CONCILIUM

Cybersecurity Tips

In our current digitally minded world, the use of internet connected devices is nearly inevitable. Cybersecurity concerns intersect frequently with our daily physical security provisions. A few simple precautions may keep you from becoming an easy target.

1. **Ensure your devices as well as applications (apps) are updated and backed up.**

   Security flaws are patched regularly with the latest updates. Ensuring your device is updated to the newest firmware is an uncomplicated way to keep these loopholes from being exploited.

   For iOS and Android, ensure your device is on the latest firmware version. If your device cannot get updates because it is too old, it is time to update your device.

   Have apps set to auto update or manually update the apps on a regular basis.

   Backing up your device saves headaches if a device is lost or stolen.

2. **Secure all devices.**

   Use a strong passcode or passphrase to secure your mobile devices. Do not use an easily guessed 4-digit pin like "1234" or "0000" to secure devices. A 6-digit pin is far more secure.

   When possible, enable encryption for each device. Most newer mobile devices will have encryption enabled by default. If not, follow tutorials online.

3. **Use strong passwords for all accounts.**

   DO NOT reuse any passwords for important accounts. This means you will have to start using a password manager app.

   Take the time to change your old account passwords to a stronger password/passphrase and save the new password to a password management app. It is time-consuming but will pay dividends for your digital security.

   There are numerous password manager apps, use one that has been 3rd party tested and has open-source code. Bitwarden, 1Password, and Keeper are all highly rated password managers.

   For a strong password:

   - 12 characters or more
   - A longer password is stronger than a short complex password
   - A randomly generated password (for example, "jHZgfoNGrGAh") is stronger than a human made password (for example, PurpleSnow1!)
   - Consider using a randomly generated 3+ word passphrase, many password manager apps can autogenerate random passphrases.

CONCILIUM

Time to Break Password*

Password/Passphrase	PurpleSnow1!	jHZgfoNGrGAh	Probation Jogging Lash
Time to Break	7 hours	3 years	Centuries

* tested using the zxcvbn password strength tool

4. **Enable two-factor/multi factor authentication (2FA/MFA) on accounts.**

   If a strong password is breached (see section 3), 2FA provides a second layer of security on accounts.

   Avoid SMS (Short Message Service, Text Message) based 2FA if possible. SMS based 2FA is vulnerable to a SIM Swap attack, in which an attacker can gain control of a cell phone number.

   2FA can be hardware based or phone app based.

   Do not forget to backup recovery codes. Printing a recovery code and placing it in secure location (locked safe or similar) keeps you from losing complete access to an account.

5. **Utilize a paid VPN (Virtual Private Network) Service.**

   A VPN can increase security when using open Wi-Fi during travels. It is not a guarantee of complete online security, so be smart with your internet traffic even when using a VPN. A VPN can also assist in bypassing certain internet restrictions.

   Try not to connect to open Wi-Fi without a VPN connection. If that is not possible, at least do not access sensitive accounts on an open network (bank accounts, etc.).

   Different VPN protocols are more likely to connect successfully in various geographic areas (Wire Guard, OpenVPN, IPsec, etc.). Know the threat level of the area you will be operating in.

   Be aware of what localities will have issue with a VPN connection on your device. (Back to threat level of area you will be operating in.)

   Use a paid VPN service versus a free VPN service. Paid services will offer greater connection speeds, reliability and, as with most free online services, if you are not paying for a product, you are the product. (Mullvad, Nord and ProtonVPN are highly rated paid VPN services.)

These tips are only the basics. For additional information, there are numerous resources available online or feel free to contact Concilium (info@concilium.us) to be connected to additional resources.

Last edit: 11/09/2022 by DPM