SECURING KEY ACCOUNTS AND DEVICES

Hacked Accounts

What are some signs that one of my online accounts may have been hacked?

- There are posts you never made on your social network page – they may be posts that encourage your friends to click on a link or download an app.
- A friend, family member or colleague reports getting email from you that you never sent.
- Your information was lost via a data breach, malware infection or lost/stolen device.

If you believe an account has been compromised, take the following steps:

- Notify all of your contacts that they may receive spam messages appearing to come from your account. Tell your contacts they shouldn't open messages or click on any links from your account and warn them about the potential for malware.
- If you believe your computer is infected, be sure your security software is up to date, and scan your system for malware. You can also use other scanners and removal tools.
- Change passwords to all accounts that have been compromised and other key accounts as soon as possible. A strong password is a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember (for example, "I love country music."). On many sites, you can even use spaces!

If you cannot access your account because a password has been changed, contact the service provider immediately and follow any steps the provider offers for recovering an account.

Resources if you become a victim of hacking:

- https://staysafeonline.org/stay-safe-online/securing-key-accounts-devices/hacked-accounts/