Email Hacking and Spoofing

Has this happened to you? You get an email from friends, family, and co-workers. The emails contain random links or requests for a money wire transfer or gift cards. It looks like the email account might have been taken over or spoofed. What do you do? We share the following tips from the Federal Trade Commission for email hacking and spoofing.

**What are some signs of hacking?**
- Friends and family are getting emails or messages you didn’t send.
- Sent messages folder has messages you didn’t send, or it has been emptied.
- Social media accounts have posts you didn’t make.
- Can’t log into your email or social media account.

**What can you do if you have been hacked or spoofed?**
- Make sure your security software is up to date.
- Create new, strong passwords.
- Check your account settings like the signature line or away messages for unusual links.
- Alert those you know.

**Take these preventive steps!**
- Do not open or click on any unknown link.
- Type the search yourself rather than clicking on a link in an email.
- If someone asks for personal information or money/gift cards, ask the person who sent the email to ensure it has not been spoofed.
- Protect your username and passwords.
- Use two-factor identification where login in requires two steps such as a password and a special code sent to a smart phone.
- Research software prior to downloading it.
- Safeguard your information when using public computers.

If you have received phishing emails, please file a report with the Federal Trade Commission at FTC.gov/complaint. Also, take steps to protect your identity by visiting Identitytheft.gov.

[https://www.consumer.ftc.gov/articles/0003-phishing](https://www.consumer.ftc.gov/articles/0003-phishing)
[https://www.consumer.ftc.gov/articles/0376-hacked-email](https://www.consumer.ftc.gov/articles/0376-hacked-email)