# Let’s Talk about Personal Digital Privacy and Security

Friends of the Enfield Library

October 29, 2024

Robert Hurlbut

RobertHurlbut.com • @RobertHurlbut

# Who am I?

**X(Twitter):**
@RobertHurlbut
**LinkedIn:**
roberthurlbut

**Robert Hurlbut**
**Principal Application Security Architect / Threat Modeling Lead**
**@ Aquia, Inc. (https://aquia.us)**
**(AWS Partner / AWS Public Sector Partner)**

- **Microsoft MVP – Dev Sec / Dev Tech**
- **(ISC2) CSSLP**
- **Boston Code Camp – Co-Organizer**
- **Boston .NET Architecture Group – Founder / Leader**
- **Amherst Security Group – Leader**
- **Application Security Podcast – Co-Host**
- **Expert Witness (Threat Modeling, Cybersecurity)**
- **Ph.D. Student – Space Cybersecurity**

# Disclaimer

- This material is provided "as is,“ with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, expressed or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose.
- This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice, nor is it any substitute for your independent investigations.
- If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor.

# Connected world

We live in a very connected and tracked world

When we …

browse the web,

send an email,

turn on our phones,

purchase items with our credit cards

- all of it is tracked for various reasons

Some of this may be useful, but in some cases, this information can be harmful or used for nefarious purposes

# Terms

- Privacy
- Confidentiality
- Security

# Privacy

The desire of a person to control the disclosure of personal information

# Confidentiality

The ability of a person to control release of personal information to another entity under an agreement limiting further release of that information

# Security

Protection of privacy and confidentiality through policies, procedures and safeguards

# Why do they matter?

Ethically, privacy and confidentiality are considered to be rights (in our culture)

Information revealed may result in harm to interests of the individual

# Solutions to Personal Digital Privacy and Security

Passwords, Password Manager, and 2FA

Email

Credit Cards

Cloud Storage

Virtual Private Network (VPN)

Browsing Options

Other Recommendations

Personal Mobile and Wi-Fi Security

# Passwords - Challenges

- Passwords are not easy to manage
- You need to remember the rules
- Many use the same <password> everywhere or vary them with this pattern:
  - <password>1, <password>2, <password>3 to keep them different
  - (NOTE: These are easy to figure out …)

# Passwords – Best Practices

1. Use unique passwords for each website or application

2. Best passwords are passphrases (25+ characters)

Green Horses Jump 40 Orange Fences

Tiny Elephant Is 35% Home Cooked

3. Check if your email/password has been compromised by entering your email:

https://haveibeenpwned.com/

# Password Manager

Helps manage passwords – one password to unlock many passwords

Helps with creating secure passwords

Helps with managing unique passwords (one per website or application)

It can also be used to keep track of answers to security questions, etc.

1Password https://1password.com/

IronVest https://ironvest.com/ (many other services)

**Low-tech/no-tech is fine!**

Keep a password book locked away.

# 2FA – Two Factor Authentication

One password is not enough for keeping accounts safe

Many services now offer 2FA – Amazon, Google, Microsoft, etc.

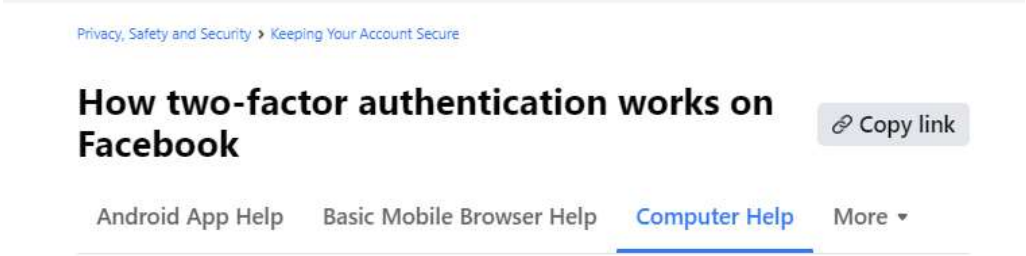
https://twofactorauth.org/

Set up with SMS, or better, with an Authenticator App:

- Google Authenticator (avail. for iOS, Android, etc.)
- Microsoft Authenticator (avail. for iOS, Android, etc.)

# 2FA – Best Practices

1. Check if the website or application provides 2FA and use it




2. Limited-time codes sent to SMS or Email are acceptable most of the time
3. If possible, prefer an Authenticator App or secure token

# Email

All email is wide open – anyone could potentially read it

Plus, it is stored in copies somewhere (even if deleted on your local email app)

Use PGP (Pretty Good Privacy)

http://openpgp.org/

Ex: Proton Mail (private, secure, encrypted – however, not free)

# Email – Best Practices

1. Check who sent the email and ask:
   *"Did I request this email or know someone was sending it to me?"*
   If the answer is no, don't:
   a. Click on any links
   b. Open or download any attachments
   Especially watch for invoice fraud (a fake bill or indicates you were already charged)

2. If you are concerned about the email and it has a link, navigate to the company website directly or call the company/sender directly (don't use any numbers included in the email).

3. Even if the email is from a company you trust, decide whether to click on the link or, to be safe, go directly to the website instead.

***These guidelines also apply if you receive an SMS/text message from someone you don't know.***

# Credit Cards

Criminals will target your debit and credit cards

- Insert chip cards – don't swipe
- Tap card for one-time use transaction


Check your free credit report (once a year)

https://www.annualcreditreport.com

Experian and TransUnion are also free once a year

Consider Fraud Alert

Watch for card skimming

Consider virtual and prepaid cards

# Cloud Storage

Cloud storage makes it convenient to back up data

~~Not all~~ (2024 - Most) cloud storage options are encrypted or secure enough

- Microsoft OneDrive (Encryption in transit and at rest – AES 256-bit, they own the keys, 2FA supported)
- Google Drive (Encryption in transit and at rest – AES 256-bit, they own the keys, 2FA supported)
- Apple iCloud (AES 128-bit/256-bit encryption, they can't decrypt – **only the user**, 2FA supported)
- DropBox (AES 256-bit encryption – they own the keys, 2FA supported)
- SpiderOak (AES 256-bit encryption – 2FA and **you** own the keys, 2FA *not supported* currently)

# Virtual Private Network (VPN)

Virtual Private Networks (VPNs) provide a good mix of security and privacy

Route internet traffic through a secure channel

Privacy – not anonymity

Available for desktop, laptop, and mobile phones

Select a reputable paid VPN provider (do not use free ones) that states no or minimal logging.

# Browsing Options

Most browsers track what you are doing (Google Chrome, Mozilla Firefox, Microsoft Edge)

This helps advertisers know what you like, etc.

Other options:

DuckDuckGo

https://duckduckgo.com


Brave

https://brave.com/

# Other Recommendations

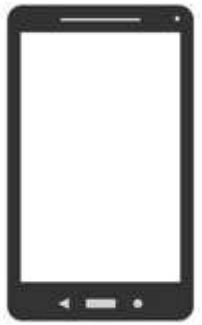
Tor – Anonymous communication

Tails – Debian Linux Distribution that runs over the Tor network

Virtual machines (VirtualBox, VMWare, Parallels, etc.)

Separate laptop / separate identities (email, etc.) – keep these separate to be anonymous and private (as much as possible)

# Personal Mobile Security



1. Update to latest version / patch
2. Password/Passcode protect your device
3. Lock your device
4. Review / adjust permissions per mobile app
5. Use anti-virus software (mainly Android)
6. Sync/back up your data
7. Install a phone finder app
8. Turn off Wi-Fi / Bluetooth when not home and not around trusted endpoints (i.e. almost everywhere!)

# Charging Devices

- “Juice Jacking” – mobile devices compromised through charging with untrusted ports
  - *Actual odds of it happening - low*
- Solutions:
  - Patching
  - Use your own charger
  - Use your own charging cable
  - Turn your phone off before charging
  - Use a USB Data Blocker device
- Watch for rental car connections

# Personal Wi-Fi Security

Ideally, don’t connect to public Wi-Fi – if so, use VPN.

*However, most places are “safe” – use caution.*

Ideally, use a Mobile Hotspot tethered to the Phone (turn off Wi-Fi/Bluetooth)

For Home Wi-Fi, set up:

**SSID with a random name (max 32 chars)**

**WPA2 (AES) with secure password with over 25 characters / random (max 63 chars)**

Never use WEP, and don’t use the automatic “button” feature on Wi-Fi routers – this is not secure.

Don’t use WPA, WPA2 (TKIP), WPA2 (TKIP + AES), etc.

# Lots of things to do!

All important methods for keeping private and secure

Mix and match – use what works best for you.

# Resources - Books

Extreme Privacy: What it Takes to Disappear (5th Edition – 2024)

*Michael Bazzell*

The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data (2019)

*Kevin Mitnick*

# Questions?

**Slides:**

**https://roberthurlbut/r/FEL2024**

**X/(Twitter):**
@RobertHurlbut
**LinkedIn:**
roberthurlbut