# Best Practices for Business Online Banking

FIRST BANK
The one who's here.

Just as you protect your business's physical location from intruders, your business's computers must also be protected. Business computer hacking has quickly gone from a growing threat to becoming a very common activity.

Business customers are contractually obligated to maintain the security of their computers and must monitor their accounts proactively and frequently. This means that you will be responsible for any fraudulent financial activity on your account if your business's computers or accounts are compromised.

The tips below provide information and security measures you can take to help protect your accounts from scams and other harmful attacks. Please be sure that all employees who participate in online banking are aware of these tips.

## Use a dedicated PC for your banking purposes

Criminals are writing malware to create fraudulent transactions and/or to steal your online credentials. Infecting a computer is much easier if that computer is regularly connected to the internet or used for email. It is recommended that banking customers carry out all online banking activities from a stand-alone, hardened and completely locked down computer system from which email and web browsing are not possible.

## Passwords

- Use strong, complex passwords that contain:
  - Alpha/numeric characters and symbols
  - Upper and lower case characters
  - Minimum of 8 characters (but longer is recommended)
  - No real words or names of family/friends/pets
  - Use the entire keyboard; avoid strings of identical characters
- Do not use the same password for banking that you use for other online accounts
- Change your passwords regularly
- Never reveal your confidential login ID, password, PIN, or answers to questions to anyone
- Never reveal your confidential login ID, password, PIN, or answers to questions by email
- We will never call or email you asking for your login ID or password. If you are contacted, do not respond to the request and contact us immediately
- Never bank online using computers at kiosks, airports, hotels, public libraries, cafes, unsecured computers or unsecured wireless networks. Unauthorized software may have been installed to trap account number and sign on information leaving you vulnerable to possible fraud
- Use only company computers. When accessing online business accounts, only use designated company computers that use the company network. Non-business computers and networks are more likely to be infected with malware
- Prohibit the use of shared user names and passwords for your online banking accounts
- Keep your password safe. Don't leave it in a file on your computer or on a note on your computer
- Contact us immediately if you suspect someone else has been in your internet banking account
- Delete online user IDs as part of the exit procedure when employees leave your company

## Computer

- The dedicated business computer should not be used for email, social media, or web browsing
- Restrict administrative rights on your computers
- The computer should be physically secured
- Install a firewall between your computers and the internet
- Keep your operating system, browser, and email patches up to date
- Anti-virus, anti-spyware, and anti-malware software should be active and up to date. Scan your computers regularly.
- Wireless connections must have strong password protection

## Login/Logout

To access your business online banking, procedures should include:

- Do not select the option to remember your password at log in
- Clearing the browser cache before starting an online banking session to eliminate copies of web pages that have been stored on the hard drive
- Boot the computer and do not open other applications or additional browser windows before initiating or using your business online banking
- Access the First Bank web site by typing the URL directly into the address bar rather than clicking links you might see in an email or an instant message, or on another web site.
- Look for anything unfamiliar, unprofessional, or out of place on the website. If you see anything different, call us and do not use the website
- Be sure the website URL is preceded by "HTTPS" indicating an encrypted communication
- Check for the browser "lock" icon, but understand that this only signifies a secure communication channel, not necessarily a legitimate website.
- When you are finished with your online banking, use the Logout option. This completely logs you out, avoiding any potential unauthorized use. When stepping away from your computer use the Logout option as well, our system will time out after a period, but not immediately.

## Transactions and Monitoring

- Only allow specialized and trained key staff members to process ACH and Wire transactions
- Establish transaction dollar limits for employees that vary by authority levels
- Business owners/managers should verify daily activity

## Online Banking Administrator Created Users

*(for more details see the Administrator's Training Manual)*

- Online banking administrators should carefully consider the level of access given to each online banking administrator created user.
- With the highest level of settings given, administrator created users could have the ability to transfer money from account to account, create and make bill payments, and/or create, approve and release Wires and ACH batches giving administrator created users significant access to the organization's funds.
- With the proper roles assigned to the different trusted administrator created users, administrators can help reduce the level of risk of fraudulent activity for the organization's online and mobile banking.

## Business Bill Pay and Administrator Created Users

*(for more details see the Administrator's Training Manual)*

- With bill payments from Business Bill Pay, Online Banking administrators should create and setup Bill Pay administrator created users with careful consideration.
- With the highest access level assigned, a Bill Pay administrator created user has the ability to create and approve bill payments on their own accord.
- When setting up a new administrator created user, carefully, assign appropriate level of access to each created administrator created user.

## Dual Control

**Dual User Administration**

- One individual performs the maintenance
- A second individual must approve it before the change is effective

**Dual Transaction Control**

- One individual initiates a transaction
- A second individual must approve the transaction before it is processed
    - Requiring two individuals to execute transactions can prevent fraudulent activity even if one employee's computer is compromised

## General Financial Management

- All businesses should perform periodic account reviews that are independent of the account's authorized signer(s). Such reviews are needed to reduce the risk of embezzlement and to verify the validity of the actual transactions being processed
- Dual control account reconciliation: One person can make deposits and write checks and another reconciles the account
- If you see something suspicious regarding your accounts contact the bank immediately

## Customer Support —ELECTRONIC BANKING 907.228.4446

Contact customer support immediately if you experience any of the following scenarios:

- If you notice a wire, ACH or bill pay transaction that you did not initiate
- If you receive a notice regarding a change of password or email address that you did not create
- If the log in screen looks different or has unusual fields or prompts
- If you see unknown transactions or balance inconsistencies on your account
- If you receive a message saying online banking is unavailable due to maintenance or another reason after you just logged in
- If you log on to First Bank's online banking and are immediately logged off, your account is locked for no apparent reason, or your computer freezes

**Phishing** is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

**Pharming** is a hacker's attack aiming to redirect a website's traffic to another, bogus website. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software.

**Malware**, short for malicious software, is software designed to secretly access a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. Malware includes computer viruses, worms, Trojan horses, spyware, dishonest adware, scareware, crimeware, most rootkits, and other malicious and unwanted software or program.

**Keystroke logging** (often called **keylogging**) is the action of tracking (or logging) the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored.

**Spyware** is a type of malware that can be installed on computers and collects little bits of information at a time about users without their knowledge. The presence of spyware is typically hidden from the user, and can be difficult to detect. Typically, spyware is secretly installed on the user's personal computer. Sometimes, however, spywares such as keyloggers are installed by the owner of a shared, corporate, or public computer on purpose in order to secretly monitor other users.

A **Trojan horse**, or **Trojan**, is malware that appears to perform a desirable function for the user prior to run or install but instead facilitates unauthorized access of the user's computer system. It's a harmful piece of software that looks legitimate. Users are typically tricked into loading and executing it on their systems

A **computer worm** is a self-replicating malware computer program. It uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. This is due to security shortcomings on the target computer. Unlike a virus, it does not need to attach itself to an existing program.

A **computer virus** is a computer program that can copy itself and infect a computer. The term "virus" is also commonly but erroneously used to refer to other types of malware, including but not limited to adware and spyware programs that do not have the reproductive ability. A true virus can spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance because a user sent it over a network or the Internet, or carried it on a removable medium such as a floppy disk, CD, DVD, or USB drive. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer.

**Adware**, or **advertising-supported software**, is any software package which automatically plays, displays, or downloads advertisements to a computer. These advertisements can be in the form of a pop-up. The object of the Adware is to generate revenue for its author. Adware, by itself, is harmless; however, some adware may come with integrated spyware such as keyloggers and other privacy-invasive software.