Princeton
Federal Credit Union
A Tradition of Financial Excellence

Email Scams

Protect yourself from Internet and email scams by keeping your private information secure. Online criminals use personal information by luring online consumers to fraudulent websites through links sent via email.

The email message often warns consumers their account will be closed if their information is not updated or verified. The links within the email direct recipients to web forms that ask for bank account information, credit card numbers, PIN numbers, passwords or social security numbers.

Criminals send millions of fraudulent email messages linked to fraudulent websites designed to look like websites you trust, like your credit union or bank. By using a familiar look and language, criminals trick victims into providing personal information which can be used for many different types of fraud. Criminals can use information obtained through phishing to steal money from your accounts, open new accounts in your name or obtain official documents using your identity.

By nature, email is not a secure form of communication. Never enter private, personal information in a form sent to you by email. Princeton Federal Credit Union will never send or request confidential account information through email.

Ways to protect you from Internet and email fraud (phishing):

- Do not click on links in unexpected emails that request confidential information. If updates to information are needed, always type the address for the institution’s website into your browser.

- Before submitting confidential information through forms, make sure you are using a secure internet connection. Verify the web address begins with “https://”, which indicates a secure connection. You should also look for a lock icon in your browser’s status bar.

- Install and run updated anti-virus and anti-spyware software regularly. Both viruses and spyware can leave your computer vulnerable to attack and intrusion.

- Keep your internet browser, anti-virus, anti-spyware and firewall up-to-date by visiting the manufacturer's website and checking regularly for software and security upgrades.

- Install a firewall, either software or hardware. A firewall will prevent attacks on your computer through the internet by determining if a requested connection is malicious.

- Review and monitor your checking account, debit card, credit card statements and your credit report regularly to be sure all transactions are legitimate.

- Watch for misspelling or grammatical errors on forms requesting confidential information. Hackers often make errors while rushing to get bogus website in place.

Princeton Federal Credit Union will never request personal information (member number, account number, social security number, personal identification number or password) through email or by phone. If you receive an email or phone call requesting your personal, confidential information that appears to be from Princeton, DO NOT respond and contact us immediately at 609.945.6200.