Internet and Member Security Tips

In light of the rise of internet security and identity theft incidents, The Partnership FCU wants to assure you that protecting the Credit Union and your information remains our highest priority. This page offers information about current internet security threats, what to do to protect yourself or if you become a victim of a phishing scam or identity theft, and what we are doing to safeguard our members' confidential information.

Internet Security Threats

The following terms are common internet security threats designed to collect confidential information from a member:

Phishing: The scam, popularly called 'phishing,' involves the use of replicas of existing Web pages to try to deceive you into entering personal, financial or password data. Often suspects use urgency or scare tactics, such as threats to close accounts.

We here at The Partnership FCU will never ask you via email to verify account information. We will never use email to threaten account closure. Please know this, as one defense against phishing. Other safeguards to help protect you from phishing scams:

- Be suspicious of any email messages that claims to be from us that use an urgent or scare-tactic tone.
- Do not respond to email messages asking you to verify personal information.
- Delete suspicious email messages without opening them. If you do open a suspicious email message, so not open any attachments or click any links.
- Install and regularly update virus protection software.
- Keep your computer operating system and Web browser current.

Spoofing: Email spoofing may occur in different forms, but all have a similar result: a user receives email that appears to have originated from one source when it actually was sent from another source. Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords).

Examples of spoofed email that could affect the security of your site include:

- Email claiming to be from a system administrator requesting users to change their passwords to a specified string and threatening to suspend their account if the user does not comply with the email instructions.
- Email claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information

Fraudulent Web Sites: From time to time, you might receive e-mails that look like they come from The Partnership FCU, but they are, in fact, falsified. Often these e-mails direct you to a Web site that looks similar to The Partnership FCU Web site, where you might be asked to provide account information such as your e-mail address and password combination. Unfortunately, these false Web sites can steal your sensitive information; later, this information may be used to commit fraud. Below are some key points to look for in order to identify these e-mails:

- Genuine The Partnership FCU web sites are always hosted on the "**ThePartnershipFCU.com**" domain–"**http://www.ThePartnershipFCU.com/**. . . " (or "**https://www.ThePartnershipFCU.com/**..."). Sometimes the link included in spoofed e-mails looks like a genuine ThePartnershipFCU.com or thepartnershipfcu.com address. You can check where it actually points to by hovering your mouse over the link–the actual Web site where it points to will be shown in the status bar at the bottom of your browser window or as a pop-up.
- We never use a web address such as "**http://thepartnershipefcu.com/**. . ." or an IP address (string of numbers) followed by directories such as **http://123.456.789.123/ThePartnershipfcu.com/**

Pharming: Unlike phishing which requires victims to voluntarily visit a criminal's website; pharming simply redirects victims to fraudulent websites without assistance. Pharming subverts a basic service of the Internet known as the 'Domain Name Service,' or 'DNS.' Each machine connected to the Internet knows the location of one or more DNS servers. This service translates a human-friendly URL name such as www.ThePartnershipFCU.com into an IP address, which is a unique number that has been assigned to each web server on the Internet.

The good news is pharming requires either an unpatched software/server vulnerability to exist on the DNS server itself, or the criminal needs an insider at the ISP or financial institution to make unauthorized DNS server changes. This is rare.

Please be assured that The Partnership FCU manages and updates its DNS server's software to maintain a high level of security. We maintain the highest standards; our members are protected from pharming that would result from a compromise of our DNS server.

What you "the Member" can do:

The Partnership FCU recommends that you never respond to email messages asking you to verify personal information. But accidents happen, and the following information could be useful if you've been scammed.

Password Complexity: It is important to verify that only authorized persons log into online banking. This is achieved by verifying your password. When you submit your password, it is compared with the password we have stored in our secure data center.

We allow you to enter your password incorrectly a limited number of times; too many incorrect passwords will result in the locking of your online banking account until you call us to reinitialize the account. We monitor and record "bad-login" attempts to detect any suspicious activity (i.e. someone trying to guess your password).

You play a crucial role in preventing others from logging on to your account. Never use easy-to-guess passwords. Examples:

- Birth dates
- First names
- Pet names
- Addresses
- Phone numbers
- Social Security numbers

Never reveal your password to another person. You should periodically change your password in the User Option section of Internet Banking.

If you have received a fraudulent email: If you receive an e-mail that appears to be from The Partnership FCU, NCUA or any other Credit Union related organization and instructs you to go online to provide or "verify" financial or sensitive personal information, don't believe it. We would never send you an e-mail asking for your credit- or debit-card, credit union or bank account information, Social Security number, login information (such as a PIN) or similarly sensitive data.

These organizations' names, logos, and other graphics have been used fraudulently in numerous phishing e-mails aimed at tricking people into providing sensitive financial and personal data on replicated Web sites. Giving these phishers your account and other sensitive information may expose you to identity theft and other types of fraud. If you have already complied with a phishing e-mail, you should contact the institution where you maintain your account and have the information changed immediately.

This e-mail activity has been reported to the Internet Crime Complaint Center run by the FBI and the National White Collar Crime Center. Recipients are also encouraged to report these incidents; that can be done online at www.ic3.org.

If you think you have received a phishing e-mail but are not certain, you may contact the **Member Services and Loans at 1-800-285-3286**; or by secure e-mail MemberServies@ThePartnershipFCU.com.

For information about the complaint-filing process at IC3, go to www.ic3.gov/faq

If you have given out your credit, debit or ATM card information:

- Report the incident to the card issuer **immediately**
- Cancel your account and open a new one
- Review billing statements carefully after the incident
- If the statements show unauthorized charges, send a letter to the card issuer via regular mail (keep a copy) describing each questionable charge

Credit Card Loss or Fraudulent Charges: Your maximum liability under federal law for unauthorized use of your credit card is $50 (policies vary). If the loss involves your credit card number, but not the card itself, you have no liability for unauthorized use; in general, you may only be liable for a very small amount but always check with your individual card company for their exact policy.

Your liability depends on how quickly the loss is reported. You risk unlimited loss by failing to report an unauthorized transfer within 60 days after your bank statement containing unauthorized use is mailed to you.

If you have given out your bank account information:

- Report the theft to the bank as quickly as possible
- Cancel your account and open a new one

If you have downloaded a virus or 'Trojan Horse':

- Some phishing attacks use viruses and/or a 'Trojan Horse' to install programs called "key loggers" on your computer. These programs capture and distribute any information you type to the phisher, including credit card numbers, usernames and passwords, Social Security Numbers, etc.
- If this occurs, you likely may not be aware.
- To minimize this risk, you should:
    - Install and/or update anti-virus and personal firewall software
    - Update all virus definitions and run a full scan
    - If your system still appears compromised, fix it and then change your password again.

Check your other accounts - suspects may have accessed different accounts: eBay account, PayPal, your email ISP, online bank accounts, and other e-commerce accounts.

If you have given out your personal identification information:

Identity theft occurs when someone uses your personal information such as your name, Social Security number, credit card number or other identifying information, without your permission to commit fraud or other crimes. If you have given this information to a phisher, you should do the following:

Report the theft to the three major credit reporting agencies, Experian, Equifax and TransUnion Corporation, and do the following:

- Request that they place a fraud alert and a victim's statement in your file
- Request a FREE copy of your credit report to check whether any accounts were opened without your consent
- Request that the agencies remove inquiries and/or fraudulent accounts stemming from the theft

Notify your credit union and/or bank(s) and ask them to flag your account and contact you regarding any unusual activity: If bank accounts were set up without your consent, close them; If your ATM card was stolen, get a new card, account number and PIN; Contact your local police department to file a criminal report; Contact the Social Security Administration's Fraud Hotline to report the unauthorized use of your personal identification information; Notify the Department of Motor Vehicles of your identity theft; Check to see whether an unauthorized license number has been issued in your name; Notify the passport office to watch for anyone ordering a passport in your name; File a complaint with the Federal Trade Commission; Ask for a free copy of "ID Theft: When Bad Things Happen in Your Good Name"; File a complaint with the Internet Crime Complaint Center(IC3) by visiting their website: www.ic3.gov/faq.

For victims of Internet fraud, IC3 provides a convenient and easy reporting mechanism that alerts authorities of suspected criminal or civil violations.

Document the names and phone numbers of everyone you speak with regarding the incident. Follow-up your phone calls with letters. Keep copies of all correspondence.

If you see a suspicious-looking email message claiming to be from The Partnership FCU please let us know. We continually monitor such reports and act on them promptly. Additionally, also consider contacting Internet Crime Complaint Center at www.ic3.gov/faq.

Useful Links Internet/E-mail Fraud Alert

- Internet Crime Complaint Center - www.ic3.org
- Internet Crime Complaint Center FAQs - www.ic3.gov/faq

Major Credit Bureaus

- Equifax - www.equifax.com
- Experian - www.experian.com
- Trans Union - www.transunion.com

Identity Theft Resources

- http://www.consumer.gov/idtheft
- http://www.identity-theft-help.us
- http://www.identitytheft.org
- http://www.usdoj.gov/criminal/fraud
- http://www.ftc.gov/bcp