Digital Citizenship Begins with You

Microsoft

Being online today is more than simply surfing the web—it's a way of life. Learning and connecting through technology is now vital to our daily routine, which means being a good digital citizen takes on greater importance. It means educating ourselves about both the benefits and risks of our online world, and then developing the habits that can help us stay safer there.

Microsoft offers six essential steps that each of us can take to help protect our devices, information, and families as we learn, explore, and interact online.

1 Defend your computer

Strengthen your computer's defenses. Microsoft can help you do this: **microsoft.com/security/pypc.aspx**.

> Keep all software (including your web browser) current with automatic updating.

> Install legitimate antivirus and antispyware software.

> Never turn off your firewall.

> Protect your wireless router with a password, and use flash drives cautiously so you don't infect your PC with malicious software (*malware*).

Don't be tricked into downloading malware.

> Be cautious about opening attachments, clicking links, or calling a number in an email or instant message (IM), or on a social network—even if you know the sender. They could be phony. Confirm with the sender that the message is authentic.

> Avoid clicking **Agree**, **OK**, or **I accept** in banner ads, in unexpected pop-up windows or warnings, on websites that do not seem legitimate, or in offers to remove spyware or viruses.

Instead, press Ctrl + F4. If that doesn't close the window, press Alt + F4.

2 Protect sensitive personal information

Look for signs that a webpage is legitimate and secure, before you enter sensitive data.

> Make sure you're at the correct site—for example, at your bank's website, not a fake.

> Look for a web address with https ("s" for secure) and a closed padlock ( ) beside it. (The lock might also be in the lower right of the window.)

Never give sensitive info (like an account number or password) in response to a request in an email message or IM, or on a social network.

Save financial transactions for your home computer.

Think carefully before you respond to pleas for money from "family members," deals that sound too good to be true, wins of lotteries you didn't enter, or other scams.

Share your location only with those you trust. Set your location data so that it's not publicly available or searchable.

3 Create strong passwords and keep them secret

Strong passwords are long phrases or sentences that mix capital and lowercase letters, numbers, and symbols. (Learn how: **aka.ms/passwords-create**.)

> Keep passwords and PINs secret. Don't share them in email or IM, or over the phone.

> Use different passwords, especially for sites that keep financial information. If someone steals it or the website is compromised, all the information it safeguards is at risk.

4 Take charge of your online reputation

> Discover what's on the Internet about you. Use search engines and include blogs and social networks in your search. Consider the story this information tells about your reputation.

> Protect your reputation online. Act in a manner that reflects the reputation you want to earn, and periodically reassess what you find about yourself.

> Cultivate an accurate, positive reputation by publishing what you want others to see.

Microsoft

5 Use social networks more safely

> Look for **Settings** or **Options** in services like Facebook and Twitter to manage who can see your profile or photos tagged with your name, how people can search for you and make comments, and how to block people.

> Don't post anything online that you wouldn't put on a postcard.

> Be selective about accepting friends. Regularly reassess who has access to your pages, and review what they post about you.

6 Take extra steps to keep kids safer online

Make online safety a family effort, a mix of ongoing guidance and monitoring.

> Negotiate clear guidelines for web and online game use that fit your children's maturity level and family's values.

> Pay attention to what kids do and who they meet online.

> Watch for signs of online bullying, such as being upset when online or a reluctance to go to school.

> Be the administrator of your home computer. Use age-appropriate family safety settings to help you keep track of what your kids are doing online.

What to do if there are problems

When reporting online abuse, save evidence whenever possible.

When using email, a social network, or other web service

> If you encounter scams, offensive material, content that exploits minors, threatening behavior, or theft of your account, report it. For example, in Microsoft services or software look for a **Report Abuse** link, or contact us at **www.microsoft.com/reportabuse**.

> If someone takes over your email account, change your password immediately (if possible), and report the incident to your email provider.

Continued harassment or physical threats

Report them to local police, and if a child or teen is involved, to the National Center for Missing and Exploited Children at **cybertipline.com**.

Your identity is stolen or you have responded to a scam

Immediately change the passwords and PINs on all your accounts, and report:

> The incident to your credit card company, bank, or health insurance company.

> Identity theft to the U.S. Federal Trade Commission (FTC) at **ftc.gov/idtheft**.

> Scams or fraud to the FTC at **ftccomplaintassistant.gov**.

More helpful info

> Create a standard user accounts to decrease your vulnerability to hackers and maintain control of computers at home: **aka.ms/user-accounts**.

> If your computer isn't running as expected (it's unusually slow or crashes frequently), it may have malware. Microsoft can help you address this: **consumersecuritysupport.microsoft.com**.

> If you're looking for ways to help monitor kids' online activity, compare these family safety tools from Microsoft: **microsoft.com/safetysettings**.

> Find more information on how to protect your computer, your privacy, and your family: **microsoft.com/security**.

1011 PN 098-108793

STOP | THINK | CONNECT™
www.stopthinkconnect.org