

RISK MITIGATION ACCOUNT RECOMMENDATIONS

Phishing, carding, or brand spoofing is when fraudsters send official looking emails or text messages that ask for verification of financial information telling the recipient there has been a problem with their account. The recipient is asked to click on a link or call, and give their financial account information. Data gathered from this type of fraud is then used to drain financial accounts, charge credit cards and steal identities. You must be careful!

- NEVER respond to a text message, email, or phone call that requests personal or account information.
- If you do get a Phishing scheme request, report the incident to the Federal Trade Commission (www.ftc.gov) and file a complaint with the Internet Crime Complaint Center (www.ic3.gov).
- Report the telephone number(s) to your local carrier immediately so it can attempt to shut it down.
- Pittsburgh Federal Credit Union would never ask its members for personal or financial information via a text message, email, or phone calls. Remember, we already have your information, so we would not contact you to get it.
- It is important that you monitor your financial accounts (deposit and credit card accounts) on a regular basis (www.annualcreditreport.com).
- Immediately report any unauthorized transactions you discover.
- Phishing scheme's can be dangerous and costly, so please be careful when giving anyone your personal information.