

Phishing

Everywhere you look articles and newswatches about about "phishing." What is it and how can you guard against this type of scam?

Definition: a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly.

These scams often request credit card numbers as well as other sensitive information. Be aware of email containing imbedded links for you to access to update your information.

- Don't open email from an unknown source/sender.
- Don't input or reveal personal or confidential information via email.
 - Personal information, such as passwords and credit card, social security, and bank account numbers. A legitimate organization already has this information.
- Be selective when giving out your email address.

PTFCU will never send you an email requesting your account number or credit card number. If you have a concern about an email received from us, contact our call center or email us at administrator@ptfcu.org.

Review your monthly account statements and credit card statements and report any irregularities immediately.

If you have opened an email and provided this type of sensitive information, contact us and your other creditors right away. Contact one or more of the national credit bureaus and ask that a fraud alert be placed on your accounts, and obtain copies of your credit report(s).

You should also visit the Federal Trade Commission's (FTC) identity theft web site at www.consumer.gov/idtheft or call 1-877-IDTHEFT to file a complaint and learn more about how to minimize your risk of damage from identity theft. If you notice any irregular activity on your credit report, contact your local law enforcement agency as well.