

# Phishing Scams: What they are and how to avoid them.

Phishing scams use mass e-mails and fraudulent websites to lure people into divulging their personal information, such as credit card numbers, social security numbers and account passwords. The information is then relayed to individuals or groups who use it to open lines-of-credit and to tap into the victim's financial accounts. Typically, the e-mails evoke a sense of panic with messages warning of possible identity theft or pending account cancellation. In some cases, the fraudulent e-mails claim to be from United States government agencies such as the FDIC (Federal Deposit Insurance Corporation) or the OCC (Office of the Comptroller of the Currency). The victim then divulges the information without carefully considering the risk involved in giving out that information.

**Listed below are some of the steps you can take to avoid becoming a victim of phishing:**

- Be wary of e-mail messages asking for personal financial information, especially those with a demanding tone or a number of spelling or grammatical errors.
- Avoid using links to sites that are provided in the e-mail. Instead, log on to the website by typing their web address into your browser or call the company directly to verify that the message is authentic. Remember, secure websites will begin with "https://" rather than "http://" and you should see a key or lock symbol on your browser.
- Never fill out forms embedded in e-mail messages that request personal information. This information should only be communicated via a secure website or telephone.
- Create passwords that are not easily guessed or learned. Avoid using birthdates, phone numbers, names of family members or pets, your social security number or your login ID. Create a strong password by using a combination of upper and lower case letters and numbers. Longer passwords are better. Make it something your can remember without writing it down. It is also a good idea to change passwords about every six months.
- Be cautious of e-mails requesting you download software.
- Keep your computer up-to-date with anti-virus software and firewall programs.
- Be sure to log into your online accounts and check financial statements (credit union, credit card, etc.) regularly for suspicious transactions. If you notice any discrepancies or unfamiliar activity on any of your accounts contact the company immediately.
- If you receive a phishing e-mail report it to: 1) the Federal Trade Commission at [uce@ftc.gov](mailto:uce@ftc.gov); 2) the Internet Fraud Complaint Center of the FBI at [www.ifcbbi.gov](http://www.ifcbbi.gov); and 3) the company that is being impersonated.

## **What does Quorum FCU do to help protect our members?**

We will never ask for — or send out — your account numbers, passwords, PINs, or personal information in any e-mail correspondence. As an added precaution, we never personalize e-mails with a member's name or address, nor do we provide direct links to websites in our e-mails.

*Visit the Federal Trade Commission's website, [www.ftc.gov](http://www.ftc.gov), to learn more about phishing and how you can protect yourself against becoming a victim.*