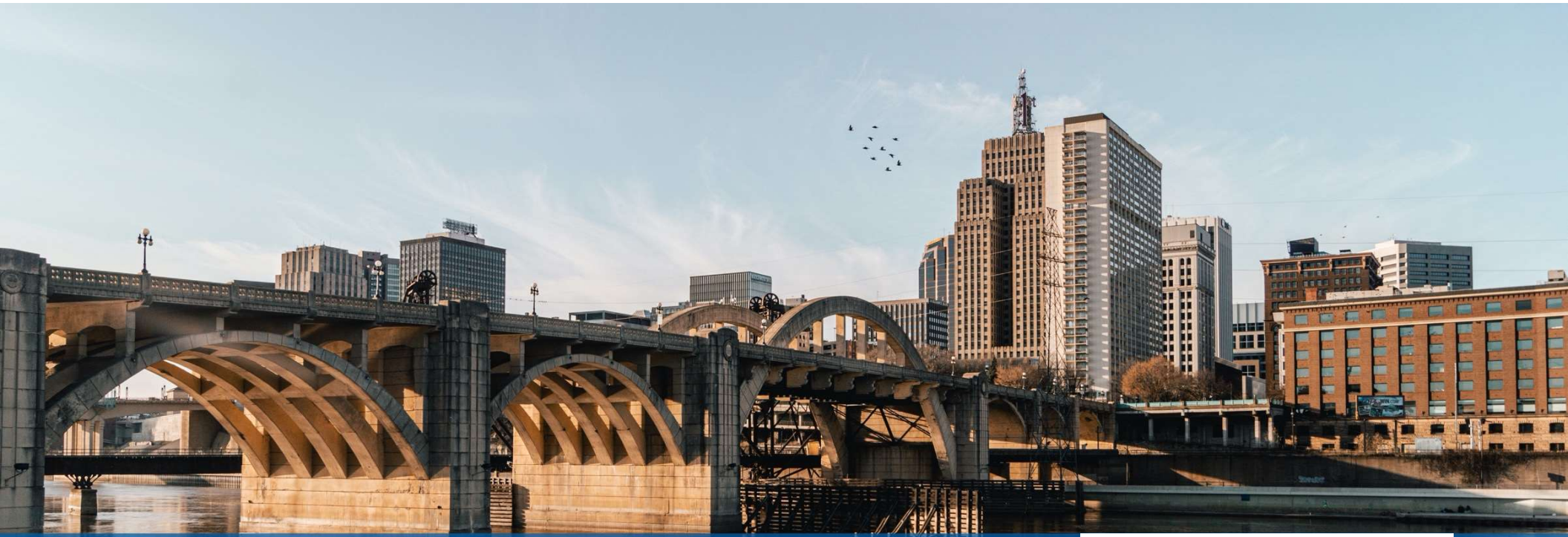


Personal Information Security

Information Security Council Update

METROPOLITAN COUNCIL

September 2024 Gretchen White – CIO, Eric Brown CISO

Contents

METROPOLITAN COUNCIL

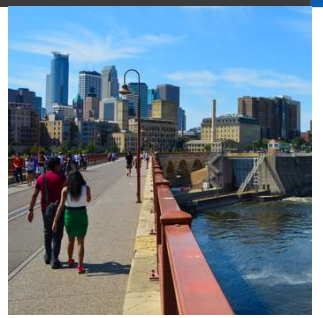
Personal Email Security

- 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 Tutanota®

- **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.

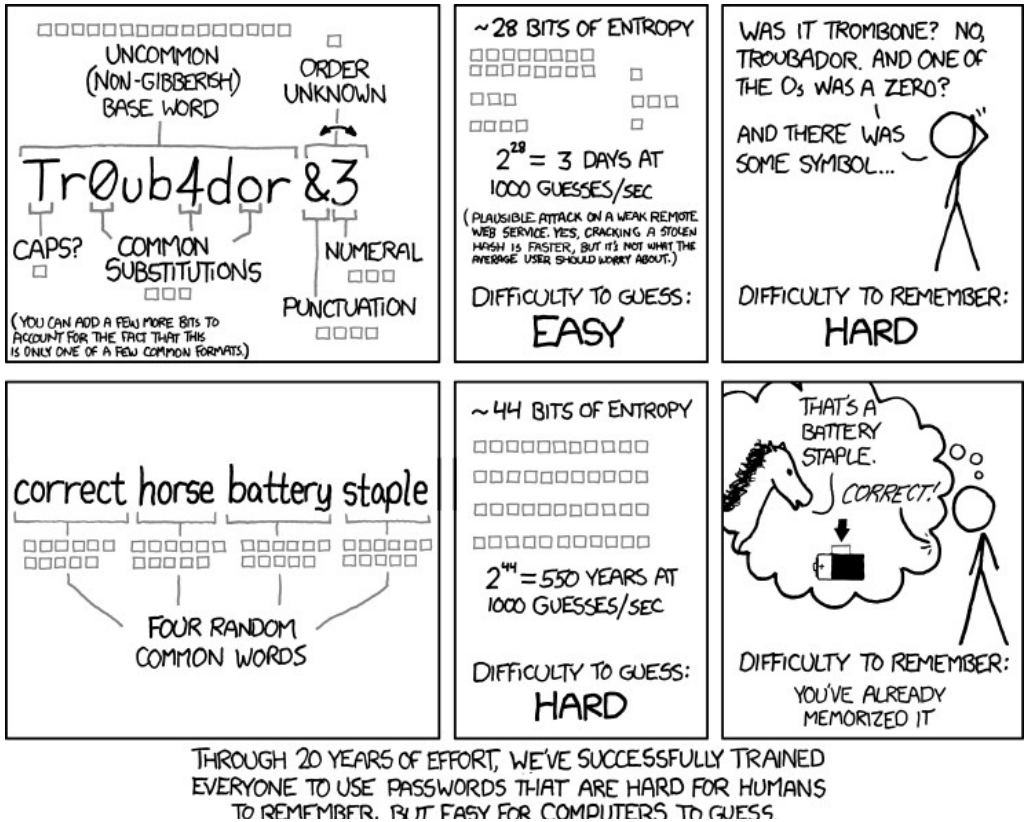
        - S.name@gmail.com
        - firstnamelastname19@yahoo.com
        - firstname19@outlook.com

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



Set Strong Passwords:

- Pearl1980 == **BAD**
- P3ArlintheD0GH@use#1980 == **OK.**
- Mydog'snameisPearlandsheisAWESOME!1980 == **Better.**

In many cases, a long password will outrank a confusing password.

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.

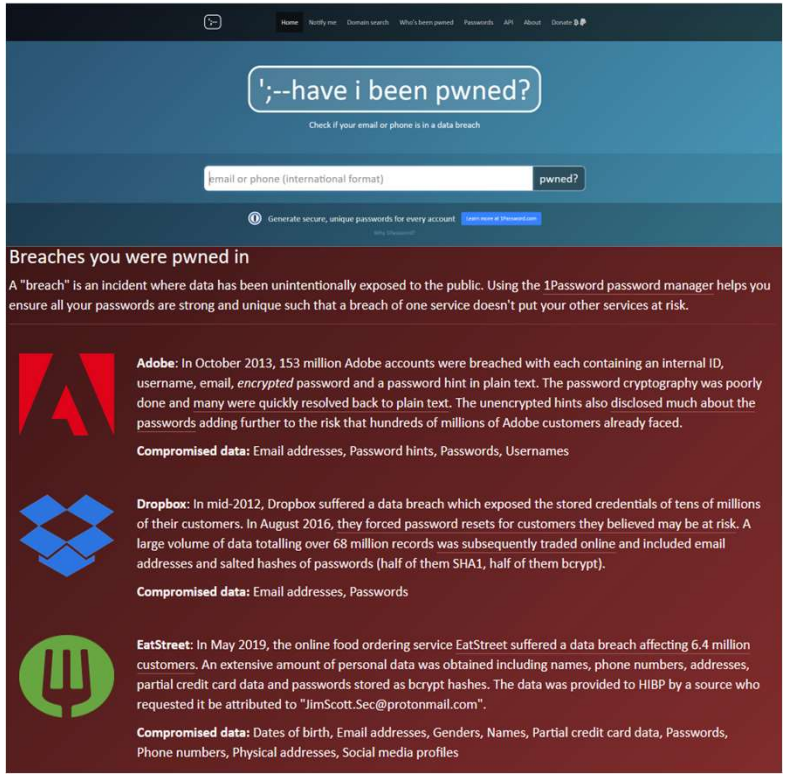
Please DON'T DO IT!

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:



- If you ***have*** been part of a breach:
  - Proceed to **Password Protection Step 2: Use a Password Manager.**

- If you ***have not*** 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:
  - https://www.nerdwallet.com/article/finance/how-to-freeze-credit
- ☐ STOP SAVING YOUR PASSWORDS IN YOUR BROWSER: Get a Password Manager:
  - https://LastPass.com
  - https://1password.com
  - https://Dashlane.com
  - https://keepersecurity.com
- ☐ Consider using Multi-Factor Authentication wherever possible
  - https://okta.com
  - Microsoft Authenticator Application
  - Google Authenticator Application
  - Last Pass Authenticator Application
- ☐ Consider using Cookie Deleters, Tracking Blockers, and Ad Blockers on your browser:
  - https://ublockorigin.com
  - https://ghostery.com
  - https://privacybadger.org

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
  - 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.
  - https://gmail.com
  - https://yahoo.com
  - https://aol.com
  - https://outlook.com
- ☐ Consider switching to Signal for messaging and encourage your contacts to do the same:
  - https://signal.org/en/
    - Other alternatives are Threema and Telegram
      - https://threema.ch
      - https://telegram.org
- ☐ Sign up for a reputable VPN Service
  - https://protonvpn.com
  - https://nordvpn.com
  - https://www.privateinternetaccess.com/
- ☐ Check out if your email has been part of any breaches:
  - https://haveibeenpwned.com

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
  - https://help.twitter.com/en/managing-your-account/new-account-settings
  - 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-privacy-settings?lang=en
  - https://www.reddit.com/settings/privacy

- ☐ Shred any old documents that contain personal information.
  - https://shredrightnow.com/events/category/shredevents/
  - 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?