Text and Email Phishing Scams

*Phishing* is when scammers use email and text messages to trick you into giving them your personal information. They are looking for information such as: passwords, account numbers, credit/debit card numbers, or Social Security numbers. If scammers obtain this information, they can gain access to your email, bank, or other accounts.

These emails and text messages may look like they are from companies you know and trust, for example, companies like Amazon, Netflix, Facebook, a bank, or online store. These often tell a story to trick you into clicking a link.

**IMPORTANT:**

Most, if not all of these types of companies will **NEVER** ask you for your personal information over email or text message.

---

**How to Protect Yourself:**

- Keep your computer and phone up to date.
- Don’t click on links in email or text message, unless you initiated the request.
- Confirm the “From” email address is actually from the company.
- Protect your accounts with multi-factor authentication. This requires an extra step to log in to your accounts.
- Use anti-virus software.
- Set strong passwords and vary them from time to time.

If you believe you have received a “Phishing” text or email, you can report it to both the company and the FTC at [https://www.ftccomplaintassistant.gov/](https://www.ftccomplaintassistant.gov/).

---

REPORT ALL SUSPICIOUS ACTIVITY TO THE POLICE

Emergency: 911 - Non-Emergency: 703-792-6500