

# Best Practices for Business PCs

## Keep PC up-to-date with the latest updates from Microsoft, Adobe, and Java

- Microsoft Update: <http://www.update.microsoft.com>
- Adobe: <http://www.adobe.com/downloads/>
- Java: <http://java.com/en/download/installed.jsp>

## Protect PC with anti-virus, anti-spyware, and anti-malware software

- Configure anti-virus, anti-spyware, and anti-malware software to update daily.
- Configure anti-virus to do a full system scan at least weekly and have it notify you if anything suspicious is found.

## Use supported operating systems and current security features when connecting to Online Banking.

- Older operating systems are no longer patched and are vulnerable to Windows attacks. These operating systems should not be used for online banking (XP, Vista, Win 7 & 8).
- Windows 10 has built-in security features and a robust firewall which should never be turned off.
- Windows 10 <https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963>

## It is highly recommended that businesses designate one PC for Business Online Banking and avoid browsing the Internet on that PC.

## Use caution with USB Flash Drives

- Never use an unknown Flash Drive.
- Hold the SHIFT key when inserting Flash Drive to prevent unwanted pop-ups.
- Use anti-virus to scan the Flash Drive (usually E: under "My Computer") before opening.

## Use caution with wireless networking

- Avoid wireless networks when doing Online Banking. A wired Ethernet connection is more secure.
- If using wireless at home/business make sure to use the WPA2 or WPA3 (newest) for WiFi security
- Make your security keys for WiFi protected access hard to guess for cyber criminals. Make the keys at least 16 characters with a mix of numbers, special characters, upper & lower case letters.
- Do not use hotspots or public accessible WiFi when doing Online Banking. If absolutely necessary use a VPN connection when connecting to these types of WiFi.

## Do not accidentally download malware

- If email is used on PC do not open attachments from unknown senders.
- Never click "Ok," "Agree," or "Accept" on any unexpected pop-up windows. If the pop-up will not let you exit, hold down CTRL+ALT+DELETE to bring up the Task Manager so that you can end the pop-up application.
- Beware of "free" downloads – only download from trusted/known sites.

## Always use strong passwords

- Passwords should be at least 10 characters in length and contain at least one number, one special character, and one capitalized letter if software allows them.
- Passwords should not be words that can be found in a dictionary. Example password12 is a weak password - P@ss1w0rd is a stronger password.
- See <https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb>

## See Microsoft's 6 rules for safer financial transactions online

- <https://support.microsoft.com/en-us/topic/making-safer-financial-transactions-online-d8e8972b-dc56-4ea2-aa72-12883d3bf0b4>

Computer threats outside the scope of American Bank & Trust Company's control can compromise security credentials. These threats include, but are not limited to: Adware, Backdoor Programs, Keystroke Loggers, Malware, Spyware, Trojans, and Viruses. If a device is infected with these unauthorized programs, it can lead to unlawful access to the system on which they reside. We recognize these threats and recommend that the computer equipment used to access ACH and Business Online Banking follow these guidelines.

- Keep your dedicated computer out of reach, or even better, under lock and key
- Set a strong password for the Administrator account
- Turn your dedicated computer off when not in use to help prevent network-based intrusions
- Keep the operating system and third party applications secure by applying patches and updates promptly
- Install a good-quality anti-virus suite and keep it updated
- Never use a wireless connection for online banking
- Use a strong password for your online banking account, and do not use that password anywhere else
- Sign up for a Security Newsletter to stay apprised of threats

The key is to use a secure, dedicated system. If you spot any unauthorized activity, or suspect your information has been compromised in any way, the Federal Trade Commission recommends you take the following actions:

- Notify your bank and credit card companies immediately
- Close all affected accounts
- Notify the major credit reporting agencies
- File a report with the Federal Trade Commission
- File a report with the police

P.O. BOX 1819  
OPELOUSAS, LA  
70571-1819  
(337) 948-3056

[www.americanbankandtrust.net](http://www.americanbankandtrust.net)

