HOSTAGE US

Cybersecurity Best Practices and Resources

There are times during or after a kidnapping when secrecy and privacy are very important. To ensure that one's devices and accounts are not being tampered with, cyber specialists recommend these best practices and resources to protect oneself from being hacked or exploited. Additionally, there is also the option to simply block or ignore and delete unknown, or unwanted calls and inquiries.

Best Cyber Hygiene Practices

- Enable multi-factor authentication (MFA)
- Create complex passwords with special characters and use a password manager service
- Enable "automatic software updates" in settings for your mobile and other digital computing devices
- If you suspect your account(s) have been breached, have an emergency response plan already in mind

Multiple Layers of Defense

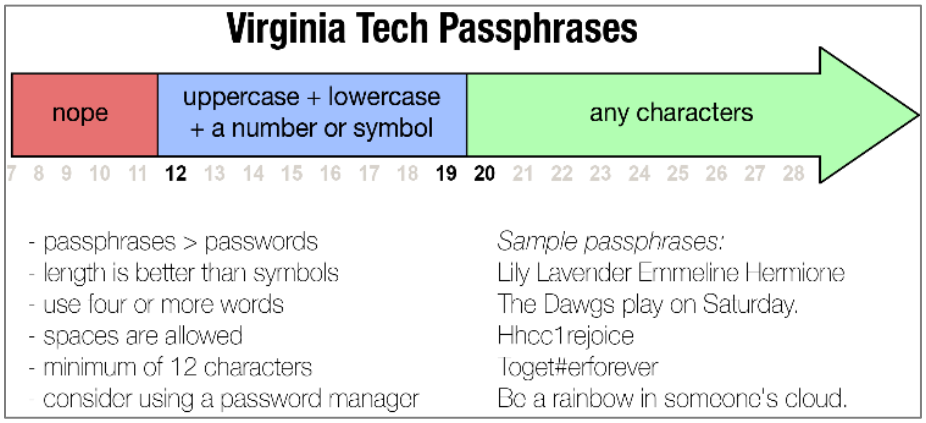
There are several free and/or commercially available cybersecurity tools and services. Here are some recommendations:

- To check if your email account has been breached: https://haveibeenpwned.com/
    - Note: A "breach" is defined as an incident where data is "inadvertently exposed in a vulnerable system, usually due to insufficient access controls or security weaknesses in the software." https://haveibeenpwned.com/FAQs
- For secure messaging, encrypt SMS/MMS messages using end to end encryption (also called E2EE), available for free using the apps: Signal or Telegram
- To keep track of all your different passwords and to have the option of using suggested strong passwords, use password manager services like: LastPass or Dashlane
    - Note: Using a passphrase is better than using a password, and length and complexity will make your passwords stronger.
- To share a password or secret message with a trusted party: One Time Secret, https://onetimesecret.com/
- To use secured and encrypted cloud storage, try: Dropbox, Google Drive, or iCloud
- Use a virtual, private network (also called a VPN) to secure your internet browsing sessions; try this free, opensource service: Tunnelblick, https://tunnelblick.net/
- To use a commercially available secure email service for work or otherwise, companies like Palo Alto Networks and Tessian provide enterprise email security services to mitigate risks of data breaches, business email compromise (BEC), and other cyber incidents.

If You Suspect a Cyber Breach

- Report cybercrime incidents to the FBI Internet Crime Complaint Center (IC3): https://www.ic3.gov/Home/ComplaintChoice/default.aspx/
- Notify your organization if your company account(s) have been breached.
- Strengthen the complexity of your passwords and change them periodically.

Passphrases Are Recommended Over Passwords:



More on Cybercrime

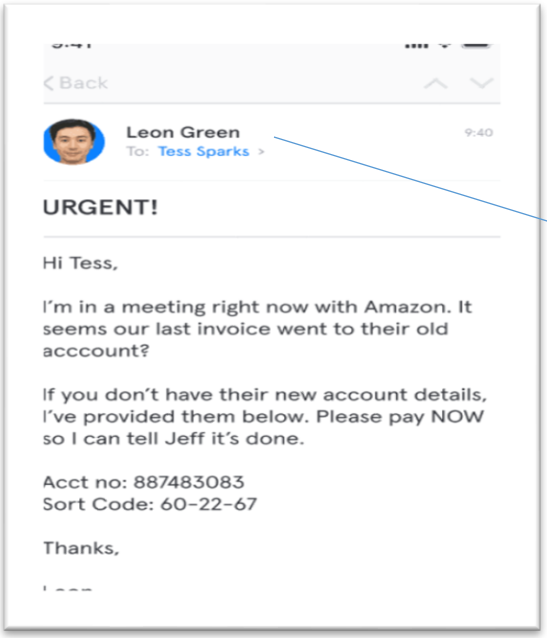
Over the past few years, the most commonly reported forms of cybercrime to the FBI's Internet Crime Complaint Center (IC3) have been phishing. For more on cybercriminal trends, read CSIS' Report on the "Hidden Costs of Cybercrime," https://www.csis.org/analysis/hidden-costs-cybercrime

When reading an email, it is recommended that you:

1. **Stop.** Verify email header information.
2. Reflect. "Is this a legitimate request?"
3. **Assess** the course of action.

Report fraudulent requests.

Here is an email phishing example:



1. Stop. Verify the email header information. For example, this is a malicious request to a Microsoft Employee pretending to be another employee, but not the FAKE email address used in the header: Leon.Green@microsott.com
2. Reflect. "Is this a legitimate request?"
3. Assess. Who should you notify in the event of a phishing email?