LIS 510
Information Security and Privacy

Information School
University of Wisconsin-Madison
Summer 2020

Instructor: Dorothea Salo (please call me "Dorothea") salo@wisc.edu
Office hours: by appointment Canvas: https://canvas.wisc.edu/courses/142682

Special course attributes: Intermediate, Graduate, Digital Studies P **Instructional mode: Online**

Course description

Students completing this course will earn three credit hours. This class carries the expectation that students will work on course learning activities (reading, writing, problem sets, studying, etc) for about 9 hours out of the classroom for each module.

This course requires sophomore standing, but has no specific prerequisites or co-requisites. No prior technology or computer-science experience is assumed.

Introduction to personal, social, organizational, and basic technical concepts and skills related to the digital privacy, safety, and security of individuals and organizations. Preparation to help individuals and organizations enhance their online privacy, safety, and security.

This course is designed to assess the following iSchool program-level learning outcomes: 1, 4, 5, 7.

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: doxxing, 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 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 and privacy professionals.

Course learning outcomes

1. Communicate clearly and effectively to non-expert audiences about security vulnerabilities and security-related incidents (both grad and undergrad).
2. Mitigate common risks to digital privacy, safety, and security (both grad and undergrad).
3. Use common command-line Linux tools related to digital security (both grad and undergrad).
4. Develop awareness of the structure of the information security and privacy fields, and career opportunities within them (both grad and undergrad).
5. Demonstrate competency with information technologies important to the information professions (graduate).
6. Demonstrate understanding of professional competencies important for management of information organizations (graduate).
7. Demonstrate understanding of societal, legal, policy or ethical information issues (graduate).

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.

These are not usual times, I'm acutely aware. I am absolutely willing to accommodate sudden unforeseen challenges. Please let me know what you need as soon as you can.

Course schedule

As with all 3-credit summer courses, this course is 14 weeks ("modules") of content compressed into 8. Please plan your work time accordingly! Each calendar week of the course will begin Monday at midnight and contain two modules of course content, *except* the week containing July 4 and the final week of the course, which will contain one module each.

Textbooks and software

REQUIRED: Schneier, Bruce. *Secrets and Lies*. Wiley, 2000 (updated edition 2015). Library ebook: `https://search.library.wisc.edu/catalog/9912219160102121` 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. 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 (mostly for my reference); exact due dates are listed on Canvas.

	Final-grade %	Due date
Lab activities	15%	(various; see below)
Tracking the zeitgeist	15%	(various; see below)
Campus privacy report	20%	Module 7
Book review(s)	15%	Module 7; Module 14 for graduates' second review
Explain a vulnerability	15%	Module 10
Incident report	20%	Final day of course

Campus privacy report

Assess the privacy and security of a specific type of data about UW-Madison students in a report and reflection. (Undergraduates: 3-5 pages. Graduates: 5-7 pages. I will discuss how my expectations differ below.) You may (and I encourage you to) **work collaboratively** on the research portion of this assignment! By all means share documents you find with everyone. Your writeup, however, must be individual, especially the final reflection.

For the data type you choose, do your best (n.b. I fully expect that some, likely most, possibly even all, of these answers will not exist or will not be available to you! say so, and think about those silences!) to find out:

- What data is collected? How? By whom? (Be open to surprises here.)
- How long is this data kept? Where is it kept, and who is responsible for its security and privacy?
- Can you, as the data originator, see the data that is collected and stored about you? If yes, what do you have to do to see the data about you?
- What types of *campus employees* (instructors, advisors, administrators, analysts, IT folks, etc) are permitted access to this data? Can they see data on individuals, or only aggregated data across the student body? Are there any hoops to jump through before access is permitted?
- Who *outside campus* is permitted access to this data? Under what circumstances? Individualized or aggregate?
- Can you request that this data not be collected and stored? How? What happens if you do?
- Was your consent sought to collect, keep, analyze, and (if relevant) share this data? When and how?
- Who has used this data recently? For what?

GRADUATES ONLY are also expected to research:

- What data-governance, privacy, and records-retention policies, if any, govern the collection, use, retention, access, and sharing of this data
- As appropriate: implications on data protection and privacy of an organizational merger, acquisition, or bankruptcy
- Incident-response plan in case of a data breach or other security incident
- Confidentiality requirements attaching to this data, individually and in aggregate, and how they are managed in practice

Finally, reflect on what you learned and your reactions to it. Do you believe these data are being handled in accordance with their potential and actual sensitivity? Do you have a threat model in mind that you didn't before? Do you believe that the data-handling policy and practice for this type of data is appropriately communicated to students? What about all this would you change, if you could? (N.b. no wrong answers here! Tell your truth. I just want to ensure you think about it.)

Suggested starting places for your research: terms of service and privacy policies for the data in question; organizational data-related policies; applicable law (usually state law, sometimes federal); the Unizin Data Platform data dictionary (`https://docs.udp.unizin.org/`). When possible, take a look at applicable websites for third-party data collection.

For some of these types of data, I have one or more contacts within the university who have given permission for students in this class to discuss the data with them; contact information will be available on Canvas. I don't want to overload these kind and generous people, so **answer as many questions as you can with documentation before you approach a contact**, and **pool your questions so that only one student approaches the contact**. You may discuss with the contact over email or via phone or video chat — defer to the contact's preferences whenever you can, please — but if you use phone/chat, ensure you take and share very good notes!

If I don't have a contact, you may try to find one, **BUT**: definitely pool questions (as above), be extra-polite when you ask, and *CC me on all email*. (I am also happy to make suggestions on a draft email.) Please explain that this is a class assignment for LIS 510 "Information Security and Privacy" (you may attach this syllabus if you like), and they are welcome to confirm that with your instructor (give them my name and wisc.edu email address). Also explain that *they need not answer* if they do not have time or energy, and thank them for considering your request.

Types of data you may choose from (others possible, but talk to me quickly!):

- Data from applications for admission to the university (n.b.: please do not include financial data)
- Library-use data (strongly recommended for iSchool students interested in librarianship; both physical and electronic resources, please)
- Campus wifi, app, and campus-computer use
- Canvas behavior-trail data (that is, data stored about what you do in Canvas)
- Student data collected by or shared with third-party educational-technology vendors (for example, any of the third-party Canvas plugins such as Piazza, Box, or Pearson MyLab; I will make available a full screenshot of the instructor-viewable "Apps" Canvas setting page in our course space for your reference)
- Student data collected by or shared with publishers of electronic textbooks, homework material, and/or tests (e.g. Cengage, McGraw-Hill Connect)

- Wiscard swipe data (that is, whenever you use your Wiscard in a *non-financial* transaction, e.g. for event attendance or to swipe into a building or room)
- Wiscard financial data (that is, data from using your Wiscard to pay for stuff)
- Student medical records

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/` For this assignment, 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*
- Marvin Waschke, *Personal Cybersecurity*
- Jacqueline Ryan Vickery, *Worried about the Wrong Things*

Society, privacy, and security

- Sanjay Sharma, *Data Privacy and GDPR Handbook* (Strongly recommended for those interested in privacy-related careers.)
- Bruce Schneier, *Data and Goliath* or *Click Here to Kill Everybody* or *Liars and Outliers* or *We Have Root*
- 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. Computer-science and software-engineering undergrads: I suggest you pick from this list!

- Adkins et al. *Building Secure and Reliable Systems* Open access from `https://static.googleusercontent.com/media/landing.google.com/en//sre/static/pdf/Building_Secure_and_Reliable_Systems.pdf`
- Shancang Li, *Securing the Internet of Things*
- Anne Kohnke, *Implementing Cybersecurity*
- Brian Kernighan, *Understanding the Digital World*
- John Bandler, *Cybersecurity for the Home and Office*

Many books on the list are available electronically: on the (legal!) open web, via UW-Madison library subscription, or for relatively-inexpensive purchase. You may be able to find some in local public libraries, but please observe all COVID-19-related precautions if you avail yourself of a print library book. 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 first 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 like *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 throughout the course; 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 (mostly toward the end of the course) come with graded lab activities attached. Typically you will take a quizlet or turn in a screenshot or text file showing that you did the activity. Completion is worth the full point total!

- Hashing (3 points)
- Basic password cracking (3 points)
- Reconnaissance tools (3 points)
- Sniffing network traffic with Wireshark (4 points)
- Recovering "deleted" files (3 points)
- NIST Greg Schardt/"Mr. Evil" forensic investigation (4 points)

Tracking the zeitgeist

Over the course term, locate **three CURRENT news stories involving information security or privacy**. Post a link, a brief summary (one paragraph max), and connect it briefly to our classwork. Editorial comments encouraged, but keep your language PG-13, please. If something in the piece confused you, I also encourage you to ask questions about it. "News" does not just mean newspapers and news-show websites; the technology and information-security trade press absolutely counts, as do relevant stories in sectoral news outlets such as the *Chronicle of Higher Education* for higher education or *American Libraries* for libraries. I absolutely encourage you to look in outlets relevant to your major or other specialty, and I'm happy to help you find them if need be.

For clarity: you're welcome to post stories that address matters we haven't yet gotten to in class. You don't have to wait! You also don't have to post all three stories at once; I have put suggested due dates in Canvas. Each story is worth five final-grade points.

Explain a vulnerability or attack

Clearly and *engagingly* explain a vulnerability or attack type to your classmates (please treat them as interested but not-necessarily-tech-savvy layfolk) in your choice of:

- an infographic
- 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

Post your explanation to the designated Canvas discussion forum. You may embed or link to a site external to Canvas as long as your explanation is world-readable. (I don't mind if you take it down once the class is over, but I want everybody to be able to look at everybody else's explanations!)

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. Make it clear, make it FUN, okay?

Your explanation should ideally include:

- what kind(s) of digital devices, software, and/or infrastructure the vulnerability/attack targets
- 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 (BIG HINT: juicy stories are interesting!)
- 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). I have starred ones I think are best for the not-as-tech-savvy.

- 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 (all of these have juicy stories attached to them somewhere!), and significance:

- * the ILOVEYOU virus (blast from the past!)
- 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 (perhaps because you're curious about it or were impacted by it), please clear it with me first. It's probably fine, though!

Incident report

Write a roughly five-page incident report (this is a flexible length; if you use graphics, tables, or timelines you are likely to have a bigger pagecount, and that's fine) that explains as clearly and concisely as possible what happened before, during, and after a major security, privacy, or safety failure (or series of failures). **UNDERGRADUATES**: Pretend that you are a security professional explaining it to the responsible organization's *non-technical* leadership. **GRADUATES**: Pretend that you are a security professional addressing *non-technical* organizational leadership that is worried about this class of failure and has asked you how it happens and how to avoid it.

N.b. security professionals in the field do not write academic term papers! **I do not want you to write an academic term paper here!** Lose the 12-point doublespaced Times New Roman, please!

The House Oversight Committee report on Equifax (`https://oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf`) 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 example is the Australian National University's public report: `https://imagedepot.anu.edu.au/scapa/Website/SCAPA190209_Public_report_web_2.pdf` Note especially (and do your best to emulate) its very professional-looking graphic design and layout. I keep a linkspam on breaches that contains additional examples of incident reports: `https://pinboard.in/u:dsalo/t:breaches`.

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: choose from the following list of specific incidents:

- Chegg data breach (2019; if you're interested in higher-ed security, this is a good one!)

- Exactis breach (2019)
- FEMA disaster-survivor data breach (2019)
- Facebook user-profile breach (2018; n.b. this is NOT the Cambridge Analytica scandal!)
- Scholarly-publisher Elsevier's password breach (2018)
- "Whisper" secret-sharing app breach (2019)
- Social Captain breach (2020)
- 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! recent is easier!) and compare and contrast the quality of prevention efforts and incident response:

- Library patron data breaches (you may need to ask me for examples)
- Internet of Things toy data breaches
- Internet of Things personal-assistant breaches (Alexa, Siri, Echo, etc)
- Student and/or employee data breaches at colleges/universities (e.g. Georgia Tech or Australian National University, both 2019)
- 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 and Zoom incidents extensively in class, they are 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**.

I will evaluate the report for:

- clarity of explanation
- appropriateness of recommendations for action
- appropriate brevity
- work-appropriate impassivity (blame-and-shame is inappropriate in an incident report), and
- completeness

Reading schedule

Unit 1: The human context of security and privacy

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."

Rasch. "The symbiotic, parasitic relationship between privacy, security." `https://securityboulevard.com/2020/01/the-symbiotic-parasitic-relationship-between-privacy-security/`

Chisholm and Hartman-Caverly. "Vitamin P: Why privacy is good for you (and good for society, too)." `https://chooseprivacyeveryday.org/vitamin-p-why-privacy-is-good-for-you-and-good-for-society-too/`

Jones and Kaminski. "An American's guide to the GDPR." `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3620198` (Introduction, Section II, and Conclusion only. This is a typical law review article: half footnotes. Ignore the footnotes!)

Madden. "Privacy, security, and digital inequality." `https://datasociety.net/pubs/prv/DataAndSociety_PrivacySecurityandDigitalInequality.pdf` (Summary of Findings, pp. 1-13)

Cox. "Zoom brings in former Facebook security head amid lawsuits, investigations." `https://arstechnica.com/tech-policy/2020/04/zoom-brings-in-former-facebook-security-head-amid-lawsuits-investigations/`

Module 2: Surveillance. Data ethics.

Learning objectives: Basic ethics. Surveillance capitalism (adtech, social media, personalization, recommender engines, data brokers). Social-media surveillance. Facial recognition. Learning analytics; educational surveillance. Responses to surveillance (personal, societal).

Linklist(s): https://pinboard.in/u:dsalo/t:surveillance/t:marketing, https://pinboard.in/u:dsalo/t:surveillancecapitalism

Consumer Reports. "Understanding the scope of data collection by major technology platforms." `https://digital-lab-wp.consumerreports.org/wp-content/uploads/2020/05/Understanding-the-scope-of-data-collection-by-major-platforms_2020_FINAL.pdf`

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

Watters. "School work and surveillance." `http://hackeducation.com/2020/04/30/surveillance`

Bauer-Wolf. "Big brother: college edition." `https://www.insidehighered.com/news/2017/12/21/georgia-techs-monitoring-students-social-media-causes-concern`

Darragh. "Here's why I'm campaigning against facial recognition in schools." `https://www.vice.com/en_us/article/z3bgpj/heres-why-im-campaigning-against-facial-recognition-in-schools`

Short. "Canvas exposed." `https://digitaltattoo.ubc.ca/2018/08/20/canvas-exposed-the-little-problem-with-ubcs-big-expensive-new-tool/` (N.b. UBC is in Canada, which obviously has different law than the US. For more information on Short's struggle with UBC, see my Pinboard: `https://pinboard.in/search/u:dsalo?query=ubc`)

Gurley. "California police used military surveillance tech at grad student strike." `https://www.vice.com/en_us/article/7kppna/california-police-used-military-surveillance-tech-at-grad-student-strike`

Chuen. "Watched and not seen." `http://gutsmagazine.ca/watched-and-not-seen/`

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`

Greenberg and Newman. "How to protest safely in the age of surveillance." `https://www.wired.com/story/how-to-protest-safely-surveillance-digital-privacy/?mid=1#cid=1103629`

Module 3: Humans exploit and abuse other humans' badness at security and privacy to harm them: personal edition

Learning objectives: Phishing attacks; catfishing; smishing. Social engineering of individuals. Cyberbullying, doxxing, SWATting. Revenge porn. Intimate-partner abuse. Identity theft. Mobbing; Zoombombing. Political manipulation. Biometrics.

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`

Levy and Schneier. "Privacy threats in intimate relationships." `https://doi.org/10.1093/cybsec/tyaa006` (Content alert: non-graphic domestic abuse, elder abuse, and child abuse.)

Cole. "How to tell if your partner is spying on your phone." `https://www.vice.com/en_us/article/bjepkm/how-to-tell-if-partner-is-spying-on-your-phone-stalkerware`

Malwarebytes. "Spearphishing 101." `https://blog.malwarebytes.com/social-engineering/2020/01/spear-phishing-101-what-you-need-to-know/`

Adamczyk. "All the... things you can do if you steal someone's identity." `https://twocents.lifehacker.com/all-the-fun-things-you-can-do-if-you-steal-someones-ide-1830030647` (I resent the adjective in this headline, so I left it out. DO NOT LET ME CATCH YOU. NOTHING IN THIS ARTICLE IS EVEN REMOTELY OKAY, MUCH LESS FUNNY.)

Malwarebytes. "Child identity theft." `https://blog.malwarebytes.com/awareness/2020/03/child-identity-theft-part-1-on-familiar-fraud/` and `https://blog.malwarebytes.com/awareness/2020/03/child-identity-theft-part-2-how-to-reclaim-your-childs-identity/` (Please protect the young people in your life!)

Cross. "From catfish to romance fraud." `https://theconversation.com/from-catfish-to-romance-fraud-how-to-avoid-getting-caught-in-any-online-scam-115227`

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/`

Elmer, Burton, and Neville. "Zoom-bombings disrupt online events with racist and misogynist attacks." `https://theconversation.com/zoom-bombings-disrupt-online-events-with-racist-and-misogynist-attacks-138389`

Module 4: Humans exploit and abuse other humans' badness at security and privacy to harm them: organizational edition

Learning objectives: Biometrics; facial recognition. Insider threat. Contractor threat. Supply-chain threat. Business-email compromise. Ransomware. Email surveillance. Business email compromise. How social engineering contributes to organizational hacks. Spearphishing. Workplace surveillance. Surveillance of public places.

Linklist(s): `https://pinboard.in/u:dsalo/t:nsa`

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`

Schneier. "Supply-chain security and trust." `https://www.schneier.com/blog/archives/2019/09/supply-chain_se_1.html`

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/`

Gallagher. "Why you can't bank on backups to fight ransomware anymore." `https://arstechnica.com/information-technology/2020/02/why-you-cant-bank-on-backups-to-fight-ransomware-anymore/`

Vaas. "Florida city sends $742K to fraudsters as it bites the BEC hook." `https://nakedsecurity.sophos.com/2019/11/05/florida-city-sends-742k-to-fraudsters-as-it-bites-the-bec-hook/`

Cox. "How big companies spy on your emails." `https://www.vice.com/en_us/article/pkekmb/free-email-apps-spying-on-you-edison-slice-cleanfox`

Satariano. "How my boss monitors me while I work from home." `https://www.nytimes.com/2020/05/06/technology/employee-monitoring-work-from-home-virus.html?smid=tw-share`

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/`

Koebler et al. "This small company is turning Utah into a surveillance panopticon." `https://www.vice.com/en_us/article/k7exem/banjo-ai-company-utah-surveillance-panopticon`

Unit 2: How can this happen?

Module 5: Humans are bad at managing 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`, `https://pinboard.in/u:dsalo/t:darkpatterns`

Check a few of your favorite passwords in Troy Hunt's `https://haveibeenpwned.com/Passwords`. IMMEDIATELY CHANGE ANY THAT HAVE BEEN PWNED. 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."

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`

Narayanan et al. "Dark patterns past, present, and future." `https://dx.doi.org/10.1145/3400899.3400901`

For reference (that is, skim it!): "Dark patterns at scale." `https://webtransparency.cs.princeton.edu/dark-patterns/`)

Cox. "Zoom is leaking peoples' email addresses and photos to strangers." `https://www.vice.com/en_us/article/k7e95m/zoom-leaking-email-addresses-photos` (Can you identify any dark patterns here?)

Module 6: 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:510/t:orgbehavior`

Singer and Perlroth. "Zoom's security woes were no secret to business partners like Dropbox." `https://www.nytimes.com/2020/04/20/technology/zoom-security-dropbox-hackers.html`

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 7: Attacks and incident response

Learning objectives: How attacks typically proceed; MITRE ATT&CK and Cyber Kill Chain frameworks. Adversarial thinking. Tactics, techniques, and procedures (TTPs). 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:incidentreponse`

Hospelhorn. "What is the Cyber Kill Chain." `https://www.varonis.com/blog/cyber-kill-chain/` (It's impossible to understand MITRE ATT&CK without understanding the Cyber Kill Chain first. MITRE communicates astoundingly poorly about ATT&CK! My annoyance at that is one reason I emphasize communication so much in this course!)

Strom. "ATT&CK 101." `https://medium.com/mitre-attack/att-ck-101-17074d3bc62`

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: Information security and privacy: models and practices

Module 8: Models, concepts, and jargon

Learning objectives: Theoretical models of cybersecurity; CIA model; Parkerian hexad. Theoretical models of privacy; contextual integrity. Privacy law; sectoral privacy; HIPAA and FERPA; "notice and consent;" privacy as data ownership. Threat modeling. Defense in depth.

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

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/`

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`

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`

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 9: 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 10: 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." `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`

Kumparak. "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 11: 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. Authentication and authorization; two/multi-factor authentication.

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

Schneier. *Secrets & Lies* chapter 9 “Identification and authentication.”

Elliott. “Two-factor authentication: how and why to use it.” https://www.cnet.com/how-to/how-and-why-to-use-two-factor-authentication/

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-apathy-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 12: Individual device security and privacy

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

Schneier. *Secrets & Lies* chapter 14 “Secure hardware.”

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/

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

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 13: 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 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`

“Jek” 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
1. Students demonstrate understanding of societal, legal, policy or ethical information issues.	In the incident report, students will analyze organizational security failures with an eye to how organizational policy shapes organizational response. In the campus privacy report, students will consider ethics vis-a-vis their data.
7. Students demonstrate understanding of issues surrounding marginalized communities and information.	The campus privacy report asks students to consider marginalized communities among students in their analysis.
5. Students demonstrate competency with information technologies important to the information professions.	All lab assignments test this outcome.
4. Students demonstrate understanding of professional competencies important for management of information organizations.	The incident report asks students to consider management actions, and to write for an audience of managers and leaders.

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, Tracking the zeitgeist
To think critically about how digital technologies work and their impact on society	Book review(s), Incident report, Campus privacy 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, Campus privacy report