Three Basic Habits to Help Protect Your Data On the Go

Staying in touch has never been so effortless, but there are risks–primarily potential theft of sensitive private data. These three simple habits can help you avoid them.

1 Lock your computer and accounts with strong passwords and your mobile phone with a PIN

Create strong passwords

Strong passwords are at least eight characters (longer is better) and mix letters, numbers, and symbols. Learn how to create them at **microsoft.com/protect/fraud/passwords/create.aspx.**

Keep passwords and PINs private

> Do not share them in email, instant, or text messages, or store them on your phone.

> Do not disclose them to friends or businesses, or be tricked into giving them away.

Avoid using the same password or PIN everywhere

2 Save financial activity for a secure network at home

Do not pay bills, bank, shop, or do other sensitive business on a public computer, or on your laptop or mobile phone over "borrowed" or public Wi-Fi (like a hotspot). The security can be unreliable. (Using the mobile phone network, which encrypts data, is acceptable.)

3 Watch for snoops

People scouting for passwords, PINs, user names, or other such data can watch your fingers or the screen as you enter them.

What to Do If There Are Problems

Report identity theft to:

> The bank, credit card company, or other financial institution, and the three major credit bureaus (Equifax, Experian, and TransUnion).

> The U.S. Federal Trade Commission (FTC) at **ftc.gov/idtheft**, or call toll free: **(877) 438-4338**.

Report scams or fraud to the web service or phone company, and to the FTC at **https://www.ftccomplaintassistant.gov**, or call toll free: **(877) 382-4357**.

More Helpful Info

> Get more information about online safety away from home: **microsoft.com/security/online-privacy/default.aspx#Mobile-and-Wireless**.

> Teach kids how to use mobile phones more safely: **go.microsoft.com/?linkid=9758045**.

> Find out how to remove any trace of specific web activity in recent versions of Windows® Internet Explorer®: **microsoft.com/windows/internet-explorer/features/safer.aspx**.

Content contributor LOOKBOTHWAYS ilookbothways.com

© 2011 Microsoft Corporation. All rights reserved. This material is provided for informational purposes only. Microsoft makes no warranties, express or implied.

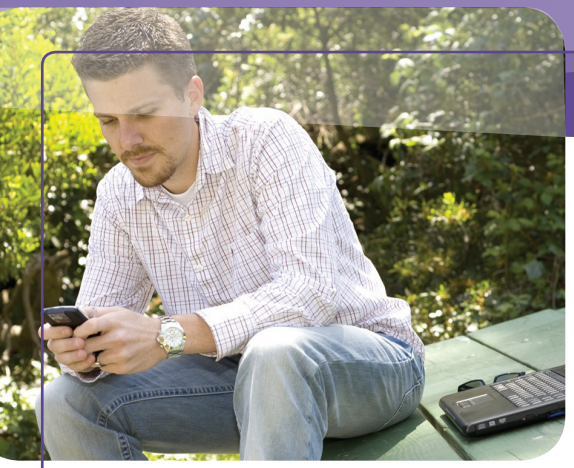
0111 PN 098-111419

Microsoft

Smarter Online = Safer Online

Protecting Your Information On the Go

How to protect your private information on mobile phones and devices, public computers, and public Wi-Fi



Safety Tips for Specific Mobile Connections

Protect your data on mobile phones and devices

Accept incoming content only from sources you trust

> If someone sends an attachment or a link, delete it unless the message is expected or typical of the sender–it could be a virus or spyware.

> If you have Bluetooth connectivity, set it to non-discoverable mode when you are not using it. This blocks unwanted downloads and keeps intruders from reading contacts, text messages, and other data stored on your phone.

Use GPS features wisely

A mobile phone's ability to pinpoint where you are or tag the location of your photos can be a threat to your privacy–you may not be able to control how that data is used and by whom.

Set your phone to activate your PIN when it is not in use

Take steps to protect private data if your mobile device is stolen

Look into a service that will enable you to locate your stolen phone on a map, and lock it or erase its data remotely.

Use public computers more safely

On a public computer in a hotel or café, criminals may try to watch as you enter sensitive data, or have planted spyware on the computer to record any passwords or account numbers you type.

Do not leave the computer, even briefly, with private information on the screen

Erase your tracks

Web browsers keep a record of your passwords and every page you visit, which can be a problem on public computers. Look for the feature that enables private or anonymous browsing and turn it on.

Use flash drives cautiously

> Avoid storing sensitive data on a USB flash (or thumb) drive. If you lose it or it is stolen, anyone can access that information.

> Using your flash drive in an infected PC could corrupt the drive and ultimately your own computer.
To avoid this: When you insert the drive, hold down the SHIFT key. If you forget to do this, click ☒ in the upper-right corner to close any flash-drive related pop-up windows.

> Do not put an unknown flash drive into your PC, or copy files from a flash drive onto your hard drive if you don't know the document owner.

> Do not open files that you find on a flash drive other than the ones you were specifically told would be there.

Protect data on your own computer on the go

If you use your computer on public Wi-Fi or unsecured wireless networks without adequate safeguards, hackers and identity thieves may be able to eavesdrop on your web activity.

Defend your laptop against Internet threats

Install antivirus and antispyware software. Never turn off your firewall, and use flash drives cautiously. Keep all software (including your Web browser) current with automatic updating. Microsoft can help you do this: **microsoft.com/security/pypc.aspx**.

Check the security level of the wireless hotspot

Choose the most secure connection even if it means paying for it.

> A password-protected connection–ideally one that is unique for your use–is better than one without a password.

> Ask about encryption–a network key or certificate that scrambles data as it travels between your laptop and the router.

Confirm the exact spelling of the network you are connecting to. Beware of clever fakes.

Turn off the wireless connection when you are not using the Internet

> If you are using an external Wi-Fi card, simply remove it.

> For an internal card, look for a button on your laptop or a combination of keys that will cut the connection.