First Midwest Bank

Personal Computers and Networks
Information Security for Personal Banking Clients

Maintaining a Secure Personal Computer - What precautions can you take?

Your computer is part of a vast electronic information highway where data moves through complex networks, making our daily communications happen quickly and easily. With that convenience comes the need to protect that valuable and private information along the way. Although your business' information security needs may require very specific solutions, much of what we do every day on our laptops or desktops is protected by following some relatively simple steps.

- Use a modern operating sytem - The most recent Operating Systems (OS) provide substantial security enhancements over earlier operating sytems.
- Set the OS to check for and install updates automatically. Also keep your other peripheral devices, such as tablet computers and smart phones up-to-date as well.
  - Make sure you renew your subscription. There are many good products available that are inexpensive or free for non-business use, and some internet service providers also offer service and can provide set-up support.
- Install a comprehensive security suite that supports anti-virus, anti-spyware, anti-phishing, safe browsing, and firewall capabilities. Remember to enable any automated updated service within the suite.
- Limit use of the administrator account. The initial account that is typically created when configuring a computer for the first time is the local administrator account. This account should be used only to install updates or software, and reconfigure the computer as needed. Browsing the web or reading email should not be done using this account. A non-privileged "user" account should be created and used for these other day-to-day activities.
- Migrate to the most recent application versions and maintain updates as needed.
- If using third party web browsers, install script disabling software to prevent execution of scripts. Allow trusted sites to execute scripts as necessary.
- Use file or full disk encryption to protect laptops and other mobile devices. These computers are easily lost and stolen and encryption is the only reliable protective security measure if a criminal has your computer.
- Use a security cable to lock the laptop to furniture when in public. A laptop can be stolen in moments, especially at a school or library.

Maintaining a Secure Home Network - What precautions can you take?

- Use a separate personally-owned router with firewall capabilities to connect to the ISP provided router/cable modem. This gives you the control of routing and wireless capabilities and will block outsiders from accessing your network.
- Administration of the home network devices should be from the inside. Disable external remote administration functions.
- A wireless network should be protected using Wi-Fi Protected Access 2 (WPA2) instead of Wired Equivalent Privacy (WEP). WEP encryption can be broken by an attacker.
- Implement strong passwords on network devices. Choose a long, complex password (at least 15 characters) for your administrative login to your router and your WPA2 encryption key. Write them down in your device manual, as they will be needed to make future changes to the device.

Want to learn more about information security for your personal banking transactions? Visit firstmidwest.com/safe for the most current resources on a wide array of information security topics.