



▶ PROTECT

Your Computer,
Your Family, and Yourself

The Internet = A World of Opportunities



Look what's at your fingertips

- A way to communicate with friends, family, colleagues
- Access to information and entertainment
- A means to learn, meet people, and explore

Online Security Versus Online Safety

Security: We must secure our computers with technology in the same way that we secure the doors to our homes.

Safety: We must act in ways that help protect us against the risks that come with Internet use.



Primary Online Risks and Threats



To Computers

- Viruses
- Worms
- Trojans
- Spyware



To Children

- Cyberbullies
- File-sharing abuses
- Invasion of privacy
- Disturbing content
- Predators



To Personal Information

- Online fraud and phishing
- Hoaxes
- Identity theft
- Spam

Primary Threats to Computer Security



Viruses/Worms

Software programs designed to invade your computer, and copy, damage, or delete your data.



Trojans

Viruses that pretend to be helpful programs while destroying your data, damaging your computer, and stealing your personal information.



Spyware

Software that tracks your online activities or displays endless ads.

Primary Online Risks for Children



Cyberbullies

Both children and adults may use the Internet to harass or intimidate other people.



File-share Abuse

Unauthorized sharing of music, video, and other files may be illegal, and download viruses or worms.



Disturbing Content

If kids explore unsupervised, they could stumble upon images or information you may not want them exposed to.



Predators

These people use the Internet to trick children into meeting with them in person.

Invasion of Privacy

If kids fill out online forms, they may share information you don't want strangers to have about them or your family.

Primary Threats to Personal Online Safety



Identity Theft

A crime where con artists get your personal information and access your cash and/or credit

Phishing

E-mail sent by online criminals to trick you into revealing personal information



Hoaxes

E-mail sent by online criminals to trick you into giving them money



Spam

Unwanted e-mail, instant messages, and other online communication

Steps You Can Take



Your computer

1. Use an Internet firewall.
2. Keep your operating system up-to-date.
3. Install and maintain antivirus software.
4. Install and maintain antispyware software.



Your family

1. Talk with your kids about what they do online.
2. Set clear rules for Internet use.
3. Keep personal information private.
4. Use family safety software.



Yourself

1. Practice Internet behavior that lowers your risk.
2. Manage your personal information carefully.
3. Use anti-phishing and anti-spam technology.

Four Steps to Help Protect *Your Computer*

- 1 Use an Internet firewall
- 2 Keep your operating system up-to-date
- 3 Install and maintain antivirus software
- 4 Install and maintain antispyware software

Use an Internet Firewall



An Internet firewall helps create a protective barrier between your computer and the Internet

Keep Your Operating System Up-to-date

- Install all updates as soon as they are available
- Automatic updates provide the best protection



Install and Maintain Antivirus Software



Don't let it expire

- Antivirus software helps to detect and remove computer viruses before they can cause damage.
- For antivirus software to be effective, you must keep it up-to-date.

Install and Maintain Antispyware Software



Use antispyware software so unknown software cannot track your online activity and potentially steal your information.

Other Ways to Help Protect Your Computer



Back up your files regularly

Read Web site privacy statements

Close pop-ups using red “X”

Think before you click

Back up Your Files



- Save to CD/DVD, USB drive, or other external source
- Use a Web-based backup service

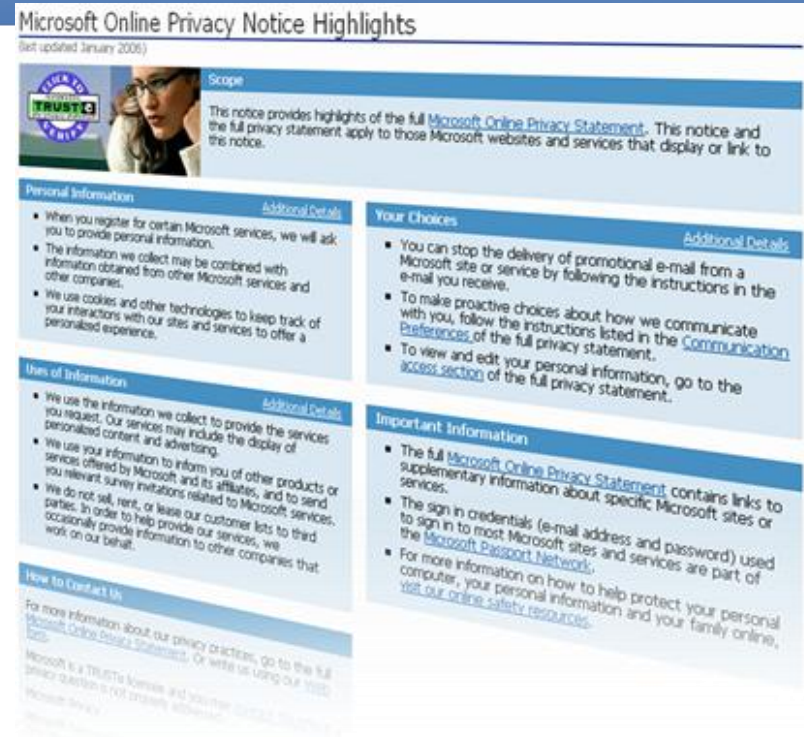
Think Before You Click

- Don't open e-mail attachments unless you expect them and already know what they contain
- Only download files from Web sites you trust



Read Privacy Statements

Understand what you are getting before you agree to download or share your personal information



Microsoft Online Privacy Notice Highlights
(last updated January 2006)

Scope
This notice provides highlights of the full [Microsoft Online Privacy Statement](#). This notice and the full privacy statement apply to those Microsoft websites and services that display or link to this notice.

Personal Information [Additional Details](#)

- When you register for certain Microsoft services, we will ask you to provide personal information.
- The information we collect may be combined with information obtained from other Microsoft services and other companies.
- We use cookies and other technologies to keep track of your interactions with our sites and services to offer a personalized experience.

Uses of Information [Additional Details](#)

- We use the information we collect to provide the services you request. Our services may include the display of personalized content and advertising.
- We use your information to inform you of other products or services offered by Microsoft and its affiliates, and to send you relevant survey invitations related to Microsoft services.
- We do not sell, rent, or lease our customer lists to third parties. In order to help provide our services, we occasionally provide information to other companies that work on our behalf.

Your Choices [Additional Details](#)

- You can stop the delivery of promotional e-mail from a Microsoft site or service by following the instructions in the e-mail you receive.
- To make proactive choices about how we communicate with you, follow the instructions listed in the [Communication Preferences](#) of the full privacy statement.
- To view and edit your personal information, go to the [access section](#) of the full privacy statement.

Important Information

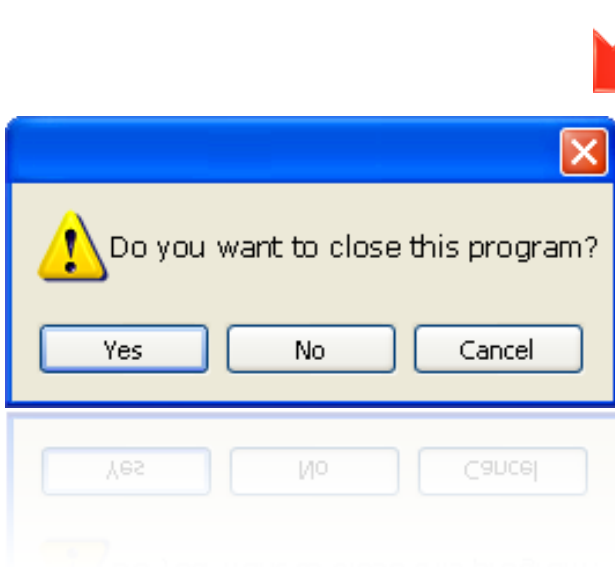
- The full [Microsoft Online Privacy Statement](#) contains links to supplementary information about specific Microsoft sites or services.
- The sign in credentials (e-mail address and password) used to sign in to most Microsoft sites and services are part of the [Microsoft Passport Network](#).
- For more information on how to help protect your personal computer, your personal information and your family online, [visit our online safety resources](#).

How to Contact Us

For more information about our privacy practices, go to the full [Microsoft Online Privacy Statement](#). Or write us using our [mailing list](#).

Microsoft is a TRUSTe Member and you may contact [Microsoft](#) if your privacy question is not properly addressed.

Use the Red “X” to Close Pop-ups



- Always use the red “X” in the corner of a pop-up screen.
- Never click “yes,” “accept” or even “cancel,” because it could be a trick that installs software on your computer.

Take Steps to Help Protect *Your Family*

- 1 **Talk** with your kids about what they do online
- 2 **Set** clear rules for Internet use
- 3 **Keep** personal information private
- 4 **Use** family safety software

Talk with Your Kids about Online Risks

- Talk frankly with your kids about Internet risks, including
 - Online criminals
 - Inappropriate content
 - Invasion of privacy
- Empower them by teaching them how their own behavior can reduce those risks and help to keep them safe when they are online.

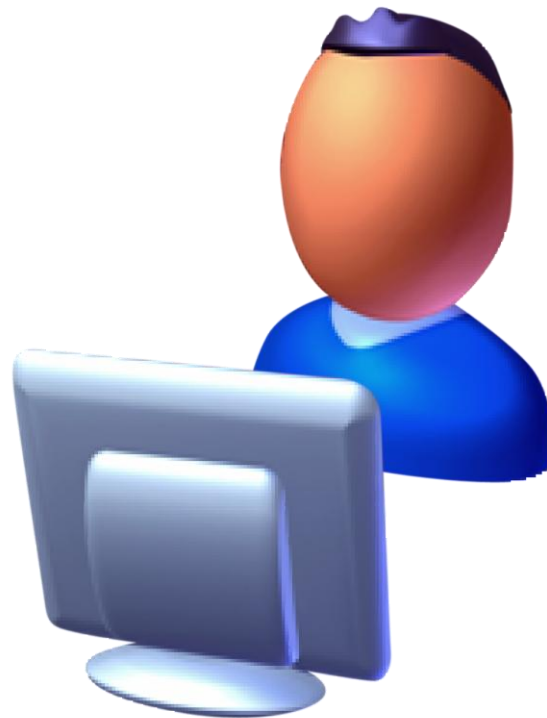


Helpful online resources

- www.staysafe.org
- www.getnetwise.org

Pay Attention to What Your Kids Do Online

- Keep the computer in a central area
- Get to know how your kids use the Internet
- Let your kids be the teacher
- Teach kids to trust their instincts
- Encourage them to report any problems



Keep Personal Information Private

- Teach children to check with you before sharing personal information online
- Monitor your children's online activities
- Teach your children to report suspicious activity
- Help children choose appropriate screen names and e-mail addresses



Set Clear Rules for Internet Use

- Do not share files or open attachments
- Do not click links in e-mail
- Treat others the way you want to be treated
- Stand up for yourself
- Respect other people's property
- Never go alone to meet an Internet "friend" in person



Use Family Safety Software

- Helps parents manage the content their children view, what they do, and who they communicate with online



How to Handle Problems

- Contact police to report any threat immediately
- Report incidents to:

CyberTipline
800-843-5678
www.cybertipline.com

Take Steps to Help Protect *Your Personal Information*

- 1** **Practice** Internet behavior that lowers your risk
- 2** **Manage** your personal information carefully
- 3** **Use** technology to reduce nuisances, and raise the alarm when appropriate

Practice Internet Behaviors that Help Reduce Your Risk



- Delete spam, don't open it
- Be on the lookout for online scams
- Use strong passwords

Manage Personal Information Carefully



- Do not share personal information in e-mail or instant messages
- Use only secure and trusted Web sites
- Make sure you are where you think you are:
Web sites can be faked.
- Avoid financial transactions over wireless networks
- When in public, stay private

Use Anti-Phishing and Anti-Spam Technology

- Most Internet service and e-mail providers filter spam
- Phishing filters help to block known scam sites and warn against suspicious sites



If Your Identity is Stolen

- Report it
- Follow up in writing
- Change all passwords
- Place fraud alert on credit reports

EQUIFAX

experian

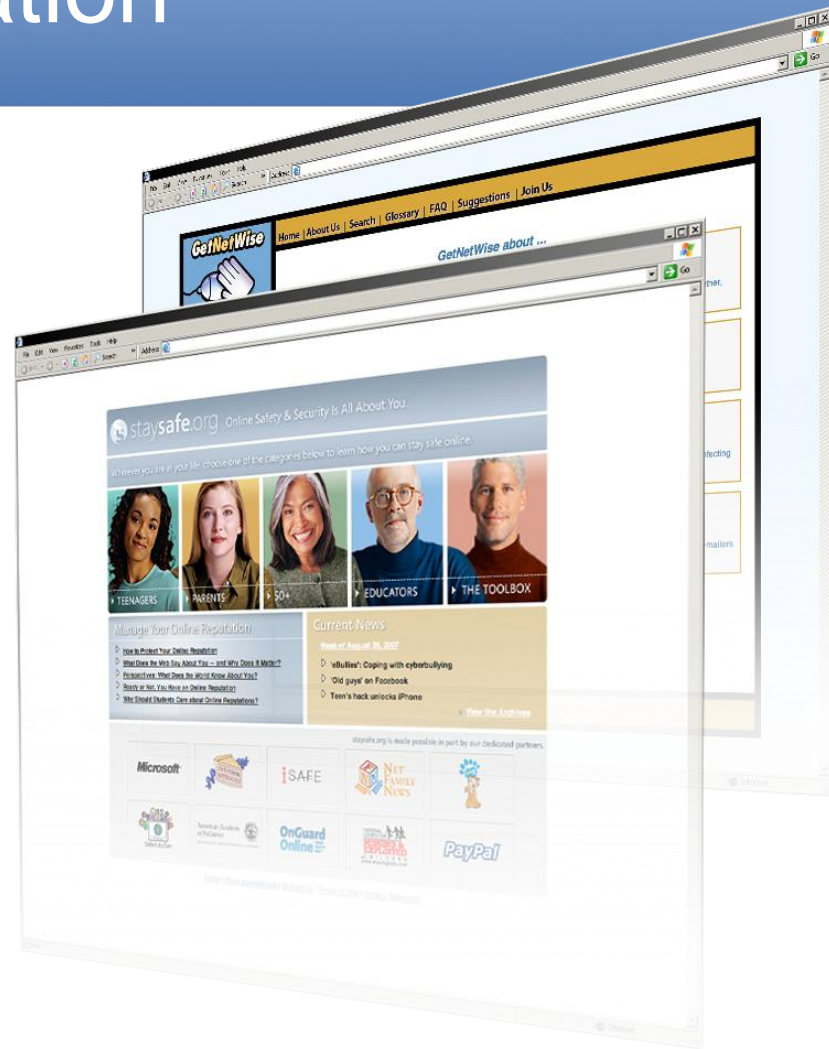
TransUnion

Get a copy of your **credit report** and ensure your account is marked “fraud alert” and “victim’s statement”

For More Information

www.staysafe.org

www.getnetwise.org





© 2007 Microsoft Corporation. All rights reserved.

Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation.

Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.