bank fivenine

Online Banking Best Practices for Businesses

The best way to avoid becoming a victim of a cyberheist is not to let computer crooks into the computers you use to access your organization's bank accounts online. The surest way to do that is to maintain a clean computer: Start with a fresh install of the operating system and all available security updates, or adopt a "live CD" approach (explained in more detail below).

Use a dedicated system to access the bank's site. The dedicated machine should be restricted from visiting all but a handful of sites necessary to interact with the bank and manage the organization's finances. This can be done using custom firewall rules and hosts files, or services like OpenDNS. Remember that the dedicated system approach only works if you *only* access your bank's site from locked-down, dedicated machines. Making occasional exceptions undermines the whole purpose of this approach.

If possible, use something other than Microsoft Windows. Most malware only runs in a Microsoft Windows environment, so using a different operating system for the dedicated machine is an excellent way to drastically reduce the likelihood of becoming a cyberheist victim. A "live CD" is a free and relatively painless way to temporarily boot a Windows PC into a Linux environment. The beauty of this approach is that even if you fail to maintain a clean Windows PC, malicious software can't touch or eavesdrop on your banking session while you're booted into the Live CD installation. For more information on how to set up a live CD for a dedicated machine, see this primer.

If you must use a multi-purpose machine where you will check email, avoid clicking links in email (see previous tip). Also, set email to display without HTML formatting if possible.

If you installed it, patch it. Keep the operating system up-to-date with patches. It's equally important to update the third-party software on your system, especially browser plugins. One leading cause of malware infections are exploit kits, which are attack tools stitched into hacked websites that exploit unpatched or undocumented vulnerabilities in widely-used browser plugins. Tools such as File Hippo's Update Checker and Secunia's Personal Software Inspector will alert you to new security updates available for third-party programs installed on your PC.

Remove any unneeded software from dedicated systems used to access the bank's site. In particular, unneeded plugins (such as Java) should be junked.

Avoid opening attachments in email that you were not expecting. Be particularly wary of emails that warn of some dire consequence unless you take action immediately.

Use a bookmark to access the bank's site. Avoid "direct navigation," which involves manually typing the bank's address into a browser; a fat-fingered keystroke may send you to a look-alike phishing website or one that tries to foist malicious software.

Remember that antivirus software is no substitute for common sense. A majority of today's cyberheists begin with malware that is spread via email attachments. Many of these threats will go undetected by antivirus tools in the first few days.

If your financial institution offers it, consider taking advantage of ACH Positive Pay. Any item that meets the criteria you establish will automatically post to your account. Your company will be notified via email and/or text message of any rejected electronic item(s) that do not meet your filter criteria. Upon receipt of the rejected items, you can then return them or conveniently add filter criteria for future electronic transactions.

Require two people to sign off on every transaction. This fundamental anti-fraud technique can help block cyberheists (and employee fraud).

Article by Brian Krebs at https://krebsonsecurity.com