Email Security Tips

Cyber fraud is on the rise, largely due to compromised email accounts being used to initiate wire fraud and other financial crimes. The following security tips can help you identify a compromised email account and prevent further exploitation.

PROTECT YOUR EMAIL ACCOUNT

- Change your password often. Make it complex and avoid using personal information.
- Enable two-factor authentication for account access. A quick Internet search will show how to set this up for most major email providers.
- Maintain and routinely update an anti-virus/malware program.
- Scrutinize email content and avoid anything that looks suspicious.
- Before you click, hover your cursor over the sender's email address along with any URLs in the message to be sure they are legitimate.
- If you suspect the 'From' address is fraudulent, you can check it with a header analyzer such as this one from Google: https://toolbox.googleapps.com/apps/messageheader/.
- Review your account activity records for suspicious logins.
- Periodically check your Sent folder to be sure emails aren't being sent or forwarded without your knowledge.
- Periodically check your email configuration to ensure automatic forwarding has not been enabled without your knowledge. A quick Internet search will show how to configure forwarding for most major email providers.

INDICATORS THAT AN EMAIL ACCOUNT HAS BEEN COMPROMISED

- You are unable to login, indicating password has been changed.
- Activity records show suspicious login times or unknown locations.
- Account configuration is set to forward emails to an unknown address.
- Friends and/or colleagues are receiving "spam" messages from your account.
- You receive replies to emails you did not send.

TIPS TO RECOVER A COMPROMISED EMAIL ACCOUNT

- Change your password immediately.
- If possible, make the account disconnect or sign out of other web sessions.
- Check the message forwarding settings to ensure hackers are not being forwarded the incoming emails.

Note that a compromised email account could be an indicator that the computer itself has been hacked. It is recommended that users complete a full virus scan and change the computer login password.

Victims of email fraud can submit a complaint via the FBI's Internet Crime Complaint Center site located at: https://www.ic3.gov

Additional information to help protect yourself from malicious emails can be found in the SANS Security Awareness Newsletters located at: https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201512_en.pdf

Contact your email service provider for more information and tips to protect your important communications.