

The following is a list of recommendations we would like to share with our members to help them Avoid be becoming a victim of phishing scams.

- * Be suspicious of any email with urgent requests for personal financial information. Phishers typically: (1) include upsetting or exciting (but false) statements in their emails to get people to react immediately; (2) ask for confidential information such as usernames, passwords, credit card numbers social security numbers, account numbers, etc.; and (3) do not personalize the email message (while valid messages from your credit union should be.)
- * Don't use the links in an email to get to any web page, if you suspect the message might not be authentic. Instead, call the company on the telephone or log onto the website directly by typing in the Web address in the browser.
- * Avoid filling out forms in email messages that ask for personal financial information. You should only communicate information such as credit card numbers or account information via a secure website or the telephone.
- * Always ensure that you're using a secure website when submitting a credit card or other sensitive information via your Web browser. To make sure you're on a secure Web server, check the beginning of the Web address in your browser address bar. Example: "https://" rather than http://.
- * Consider installing a Web browser tool bar to help protect you from known phishing fraud websites.
- * Regularly log into your online accounts and don't wait for as long as a month before you check each account.
- * Regularly check your financial institution, credit, and debit card statements to ensure that all transactions are legitimate. If anything is suspicious, contact your financial institution(s) and card issuers.
- * Ensure that your browser is up to date and security patches applied.
 - Always report "phishing" or "spoofed" emails to the following groups:
 - Forward the email to reportphishing@antiphishing.com
 - Forward email to the Federal Trade Commission at spam@use.gov
 - Forward the email to the "abuse" email address at the company that is being spoofed.
 - When forwarding a spoofed messages, always include the entire original email with its original header information intact and notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their website: www.ifccfbi.gov.