

## **Personal Information Security**

Information Security Council Update



September 2024 Gretchen White – CIO, Eric Brown CISO



Personal Email Security	2
VPN Security	4
Password Security	5
Offline Data Protection	10
Protecting Credit	12
Checklist	13

# **Personal Email Security**

- Free email services scrape email contents for information to help them advertise to you.
  - Message Times, Message Contents, Message Recipients, Contacts in your Mailbox, Message lengths, message attachments, etc.
- Think of using a paid subscription:

### **ProtonMail**

.....

mailbox.org



- Pros:
  - All contents are fully encrypted at rest and in transit -- E.G. No snooping on contents.
  - Feel more secure in sending // storing personal information.
  - Tutanota and ProtonMail Subscriptions contain other applications similar to Google Calendar, Drive, and VPN.
- Cons:
  - · Sometimes run into non-deliverable emails to corporate entities.
  - \$\$\$\$.







### **Personal Email Security Quick Tips**

- Maintain Multiple Inboxes:
  - 1. Paid and Secure Inbox for personal correspondence and use.
  - 2. Free and Open Inbox for giving out for rewards programs, marketing emails, etc.
    - Cub Rewards, Speedy Rewards, Walgreens, CVS, Caribou, Starbucks, O'Reilly's Rewards, etc.
      - <u>S.name@gmail.com</u>
      - firstnamelastname19@yahoo.com
      - firstname19@outlook.com

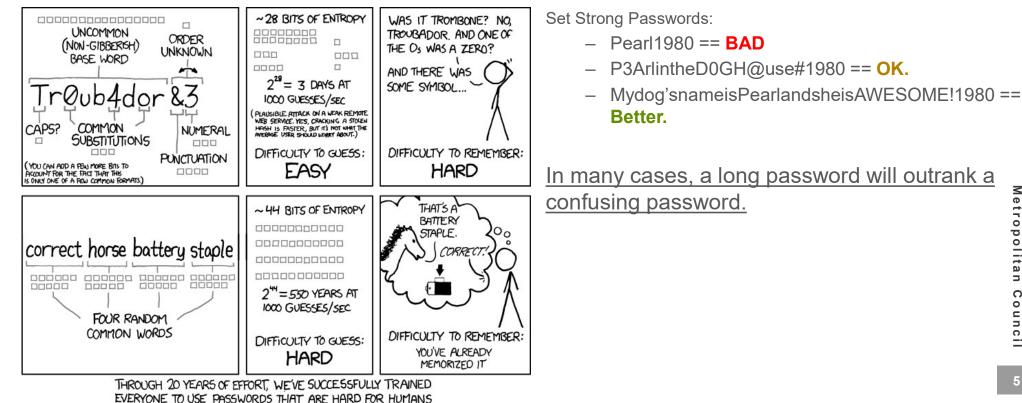
### **Personal VPN – Reputable Options**



#### **BUY A SUBSCRIPTION!**

- They do not store web logs.
- They encrypt your Internet Traffic
- The offer Cross-Platform Support.
  - Windows // MacOS // Android // iOS // Linux
- They anonymize and privatize your browsing.
- · Creates a safe tunnel from which to use Public WiFi.
  - Public WiFi is notorious for being unsafe as anyone else on the same network can view what your computer is interacting with.

### **Password Security – Setting Strong Passwords**



Metropolitan

Council

TO REMEMBER. BUT FASY FOR COMPLITERS TO GUESS

## Web Password Security

Web browsers like Mozilla, Google Chrome, Microsoft Edge, Safari, and Internet Explorer give you the option to save your passwords and form data in the browser.

#### Please DON'T DO IT!

Hackers can easily extract this data from your browser and steal your passwords, addresses, credit card information, etc.

If your passwords are similar, or the same, across websites; a single breached password can compromise your entire online identity.

### **Password Protection**

How to tell if your passwords have been breached:

	Paramer Northy new Domens trench While's been proved Pressents API About Dimeter's
	';have i been pwned?) Check if your email or phone is in a data breach
	email or phone (international format) pwned?
	Generate secure, unique pasiworth for every account      Tormerate ?ecured
Breaches you	were pwned in
	dent where data has been unintentionally exposed to the public. Using the <u>1Password password manager</u> helps you words are strong and unique such that a breach of one service doesn't put your other services at risk.
	Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, <i>encrypted</i> password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced. <b>Compromised data:</b> Email addresses, Password hints, Passwords, Usernames
*	Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).
0	EatStreet: In May 2019, the online food ordering service EatStreet suffered a data breach affecting 6.4 million customers. An extensive amount of personal data was obtained including names, phone numbers, addresses, partial credit card data and passwords stored as bcrypt hashes. The data was provided to HIBP by a source who requested it be attributed to "JImScott.Sec@protonmail.com". Compromised data: Dates of birth, Email addresses, Genders, Names, Partial credit card data, Passwords, Phone numbers, Physical addresses, Social media profiles

- If you <u>have</u> been part of a breach:
  - Proceed to Password
     Protection Step 2: Use a
     Password Manager.
- If you <u>have not</u> been part of a breach:
  - Proceed to Password
     Protection Step 2: Use a
     Password Manager.

Source: https://haveibeenpwned.com

### **Password Protection**

### Use a Password Manager



#### PROS:

- Have unique passwords for every site.
- Generate random passwords that are harder to guess than:
  - Pearl1980.
- Autofill features that don't save to the browser.
- Encrypted Vaults.

#### CONS:

- All the eggs are in one basket.
  Have a good key.
- \$\$\$\$
- Can be tedious to set up

### **Password Protection**

### Use Multi-Factor Authentication for Password Access



**BONUS TIP:** Using MFA on any site where it's available adds an additional layer of security to any online platform. (Many of the applications above can integrate with MFA on other sites).

### **Offline Data Protections**

- · Be aware of how your data is exposed
  - · Shred sensitive documents before disposing of them
  - · Remove labels from medications before discarding
  - If able, put trash out the day of collection to prevent dumpster diving
  - Mail payments from a secure mailbox or put out close to pickup time, if able.
- Avoid leaving mail, or other documents with your name or address on them in plain sight (ex: back seat or console of your car)

#### **QUICK NOTE:**

 Identity theft is rarely due to a single breach. Identity thieves, hackers, and other malevolent actors are professionals at piecing together disparate sources of information to create a full picture from which they can pull off a successful crime.



# Cellular

- Use a random pin for your account information and store the PIN in your password manager
- Avoid using your (real) mobile number as an identifier for services.
- Think about using a cellular masking service like Burner (\$46 / year) or Google Voice (Free - Less Private) to hide your true phone number when making calls.



## **Protecting Your Credit**

- Store your social security card in a safe/secure place Don't carry with you.
- Freeze Credit (Experian, TransUnion, Equifax, Innovis)
- File taxes early.



- Check Credit Report Annually
  - You are entitled to get a free copy of your credit report from each of the credit reporting agencies at AnnualCreditReport.com. Review it carefully for inaccurate, incomplete or unfamiliar information.
- Review Annual Social Security Earnings Statement
- Mobile alerts from Bank/Credit cards on each transaction

## **Checklist Part 1**

- □ Freeze your credit at all four major credit bureaus:
  - o https://www.nerdwallet.com/article/finance/how-to-freeze-credit
- □ STOP SAVING YOUR PASSWORDS IN YOUR BROWSER: Get a Password Manager:
  - o <u>https://LastPass.com</u>
  - o https://1password.com
  - o https://Dashlane.com
  - https://keepersecurity.com
- Consider using Multi-Factor Authentication wherever possible
  - o https://okta.com
  - Microsoft Authenticator Application
  - o Google Authenticator Application
  - o Last Pass Authenticator Application
- □ Consider using Cookie Deleters, Tracking Blockers, and Ad Blockers on your browser:
  - <u>https://ublockorigin.com</u>
  - o <u>https://ghostery.com</u>
  - <u>https://privacybadger.org</u>

## **Checklist Part 2**

- Download Your Google // Social Media Data and determine if you are happy with what they know about you.
  - https://support.google.com/accounts/answer/3024190?hl=en
  - o https://www.facebook.com/help/212802592074644
- Test out a free account on Protonmail or Tutanota and consider purchasing a subscription.
  - https://www.protonmail.com
  - https://www.tutanota.com
- Use a free email account for all your marketing emails.
  - <u>https://gmail.com</u>
  - o <u>https://yahoo.com</u>
  - o <u>https://aol.com</u>
  - o <u>https://outlook.com</u>
- Consider switching to Signal for messaging and encourage your contacts to do the same:
  - https://signal.org/en/
    - Other alternatives are Threema and Telegram
      - <u>https://threema.ch</u>
      - https://telegram.org
- □ Sign up for a reputable VPN Service
  - o <u>https://protonvpn.com</u>
  - o <u>https://nordvpn.com</u>
  - <u>https://www.privateinternetaccess.com/</u>
- Check out if your email has been part of any breaches:
  - <u>https://haveibeenpwned.com</u>

### **Checklist Part 3**

- □ Check out the privacy settings on your social media and determine if you're content with the amount of information you are giving to the platform.
  - https://www.facebook.com/help/325807937506242
  - o <a href="https://help.twitter.com/en/managing-your-account/new-account-settings">https://help.twitter.com/en/managing-your-account/new-account-settings</a>
  - o https://help.instagram.com/196883487377501
  - https://support.snapchat.com/en-US/a/privacy-settings2
  - https://support.tiktok.com/en/account-and-privacy/account-privacy-settings
  - https://www.linkedin.com/help/linkedin/answer/92055/understanding-your-privacysettings?lang=en
  - https://www.reddit.com/settings/privacy
- □ Shred any old documents that contain personal information.
  - https://shredrightnow.com/events/category/shredevents/
  - o https://twincitiesonthecheap.com/your-guide-to-free-paper-shredding-in-the-twin-cities/
  - Check your City Website for Local Shredding Events.
- Change Default passwords on your router/modem/internet access point at home:
  - Going to a web browser and typing 192.168.1.1 will typically get you to the administrative panel of your home internet connection.
- □ Consider giving out fake phone numbers for rewards program, or a fake phone number that you keep in your password manager.

# **Questions?**