Microsoft

How can someone steal your identity online?

Phishing scams are an attempt to trick you into divulging sensitive personal information. Thieves send phony e-mail or instant messages that appear to come from a company you trust (like your bank) or one that seems reputable. The forged messages (the "bait") typically contain a link (the "hook") to an equally fake Web page or request to call a toll-free number. There, you're asked to reveal financial or other personal data.

This type of fraud is alarming in its ingenuity. The message may suggest that someone has tried to break into your account, made an unauthorized charge on your credit card, or that your account is about to be closed unless you give the personal data needed to correct the problem.

Thieves also harness the sheer power of technology to collect personal information. For example, opening e-mail attachments or clicking in a pop-up window may plant harmful software on your computer that can let a crook record any passwords or account numbers that you type.

Identity thieves may breach the security of insurance, hospital, government, and other databases to steal the personal information of thousands.

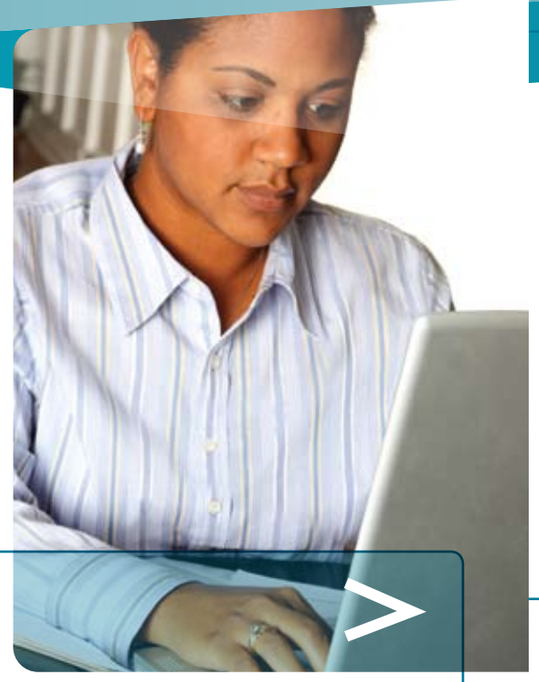
TIP

Test your identity theft IQ by playing this online game: **onguardonline.gov/games/id-theft-faceoff.aspx**.

Microsoft

More Helpful Info

- Contact the three major credit bureaus:
  Equifax: **www.equifax.com/credit-report-customer-service** for answers to questions and for phone numbers.
  Experian: **experian.com** or **(888) 397-3742**
  TransUnion: **transunion.com** or **(800) 680-7289**
- Get more Microsoft advice about how to recognize and protect yourself from phishing scams: **microsoft.com/protect/yourself/phishing/identify.mspx**.
- The U.S. FTC offers details to help you deter, detect, and defend against identity theft. **ftc.gov/bcp/edu/microsites/idtheft**.



Smarter Online = Safer Online

Protecting Yourself From Identity Theft on the Internet

0309 PN 098-111191

Microsoft

What Is Identity Theft?

When a thief gathers up personal information about you and then uses it to impersonate you, that's called identity theft. Age is no barrier–thieves may steal the identities of teens and children, too. (In fact, the ages of greatest risk for identity theft are 18 to 29.)

It doesn't take much of the right kind of personal information–your Social Security number, password, address, mother's maiden name, a bank account number or PIN–for a thief to make purchases on your credit card, cash in on government benefits, open bank accounts, take out loans–even commit crimes–all in your name.

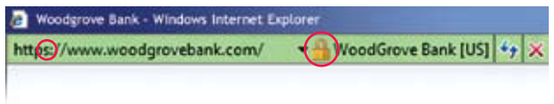
Four Simple Ways to Help Protect Your Identity Online

1 Be defensive with sensitive personal information

Avoid sending sensitive information in an e-mail or instant message. These may not be secure.

Look for signs that a Web page is safe, before you enter sensitive data. Check for evidence that:

- You are at the correct site–for example, at your bank's Web site, not a fake. If you're using Windows® Internet Explorer®, one sign of trustworthiness is a green address bar like the one below.
- The site uses data encryption, a security measure that helps protect your data as it traverses the Internet. Good indicators include a Web address with https ("s" stands for secure) and a closed padlock. (The lock might also be in the lower right corner of the window.)



Save financial transactions for your home computer at home. Never bank, shop, pay bills, or do other personal business on a public computer or on your own computer over a public wireless connection. The security is unreliable.

Be cautious when clicking links in an e-mail or instant message, or pop-up window, even if you know the sender. If you're unsure if the message is genuine, confirm with the sender. To visit a Web site, type the address or use your own bookmark.

2 Create strong passwords and keep them secret

Strong passwords are at least eight characters long (longer is better) and include a combination of letters (both upper and lower case), numbers, and symbols. They are easy for you to remember but difficult for others to guess.

- Keep passwords to yourself. Remember them by writing them down on a well-protected piece of paper.
- Avoid using the same password everywhere. If someone steals it, all the information protected by that password is at risk.

TIP

Learn how to create strong, memorable passwords and keep them safe at **microsoft.com/protect/yourself/password/create.mspx**.

3 Protect your credit

The three major U.S. credit bureaus (Equifax, Experian, TransUnion) can help you protect your credit.

- Every year, get your free credit report (and that of any family member over age 14) from each of the three bureaus. Review them carefully for inquiries you didn't initiate, accounts you didn't open, or any other transactions you didn't authorize. Get these through **AnnualCreditReport.com** or call toll-free: **(877) 322-8228**.
- Unless you are actively seeking a loan or other credit, contact the three bureaus (details on the back panel) to freeze your credit, which restricts access to your reports.

4 Get help from technology

Improve your computer's security. You can greatly reduce your risk of identity theft by using firewall, antivirus, and antispyware software. Password-protect your wireless connection at home. Keep all software current (including your Web browser) with automatic updates. Microsoft can help: **microsoft.com/protect/computer/default.mspx**.

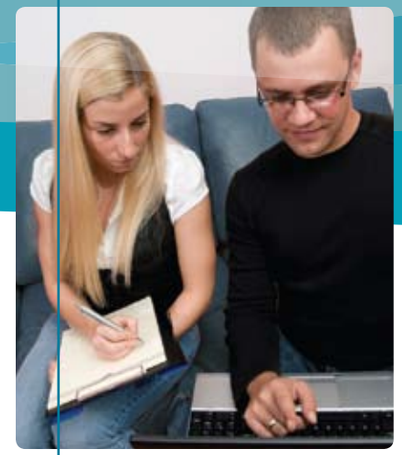
Use a special filter that warns you of suspicious Web sites and blocks you from visiting reported phishing sites. For example, try the SmartScreen® Filter included in Windows Internet Explorer 8, or the Microsoft Phishing Filter in Internet Explorer 7 and Windows Vista®, which Microsoft updates many times an hour.

Warning signs of online phishing scams

It can be difficult (even for experts) to distinguish between a slick scam and an authentic message. Your best protection, therefore, is caution–and staying alert to these signs:

- Generic introductions, like "Dear Customer," rather than using your name.
- Requests for personal information in an e-mail or instant message. Legitimate businesses will not make these requests.
- Alarmist messages. Criminals attempt to create a sense of urgency so you'll respond without thinking.
- Misspellings and grammatical errors.
- Amazing offers–if it sounds too good to be true, it probably is.

Microsoft



What You Can Do If Someone Steals Your Identity

Act *immediately* to correct your records and document your efforts as you go. Make copies of all e-mail and letters, and keep detailed notes of phone calls.

- File a police report, and get a copy to show your bank and other financial institutions that you are a crime victim, not a credit abuser.
- Put a fraud alert on your credit reports with one of the three major U.S. credit bureaus (details on the back panel) so no new credit will be granted without your approval. This entitles you to free reports; review them carefully.
- Close accounts accessed or opened fraudulently. Speak with the fraud department of each of those companies, and follow up with a letter.
- Change the passwords on all compromised accounts.
- Report the theft to the U.S. Federal Trade Commission (FTC) at **ftc.gov/idtheft** or call **(877) 438-4338**.
- Report suspicious or fraudulent incidents to the service provider.