Microsoft

Top Tips for Online Safety at Home

1 Defend your computer

- Strengthen your computer's defenses. 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.
- Don't be tricked into downloading malicious software. Think before you open attachments or click links in email or IM, or on a social network—even if you know the sender. Confirm with the sender that the message is authentic. Don't click links or buttons in pop-up windows.

2 Protect sensitive personal information

- Before you enter sensitive data, look for signs that a webpage is secure—a web address with https and a closed padlock () beside it.
- Never give sensitive info (like an account number or password) or call a number in response to a request in email or IM or on a social network.
- Think carefully before you respond to pleas for money from "family members," deals that sound too good to be true, or other scams.

3 Create strong passwords and keep them secret

Make them long phrases or sentences that mix capital and lowercase letters, numbers, and symbols. Use different passwords, especially for sites that keep financial information.

4 Take charge of your online reputation

Discover what is on the Internet about you and periodically reevaluate what you find. Cultivate an accurate, positive reputation.

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 you wouldn't want to see on a billboard.
- 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 guidance and monitoring. Negotiate clear guidelines for web and online game use that fit your kid's maturity and family's values. Pay attention to what kids do and who they meet 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 **microsoft.com/reportabuse**.

- If your email account is taken over by someone, change your password immediately (if possible) and report the incident to your email provider.

Continued harassment or physical threats

Report it 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 insurer.
- 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

- Microsoft can help you take steps to better defend your computer: **microsoft.com/security/pypc.aspx**.
- Learn how to create strong passwords: **aka.ms/passwords-create**.
- Create a standard user account to decrease your vulnerability to hackers: **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**.

STOP | THINK | CONNECT™

www.stopthinkconnect.org

1011 PN 098-115259