

Stay Secure: Best Practices for Safe Computing

Protect Yourself

New viruses routinely make headlines, as do incidents of electronic fraud and data theft. The costs, both in time and money, quickly escalate. To effectively protect your PC and sensitive information—both at home and work—know how malicious hackers and electronic criminals operate and how to protect yourself.

Physical Security

- Prevention of intrusions, viruses, spyware infestations, stolen data, and other security incidents begins with physical security.
- Log off systems when stepping away.
- Use screen saver password protection. To set screen saver protection:
 - Right-click the Windows desktop.
 - Select Properties.
 - Click the Screen Saver tab.
 - Ensure a screen saver is selected from the drop down menu.
 - Set the Wait period to five or six minutes.
 - Check the On Resume, Password Protect box.
 - Click Apply, then click OK.
- When traveling with laptops, handheld computers, a Blackberry, or even a data-enabled cell phone, such as a Treo, keep the unit in site at all times.

Passwords

- Account names and passwords are a powerful combination; guard them carefully.
- Never use passwords that are based on any form of the following:
 - Your name
 - Names of spouses, children or pets
 - Social security numbers
 - Anniversary or birth dates
 - Favorite sports teams
 - Words that can be found in a dictionary
- Always create complex passwords that contain both letters and numerals, and special characters (such as #, \$, %, &, *, and !) when possible.

Social Engineering

- Social engineering describes the nontechnical attacks reprobates undertake. These efforts rely upon sociability and people's natural inclination to help one another.
- Culprits try conning users into revealing their account names, passwords, and other information.
- Miscreants try tricking users into revealing sensitive data by posing as authorities or IT personnel.

Stay Secure: Best Practices for Safe Computing

- Criminals also rifle through trash seeking account data or try to see account names users type into PCs in public PCs or on telephones.
- Always be aware of your surroundings when working remotely in public locations; never provide sensitive account information over the telephone (even if you believe you're talking to a legitimate authority).

Phishing

- Phishing describes a con in which victims are tricked into revealing sensitive information.
 - The most common method utilizes fraudulent e-mail messages.
 - Messages appear legitimate:
 - often stating there's been trouble with an account and information must be confirmed.
 - often including actual organization's logo, which is actually only copyright infringement.
 - appearing to contain legitimate URL, which actually redirects, often to fake sites hosted overseas.
 - appearing to come from legitimate e-mail address, which is actually spoofed or forged.
 - Avoid Phishing scams by never providing sensitive, proprietary, confidential, account, password, or financial information in response to an e-mail or instant message.

Network Security

- Several layers of security protect networks, including:
 - Physical access
 - Valid accounts and passwords
 - Firewalls
- Organizations almost always deploy firewalls; consider protecting yourself with a software- or hardware-based firewall at home.

Remote Access

- Enabling remote access presents unique challenges.
 - Remote users must be authorized.
 - Communications between the organization's network and the authorized remote user must be secured.
- VPNs are the most common method of providing secure remote connections.
 - Other programs—such as GoToMyPC and pcAnywhere – offer remote connectivity options.
 - Never install such third-party applications without first contacting the IT department.
- IT department staff can provide assistance in establishing VPN connections.

Stay Secure: Best Practices for Safe Computing

Wireless Networks

- Wireless access points are appearing everywhere, from local coffee shops to bookstores.
- Most wireless networks are highly insecure.
 - Your network communications—including account, password, and other sensitive information—could easily be monitored by another patron or hacker.
 - Others may be able to access files on your PC.
 - Ensure File And Printer Sharing For Microsoft Networks is disabled when accessing public wireless networks:
 - Click Start, then select Control Panel.
 - Select Network Connections.
 - Select the wireless connection.
 - Click Properties from the connection's dialog box.
 - Highlight File And Printer Sharing For Microsoft Networks and deselect its checkbox.
 - Click OK.
- Always leverage WEP and WPA protection, when supported.
- Contact the IT department for further assistance when using work systems on wireless networks.

Encryption

- Encryption technologies, such as those used by VPNs, add an element of complexity that makes life more difficult for hackers.
- Encryption essentially jumbles the contents of files, messages, and communications.
- Without the proper cipher, or algorithmic key, recipients see only unintelligible gibberish.
- Windows Encrypted File System (EFS) enables encrypting files.
 - To encrypt files, first verify your system uses the NTFS file system by:
 - Clicking Start, then selecting All Programs.
 - Click Administrative Tools.
 - Click Computer Management.
 - Highlight Disk Management to reveal system information.
 - If the system doesn't use NTFS, contact an IT staff member for assistance.
 - To encrypt files:
 - Right-click files or folders containing sensitive information.
 - Select Properties from the pop-up menu.
 - Click the Advanced tab.
 - Check the box for Encrypt Contents To Secure Data.
 - Click OK.

Stay Secure: Best Practices for Safe Computing

Public Computers

- Public computers offer no security.
- Accessing e-mail or making purchases on public computers, such as those found in Internet cafes, airport kiosks, universities, and libraries, could result in others accessing your e-mail or making purchases using your accounts.
- Use public systems only for innocuous activities, such as:
 - Conducting general research
 - Viewing weather reports
 - Catching up on news
 - Checking flight information
- If you absolutely must use a public computer to access e-mail or make a purchase, be sure:
 - The browser's not set to record passwords and passwords are deleted:
 - In Internet Explorer, click Tools.
 - Click Internet Options.
 - Select the Content tab.
 - Click Autocomplete.
 - Verify the checkbox for User Names And Passwords On Forms under the Use AutoComplete For section is unchecked.
 - If the box has been checked and you entered passwords, click the Clear Forms and Clear Passwords buttons.
 - Click OK.
 - You flush the browser's cache:
 - In Internet Explorer, click Tools.
 - Click Internet Options.
 - On the General tab, click the Delete Files and Delete Cookies buttons in the Temporary Internet Files section.
 - You delete History settings:
 - In Internet Explorer, click Tools.
 - Click Internet Options.
 - On the General tab, click the Clear History button found in the History section.

Viruses and Spyware

- Don't click attachments that arrive in e-mail or instant messages.
- When you must receive files via e-mail, open them only after confirming you were expecting the file and verifying the file is virus free.
- Install only programs from trusted vendors at home; use only authorized programs at work.
- Always run antivirus and antispyware applications. Update antivirus and antispyware applications, and conduct full system scans, once a week.