

Your Security:

It's a top priority!



Online Precautionary Checklist for WSFS Online Banking Customers

It's important that you take the proper precautions to protect you and your business. Use this as a checklist to verify that you have the proper controls in place to protect your computer system. You should try to review this information on a regular basis.



Best practices for online banking and steps to help protect your computer:

- Access the online banking website by typing the URL www.wsfsbank.com into the address bar, rather than any link embedded in an email.
- Always check the browser for a "lock" icon. It is important to understand that the lock signifies a secure communication channel to a website; however it does not indicate a legitimate website.
- Reconcile your accounts daily. Strong account oversight is essential in today's ever changing technological environment.
 - NACHA Rules (National Automated Clearing House Association) allows businesses only 2 banking days to notify the bank of unauthorized ACH debits
- When logging into Online Banking be sure to check for your personalized image. This image indicates that you are performing Online Banking on a legitimate website which has confirmed your identity.
- Check for anything that looks unfamiliar, unprofessional or out of place to you.
- Avoid accessing online banking or making purchases at wireless hot spots, Internet cafés and public Internet access points.

Keep your firewall turned on

A big part of staying safe online is paying attention, applying common sense and learning to recognize and avoid spam scams and phishing.

Your firewall operates as a kind of security checkpoint that information must pass through before it can enter or leave your computer.

Your firewall also helps to prevent software on your computer from accepting unauthorized updates or changes sent over the Internet.

- Make sure your firewall is always turned on.

Keep your software updated

One of the most important things you can do to help protect your computer is also one of the easiest: keep your operating system and other software up-to-date.

- Hackers work tirelessly to exploit weaknesses in software, and new security threats emerge every day. That's why software companies work even harder to help keep your computer safe with updates, and it's why you should install updates.

Use up-to-date antivirus software

Antivirus programs scan everything that goes into your computer—including email, discs, and data files—searching for thousands of known viruses.

- Antivirus software requires regular signature updates to help protect against emerging threats. Installing antivirus software without updating it is like buying home insurance but not making the payments. Keep your antivirus software current by subscribing to an antivirus service and automatically downloading the latest updates.

Use up-to-date antispyware software

Antispyware programs monitor your computer, looking for known spyware and watching for programs that try to install themselves without your knowledge or permission.

When antispyware programs find something, they warn you and help you take action against the spyware.

- As with antivirus software, keep your antispyware software current, and automatically download the latest updates.

Continued on next page...

Think before you click

Clicking the wrong link or attachment can expose your computer to spyware, a virus or ads that could clutter your screen and slow your computer.



- Be very cautious with attachments or links in email or instant messages. If you know the sender, but the message looks suspicious, check before you proceed. If they didn't send the message, delete the email or close the IM window.
- Think twice before you click pop-up windows or banner ads.
- Never click Agree, OK, or I accept to get rid of a pop-up ad, an unexpected warning, or even an offer to remove spyware. Instead, close the window by clicking X in the upper-right corner.
- Download software only from websites you trust. File-sharing programs, and sites that offer "free" music, movies, games and other information are notorious for including unwanted software in downloads.

Keep your password protected

- Use a strong password—at least eight characters, with a combination of numbers, letters and symbols.
- DO NOT use the same password for banking that you use for other online accounts.
- Keep your password safe—Don't leave your password stored in a file on your computer or written on paper.
- Change your password often. WSFS believes very strongly in your security and has invested in securing our website using tools such as Cyveillance to prevent customer phishing attempts. WSFS will not solicit you for passwords, account numbers or other personal information—if you receive an email or text message requesting such; call WSFS immediately using the number on your debit card or credit card, not the one in the email or text message.

Set up Alerts in Online Banking

- Customize alerts to automatically notify you when certain transactions are processed or when your balance reaches a certain level.

What to do if you suspect fraud:

- Immediately cease all activity from computer systems that may be compromised.
- Unplug the Ethernet or cable modem connections to isolate the system from remote access.
- Immediately contact WSFS Bank at 302-792-6044, so that the following actions may be taken as a priority to contain the incident:
 - Online access to the accounts be disabled
 - Online Banking passwords changed
 - New account(s) opened as appropriate
 - Request a WSFS customer service representative review all recent transactions and electronic authorizations on the account
 - Additionally, ensure that no one has requested an address change, title change, PIN change or ordered new cards, checks or other account documents be sent to another address

Back up your files

- No security method is completely foolproof. It's important to back up critical files regularly, before you get hit with a problem.

Additional Useful WSFS Services for Businesses:

Business Online Banking offers multiple user ID's, additional modules for ACH & wire transfers, secured transactions by tokens and the ability to download to Quickbooks.

Ask about our Fraud Protection Services to help protect your accounts: ACH Debit Block prevents ACH debits from being removed from your business account. Use the ACH Debit filtering capability to allow only designated ACH debits to be moved from your account; i.e.—payroll debits, insurance premiums or merchant services fees.

Positive Pay Service provides the means to identify and return fraudulent checks posting against your account.

For more information, please call 1-888-WSFSBANK.

Know the leading threats to the security of your computer:

Viruses—software programs designed to invade computers, and to copy, damage or delete data.

Worms—sophisticated viruses that can reproduce themselves and spread to other computers without your interaction.

Trojans—named for the Trojan horse, are viruses that pretend to be helpful programs while destroying your data, damaging your computer and stealing personal information.

Spyware—software that tracks your online activity. Spyware may bombard you with pop-up advertising, collect your personal information, or change the settings on your computer without your knowledge or consent.

Malware—short for malicious software, is software designed to infiltrate a computer system without the owner's consent. Malware includes all the above and dishonest adware, crime ware and other malicious and unwanted software. Its purpose is primarily to steal or modify confidential information for purposes of illegal profit.

Phishing—is the fraudulent process of attempting to acquire confidential information such as usernames, passwords, credit card numbers, account numbers, etc. by masquerading as a trustworthy website. Phishing is typically carried out by email or instant messaging, and it often directs users to enter confidential information at a fake website whose look and feel are almost identical to the legitimate one.

Text Phishing—The phishing attack begins with identity thieves sending you text messages that appear forwarded from your bank or credit card company. The messages state a breach in security of your bank account or credit card account and gives you a number to call. When you call this number, an automated system directs you to give your personal information for the sake of "security." This is a phishing scam; the thieves are collecting all of your personal information for immediate theft of your identity.

Helpful links:

www.antiphishing.org
www.sans.org



WSFSbank
We Stand For Service®

www.wsfsbank.com
1-888-WSFSBANK