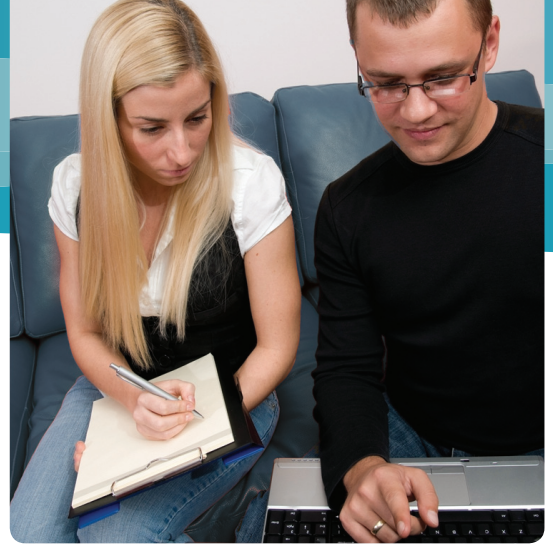

What is identity theft?

When a thief gathers information about you and uses it to impersonate or defraud you, it's called identity theft.

Even a small amount of data—your Social Security number, password, address, mother's maiden name, account number or PIN—is enough for a thief to make credit card purchases, open bank accounts, take out loans, or commit crimes in your name.

So, how can someone steal your identity online?

Phishing scams. Identity thieves attempt to trick you by sending a phony email or instant message (IM) that appears to come from a reputable organization (like your bank or favorite charity). The message tries to alarm you by suggesting that your account was compromised or will be closed unless you respond.

The phony message typically contains a link to a webpage or a request to call a toll-free number. There, you're tricked into revealing financial or other sensitive information on a realistic (but fake) webpage or to a "representative."

Malicious software. Opening email attachments or clicking in a pop-up window may secretly plant harmful software on your computer that can let a thief collect your passwords or account numbers.

Data breaches. Identity thieves may break into insurance, hospital, government, and other databases to steal the personal information of thousands.

More helpful info

> Learn how to create strong passwords: **aka.ms/passwords-create**.

> Contact the major U.S. credit bureaus:
Equifax. Answers to questions and for phone numbers: **equifax.com/cs/Satellite?pagename=contact_us**
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: **aka.ms/onlinefraud**.

1011 PN 098-111191

Microsoft

Protecting Yourself From Identity Theft Online

Four simple ways to help protect your identity online

It can take years to discover you're a victim of identity theft, and even longer to clear your name and credit rating, so prevention is key.

1 Be defensive with sensitive information

Don't put sensitive information in email, instant, or text messages. These methods may not be secure.

Look for signs that a webpage is secure and legitimate.
Before you enter sensitive data, check for evidence:

> Of a web address with http**s** ("**s**" stands for secure) and a closed padlock. (The lock might also be in the lower right corner of the window.)

> That you're at the correct site—for example, at your bank's website, not a fake. One sign of trustworthiness is a green address bar like the one above.

Save banking, shopping, and other financial transactions for your home computer. The security of a public computer, or your own computer over a public wireless connection, may be unreliable.

Be cautious about clicking links in a message or pop-up window. If you're unsure if a message is genuine—even if you know the sender—contact him or her using a different device or account.

2 Create strong passwords and keep them secret

Strong passwords are long (phrases or sentences) that mix capital and lowercase letters, numbers, and symbols.

> Don't use the same password everywhere. If it's stolen, all the information the password protects is at risk.

> Don't share your passwords. Remember them by writing them down on a well-protected piece of paper away from your computer.

3 Protect your accounts and your credit

Stay on top of existing account balances by reconciling account activity regularly. Report discrepancies quickly.

Protect your credit with help from the major U.S. credit bureaus (details on the back panel):

> Every year, get your free credit report (and that of any family member over age 14) from each credit bureau, and review them carefully. Order through **AnnualCreditReport.com** or call toll-free **(877) 322-8228**.

> Unless you are actively seeking a loan or other credit, contact the three bureaus to freeze your credit, which restricts access to your reports.

4 Boost your computer's security

Reduce your risk of identity theft by keeping all software (including your web browser) current with automatic updating. Install legitimate antivirus and antispyware software. Never turn off your firewall. Protect your wireless router with a password, and use flash drives cautiously. Microsoft can help: **microsoft.com/security/pypc.aspx**.

Spot that scam

Learn the warning signs of scams and how to avoid and report them: **aka.ms/scam-protection**.

Microsoft

What you can do if someone steals your identity

Act *immediately* to correct your records. Document your efforts as you go: make copies of all email 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 major U.S. credit bureaus (details on the back panel) so that no financial institution grants new credit without your approval.

> Close accounts accessed or opened fraudulently. Speak with the fraud department of each of those companies, and follow up with a letter. When you open new accounts, use new passwords and PINs.

> Report the theft to the U.S. Federal Trade Commission (FTC) at **ftc.gov/idtheft** or call toll-free **(877) 438-4338**.

> Report suspicious or fraudulent incidents to the service provider. For example, in Microsoft services or software, look for the **Report Abuse** link, or contact us at **microsoft.com/reportabuse**.