Peoples Bank

BUSINESS INTERNET BANKING EDUCATION

Purpose: The purpose of the Peoples Bank Business/Commercial Clients Internet Banking Awareness and Education information is to ensure that our Internet Banking clients are aware of potential risks of 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.

Business/Commercial clients are not covered by Regulation E:

As a result, it is critical that business/commercial clients implement sound security practices within their places of business as outlined in this information to reduce the risk of fraud and unauthorized transactions from occurring.

Corporate Account Takeover is a form of identity theft in which criminals steal your valid online banking credentials. The attacks are usually stealthy and quiet. Malware introduced onto your systems may go undetected for weeks or months. Account-draining transfers using stolen credentials may happen at any time and may go unnoticed depending on the frequency of account monitoring efforts.

By practicing good business practices, you can protect your company:

- Use layered system security measures: Create layers of firewalls, anti-malware software and encryption. One layer of security might not be enough. Install robust anti-malware programs on every workstation and laptop. Keep the programs updated.
- Manage the security of online banking with a single, dedicated computer used exclusively for online banking and dash management. This computer should not be connected to your business network, should not retrieve any email messages, and should not be used for any online purpose except banking.
- Educate your employees about cybercrimes. Make sure your employees understand tht just on infected computer can lead to an account takeover. Make them very conscious of the risk, and teach them to ask the question: "Does this email or phone call make sense?" before they open attachments or provide information.
- Block access to unnecessary or high-risk websites. Prevent access to any website that features adult entertainment, online gaming, social networking and personal email. Such sites could inject malware into your network.
- Establish separate user accounts for every employee accessing financial information and limit administrative rights. Many malware programs require administrative rights to the workstation and network in order to steal

credentials. If your user permissions for online banking include administrative rights, do not use those credentials for day-to-day processing.

- Use approval tools in cash management to create dual control on payments. Requiring two people to issue a payment, one to set up the transaction and a second to approve the transaction. By doing this, it will double the chances of stopping a criminal from draining your account.
- Review or reconcile accounts online daily. The sooner you find suspicious transactions, the sooner the theft can be investigated.

Unsolicited Client Contact:

Peoples Bank will never contact our Business/Commercial 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. You will always have the option of hanging up and calling Peoples Bank to confirm that validity of your request.

Self-Assessment:

Internet Banking Business/Commercial clients are strongly encouraged to perform an annual Self-Assessment focusing on their internet banking practices and network security. A Self-Assessment will evaluate whether the client has implemented sound business practices to address the five key principles outlined in the "Securing Your Business" which include Take Stock, Scale Down, Lock It, Pitch It, and Plan Ahead.

Take Stock: Know the scope and nature of the sensitive information contained in your files and on your computers

- Talk with your employees and outside service providers to determine who sends sensitive information to your business, and how it is sent.
- Take inventory of all file storage and electronic equipment and where your company stores sensitive data.
- Consider all of the methods with which you collect sensitive information from customers, and what kind of information you collect.
- Review where you keep the information you collect, and who has access to it.

Scale Down: Keep only what you need for your business

- Use Social Security numbers only for required and lawful purposes. Don't use SSNs as employee identifiers or customer locators.
- Keep customer credit card information only if you have a business need for it.
- Review the forms you use to gather data, for example, credit applications and fill-in-the-blank web screens for potential customers and revise them to eliminate requests for information you don't need.
- Change the default settings on your software that reads customers' credit cards. Do not keep the information that you do not need.
- Truncate the account information on any electronically printed credit and debit card receipts that you give your customers. You may include no more than the last five digits of the card number, and you must delete the card's expiration date.
- Develop a written retention policy, especially if you must keep information for business reasons or to comply with the law.

Lock It: Protect the information that you keep

- Put documents and other materials containing sensitive information in a locked room or file cabinet.
- Remind employees to put files away, log off their computers, and lock their file cabinets and office doors at the end of the day.

- Implement appropriate access controls for your building.
- Encrypt sensitive information if you must send it over public networks.
- Regularly run up-to-date anti-virus and anti-spyware programs and individual computers.
- Require employees to use strong passwords.
- Caution employees against transmitting personal information via email.
- Create security policies for laptops used both within your office, and while traveling.
- Use a firewall to protect your computers and your network.
- Set “access controls” to allow only trusted employees with a legitimate business need to access the network.
- Monitor incoming Internet traffic for signs of security breaches.
- Check references and do background checks before hiring employees who will have access to sensitive data.
- Create procedures to ensure workers who leave your organization no longer have access to sensitive information.
- Educate employees about how to avoid Phishing and phone pre-texting scams.

Pitch It: Properly dispose of what you no longer need

- Create and implement information disposal practices.
- Dispose of paper records by shredding, burning, or pulverizing them.
- Defeat “dumpster diving” by encouraging your staff to separate the information that is safe to trash from sensitive data that needs to be discarded with care.
- Make shredders available throughout the workplace, including next to the photocopier.
- Use a “wipe” utility programs when disposing of old computers and portable storage devices.
- Give business travelers and employees who work from home a list of procedures for disposing of sensitive documents, old computers, and portable devices.

Plan Ahead: Create a plan for responding to security incidents

- Create a plan to respond to security incidents, and designate a response team led by a senior staff person(s).
- Draft contingency plans for how your business will respond to different kinds of security incidents. Some threats may come out of left field; others like a lost laptop or a hack attack, to name just two are unfortunate, but foreseeable.
- Investigate security incidents immediately.
- Create a list of who to notify, inside and outside you organization in the event of a security breach.
- Immediately disconnect a compromised computer from the internet.

Peoples Bank Contacts:

You are protected in a variety of ways when you use Internet Banking; however, it is important to contact us in the event your company’s internet banking access has been compromised. Also, notify Peoples Bank immediately of any unauthorized or unexpected transactions.

Your account is protected against fraudulent transactions in a number of ways, so monitor your account balances and transactions frequently. If you want to report suspicious activity in your account(s), or if you have questions about the security of your account(s), you can call us at 601.847.9333 or email us at askus@peoplesbank-ms.com.