CONSUMER INTERNET BANKING EDUCATION

Purpose: The Purpose of the Peoples Bank Retail/Consumer Internet Banking Awareness and Education is to ensure that our Internet Banking clients are aware of potential risks using Internet Banking. The information provided will remind clients about the importance of security measures that can protect them from being victims of fraud. Specifically, this information will address the importance of password security, using unique user accounts, and ensuring their computer systems that are used for Internet Banking have security software, such as firewalls and updated anti-virus protection. The information provided will also include education about security threats, provide information to help them increase and maintain password security by enforcing a strong password requirement, and periodic password changes. At Peoples Bank, we strongly believe that public awareness of Internet Banking risks and how to avoid them is the strongest weapon in the defense against monetary losses.

Regulation E: Electronic Fund Transfers

This law is designed to protect consumers making electronic fund transfers. The term "electronic fund transfer: (EFT) generally refers to a transaction initiated through an electronic terminal, telephone, computer, or magnetic tape that instructs a financial institution either to credit or debit a consumer's asset account. The Electronic Fund Transfer Act (also known as Regulation E), which was issued by the Board of Governors of the Federal Reserve System and adopted in 1978 as an add-on to the Consumer Credit Protection Act. The law and regulation established the basic rights, liabilities and responsibilities of consumers who use electronic fund transfer services and of financial institutions that offer these services. The following describes some examples of what is covered and not covered under Regulation E:

What is covered?

Any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instruction, or authorizing a financial institution to debit or credit a consumer's account. The term includes, but is not limited to:

- Point-of-sales;
- Transfers initiated by telephone;
- Automated teller machine transfers;
- Direct deposits or withdrawals of funds;
- Transfers resulting from debit card transactions, whether or not initiated through an electronic terminal;
- Electronic check conversion, whereby you may authorize a merchant or other payee to make a one-time electronic payment from your checking account using information from your check to pay for purchases or pay bills; and
- Electronic returned check charge, whereby you authorize a merchant or other payee to initiate an electronic fund transfer to collect a charge in the event a check is returned for insufficient funds.

What is not covered?

- Checks;
- Check guarantee or authorization;
- Securities and commodities transfers;
- Wire or other similar transfers through Fedwire;
- Automatic transfers by account-holding institutions
- Any preauthorized transfer to or from an account if the assets of the account-holding financial institution were $100 million or less on the preceding December 31
- Telephone-initiated transfers
  Any transfer of funds that:
- Is initiated by a telephone communication between a consumer and a financial institution making the transfer; and
- Does not take place under a telephone bill-payment or other written plan in which periodic or recurring transfers are contemplated.

Please Note: When a banking account is opened, all retail/consumer clients receive a Regulation E Disclosure, as required by the EFT Act, which will contain detailed information related to the regulation.

Unsolicited Client Contact:

Peoples Bank will never contact our retail/consumer clients on an unsolicited basis to request their security logon information. If you receive a request of this type, do not respond to it. Please call us immediately at 601-847-9333 or email us at askus@peoplesbank-ms.com to report any activity of this nature. If you receive any unsolicited contact from a Peoples Bank team member, your identity will be confirmed through a series of security questions.

Securing Your Environment:

It's important to keep your identity from being stolen by someone who can potentially harm your good name and financial wellbeing. Identity theft occurs when someone uses your name, address, Social Security Number, credit card or financial account numbers, passwords, and other personal information without your knowledge to commit fraud or other crimes. While the words may sound like foreign language – Phishing, Pharming, Vishing, Spyware, and Dumpster Diving – are the names of various techniques used by thieves to put your identity and finances at risk. These types of attacks grow more frequent and sophisticated every year.

Email Risk:

Phishing is an email scam that is used to steal your personal information. You may receive an email in your inbox claiming to be from your financial institution, credit card company, or another source. It may appear authentic but be careful, any email requesting personal information or asking you to "verify" account information is usually a scam. DO NOT respond to this type of email and DO NOT click on any link from this type of email.

Peoples Bank

CONSUMER INTERNET BANKING EDUCATION

How to spot a Phishing and other email scams:

- Any email requesting personal information, or asking you to verify an account, is usually a scam, even if it looks authentic.
- The email may instruct you to click on a link, or call a phone number to update your account, or even claim a prize.
- The message will often threaten a dire consequence if you don't respond immediately, such as closing your account.

In order to avoid email scams, we suggest the following steps:

- Never respond to any email asking for confidential information, even if it appears urgent.
- Never click on a link from an email. Instead, type the known Website address for your bank or financial institution into your Internet Browser.
- Do not call any phone number provided in a suspicious email. It could be a fake phone number.
- Always use anti-virus and anti-spyware on your computer and keep them up-to-date.

Remember, email is not a secure form of communication. So, feel free to use your email, but do not use it to send or receive confidential information such as account information, social security numbers, etc.

Internet Risks:

There are several types of malware, which means malicious software, that can infect your computer as you surf the web. Some of these include:

- Spyware
- Trojan Horses
- Viruses
- Keystroke Loggers

These programs are becoming more sophisticated and ingenious in their ability to infect your computer. Many are designed to steal your personal information. While "surfing" the Internet, follow the steps below to protect your computer from the majority of Internet crime:

- Keep your computer operating system up to date, and your firewall turned on.
- Make sure you have an anti-virus and anti-spyware installed on your computer, keep them up-to-date, and run a full system scan at least once a week.
- Use strong passwords for secure sites. These should include at least eight or more characters with random numbers and upper and lower case letters. It is also recommended to change your passwords every six months.
- Watch for signs of spyware-frequent pop up ads, unexpected icons on your desktop, random error messages or sluggish computer performance are all signs of infection.
- Be careful when using public computers to perform any type of personal transactions. Just logging into a Website may give away passwords and other private information if spyware has been installed on that computer.

CONSUMER INTERNET BANKING EDUCATION

Telephone Risk:

The telephone is one of the most used sources for criminal activity. Here's how it works. First, your phone rings and the caller claims to be from another financial institution or any other source. They begin asking questions about you and your account. This could be a telephone scam called Vishing. Someone is attempting to steal your identity, and it happens to millions of Americans every year. To better protect yourself from this type of scam, follow these simple steps:

- Never offer personal or account information over the phone without verifying the caller's identity.
- If you are uncertain of the identity of a caller, hang up and initiate the call yourself using a known phone number.
- Do not call any phone number received in a voice message or email asking for personal information. It could lead you to a phony answering system.
- As a general guideline, be highly suspicious anytime you are requested to provide personal information over the phone.

Payment Risk:

Payment fraud happens when someone uses information from your checks, credit and debit cards, or any other form of payment, without your knowledge, to commit fraud. Following these steps will help make it harder for criminals to steal your personal information:

- Keep all checks, credit cards, and debit cards in a safe place.
- Don't leave outgoing check or paid bills in your mailbox, and report lost or stolen items immediately.
- Balance your checkbook and verify all account and credit card statements as soon as they arrive.
- Don't write PIN numbers on your credit or debit cards, or leave them in your wallet for a thief to find.
- Make online purchases only from trusted Web sites. If you have questions about a company, you can check them out on the Better Business Bureau.
- Consider paying all your bills electronically with online bill pay. This method is considered more secure than mailing paper checks.
- Use a paper shredder to securely dispose of any documents containing personal information.

Home Risks:

The simple act of sending and receiving mail and putting your trash out at night can put your personal information at risk. Financial information, checks, account and credit card statements, and monthly bills can be stolen from your home, mailbox, or even from your trash, and used to access your accounts and steal your identity. By following these steps, you are on the right track to protecting your identity:

- Invest in a personal shredder. This if the first line of defense. Shred checking account statements, credit card statements, cancelled checks, pre-approved credit card offers, and any type of documentation that has any personal information on it before disposal.

CONSUMER INTERNET BANKING EDUCATION

- Place your garbage out on the morning pickup rather than the night before. This gives "dumpster divers" less opportunity to go through your trash.
- Install a mailbox with a locking mechanism, or pick up your mail immediately after it has been delivered each day.
- Always place out-going mail in an official, secure mailbox.
- Store your mail, account statements, and other papers where they are out of sight and out of reach of anyone who might be in your home.

Detect Unauthorized Activity:

- Contact your bank, credit card company, or merchant immediately if your wallet, checkbook, credit/debit cards are lost or stolen or if you have not received any statements, invoices, or new or renewed debit/credit cards.
- Monitor all credit card and banking account activity on a regular basis. Check account balances as often as possible through the phone, ATM, or Internet.
- Review your credit information regularly. Free reports are available at www.annualcreditreport.com or by calling 1.877.322.8228.
- Use telephone alerts, email, or mobile banking alerts to monitor transfers, low balances, withdrawals, and payments.

If you think you have fallen victim to fraud, please act immediately:

- Notify all your financial providers.
- Close any accounts affected immediately.
- Place an "Alert" at all three credit bureaus (Equifax, Experian, and TransUnion).
- File a report with your local police where the identity theft took place. Also, get a copy of the police report for your records.

We have provided contact information for Peoples Bank along with the contact information pertaining to three credit bureaus for your convenience.

Peoples Bank Internet Banking Department:
PO Box 7
Mendenhall, MS 39114
601.847.9333
askus@peoplesbank-ms.com

Equifax
PO Box 740241
Atlanta, GA 30374
1.800.685.1111

Experian
PO Box 9556
Allen, TX 75013
1.888.397.3742

TransUnion
Trans Union Consumer Relations
PO Box 2000
Chester, PA 19022-2000
1.800.916.8800