Top Tips for Internet Security at Work

1 **Defend your computer**

   **Strengthen your computer’s defenses.** Keep all software (including your web browser) current with automatic updating (or follow the directions of IT staff). Install legitimate antivirus and antispyware software. Never turn off your firewall.

   **Don’t be tricked into downloading malicious software.** Stop and think before you open attachments or click links in unusual email, text, or instant messages (IM), on social networks, or in random pop-up windows. If you’re unsure if a message is legitimate—even from a coworker—contact the sender to confirm using a different device and another account.

2 **Protect company data and financial assets**

   > Don’t put confidential information in email, instant, or text messages; they may not be secure.

   > Beware of scams. Never give information like an account number or password in response to a phone call, or email or other online request.

   > For the most sensitive transactions—Automated Clearing House (ACH) payments, payroll, and the like—consider a dedicated computer not used for email or web browsing.

3 **Create strong passwords and keep them private**

   > Lock devices, company routers, and online accounts with strong passwords or PINs. Strong passwords are long phrases or sentences and mix capital and lowercase letters, numbers, and symbols.

   > Don’t disclose passwords or PINs to coworkers.

   > Use a unique password on each account or device containing personal or business data, and change them regularly.

4 **Guard company data when you’re on the go**

   **Treat all public Wi-Fi networks as a security risk.**

   > Choose the most secure option—it could include password-protection or encryption—even if you have to pay for it.

   > Confirm the exact spelling of the wireless network you’re connecting to—beware of clever (slightly misspelled) fakes, such as www.microsoft.com.

   > Encrypt all confidential data on smartphones, laptops, flash drives, and other portable devices in case they’re lost or stolen.

   > Never make financial and other sensitive transactions on any device over public wireless networks.

   **Use flash drives carefully.** Minimize the chance that you’ll infect your company network with malware:

   > Don’t put any unknown flash (or USB) drive into your computer.

   > On your flash drive, don’t open files that are not familiar.
What to do if there are problems

Using a web service

When using email, a social network, or other service, report:

➢ Scams, obscene material, or aggressive behavior to the service. For example, in Microsoft services or software, look for a Report Abuse link or contact us at microsoft.com/reportabuse.

➢ Any misrepresentation of your organization—for example, a phishing scam that pretended to be from your company—to your system administrator and the Anti-Phishing Working Group at www.antiphishing.org/report_phishing.html.

Theft or loss of company data or other assets

If sensitive company data or accounts have been compromised because of theft or loss of a laptop, smartphone, or other device, or because of a breach of network security or an account:

➢ Report it immediately to IT or security personnel, if your organization has them, and to the bank, when appropriate.

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

➢ Contact the service provider for help in wiping the data from smartphones and other devices.

More helpful info

➢ Find out how to create strong passwords (aka.ms/passwords-create) and then check their strength (microsoft.com/passwordchecker).

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

If you run a business without IT support


➢ The National Cyber Security Alliance can help you create a cyber security plan for your business: aka.ms/Cyber_security_plan.

➢ If a computer isn’t running as expected (it’s unusually slow or crashes frequently), it might have been damaged by malware. Microsoft can help you address this: aka.ms/Troubleshooting_101.