



Top Threats for 2024 Recap

1. You

- Training Available:
 - <https://www.cisa.gov/topics/cybersecurity-best-practices>
 - <https://staysafeonline.org/resources/>
 - <https://internetsafety101.org/cybersecurity-seniors>

2. Social Media Hacking

- Protect your accounts with good credentials and Multifactor Authentication.

3. Ransomware-as-a-service

- Back up your data on all your devices and you remove the leverage of malicious encryption.
- It is recommended to have 2 different copies, such as 1 with Verizon, Google, Microsoft, Apple, Dropbox, etc., and another somewhere else, preferably offline.

4. Crypto-Mining

- Subscribe to and USE a good Antivirus, Antimalware, and Internet Security software package.
 - Norton 360 Deluxe
 - Bitdefender
 - ESET
 - Webroot
 - Trend Micro
- Check with your Internet Service Provider, Comcast provides Norton Security as part of your service.

5. Nation-backed Cyber Attacks against Public Infrastructure

- Get a generator for home use with enough gas to run it, as needed.
- Stock a week's worth of food and water.
- Get a backup battery for your cell phone able to recharge your devices at least twice
- Have a Go-Bag packed with essentials for 3 days away from home.

6. Internet of Things (IoT devices)

- All devices in your house that are connected to the internet
 - Wi-Fi Cameras
 - TVs
 - Smart Speaker (Alexa/Google)
 - Smart Appliances
 - Doorbell Cameras
- If you aren't sure check with the manufacturer.
- If auto-update function is available, turn it on.

7. Vishing (Phone Call Phishing)

- A call was placed to the victim requiring immediate payment to stop a bad thing from happening.
 - Family member needs money now or goes to jail
 - IRS demanding payment for back taxes
 - Collections call on utilities/medical bills, credit card, insurance
- If you answer the call, then be suspicious of any demand that is urgent and cannot wait for verification.

8. Compromised Accounts

- Multifactor Authentication (MFA)
- Use an authenticator system on your smart device
 - Google Authenticator
 - Microsoft Authenticator
 - Duo
- For any account that you use, if MFA can be enabled, then it must be turned on.

9. Illicit transfers from your checking account

- Watch for small/microtransactions coming from your account as preparation for a large withdrawal or just a small amount forever.
- \$1.99, \$19.99, \$9.99, \$14.99
- Were you expecting that transaction?

10. Smishing

- Receiving text messages with/without links that relate to financial transactions.
- The goal is to get you to respond either with the link or a reply.
- Don't Respond

Refresher

- Be suspicious
- Turn on MFA/2FA
- Keep devices up to date
- Back up all your data
- Subscribe to Antivirus Software
- Use long passwords & a password manager
- Watch for illicit transfers from your bank accounts

Brophy Wealth Management, LLC is a Registered Investment Advisor. Certain representatives of Brophy Wealth Management, LLC are also Registered Representatives offering securities through APW Capital, Inc., Member FINRA/SIPC. 100 Enterprise Drive, Suite 504, Rockaway, NJ 07866 (800) 637-3211.
Brophy Wealth Management, LLC is independent of APW Capital, Inc.