Security

October 2023

Passwords

<u>When to use passwords?</u>

- Always … if you want to remain secure.
  - Phone
  - Tablet
  - Portable computer
  - Desktop computer

<u>Good password characteristics</u>

- Adequate length (8 or more characters)
- Random sequence of letters (upper and lower), digits, and special characters ($, %, etc.).
- Different than the passwords you use for other sites or devices.
- It has been said that there is no such thing as a secure password.
  - If you make it simple enough to remember, it can be cracked.
  - If you make it difficult to remember, you will write it on a post-it and put it under your keyboard or in a notebook.

<u>Most common passwords 2023</u>
(https://www.safetydetectives.com/blog/the-most-hacked-passwords-in-the-world/)

1. 123456
2. password
3. 123456789
4. 12345
5. 12345678
6. qwerty
7. 1234567
8. 111111
9. 1234567890
10. 123123
11. abc123
12. 1234
13. password1
14. iloveyou
15. 1q2w3e4r
16. 000000

Best Practices

- Use of a *password vault*.
  - A single collection of passwords secured under a single, tough-to-crack password or *passphrase*.
  - Usually includes tools to generate new, secure passwords on demand.
- Examples include:
  - LastPass (https://www.lastpass.com)
  - 1Password (https://1password.com)
  - BitWarden (https://bitwarden.com)

Passphrases

What Is a passphrase?
(https://www.techtarget.com/searchsecurity/definition/passphrase)

- A *passphrase* is a sentence-like string of words used for authentication that is longer than a traditional password, easy to remember and difficult to crack. Typical passwords range, on average, from eight to 16 characters, while passphrases can reach up to 100 characters or more.
- You could create your own passphrase, or you can use an online tool, such as:
  - https://www.useapassphrase.com
  - https://passwords-generator.org/passphrase
- Sometimes I will use such a tool, then modify the generated passphrase to make it easier for me to remember.

Multi-Factor Authentication (MFA)

What is an MFA?
(https://en.wikipedia.org/wiki/Multi-factor_authentication)

- *Multi-factor authentication (MFA)* is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.
  - MFA usually takes the form of *two-factor authentication (2FA)*, in which two pieces of evidence are presented.

- A *third-party authenticator (TPA)* app enables MFA, usually by showing a randomly generated and frequently changing code to use for authentication.

How does it work?

- For example, let's say you access a bank account online using 2FA:
  - Factor 1: You navigate to the website in your browser and login using your *credentials* (username and password).
  - Factor 2: A *verification code* is emailed to an address you provided earlier or texted to you, and you must enter that code on the website to confirm your identity and access your account.
- Another example – to access OSU accounts – is the *DUO Mobile app*.
- Many online services (especially those involving sensitive personal or financial information) require MFA or provide you with the option of using MFA.

Virtual Private Networks

What is a Virtual Private Network?

- Whether at home or on the road, a *virtual private network (VPN)* can provide you with privacy and anonymity.
- A VPN creates an encrypted *tunnel* between your device and the Internet, preventing others learning anything regarding your network usage.

Choosing a VPN

- There are many VPN services available (for a fee).
- If you want to compare them regarding ease of use, features, and price, I suggest you check sites such as these:
  - https://www.pcmag.com/picks/the-best-vpn-services
  - https://www.tomsguide.com/best-picks/best-vpn
  - https://www.cnet.com/tech/services-and-software/best-vpn/
- If you search for something such as, *"best vpn 2023"* in your favorite search engine, be cautious to avoid comparisons located on VPN provider website; they are likely to be biased.

Biometrics

<u>What are biometrics?</u>

- Biometrics is a form of access controlled by something about your person.
- The most commonly occurring examples are:
  - Fingerprint recognition
  - Facial recognition
  - Retinal recognition (only in advanced systems)
- Should you use biometrics?
- Advantage: You can access a particular device or app – such as a banking app – quickly, safely, and without entering a username and password.
- Disadvantage: You may need to share your username and password if you want someone else to use the app or device.

Other Matters

Is there more to learn?

- Definitely!
  - The online archive of *earlier Emeriti Tech Talk presentations* contains several on the topics of safety and security.
  - *Your favorite search engine is your friend!* There are many online sources of information on using your devices safely.