ir-report-template/>

You must choose the subject of your incident report no later than the end of the second class module (so, in spring/fall, the end of week 2; in summer's eight-week session, the end of week 1).

UNDERGRADUATES: you may choose from the following list of specific incidents:

- US Office of Personnel Management employee-record breach ("OPM breach")
- Target customer data breach
- Home Depot point-of-sale credit-card breach
- Edward Snowden NSA breach
- Yahoo! personal and financial information breach
- Sony Pictures email and server breach
- Anthem health insurance breach
- Breaches in India's Aadhaar government-services system (there have been several)

GRADUATES, please choose from the following list of *classes* of incident. Please research *at least two* real-world case studies (more is fine!) and compare and contrast the quality of prevention efforts and incident response:

- Internet of Things toy data breaches
- Internet of Things personal-assistant breaches (Alexa, Siri, Echo, etc)
- Student data breaches at colleges/universities
- Student data breaches at K-12 schools (see <https://www.edtechstrategies.com/k-12-cyber-incident-map/> for help locating examples and coverage)
- Major ransomware attacks (choose an industry to focus on: I suggest health care, transit, or government)

Because we will be analyzing the Equifax breach extensively in class, it is off-limits for this assignment.

If you wish to analyze a different incident or (for graduates) class of incident, please clear it with me first. (Word to the wise; bigger, more complex, and more difficult failures are better! I will refuse simple obvious failures.) Keep a running list in a shareable online fashion (e.g. Google doc, Pinboard list, public Zotero list are all fine) of every source you discover about your subject, whether or not you use it in your deliverables; **add a link to your list to each deliverable you turn in.**

Components of this report are assigned during the relevant class module, and are due at the end of that module:

- Module 5: Password practices.
- Module 6: Social-engineering attacks, including but not limited to spamming, phishing, contractor attacks, insider attacks.

- Module 7: Poor security practices by organizational IT and the organization as a whole, including but not limited to ineffective organizational structures, slow patching, poor security awareness (anywhere in the organization), poor security training, security-poor software-development practices, insufficient support or authority given to security team.
- Module 8: Physical security. Poor incident response.
- Module 9: Access-control system failures. Biometrics failures (including leaks).
- Module 10: Failures in securing devices used by individuals, including but not limited to loss, theft, shoulder-surfing, and BYOD failures.
- Module 11: Failures of network security, including but not limited to DDoS attacks and network-infiltration attacks.
- Module 12: Failures of web-server or other server security, including but not limited to DDoS attacks and cloud attacks.
- Module 13: Glue text (executive summary, timeline, etc.) and integration of previous components into the report

Reasonable component drafts *turned in on time* will receive automatic credit toward your final grade; I am requiring them so that they receive feedback and to avoid end-of-semester all-nighters. **Note:** I do expect that at least one and quite likely more of the component modules will be irrelevant to your chosen subject. That's fine! Your report, in that case, only needs to say that no issues of this specific type were noted.

All report components except the last will be *peer-reviewed*; reviews are due one week after the component has been turned in. Peers are to evaluate the writeup for:

- clarity
- appropriate brevity
- work-appropriate impassivity (blame-and-shame is inappropriate in an incident report), and
- completeness

as well as any component-specific criteria I explain. For any component that states “no failure of this specific type was noted,” peer reviewers must use the author’s public source list to check the assertion for truth! The goal is to improve everyone’s final incident report. (Word to the wise: going easy on someone does not improve their final report! Constructive critique is a vital school and work skill.)

You may, if you prefer, build up your report over the course of the semester by adding components to it. If you do this, please be kind to your peer reviewer—mark new components as you add them.

Reading schedule

Please come to class (except the first, for obvious reasons) prepared to discuss the readings assigned for that week/module. Having questions to ask about the readings absolutely counts as coming prepared!

Unit 1: Context and prerequisites

Module 1: Why digital privacy and safety? How does digital security contribute?

Learning objectives: Why individuals and organizations need digital privacy, safety, and security. Corrosive effects of widespread surveillance. Personal, social, financial, and reputational risks of poor security practices.

Schneier. *Secrets & Lies* chapter 5 “Security needs.”

Equifax report, section 1, pp. 13-19. (Skim this for how and why the information Equifax has on people causes problems when breached.)

Matwyshyn. “CYBER!” <https://digitalcommons.law.byu.edu/lawreview/vol2017/iss5/6/> (Section B.1, “Ermahgerd, cybers: Privacy conflation” pp. 1135-1145.)

“Lurkers, creepers, and virtuous interactivity.” <https://firstmonday.org/article/view/6948/5628> (Skip section 2.)

Berinato and Nissenbaum. “Stop thinking about consent: it isn’t possible and it isn’t right.” <https://web.archive.org/web/20181002060539/https://hbr.org/2018/09/stop-thinking-about-consent-it-isnt-possible-and-it-isnt-right>

Stark. “The emotional context of information privacy.” <https://doi.org/10.1080/01972243.2015.1107167>

Madden. “Privacy, security, and digital inequality.” <https://datasociety.net/pubs/prv/>

[DataAndSociety_PrivacySecurityandDigitalInequality.pdf](#) (Summary of Findings, pp. 1-13)

Module 2: Cryptography and encryption

Learning objectives: Encryption algorithms. Hashing, salts/nonces, passwords, password stretching. Password attacks: brute-force, rainbow tables, dictionary attack. Public-key infrastructure: public and private keys, certificates, (root) authorities, certificate checking, certificate revocation. Digital signatures, digests. Non-repudiation. “Key escrow,” “backdoors,” and why they are a bad idea.

Linklist(s): <https://pinboard.in/u:dsalo/t:cryptography>

“Introduction to public-key cryptography.” [http://docs.oracle.com/cd/E19957-01/816-6154-10/ AND/OR “About Gatekeeper.”](http://docs.oracle.com/cd/E19957-01/816-6154-10/AND/OR>AboutGatekeeper) <https://panic.com/blog/about-gatekeeper/> (friendlier, but also longer!)

“What do security certificates actually do?” <https://duck.co/blog/post/227/what-do-security-certificates-do>
Kumarak. “How Dropbox knows when you’re sharing copyrighted stuff.” <https://techcrunch.com/2014/03/30/how-dropbox-knows-when-youre-sharing-copyrighted-stuff-without-actually-looking-at-your-stuff/> (Read this for how hashing and checksumming work.)

Gallagher. “What the government should’ve learned about backdoors from the Clipper chip.” <https://arstechnica.com/information-technology/2015/12/what-the-government-shouldve-learned-about-backdoors-from-the-clipper-chip/>

Ducklin. “Serious security: how to store your users’ passwords safely.” <https://nakedsecurity.sophos.com/2013/11/20/serious-security-how-to-store-your-users-passwords-safely/> (Make sure you understand the ATTACKS as well as the techniques that guard against them.)

Gibbs. “Passwords and hacking: the jargon of hashing, salting, and SHA-2 explained.” <https://www.theguardian.com/technology/2016/dec/15/passwords-hacking-hashing-salting-sha-2>

“EFF introduces actual encryption experts to US Senate staff.” <https://www.eff.org/deeplinks/2018/05/bring-nerds-eff-introduces-actual-encryption-experts-us-senate-staff>

Module 3: Models, concepts, and jargon

Learning objectives: Theoretical models of cybersecurity. Risk assessment; threat assessment. Adversarial thinking. Definitions: vulnerability, exploit, “pwning,” malware (and types of malware), zero-day, ransomware, attack surface. Bug, patch. Defense in depth. Supply chain attack. “Visibility.”

Linklist(s): <https://pinboard.in/u:dsalo/t:riskmgmt>, <https://pinboard.in/u:dsalo/t:vulnerabilities>

Equifax report, section III, pp. 27-34. (Don’t get bogged down in the techie details unless you want to—you don’t have to know or care what Apache Struts is! Instead, pay attention to why Equifax had such a hard time patching a known vulnerability.)

Schneier. *Secrets & Lies* chapter 2 “Digital threats,” chapter 4 “Adversaries,” chapter 19 “Threat modeling and risk assessment.”

Gallagher. “How I learned to stop worrying and love my threat model.” <https://arstechnica.com/information-technology/2017/07/how-i-learned-to-stop-worrying-mostly-and-love-my-threat-model/>

Brodkin. “Viruses, Trojans, and worms, oh my: the basics on malware.” <https://arstechnica.com/information-technology/2013/02/viruses-trojans-and-worms-oh-my-the-basics-on-malware/>

Gault. “The CIA secret to cybersecurity that no one seems to get.” <https://www.wired.com/2015/12/the-cia-secret-to-cybersecurity-that-no-one-seems-to-get/>

Packel. “Encryption: the battle between privacy and counterterrorism.” <https://www.dataprivacymonitor.com/cybersecurity/encryption-the-battle-between-privacy-and-counterterrorism/>

Newman. “What is steganography?” <https://www.wired.com/story/steganography-hacker-lexicon>

Fruhlinger. “What is ransomware? How it works and how to remove it.” <https://www.csoonline.com/article/3236183/ransomware/what-is-ransomware-how-it-works-and-how-to-remove-it.html>

FOR REFERENCE ONLY (for pity’s sake don’t try to read the whole thing!) NICCS Explore Terms: <https://niccs.us-cert.gov/glossary>

Module 4: Surveillance capitalism. Government surveillance. Learning analytics. Big data and its dangers.

Learning objectives: Surveillance capitalism (adtech, social media, personalization, recommender engines, data brokers). Government surveillance (local through federal; camera proliferation, vulnerability hoarding, stingrays). Learning analytics. Responses to surveillance (personal, societal).

Linklist(s): <https://pinboard.in/u:dsalo/t:surveillance/t:marketing>

Kaltheuner. “I asked an online tracking company for all of my data.” <https://privacyinternational.org/feature/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found>

Fitzpatrick. “In America’s panopticon.” <https://www.thenation.com/article/in-americas-panopticon/>

Chuen. “Watched and not seen.” <http://gutsmagazine.ca/watched-and-not-seen/>

Tisne. “It’s time for a bill of data rights.” <https://www.technologyreview.com/s/612588/its-time-for-a-bill-of-data-rights/>

“Cybersecurity Information Sharing Act—frequently asked questions.” https://www.us-cert.gov/sites/default/files/ais_files/CISA_FAQs.pdf

O’Carroll. “How ads hijacked the dream of the Internet.” <https://www.csmonitor.com/Technology/2018/1206/How-ads-hijacked-the-dream-of-the-internet.-Can-digital-citizens-fight-back>

Kaplan. “Spy and conquer.” <https://slate.com/technology/2018/12/roger-ailles-divide-and-conquer-workplace-surveillance-technology.html>

Frischmann. “How personalization leads to homogeneity.” <https://blogs.scientificamerican.com/observations/how-personalization-leads-to-homogeneity/>

Regan and Jesse. “Ethical challenges of edtech, big data and personalized learning.” <https://doi.org/10.1007/s10676-018-9492-2>

Unit 2: You ARE the weakest link, goodbye!

Module 5: Humans are bad at security and privacy.

Learning objectives: Security vs. usability. Security and risk awareness. Password practices. Security by obscurity. “Dark patterns,” exploiting human cognitive habits. Security and privacy balanced against other priorities.

Linklist(s): <https://pinboard.in/u:dsalo/t:socialengineering>, <https://pinboard.in/u:dsalo/t:passwords>

Check a few of your favorite passwords in Troy Hunt’s <https://haveibeenpwned.com/Passwords>. IMMEDIATELY CHANGE ANY THAT HAVE BEEN PWNEED. Also check your email addresses in <https://haveibeenpwned.com/> and change passwords on any accounts that come up that you didn’t already know about and change the password for.

Schneier. *Secrets & Lies* chapter 17, “The human factor.”

Krebs. “¡Ayuda! (Help!) Equifax has my data!” <https://krebsonsecurity.com/2017/09/ayuda-help-equifax-has-my-data/> (I assume this was out-of-scope for the US-based House report—it’s not there!—but here you go.)

Take the quiz at <http://www.pewinternet.org/quiz/cybersecurity-knowledge/> and then read Olmstead and Smith “What Americans know about cybersecurity.” <http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/>

Play “The Password Game” at <https://www.surveygizmo.com/s3/2758757/The-Password-Game-Carnegie-Mellon-University-website>

“Unmasked: what 10 million passwords reveal about the people who choose them.” <https://wpengine.com/unmasked/>

Francis. “Vendors approve of NIST password draft.” <https://www.csoonline.com/article/3195181/data-protection/vendors-approve-of-nist-password-draft.html>

Abu-Salma et al. “Obstacles to the adoption of secure communication tools.” <https://www.ieee-security.org/TC/SP2017/papers/84.pdf>

McGregor et al. “Investigating the computer security practices and needs of journalists.” <https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-mcgregor.pdf>

Nield. “Dark patterns: the ways websites trick us into giving up our privacy.” <https://fieldguide.gizmodo.com/dark-patterns-how-websites-are-tricking-you-into-givin-1794734134>

Module 6: Humans exploit and abuse other humans’ badness at security and privacy to harm them.

Learning objectives: Insider threat. Contractor threat. Phishing attacks; spearphishing; catfishing; smishing. Social engineering. Cyberbullying, doxing, SWATting. Revenge porn. Cryptomining attacks. Ransomware. Dark [design] patterns.

Linklist(s): <https://pinboard.in/u:dsalo/t:insiderthreat>, <https://pinboard.in/u:dsalo/t:phishing>

Rosenthal. “Living with insecurity.” <http://blog.dshr.org/2017/10/living-with-insecurity.html>

Dancstep. “We got phished.” <https://www.exploratorium.edu/blogs/tangents/we-got-phished-2>

Pompon. “Phishing for your information: how phishers bait their hooks.” <https://www.darkreading.com/partner-perspectives/f5/phishing-for-your-information-how-phishers-bait-their-hooks-/a/d-id/1329753>

Weise. “A hacker’s best friend is a nice employee.” <https://www.usatoday.com/story/tech/news/2016/08/15/hacker-social-engineering-defcon-black-hat/88621412/>

Williams. “Actress Felicia Day opens up about GamerGate fears, has her private details exposed minutes later.” <https://thinkprogress.org/actress-felicia-day-opens-up-about-gamergate-fears-has-her-private-details-exposed-minutes-later-c8598dad9835/>

Fagone. “The serial SWATter.” <https://www.nytimes.com/2015/11/29/magazine/the-serial-swatter.html>

Schneier. “The doxing trend.” https://www.schneier.com/blog/archives/2015/10/the_doxing_tren.html

Schneier. "The meanest email you ever wrote, searchable on the internet." <https://www.theatlantic.com/technology/archive/2015/09/organizational-doxing-ashley-madison-hack/403900/>

Module 7: Privacy, security, and safety out of sight, out of mind... until a crisis

Learning objectives: Security practices within businesses; reporting lines. "Shadow IT," BYOD. Relationships between IT and information-security professionals. Security practices in software development. Why security is often ignored until a crisis happens. "The market" and security incentives. Vulnerability disclosure practices, vulnerability hoarding, CVEs, CISA, bug-bounty programs.

Linklist(s): <https://pinboard.in/u:dsalo/t:vulnerabilities>, <https://pinboard.in/u:dsalo/t:cybersecurity/t:orgbehavior>

Equifax report, section IV.C pp. 49-50 and section V, pp. 55-75.

Anderson and Moore. "The economics of information security." <http://science.sciencemag.org/content/314/5799/610.full>

Magee. "Who owns cybersecurity risk management?" <https://blog.gigamon.com/2017/05/26/owns-cybersecurity-risk-management/>

Baxter. "The risk of shadow IT to business continuity." <https://www.csoonline.com/article/3237226/business-continuity/the-risk-of-shadow-it-to-business-continuity.html>

Nather. "Four reasons why organizations can't 'just patch.'" <https://duo.com/blog/opinion-4-reasons-why-organizations-cant-just-patch>

Schneier. *Secrets & Lies* chapter 13 "Software reliability" and chapter 22 "Product testing and verification."

Krebs. "Supply-chain security is the whole enchilada..." <https://krebsonsecurity.com/2018/10/supply-chain-security-is-the-whole-enchilada-but-whos-willing-to-pay-for-it/>

Hunt. "The effectiveness of publicly shaming bad security." <https://www.troyhunt.com/the-effectiveness-of-publicly-shaming-bad-security/> (Contrast this with my repeated "no blame" exhortations. Which is useful or appropriate in which situations? We will discuss this question in class!)

"Common Vulnerabilities and Exposures: About." <http://cve.mitre.org/about/>

Varmazis. "Good guys and bad guys race against time over disclosing vulnerabilities." <https://nakedsecurity.sophos.com/2017/08/07/good-guys-and-bad-guys-race-against-time-over-disclosing-vulnerabilities/>

Module 8: Incident response

Learning objectives: How attacks typically proceed. Attribution, and why it is difficult. Good and bad incident-response practices. Incident reports ("post-mortems"). Planning for good incident response. Incident-response teams.

Linklist(s): <https://pinboard.in/u:dsalo/t:incidentresponse>

Equifax report, section IV, pp. 40-54.

Infosec Institute. "The seven steps of a cyber attack." <https://resources.infosecinstitute.com/the-seven-steps-of-a-successful-cyber-attack/>

"Best practices for victim response and reporting of cyber incidents." <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf>

Hunt. "Data breach disclosure 101: How to succeed after you've failed." <https://www.troyhunt.com/data-breach-disclosure-101-how-to-succeed-after-youve-failed/>

Ruefle. "Defining computer security incident response teams." <https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams>

Aucsmith. "The technology and policy of attribution." <https://cyberbelli.com/papers/attribution/>

Cooper. "The day after: your first response to a security breach." <https://technet.microsoft.com/en-us/library/2005.01.incidentresponse.aspx>

McLaughlin. "Post Mortem: Death Star data breach by ROGUE ONE." <https://www.threatstack.com/blog/post-mortem-death-star-data-breach-by-rogue-one/> (Humor, but also a solid, if brief, example of an incident report!)

Tilbury. "How not to build a digital archive: lessons from the dark side of the force." <https://preservica.com/blog/how-not-to-build-a-digital-archive-lessons-from-the-dark-side-of-the-force/> (Likewise.)

Unit 3: Privacy, security, and safety mechanics

Module 9: Access control

Learning objectives: Establishing identity. Authentication and authorization; two/multi-factor authentication. Access-control lists. Biometrics. "Least privilege." Privilege escalation attacks, rootkits. Logging and log analysis.

Linklist(s): <https://pinboard.in/u:dsalo/t:authentication>

Schneier. *Secrets & Lies* chapter 9 "Identification and authentication."

McKenzie. "Security lessons learned from the Diaspora launch." <http://www.kalzumeus.com/2010/09/22/security-lessons-learned-from-the-diaspora-launch/> (Read this until you understand *in your bones* the difference between authentication and authorization!)

Elliott. "Two-factor authentication: how and why to use it." <https://www.cnet.com/how-to/how-and-why-to-use-two-factor-authentication/>

"What is the difference between RBAC and DAC/ACL?" <https://security.stackexchange.com/questions/346/what-is-the-difference-between-rbac-and-dac-acl/348> (Read the top answer.)

Kolachalam. "The privacy battle over the world's largest biometric database." <https://www.theatlantic.com/technology/archive/2017/09/aadhaar-worlds-largest-biometric-database/538845/>

Morse. "Why the iPhone X's facial recognition could be a privacy disaster." <http://mashable.com/2017/08/28/trouble-facial-recognition-technology-smartphones/>

Module 10: Server and web-application security

Learning objectives: HTTPS and its implementations; SSL/TLS. Cloud security. DDOS attacks. Botnets. Typosquatting/homograph/IDN attacks. Common web application attacks; application security. More on logging/log analysis.

Linklist(s): <https://pinboard.in/u:dsalo/t:cybersecurity/t:webapps>

Apache. "SSL/TLS Strong Encryption: An Introduction." https://httpd.apache.org/docs/current/ssl/ssl_intro.html (Don't worry about the technical details.)

Wilson. "Our apathy toward privacy will destroy us. Designers can help." <https://www.fastcodesign.com/3067094/our-apaty-toward-privacy-will-destroy-us-designers-can-help>

Starr. "Fridge caught sending spam emails in botnet attack." <https://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/>

Arciszewski. "A gentle introduction to application security." <https://paragonie.com/blog/2015/08/gentle-introduction-application-security>

Bright. "Can a DDoS break the Internet?" <https://arstechnica.com/information-technology/2013/04/can-a-ddos-break-the-internet-sure-just-not-all-of-it/>

Ponemon. "Breaking bad: the risk of insecure file sharing." https://img.en25.com/Web/IntraLinks/%7B6988b757-8c9f-4d09-9dd6-da59f4083f1f%7D_Intralinks_Ponemon_Research_Report_Q4_2014%5B1%5D.pdf (Ignore the appendix.)

"Out of character: Homonym attacks explained." <https://blog.malwarebytes.com/101/2017/10/out-of-character-homograph-attacks-explained/>

Module 11: Individual device security and privacy

Learning objectives: Computer, tablet, and phone security. Internet of Things security. Ransomware. Side-channel attacks. Protection: anti-virus, endpoint protection, behavioral (anomaly) detection systems.

Schneier. *Secrets & Lies* chapter 14 "Secure hardware."

Enis. "Ransomware hackers target government offices, libraries." <http://lj.libraryjournal.com/2017/04/industry-news/ransomware-hackers-target-government-offices-libraries/>

the grugq. "Ransomware changed the rules." <https://medium.com/@thegrugq/ransomware-changed-the-rules-2f9346197663>

Williamson. "Going deeper on behavioral detection." <http://www.securityweek.com/going-deeper-behavioral-detection>

Griffey. "Personal international infosec." <http://jasongriffey.net/wp/2017/03/14/personal-international-infosec/>

Fairfield. "The 'internet of things' is sending us back to the Middle Ages." <https://theconversation.com/the-internet-of-things-is-sending-us-back-to-the-middle-ages-81435>

Feamster. "Who will secure the Internet of Things?" <https://freedom-to-tinker.com/2016/01/19/who-will-secure-the-internet-of-things/>

Cunningham. "Phone and laptop encryption guide." <https://arstechnica.com/gadgets/2015/08/phone-and-laptop-encryption-guide-protect-your-stuff-and-yourself/> (Do these things. Do them!)

Hornby. "Side-channel attacks." <http://www.cryptofails.com/post/70097430253/crypto-noobs-2-side-channel-attacks>

Module 12: Network security and privacy

Learning objectives: Switches, routers, network segmentation. DMZs. Firewall basics. Packet analysis basics. Intrusion-detection systems. DNS-poisoning attacks; DNSSEC. Distributed denial-of-service attacks. VPNs. Even more on logging/log analysis (including in real time): IDS/IPS systems, SIEM systems.

Schneier. *Secrets & Lies* chapter 11, "Network security."

Tyson. "How firewalls work." <http://computer.howstuffworks.com/firewall.htm> (Pages 1-5.)

"What is a packet?" <http://computer.howstuffworks.com/question525.htm>

"Data encapsulation and the TCP/IP protocol stack." <https://docs.oracle.com/cd/E19455-01/806-0916/ipov-32/>

Bradley. "Introduction to packet sniffing." <https://www.lifewire.com/introduction-to-packet-sniffing-2486803>

Timberg. "The long life of a quick fix." <http://www.washingtonpost.com/sf/business/2015/05/31/net-of-insecurity-part-2/>

Goodin. "DIY stalker boxes spy on Wi-Fi users cheaply and with maximum creep value." <https://arstechnica.com/information-technology/2013/08/diy-stalker-boxes-spy-on-wi-fi-users-cheaply-and-with-maximum-creep-value/>

Shinder. "SolutionBase: Strengthen network defenses by using a DMZ." <http://www.techrepublic.com/article/solutionbase-strengthen-network-defenses-by-using-a-dmz/>

Andrus. "Network security: three keys to effective network segmentation in a world of targeted cyber-attacks." <https://www.bradfordnetworks.com/network-security-three-keys-effective-network-segmentation-world-targeted-cyber-attacks/>

Crawford. "VPNs for beginners." <https://www.bestvpn.com/vpns-beginners-need-know/>

Module 13: Forensics

Learning objectives: Steps of an attack. Storage-device forensics; filesystems and forensics. Memory forensics. Remanence. Ethics, the Fourth Amendment, and forensics.

Linklist(s): <https://pinboard.in/u:dsalo/t:digitalforensics>

Equifax report, sections VI and VII, pp. 85-96 (also a good idea to reread section IV.E p. 54).

Strickland. "How computer forensics works." <http://computer.howstuffworks.com/computer-forensic.htm> (Pages 1-6.)

US Department of Justice. "Digital forensic analysis methodology." https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/03/26/forensics_chart.pdf

Wade. "Memory forensics: where to start." <https://www.forensicmag.com/article/2011/06/memory-forensics-where-start>

Sartin. "Network postmortem: forensic analysis after a compromise." <https://www.computerworld.com/article/2573728/security0/network-postmortem--forensic-analysis-after-a-compromise.html>

Wilson. "Legal issues with cloud forensics." <https://www.forensicmag.com/article/2015/05/legal-issues-cloud-forensics>

Module 14: Security auditing

Learning objectives: Vulnerability scans. Penetration testing; white/gray/black box testing. Physical penetration testing and security exploits. OSINT. Red teams/blue teams. Ethics of certain pentesting techniques deployed against local staff.

Linklist(s): <https://pinboard.in/u:dsalo/t:osint>, <https://pinboard.in/u:dsalo/t:pentesting>

"Information supplement: penetration testing guidance." https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf (Sections 1-4.)

"Open source intelligence." <https://www.thecybersecurityexpert.com/open-source-intelligence-what-is-it-and-how-can-you-use-it-to-defend-your-organisation/>

McLaughlin. "Using open-source intelligence software for cybersecurity intelligence." <http://www.computerweekly.com/tip/Using-open-source-intelligence-software-for-cybersecurity-intelligence>

Drinkwater and Zurkus. "Red team versus blue team." <https://www.csoonline.com/article/2122440/disaster-recovery/emergency-preparedness-red-team-versus-blue-team-how-to-run-an-effective-simulation.html>

Murdoch and Sasse. "Should you really phish your own employees?" <http://tech.newstatesman.com/guest-opinion/phishing-employees>

Hyde. "Smiling your way past the guard." <https://twitter.com/i/moments/886241619992862720> (Jargon alert: read about Bash Bunnies at <https://wiki.bashbunny.com/> and Rubber Duckies at <http://usbrubberducky.com/>)
 Daniel. "How I socially engineer my way into high security facilities." https://motherboard.vice.com/en_us/article/qv34zb/how-i-socially-engineer-myself-into-high-security-facilities

iSchool learning outcomes

iSchool learning outcomes	Course measurable outcomes
1a. Students apply key concepts with respect to the relationship between power, knowledge, and information.	In the Module 6 and Module 7 parts of the final Incident Report, students will analyze organizational security failures with an eye to how organizational power shapes organizational response.
3c. Students analyze information needs of diverse individuals and communities.	In the Module 6 part of the final Incident Report, students will analyze training and security awareness as contributors to security failures. The vulnerability/attack explanation is also designed to make students consider the existing knowledge among their classmates.
3d. Students understand and use appropriate information technologies.	All lab assignments test this outcome.
4a. Students evaluate, problem solve, and think critically, both individually and in teams.	All assignments in this course require critical thinking and problem solving.
4b. Students demonstrate good oral and written communication skills.	All non-lab assignments test this outcome.
4d. Students demonstrate innovation and skills necessary for leadership.	The Incident Report is designed to help students learn to "lead from below" by communicating clearly and persuasively to colleagues at all organizational levels.

Digital Studies Learning Outcomes

For Digital Studies students, this course fulfills the P requirement, and is designed to develop masteries related to the following program learning objectives:

Digital Studies Program Learning Objective	Course Material that Addresses LO
To understand key theories and concepts related to digital studies and the historical context surrounding the creation of digital technologies	Explain a vulnerability/attack, Book review(s)
To gain familiarity with methods, concepts and tools needed to research and evaluate information related to digital studies	Explain a vulnerability/attack, Incident report
To think critically about how digital technologies work and their impact on society	Book review(s), Incident report
To be able to create strategic communication content and self-expression using digital tools	All assignments
To understand the professional and ethical principles related to the field of digital studies	Book review(s), Incident report

