Top Tips for Internet Safety at Work

1 Defend your computer

Keep all software current (including your Web browser) with automatic updates and install all security updates that your IT department recommends. Use antivirus, antispam, and antispyware software and activate your firewall.

2 Think before you share sensitive information

➤ Look for signs that a Web page is safe, before you enter sensitive personal or business data–a Web address with http**s** ("**s**" for secure) and a closed padlock (🔒) beside it.

➤ Never give sensitive info in response to an e-mail or instant message (IM) request.

3 Think before you click

➤ Pause before you open attachments or click links in e-mail or IM even if you know the sender; they could be phony. Confirm with the sender that the message is real or visit the official Web site by typing the address yourself.

➤ Be wary of clicking links or buttons in pop-up windows.

4 Use strong passwords

➤ Lock your online accounts, computer, phone, and other devices with passwords at least eight characters (longer is better), and include upper and lower case letters, numbers, and symbols.

➤ Keep passwords and PINs secret. Don't disclose them to coworkers or businesses (like an Internet café operator), or be tricked into giving them away.

➤ Don't use the same password everywhere.

5 Protect yourself from e-mail scams

Look out for alarmist messages, misspellings and grammatical errors, deals that sound too good to be true, requests for sensitive info like account numbers, and other signs of a scam. Turn on a filter that warns you of suspicious Web sites.

6 Protect your data on the go

➤ When you use public Wi-Fi, choose the most secure option, even if you have to pay for it. It could include password-protection and encryption.

➤ Confirm the exact spelling of the wireless network you're connecting to. Beware of clever (slightly misspelled) fakes.

➤ Encrypt the data on your laptop (or USB flash drive) in case you lose it or it's stolen.

➤ Guard your laptop, smartphone, and PDA as carefully as your wallet.

What To Do If There Are Problems

When using a Web service

When using e-mail, a social network, or other service, you may encounter scams, obscene material, or aggressive behavior, or theft of your account or identity.

➤ Report it to the service. For example, in Microsoft® services or software, look for a **Report Abuse** link as available, or send e-mail to **abuse@microsoft.com**.

➤ Report any misrepresentation of your organization to your IT department– for example, an e-mail phishing scam that pretended to be from your company.

Theft or loss of sensitive company information

If customer or other sensitive company data has been compromised because of theft or loss of a laptop, smartphone, or other mobile device, or because of a breach of network security:

➤ Report it immediately to your IT and security departments.

➤ Change all passwords used to log on to the device.

➤ For smartphones and PDAs, contact the service provider for help in wiping the data from the device.

More Helpful Info

➤ If you run a business without IT support, Microsoft can help you better defend company computers: **microsoft.com/protect/computer/default.mspx**.

➤ Look for thorough information on how to help protect your computer and your privacy at **microsoft.com/protect**.

➤ For other ideas about how to work more securely, visit: **microsoft.com/atwork/security/worksecure.aspx**.

➤ If your computer isn't running as expected (it's unusually slow or crashes frequently), it might have been damaged by malicious software like a virus or spyware. Microsoft can help you address this: **safety.live.com**.

➤ Learn more about how to secure your laptop when you're on the road: **microsoft.com/atwork/security/laptopsecurity.aspx**.

0809 PN 098-115260