HACKED ACCOUNTS

If your account has been compromised or hacked, here are ways to regain control.

How do I know if my email or social network account has been hacked?

- There are posts you never made on your social network page. These posts often 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 that appear 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 ASAP. Remember, passwords should be long and strong and use a mix of upper and lowercase letters, and numbers and symbols. You should have a unique password for each account.

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

Protect Yourself with these STOP. THINK. CONNECT. Tips:

- **Keep security software current:** Having the latest security software, web browser and operating system is the best defense against viruses, malware and other online threats.
- **Make your password a sentence:** 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!
- **Unique account, unique password:** Having separate passwords for every account helps to thwart cybercriminals. At a minimum, separate your work and personal accounts and make sure that your critical accounts have the strongest passwords.
- **Lock down your login:** Fortify your online accounts by enabling the strongest authentication tools available, such as biometrics, security keys or a unique one-time code through an app on your mobile device. Your usernames and passwords are not enough to protect key accounts like email, banking and social media.
- **When in doubt, throw it out:** Links in email, tweets, posts and online advertising are often how cybercriminals try to steal your personal information. Even if you know the source, if something looks suspicious, delete it.

Source:
Stay Safe Online, powered by National Cyber Security Alliance. "Hacked Accounts."