Online Privacy & Security

Digital Life at Corvallis-Benton Co. Public Library with Bonnie Brzozowski (Public Services Librarian)

Brought to you by:

- Much of this presentation includes direct quotes and information from Surveillance Self-Defense, a website provided by the Electronic Frontier Foundation: https://ssd.eff.org

Corvallis-Benton County
PUBLIC LIBRARY

Class Outline

- Security is a process
- Threat modeling
- Software updates
- Secure passwords
- Malware, phishing attacks, & antivirus
- Metadata and Encryption
- Private browsing & sear ching
- Privacy on social networks
- Safety on public Wi-Fi
- Privacy on mobile phones
- Secure lost phone
- Facial recognition
- Contact tracing

Security is a process

- Protecting all data from everyone all the time is impractical and exhausting: *threat model*
- What's secure today may not be secure tomorrow (https://ssd.eff.org)
- It's okay to trust someone (but know who you are trusting)
- Security is not a purchase
- Think of security holistically

Threat modeling

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

Example of threat modeling

- What do I want to protect?
  - Bank info/financial info
- Who do I want to protect it from?
  - Hackers and thieves
- What are the consequences if I fail? How bad are they?
  - Identity theft, asset loss – pretty bad!
- How likely is it that I will need to protect it?
  - Malware is common and there's a lot to gain by getting this info, so highly likely
- How much trouble am I willing to go through to try to prevent potential consequences?
  - A lot! ID theft and asset loss are no joke!

Example of threat modeling

- What do I want to protect?
  - Reading history
- Who do I want to protect it from?
  - People I do not know that might try to use it against me or corporations that exploit the info to market to me
- What are the consequences if I fail? How bad are they?
  - Using the info in a way I did not intend, but that may not be very bad
- How likely is it that I will need to protect it?
  - Not especially sensitive info, but malware is a real threat, so there's no reason to assume it is safe.
- How much trouble am I willing to go through to try to prevent potential consequences?
  - Not much! I share this info with many people already and it's not especially sensitive info, so I'm okay with it not being as secure as other personal online info

Software updates

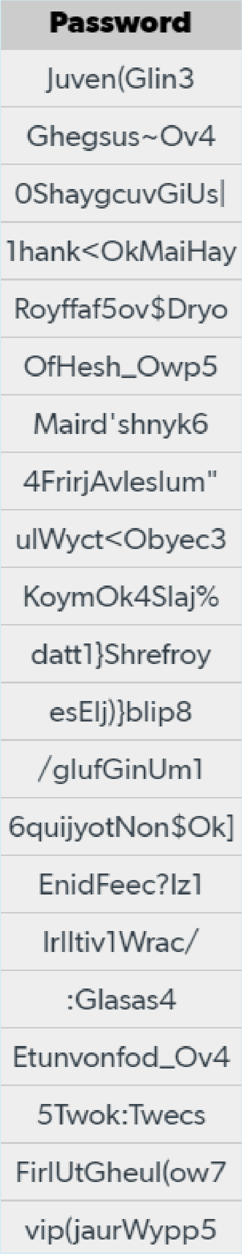
- Update your software!! (and apps!)
  - And, make it automatic!
- Easiest, most general advice you'll ever get that EVERYONE should be doing
- STOP using Microsoft Windows 7, Vista, and XP as well as Mac OS X before 10.11 (El Capitan)

Passwords

- Secure passwords are a MUST!
  - Make your password at least 12-16 characters long
  - Passwords should contain a combo of numbers, symbols, uppercase letters, lowercase letters, and/or spaces
  - Avoid names, places, and dictionary words
  - Avoid repetition (e.g., 1111)
  - Avoid simple patterns; e.g., g0be@r$
  - Do not put all the special characters at the beginning or end
  - NEVER reuse a password

Passwords

Examples of secure passwords



Password
Juven(Glin3
Ghegsus~Ov4
0ShaygcuvGiUs|
1hank<OkMaiHay
Royffaf5ov$Dryo
OfHesh_Owp5
Maird'shnyk6
4FrirjAvleslum"
ulWyct<Obyec3
KoymOk4Slaj%
datt1}Shrefroy
esElj)}blip8
/glufGinUm1
6quijyotNon$Ok]
EnidFeec?Iz1
Irlltiv1Wrac/
:Glasas4
Etunvonfod_Ov4
5Twok:Twecs
FirlUtGheul(ow7
vip(jaurWypp5

Passwords

- Do yourself a favor: **use a password manager!**
- Password managers are safer than any practical alternative
- If you’re not convinced, use the Diceware method to create passwords, write them down somewhere, and store them somewhere safe

https://askleo.com/are_password_managers_safe/

Security Questions

- Honest answers to these questions are often publicly discoverable facts that a determined adversary can easily find and use to bypass your password
- Advice: give fictional answers that no one knows but you
  - Your answer could be a random password generated from your password manager. You can store the answers in your password manager.

Two-Factor Authentication

- Also called 2FA, multi-factor authentication, or two-step verification
- User must possess two components (a password and a 2nd factor) to gain access to their account. 2nd factor is often a one-off secret code or number

Malware

- Short for “malicious software”; intended to harm computer users and is usually criminal
- Capabilities of malware include:
  - disrupting computer operation
  - gathering sensitive information
  - impersonating a user to send spam or fake messages
  - gaining access to private computer systems

Malware

- How do I protect myself against malware?
  - Be wary of suspicious attachments – well-targeted attacks can be very convincing!
  - Run software updates
  - Use Windows Defender if using PC
  - Bonus: Bitdefender (but, it's unlikely you need this unless your behaviors are risky or you are trying to secure especially sensitive data): https://bit.ly/3g0CUox
  - Bonus: Malware Bytes (see caveat next to Bitdefender; there's a free version that works well enough for most: https://www.malwarebytes.com/

Malware

- How malware can take over:
  - Email attachment: you can get tricked into clicking an email attachment that appears innocent, but is actually infected with malware. Be very careful opening strange email attachments.
  - Malicious weblink: It's possible to infect a computer remotely just by visiting a webpage. If a link prompts you to install software, do not agree. If your web browser or search engine warns you a site may be malicious, hit the back button.
  - Downloading third-party apps or software: Only download apps from your App Store or Google Play Store. Only download browser extensions from your browser's official store. Pay attention to who created it as well as reviews and comments.
  - USB, CD, etc: attackers can copy malware to your machine or device by plugging in a USB or inserting an infected CD or DVD. Be careful what you put in your computer and do not give strangers access to your computer or device.

Phishing Attacks

- When an adversary sends an email or link that looks innocent, but is actually malicious it's called phishing.
- A phishing attack usually comes in the form of a message meant to convince you to:
  - click on a link
  - open a document
  - install software or an app on your device
  - enter your username and password into a website that's made to look legitimate

Phishing for Passwords

- Phishers can trick you into giving them your passwords by sending you a deceptive link.
- Before typing any passwords, look at the address bar of your web browser. It will show the real domain name of the page.
  - A corporate logo on a page does not confirm it is real
  - Some phishers use sites that look like popular web addresses: e.g., wwwpaypal.com OR www.paypal.co

Protecting Against Phishing

- Keep your software updated
- Use a password manager with auto-fill
- Verify emails with senders (is it really from Uncle Bob? Call him and find out.)
- Open suspicious documents in Google Drive (or, other service)
- Be careful of emailed instructions

Antivirus Software?

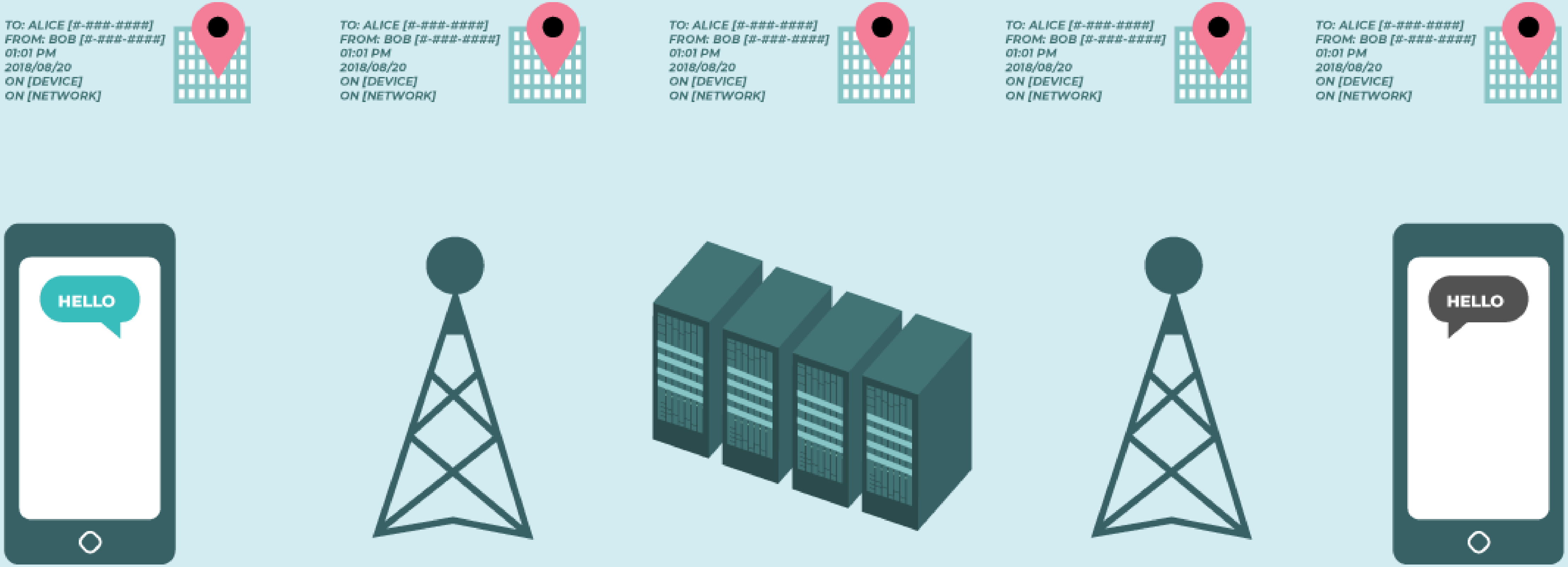
- Most people do not need a traditional antivirus software such as Norton or McAfee
- Windows 10 users should also be using Windows Defender (free).
- This is one of multiple layers of security you need for your devices, coupled with good habits. Relying on any one app to protect your system, data, and privacy is a bad bet.
    - You also need secure passwords, two-factor logins, data encryption, and smart privacy tools added to your browser

https://thewirecutter.com/blog/best-antivirus/

Metadata

- In the context of digital communications, metadata is the digital equivalent of an envelope—it's information about the communications you send and receive.
  - The subject line of your emails, the length of your conversations, and your location when communicating (as well as with whom) are all types of metadata.
- Metadata is often described as everything except the content of your communications.

https://ssd.eff.org/en/module/why-metadata-matters



TO: ALICE [#-###-####]
FROM: BOB [#-###-####]
01:01 PM
2018/08/20
ON [DEVICE]
ON [NETWORK]

TO: ALICE [#-###-####]
FROM: BOB [#-###-####]
01:01 PM
2018/08/20
ON [DEVICE]
ON [NETWORK]

TO: ALICE [#-###-####]
FROM: BOB [#-###-####]
01:01 PM
2018/08/20
ON [DEVICE]
ON [NETWORK]

TO: ALICE [#-###-####]
FROM: BOB [#-###-####]
01:01 PM
2018/08/20
ON [DEVICE]
ON [NETWORK]

TO: ALICE [#-###-####]
FROM: BOB [#-###-####]
01:01 PM
2018/08/20
ON [DEVICE]
ON [NETWORK]

What can metadata reveal?

- They know you rang a phone sex line at 2:24 am and spoke for 18 minutes. But they don't know what you talked about.
- They know you called the suicide prevention hotline from the Golden Gate Bridge. But the topic of the call remains a secret.
- They know you got an email from an HIV testing service, then called your doctor, then visited an HIV support group website in the same hour. But they don't know what was in the email or what you talked about on the phone.
- They know you called a gynecologist, spoke for a half hour, and then searched online for the local abortion clinic’s number later that day. But nobody knows what you spoke about.

Encryption

- Generally, encryption refers to the mathematical process of making a message unreadable except to a person who has the key to “decrypt” it into readable form

Encryption

- End-to-end encryption: info is encrypted from one end to another
- Transport-layer encryption: info is encrypted as it travels, but the app or website you are using can see it unencrypted

Tools for Encryption

- End-to-end encryption:
  - Signal: https://www.signal.org/
  - Whatsapp: https://www.whatsapp.com/
- Transport-layer encryption:
  - VPN: virtual private network: https://ssd.eff.org/en/module/choosing-vpn-thats-right-you
  - HTTPS Everywhere: https://www.eff.org/https-everywhere

Cookies

- What is a cookie?
  - Info saved by your web browser. When you visit a website, the site may store a cookie so it can recognize your device in the future.
- First-party and third-party cookies
  - First-party: placed by the site you visit
  - Third-party: placed by someone other than the site you are on
- Cookies allow companies to develop detailed histories of the types of sites you frequent, and they may use this info to deliver tailored ads to you

Browser finger-printing

- What is browser fingerprinting?
  - A method of tracking web browsers by the configuration and settings info they make visible to websites, rather than traditional tracking methods such as cookies.
- If your browser is unique, it's possible an online tracker can identify you without cookies. Deleting your cookies won't help.

Browser finger-printing

- Is it possible to defend against it?
  - It's difficult, but there are some measures you can take:
    - Tor browser: not a great everyday option-too slow!
      https://www.torproject.org
    - Privacy Badger, Disconnect, or Brave
      https://www.eff.org/privacybadger
      https://disconnect.me/
      https://brave.com/download/
    - Panopticlick: will analyze how well your browser and add-ons protect your privacy
      https://panopticlick.eff.org/

Privacy on Social Networks

- Read the privacy policies
  - I know, they're ridiculously long – just understand the portions that discuss how your data is used and when it is shared w/ 3rd parties
- Remember that social networking sites are usually for-profit businesses: you are the product! Blocking 3rd party cookies is a good idea when using these services (e.g., Privacy Badger, Disconnect, or Brave)
- Look for privacy and security/safety settings
- Remember privacy settings are subject to change
- Privacy is a team sport

Protect Yourself on Public Wi-Fi

- Choose your network wisely
- Check for HTTPS or use HTTPS Everywhere
- Use a VPN
- Keep apps and operating systems up-to-date
- Enable 2-factor authentication (2FA)
- Forget the network

Lack of privacy on mobile phones

- Your location is never private when using a mobile phone
- Calls and texts are easy to surveil unless you are taking special measures (e.g., using a service like Signal)
- Does turning phones off keep you safe?
    - Maybe/sometimes/it depends
    - Malware can be installed w/o your knowledge that might make it appear to be off (remove battery to ensure against this)
    - Turning off can sometimes look suspicious

Corvallis-Benton County
PUBLIC LIBRARY

Lock Down Your Phone

- Use a strong passcode alongside your biometric (fingerprint or face) login
  - iPhone: Settings > Face ID & Passcode or Touch ID & Passcode
  - Android phone: Settings > Security and location
- Set up your phone’s remote-tracking feature
  - iPhone: Settings, tap your name, and then go to iCloud > Find My iPhone
  - Android: Settings > Security & location and enable Find My Device.

Facial Recognition

- We are all potentially identifiable and trackable via facial recognition (no opting out)
- Facial recognition is biased – e.g., black women and black men are regularly misidentified
- Companies such as Amazon and Microsoft are banning the use of facial recognition for one year due to its use on BLM protestors
- Clearview AI seems to have no intention of slowing or changing service terms
- For a good overview (note: it includes opinion and adult language) check out John Oliver's recent segment: https://www.youtube.com/watch?v=jZjmlJPJgug

Also see The Perpetual Line-Up: Unregulated Police Face Recognition in America: https://www.perpetuallineup.org/

Contact Tracing

- Google and Apple have partnered to make contact tracing apps possible
- However, few states have agreed to use the technology; none are actively using it (read more here: https://bit.ly/2BEP1s9)
- Concerns that this technology could be used beyond COVID-19

Corvallis-Benton County
PUBLIC LIBRARY

Privacy & Security Cheat Sheet

- Secure your accounts
- Update your software and devices
- Protect your web browsing
- Don’t install sketchy software
- Use Windows Defender
- Encrypt your communication (optional)
- Lock down your phone in case lost
- Enable encryption on your laptop

https://thewirecutter.com/blog/7-simple-ways-to-protect-your-digital-privacy/

Questions?

bonnie.brzozowski@corvallisoregon.gov
541-766-6965