Fraud Prevention

Internet Phishing

Internet phishing is the criminal attempt to acquire sensitive information, such as passwords, account information, credit card details, etc. Often the message includes a warning regarding a problem related to your account and requests that you respond by following a link to a fraudulent website and providing specific confidential information. The following is a list of recommendations that will help you **avoid** becoming a victim of a phishing scam:

- 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, such as "Immediate action required" or "Please contact us immediately about your account"; (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). **It is the policy of the Walker County Educators FCU not to ask you for sensitive information such as listed above by email.**

- 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 your 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 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 browsers address bar – it should be **https://** rather than just **http://**.

- 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 ensue that all transactions are legitimate. If anything is suspicious, contact your financial institution(s) and card issuers.

- Ensue 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 the email to Federal Trade Commission at spam@uce.gov;
  - forward the email to the "abuse" email address at the company that is being spoofed;
  - when forwarding 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/.

Identity Theft

Identity theft is increasing at an alarming rate. Avoid becoming a victim by following these basic tips:

- Don't give out personal information such as personal account information, account numbers, or social security numbers over the telephone, Internet, or by mail unless you know who you are dealing with, and you initiated the contact.

- Protect PINs and passwords by keeping them in a secure location. Don't set up PINs or passwords that are easily obtainable such as mother's maiden name, your date of birth, social security number, or phone number.

- Dispose of sensitive personal information such as unused credit card offers, ATM receipts, account statements, or any information with social security numbers or account numbers by shredding.

- Carry only identification information you routinely use on a daily basis such as driver's license and credit card.

- Be aware of your account information and billing statement cycles and review them carefully.

- Don't allow mail to accumulate in your mailbox.

- Review copies of your credit report annually and check for any errors or signs of fraudulent activity. To receive your free annual credit reports:

    - Visit **www.annualcreditreport.com**

    - Call **1-877-322-8228**

    - Mail request to:
      Annual Credit Report Request Service
      P. O. Box 105281
      Atlanta, GA 30348-5281

If you become a victim of identity theft, take the following steps immediately:

- File a police report with your local law enforcement agency.

- Contact your financial institutions immediately and alert them to the situation.

- Contact the fraud departments of each of the three major credit bureaus and place a fraud alert on your file:

    Experian……...888-397-3742
    Equifax…….800-525-6285
    TransUnion……..800-680-7289

- Contact the Federal Trade Commission's Identity Theft Hotline:
  1-877-ID-THEFT (1-877-438-4338).