

Security Alert

Account Hijacking of Corporate Customers

There has been a shift in the online criminal world from primarily targeting individuals to increased targeting of corporations. In the past six months financial institutions, security companies, the media and law enforcement agencies are all reporting a significant increase in funds transfer fraud involving the exploitation of valid online banking credentials belonging to small and medium sized businesses.

Given the above, TIB Bank is encouraging all TIBLINK Plus customers to increase their focus on security. Below you will find information that will assist you in protecting your account data.

TIB Bank provided Fraud Service

Positive Pay/Check Guard will allow you to upload your issued checks to us and we will compare your list to what has been paid against your account. You will be alerted via email when there is an exception item for you to review.

Prudent internal controls to protect your data

- Utilize Positive Pay/Check Guard
- Reconcile your account(s) daily
- ACH and Wire Transfers should be handled under dual control. One individual to initiate the transaction and one to approve.

Best practices to secure computer systems

- Install commercial anti-virus and desktop firewall software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.
- Ensure that virus protection and security software are updated regularly.
- Install spyware detection programs.
- Install a dedicated, actively managed firewall, especially if you have broadband or dedicated connection to the Internet, such as DSL or cable. A firewall limits the potential for unauthorized access to a network and computers.
- Be suspicious of emails purporting to be from a financial institution, government department or other agency requesting account information, account verification or banking access credentials such as usernames, passwords, PIN codes and similar information. Opening file attachments or clicking on web links in suspicious emails could expose the system to malicious code that could hijack your computer.

- Create a strong password with at least 8 characters that includes a combination of mixed case letters, numbers and special characters.
- Prohibit the use of “shared” usernames and passwords for online banking systems.
- Use a different password for each website that is accessed.
- Change the passwords a few times each year.
- Never share your username and password information for Online Services with third-party providers.
- Limit administrative rights on users’ workstations to help prevent the inadvertent downloading of malware or other viruses.
- Ensure computers are patched regularly, particularly operating systems and key applications, with security patches. It may be possible to sign up for automatic updates for the operating system and many applications.
- We recommend that you clear your browser cache before accessing TIBLINK in order to eliminate copies of web pages that have been stored on the hard drive.
- Verify that you are on a secure session (https not http) in the browser for all online banking.
- Avoid using an automatic login feature that saves usernames and passwords for online banking.
- Never leave a computer unattended while using any online banking or investing service.
- Never access bank, brokerage or other financial services information at an Internet Café, public library, etc. Unauthorized software may have been installed to trap account number and login information.