Know the risks

Online conversations can give talking with family, friends, and coworkers the immediacy of conversing in person—in email, IM, and texting, using Skype one-on-one or with a group, in social network messaging, or game chat.

But online conversations are not without risks:

> Although Skype conversations are secure, others may not be, and it's easy to forward them.

> People on the other end may not be who they say they are. By impersonating a friend or a reputable organization, they may try to trick you into installing malicious software *(malware)*.

> Opening attachments or transferred files and clicking links can release malware. This can let a criminal record passwords or account numbers that you type, take over your computer, or steal your contacts.

> Some scammers try to trick you into simply giving them your money. They may promise big returns on your "investment," ask for donations to a fake charity, or beg you to send money to a "family member" in distress.

Others, using a method known as phishing, may send a message or make an automatic phone or Skype call that poses as one from a company you trust, like your bank or web service. The forged messages typically direct you to an equally phony webpage or toll-free number. There, you're asked to reveal financial or other personal data.

What to do if there are problems

What to do if your account has been compromised

1. Report it to the online account provider right away.
2. Update or install antivirus software on your computer. Run it to clean your computer of malware.
3. Change your password (or reset it), and make it stronger. Don't use passwords you've used before.
4. Make sure you have the latest version of all your software and keep it up to date.

Report abusive, threatening, or harassing messages

Report any incidents to the email or web service or Skype. For example, in Microsoft services or software look for the **Report Abuse** link, or contact us at **www.microsoft.com/reportabuse**.

What to do if you've responded to a phishing scam

> Immediately change the passwords and PINs on all compromised accounts, and on any accounts where you have used that same password.

> Report it to your credit card company or your bank.

> If you've been the victim of identity theft, find out what steps to take at **ftc.gov/idtheft**.

Content partner AARP

This material is provided for informational purposes only. Microsoft makes no warranties, express or implied.

0212 PN 098-111020

Talking Safely Online

> Know the risks

> Practical advice for safer online conversations

> What to do if there are problems

Practical advice for safer online conversations

Reduce spam in your inbox

- Share your primary email address or IM, Skype, or gamer name only with people you know or with reputable organizations. Avoid listing them on your social network page, in Internet directories (such as white pages), or on job-posting sites.
- Set up a secondary email address for your public web activities—shopping, joining organizations, subscribing to newsletters, signing petitions, and so on.
- Set the spam filters in your email service to **Standard** or **High**. In Windows Live Hotmail, for example, click **Options** and then **More Options**. Under **Preventing junk email**, click **Filters & Reporting**, and then make your choices.

Think, then click

In general, be wary of the sender, even someone you know or a company you trust. Someone may have hijacked a friend's account and sent a message to everyone in the friend's address book.

- Pause before you click links, open photos, songs, or other attachments, share files, or call a number in the message. (Be especially cautious about messages that your account is about to be closed or has been compromised.)

  Instead, confirm with the sender over a different medium that the message is legitimate.
- Mark junk email as spam and delete it. Don't reply to spam even to "unsubscribe."

Guard your privacy

Be selective about friends.

- Think twice about who you accept as a contact. Consider adding only those you or your friends have met in person or with whom you have friends in common.
- Be skeptical of messages from those you don't know. Limit communication to those on your contact list.

Don't share sensitive information in messages or profiles. Once you disclose it, it's out of your control forever, even if it was intended for one person. Sensitive data includes your home address, current location, account numbers, and passwords.

Meeting an online "friend" in person can be risky. Connect in a busy public place and bring a friend.

Watch out for scams

The most dangerous scams are those that seem genuine. Look for misspellings and grammatical errors or deals or prizes that sound too good to be true. Be suspicious of alarmist messages with urgent requests for personal information, to update your account, or to stop payment on a charge.

- When in doubt, check with a site like **snopes.com** to see if it's a known scam.
- Get more detail on how to spot a phishing scam and defend against it at **aka.ms/spot-that-scam**.

Defend your computer and accounts against Internet threats

Boost 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. (Microsoft can help: **microsoft.com/security/pypc.aspx**.)

Protect accounts with strong passwords.

- Use long phrases or sentences and mix capital and lowercase letters, numbers, and symbols. (Learn how: **aka.ms/passwords-create**.)
- Don't share your passwords with anyone or be tricked into giving them away. Many account takeovers occur because the owner disclosed the password.
- Don't use the same password everywhere. If it's stolen or inadequately protected by the site, all the accounts it protects are at risk.

Take extra steps to help protect children

In addition to paying close attention to the online lives of kids and following the advice above, here are some other measures to help you watch over children online.

- Help kids create screen names and gamer tags that don't reveal anything personal and aren't suggestive.
- Teach kids not to say, text, or post anything that would hurt or embarrass someone. NO bullying. Period.
- Use the GPS in mobile phones cautiously. If you use a family location service to monitor your kids' whereabouts, make sure others cannot locate them. Otherwise, consider disabling the feature. At the very least, turn it off for the phone's camera.
- Make video calls in central family spaces and monitor them. Explain why video calling can be risky and what to do if your child feels threatened.
- Monitor your child's list of contacts.