Online Banking Safety and Tips to keep your information secure

Fraudsters are using increased sophistication to gain control of your account and transfer funds beyond the reach of any recovery. These schemes not only target individual consumers, but also target businesses hoping to transfer larger amounts and mask their fraudulent transfers with the normal business activity.

Threats

Phishing
There is a type of Internet piracy called "phishing." It's pronounced "fishing," and that's exactly what these thieves are doing: "fishing" for your personal information. What they want are account numbers, passwords, Social Security numbers, and other confidential information that they can use to loot your bank account or run up bills on your credit cards.

In a typical case, you'll receive an email that appears to come from a reputable company that you recognize and do business with. In some cases, the email may appear to come from a government agency.

The email will probably warn you of a serious problem that requires your immediate attention. It may use phrases, such as "Immediate attention required," or "Please contact us immediately about your account." The email will then encourage you to click on a button to go to the institution's website. Often the email will include a link or attachment that could lead to a malicious website or attempt to install software to your computer.

In a phishing scam, you could be redirected to a phony website that may look exactly like the real thing. Sometimes, in fact, it may be the company's actual website. In those cases, a pop-up window will quickly appear for the purpose of harvesting your financial information. In either case, you may be asked to update your account information such as your Social Security number, account number, or password. It may also ask you to provide information for verification purposes such as your mother's maiden name or your place of birth.

If you suspect an email to be a phishing scam, do not click on any links or attachments and delete the email immediately. You can also contact the source of the email to verify its authenticity.

Malware
Short for malicious software, malware consists of software that is designed to gather information that leads to loss of privacy or that gains unauthorized access to system resources. Malware includes computer viruses and is sometimes referred to as worms, Trojan horses, spyware, and other malicious and unwanted software or program.

Malware can be installed without detection on your PC by simply visiting an infected website, banner, or email link or attachment.

You may have malware on your computer if you notice more pop-up windows appearing, software on your desktop that you did not install, your computer slows down, or websites do not load properly. If you believe your computer may be infected, an anti-virus scan or anti-malware scan should be run to remove the unwanted software from your system.

Pharming/Spoofing
Similar to phishing, pharming redirects to a fake/phony website address that looks very legitimate or exactly like the website you intended to visit. The purpose of this fake website is to obtain personal information or install software to your computer.

Pay close attention to the website in your browser's address bar to ensure it is spelled properly and that it is the website you intended to visit. If a pop-up window appears or you see the website load and then quickly refresh to a different website, you may have been redirected to a spoofed website. Close the website immediately and run an anti-virus or anti-malware scan to ensure your computer is not infected with illegitimate software.

Keylogging
Keylogging is malware software that records keystrokes entered on your PC and transfers stolen information such as your login ID, password, and challenge question answers to a fraudster over the Internet. This information can enable fraudsters to log into your account and transfer funds to accounts controlled by the fraudster. This can be done through bill pay service, ACH transactions, or even a wire request.

Keyloggers can be installed like any other malware, but also can be installed by a hardware device plugged into your PC which stores the information for later use.

Man-in-the middle (MIM)
In a MIM attack, the fraudster, using sophisticated malware, inserts themselves between you and your banking service over the Internet and hijacks the online banking session. The fraudster can steal your information used to sign on to your Internet banking and log into your account or change and insert additional data into your transactions for the purpose of transferring funds to the fraudster's account. The fraudster conceals their actions by directing you to a fraudulent website that is a mirror image of the financial institution.

Your information can also be stolen if your computer or mobile browser is Wi-Fi enabled, and not using protected access or you are using a public channel.

How to Protect Yourself

If you are suspicious of any contact you receive, do not respond. If you want to contact the sender, you should initiate the contact through a channel that you have verified, such as a publicly known website or telephone number.

Do not be intimidated by an email or caller who suggests dire consequences if you do not immediately provide or verify financial information.

Maintain virus protection and anti-malware software on any computer or mobile device

connected to the Internet to provide a defense against malware, keyloggers and MIM attacks.

Never click on the link provided in an email you believe is fraudulent. It may contain a virus that can contaminate your computer. To verify a link in an email, hover your cursor over the link to display the URL it is directing to.

Always install current updates for your computer or mobile device operating system, as well as your mobile device applications.

Properly log off and disconnect from the Internet when not in use.

Always keep your computer or mobile device physically secure and never store password or other access data on the device.

Before you upgrade or recycle your computer or mobile device, delete all personal or business details.

Never provide your personal information in response to an unsolicited request, whether it is over the phone or over the Internet. If you did not initiate the communication, you should not provide any information. If JTNB was to contact you about suspicious transactions, we would be providing the transaction information, and only for the purpose of verifying that you authorized it. We would not ask you to provide information.

If you believe a contact from Jim Thorpe Neighborhood Bank is suspicious, contact us immediately at 570-325-3400

Review account activity regularly to ensure all charges are correct. If your account statement is late in arriving, call us at 570-325-3400 to find out why. Use your Online Banking service to review your account more frequently and catch suspicious activity.

You can learn more about safe, secure, and responsible online use by visiting www.OnGuardOnline.gov.

Protection Information

Jim Thorpe Neighborhood Bank will never make an unsolicited request through email, our website over the phone or by text message for any personal information such as:

- Account Number
- Social Security or Tax ID Number
- Date of Birth
- Credit or Debit Card Numbers
- PIN Information
- Expiration Dates or Security Codes on Credit or Debit Cards
- Any other Sensitive Financial or Personal Information

If you get a request for this information, **DO NOT GIVE OUT YOUR PRIVATE INFORMATION**. If you have any questions call us at (570)325-3400.

What to do if you fall victim:

Alert us by calling 570-325-3400

If you have disclosed sensitive information in a phishing attack, you should also contact one of the three major credit bureaus and discuss whether you need to place a fraud alert on your file, which will help prevent thieves from opening a new account in your name. Here is the contact information for each bureau's fraud division:

Equifax (www.equifax.com)
888-766-0008

Experian (www.experian.com)
888-397-3742

TransUnion (www.transunion.com)
800-680-7289

Consumer Protections Provided for Electronic Funds Transfers (EFT)

The Federal Government has established rights and responsibilities for certain EFTs initiated by a consumer through an electronic terminal, including a computer, under a law known as the Electronic Funds Transfer Act implemented by Regulation E. To limit your liability under the law for unauthorized transaction, you must notify us promptly of suspicious activity, but no later than 60 days after we send the first statement on which a problem or error appears. Refer to the EFT disclosure given to you at account opening, or visit your local Jim Thorpe Neighborhood Bank office for additional information.

Risk Assessment
The Federal protections afforded to consumers for electronic funds transfers do not apply to business accounts. Additionally, business accounts can be more susceptible to frauds because of the higher volume and higher dollar value of transactions. Therefore, in addition to the protection measures previously mentioned, it is suggested that commercial customers perform a risk assessment and control evaluations of their online functions. Consider the following factors:

- Internal and external threat environment such as recent publicized security breaches, identity theft, or fraud, and the threats described above.
- Changes in your operation, especially the use of electronic transactions service, such as Online Banking, ACH origination, and other Internet services.
- Changes in staffing, such as the amount of turnover; and staff procedures related to downloading information from the Internet or handling unsolicited requests for information.

- Dual control procedures for critical transaction, such as transfers to a third party.
- Physical security over computer equipment, passwords, keys, and other access devices or security information.
- How frequently banking transactions or account balances are verified for accuracy.