Microsoft

Protecting Your Privacy Online

Around the world, online activities have increasingly become a central part of daily life. You send email, check your social network account or the weather, stream videos, tweet, share photos, download music, back up files using online services like OneDrive or Dropbox, and create documents.

When you use a web browser (like Internet Explorer or Firefox) or an app, all this information that you post, send, or create online goes from your computer, phone, or other Internet-connected device into the cloud. From there it is sent to the services and people you interact with.

With so much information being stored in the cloud you may wonder about your privacy and the security of your data, so it's important to learn some basic ways to help protect them.

Not all cloud services are alike. Just as you do when you bank or shop, use well-established services—social networks, email, photo sharing, data backup, and so on—whose brands and policies you trust to manage your data appropriately. This will help minimize your risk.

You can also play your part in strengthening your privacy online by following the practical tips below to help control what you reveal about yourself and who has access to that information.

Guard your information

Boost your computer's security. (Microsoft can help you do this: microsoft.com/security/pypc.aspx.)

- Keep all software (including your web browser and apps) current with automatic updating. Install antivirus and antispyware software from companies you trust. Password-protect your wireless router, and use flash drives cautiously.
- Ignore any email message, pop-up warning, or other notice that claims it will protect your device or offers to remove viruses. It is highly likely to do the opposite.

Create strong passwords. Use long phrases or sentences that mix capital and lowercase letters, numbers, and symbols. Keep your passwords private, and use unique passwords for each site. (Learn how: aka.ms/passwords-create.)

Your information is already in the cloud!

The cloud is a network of computers on the Internet—a "cloud" of computers—where data, including yours, can be stored. When you check your email or the news, or pay bills or play a game online, you're accessing the cloud. Your information is also in the cloud if you store files there.

Because the data is in the cloud, you can access it from—and share it between—your phone or computer or any other device connected to the Internet.

Microsoft

Report identity theft

If you've been a victim of identity theft in the United States, report it right away to the U.S. Federal Trade Commission at **ftc.gov/idtheft**, and get recommendations there about other steps you can take.

More help

- Get more information about how to guard your privacy on the Internet: **aka.ms/protect-privacy**.
- Learn how to protect yourself from identity theft online: **aka.ms/protect-identity**.
- Find out how Microsoft helps protect your privacy: **www.microsoft.com/yourprivacy**.
- Learn to recognize phishing messages, links, or phone calls: **aka.ms/spot-that-scam**.
- Get general advice about how to use the Internet more safely and securely: **www.staysafeonline.org**.

Save sensitive activity for a secure network at home. Do not bank, shop, check email, or do other business that exposes your user names or passwords over "borrowed" or public Wi-Fi (like a hotspot). Others using the network may be able to see what you are sending. (Learn how to use Wi-Fi more safely: **aka.ms/Wi-Fi-safety**.)

Give nonsense answers to security questions—answers that can't be found by trolling Facebook, for example, but which you can remember. For instance, if the question is "Where were you born?," you might answer "Green."

Think before you share

- Don't post anything online you wouldn't want to see on a billboard. Guard account numbers, user names, and passwords with special care.
- Adopt tight privacy controls to manage who can see your profile or photos, how people can search for you, and who can make comments, and to block unwanted access.
- Read the privacy policy of the website or app. It should explain what data it gathers about you, how it's shared and secured, and how you can access and update it.

Protect yourself from fraud

Spot the signs of scams. The most dangerous are those that appear to be genuine. Be wary of requests from your "bank" for your password, notices that you've won a lottery, appeals to help a distant stranger "transfer funds," offers for credit repair or virus protection, and other enticements. (Learn how to recognize and avoid scams: **aka.ms/scam-protection**.)

Use caution *before* you open attachments or click links in unexpected or odd messages, even from friends or companies you trust. You might fall victim to an online scam like phishing, or download software that lets hackers remotely control your computer or record sensitive personal data—like passwords or account numbers—as you type. Instead, first check with the sender that the message is genuine by some means other than hitting Reply.

Look for evidence that a webpage is secure and legitimate *before* you enter sensitive data, and make sure you got to the site through a path you trust, such as a bookmark or favorite you've set.

Good signs of a secure connection include a web address that starts with https ("s" stands for secure) and a closed padlock. A better indicator (for those websites that support it) is a green address bar.

0913 PN 098-117651