Microsoft

ONLINE FRAUD

YOUR GUIDE TO PREVENTION, DETECTION, AND RECOVERY

Educate yourself about online fraud, the steps you can take to help guard against it, and what you can do if you fall victim to it.

CONTENTS

ONLINE FRAUD:
An introduction

The Internet has transformed our lives. It offers tremendous opportunities to learn, share, connect, shop, and bank. Yet as we increasingly engage online, criminals follow the traffic.

Online fraud victimizes millions of unsuspecting people every year. In the United States alone, the FBI's Internet Crime Complaint Center recorded 300,000 fraud complaints in 2011 with an adjusted dollar loss of nearly half a billion dollars. For victims reporting financial losses, the average was $4,187.

Most online theft targets money or sensitive personal information, the currency of the cybercrime economy. 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 official identification number (like a Social Security number in the United States), password, address, account number, or PIN—could be enough for a thief to make credit card purchases, open bank accounts, take out loans, or commit crimes in your name. This is online fraud.

Criminals do big business running illicit websites where they buy and sell stolen identities (as well as credit cards), which are used to commit further fraud. They use *social engineering* techniques to try to trick you into installing software that can spy on what you type. Criminals may also use fraudulent methods to hijack computers, which they control remotely, to host illicit websites, attack other computers, and send spam.

? *What's social engineering?*

Online criminals can use sophisticated technology to try to gain access to your computer, or they can use something simpler and more insidious: social engineering.

Social engineering exploits trust—yours—to help a criminal gain access to your computer and sensitive personal information.

Phishing is a good example of social engineering. As illustrated on page 5, a scammer tried to deceive people into believing that an email message came from the Outlook team, threatening them with account closure if they didn't submit their account information. Anyone who followed the instructions to submit account information put their identity and bank account at risk.

Scammers use social engineering techniques to trick people into giving them access to computers to gain access to bank accounts or sensitive information, secretly install spyware, or enlist a computer in a network of illegal computers.

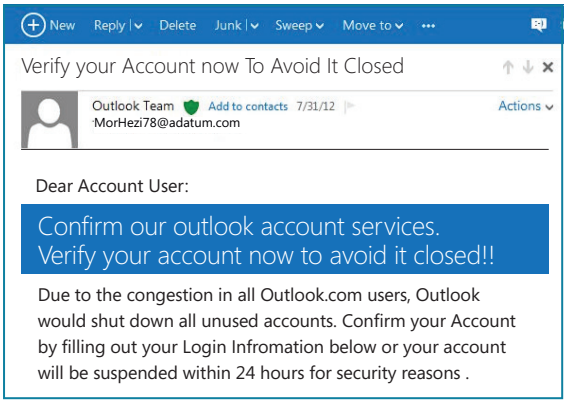
Examples of online fraud

There are many ways criminals exploit the Internet for online fraud. Here are a few of the most common, many of which rely on social engineering techniques to deceive people.

Phishing scams

These scams use email, text, or social network messages that appear to come from a reputable organization like your bank or a favorite charity—or, in our example, the Outlook team. The message is often so realistic that it can be difficult to tell it is not legitimate.

The convincing message entices you to divulge sensitive information like an account number or password. Or it might ask you to call a phony toll-free number or to click a link that goes to a fake webpage where you're asked to reveal personal data.

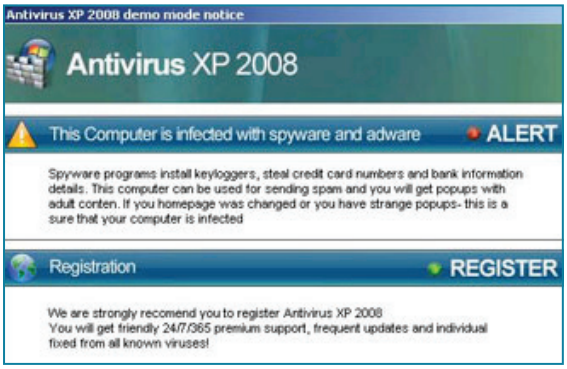


In this example, phishers try to trick Outlook users into giving sensitive information using the threat of account closure.

Rogue security software

Cyber criminals create legitimate-looking pop-up windows that promote software offerings that claim to protect your computer from malicious software (malware) or to fix your "infected" computer. It's highly likely to do the opposite.

Clicking in the window downloads and installs the rogue security software to your computer. Then it may lure you into a fraudulent transaction (for example, upgrading to a non-existent paid version of a program), or install malware that goes undetected as it captures passwords, user names, account numbers, and other sensitive data, and sends it to a criminal's computer.



This fake warning, disguised as a Microsoft alert, promotes a rogue security program.

Fake technical support

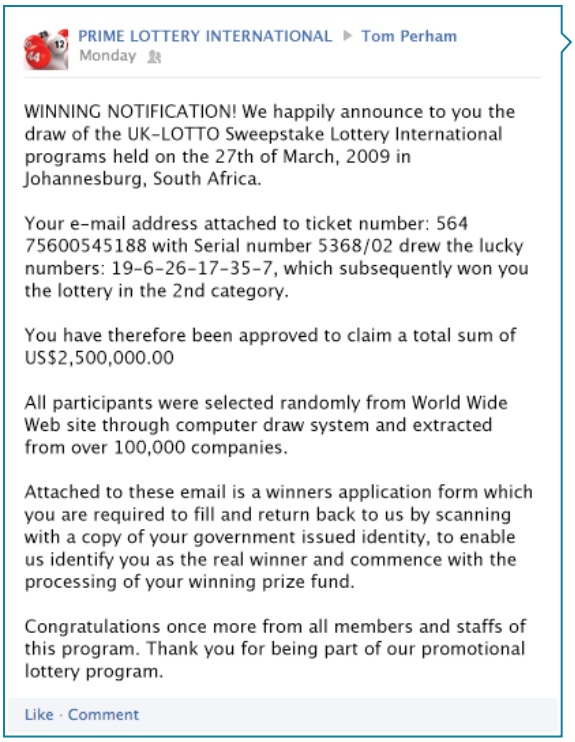
Scammers, pretending to be from a major technology company like Microsoft, make unsolicited calls claiming that they "have been alerted that your computer is infected." They may try to convince you to let them take control of your computer—for example, to remove a "virus." Instead they may install bogus software or even malware, and then charge you up to hundreds of dollars.

> As you have already seen, this means that your computer is also one of those computers which has been badly infected with those online infections, okay?

Here a scammer tried to convince an FTC investigator that her computer was infected with a virus.

Fraudulent contests and winnings

Fraudsters try to convince you that you've won a large sum of money through a contest, lottery, inheritance, or other fraudulent giveaway. These criminals promise to deliver the "winnings," but only after you pay a processing fee or the taxes either through a bank transfer or a credit card. Typically, once you pay these "fees," you never hear from them again. The crooks may also sell to other criminals the account data they gathered.



PRIME LOTTERY INTERNATIONAL ▸ Tom Perham
Monday

WINNING NOTIFICATION! We happily announce to you the draw of the UK-LOTTO Sweepstake Lottery International programs held on the 27th of March, 2009 in Johannesburg, South Africa.

Your e-mail address attached to ticket number: 564 75600545188 with Serial number 5368/02 drew the lucky numbers: 19-6-26-17-35-7, which subsequently won you the lottery in the 2nd category.

You have therefore been approved to claim a total sum of US$2,500,000.00

All participants were selected randomly from World Wide Web site through computer draw system and extracted from over 100,000 companies.

Attached to these email is a winners application form which you are required to fill and return back to us by scanning with a copy of your government issued identity, to enable us identify you as the real winner and commence with the processing of your winning prize fund.

Congratulations once more from all members and staffs of this program. Thank you for being part of our promotional lottery program.

Like · Comment

This fake Facebook message claimed that the recipient had won a lottery and asked him to provide a copy of his government-issued identity.

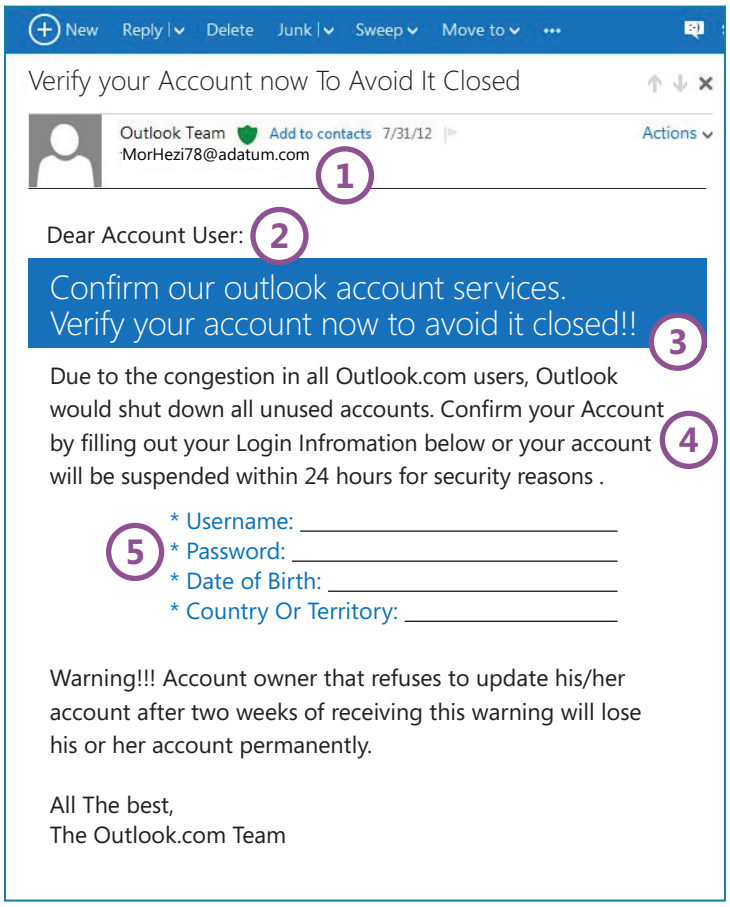
Financial scams

Criminals try to take advantage of people who are struggling financially with offers to repair a damaged credit report instantly or make debt disappear—for a fee paid before they provide any service. Other financial scams tempt with investment offers of high rates of return for little risk.

These are examples of false promises made in financial scams.

Spot the signs of online fraud

Stay alert to the signals of a scam, some of which appear in the email message below.



1. A suspicious email address. (Note that although it says it's from the Outlook team, the email address is not an Outlook address.)
2. Generic salutations rather than using a name.
3. Alarmist messages or urgent requests to download or install something. The scammer is trying to create a sense of urgency so you'll respond without thinking.
4. Grammatical errors and misspellings, which are used to break through phishing filters.
5. Requests to verify or update your account, stop payment on a charge, and the like.

PREVENTION:
Help guard against online fraud with four simple steps

Your best defense against online fraud is to heed this age-old advice—if it sounds too good to be true, it probably is—and take defensive steps including:

1 Treat suspicious messages cautiously

The most dangerous scams are those that look genuine. In general, be wary of the sender, even someone you know or a company you trust.

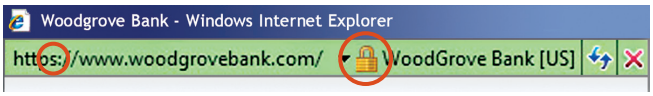
- Don't respond to the message even to remove your address from the sender's list. Responding lets the sender know that you exist and could result in even more messages.
- Think before you click links or call a number in a message, even if you know the sender; the links, phone number, and sender's identity could all be phony. Instead, confirm with him or her, using a different device and another account, that the message is genuine.

2 Protect sensitive information

Don't put sensitive information in an email, instant, or text message or unexpected pop-up windows.

Look for evidence that a webpage is secure and legitimate before you enter sensitive data.

- Check the web address for https ("s" stands for secure) and a closed padlock. (The lock might also appear in the lower right corner of the window.)



- Make sure that you're on the correct site—for example, on your bank's website, not a fake. One sign of trustworthiness is a green address bar, like the one above.

Save banking, shopping, downloading software, and other sensitive business for your home computer. When you use a public computer, or your own computer or mobile device over a public wireless connection, the security may be unreliable.

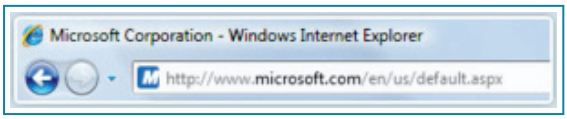
Back up your data regularly. Make it a habit to save your data using either a cloud service or a detached hard drive (ideally, both). That way, you can recover it in case of loss.

Review your bank and credit card statements monthly. Look for unexplained charges or inquiries that you didn't initiate.

Keep your primary email address private. Only share it with people you know or with reputable organizations. Avoid listing your address or name on Internet directories and job-posting sites.

Tip

Windows Internet Explorer emphasizes the domain name in the address bar with black type and the remainder of the address is gray to make it easier to see a website's true identity.



3 Strengthen your computer's defenses

Criminals try to install malware on computers that haven't been updated by exploiting older weaknesses in their software.

Keep all software up to date, including your web browser (like Windows Internet Explorer), operating system (like Windows), word processing, and other programs.

Subscribe to automatic updates whenever they are offered. For example, to automatically update all Microsoft software, go to www.update.microsoft.com.

Install antivirus and antispyware software from a trusted source. For example, Microsoft Security Essentials is a free program that helps guard against viruses, spyware, and other malware: www.microsoft.com/security-essentials.

Protect your wireless router with a strong password.

Never turn off the firewall on your computer. Turning it off even for a minute increases risk.

Don't follow the instructions of unsolicited callers or let them take control of your computer.

Tip

Microsoft can help you boost your computer's defenses: www.microsoft.com/security/pypc.aspx.

4 Create strong passwords

Criminals often use automated programs to break into accounts guarded by simple passwords, such as "password" or "12345678."

Strong passwords are long (phrases or sentences) that mix capital and lowercase letters, numbers, and symbols. They are easy for you to remember but difficult for others to guess.

Don't share your passwords with anyone.

Don't use the same password everywhere. If someone steals it, all the information that password protects is at risk.

Remember your passwords by storing them on a well-protected piece of paper away from your computer.

Tip

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

Tip

Test the strength of your passwords: www.microsoft.com/passwordchecker.

DETECTION:
Are you a victim of online fraud?

Even some of the most technically savvy people sometimes fall victim to online fraud through an imperfectly secured computer or a mistaken mouse click.

Is your computer infected with malware?

Some of the problems below could be the result of a failing hard drive, a recently installed program or update, or other computer malfunction. However, these are also signs that your computer could be infected with malware.

Your computer is suddenly slower, less responsive, or crashes frequently. If this behavior began suddenly after visiting a suspicious website or installing a program from an unknown source, it could be the result of an infection.

Your files or software programs are suddenly missing or inaccessible. If key system files, (especially security software) are unavailable, your computer might be compromised.

Pop-up windows suddenly appear when you're not on the Internet. Many types of spyware or rogue security software produce pop-up windows that ask for money or display ads.

Has your identity been compromised?

These are some signs that your identity may have been stolen:

- Mysterious and unexplained charges appear on your credit card or other online accounts.
- You are unable to access your bank or other accounts online.
- You are contacted by a collection agency to pay a bill for something you never bought.
- Your bank or credit card statements don't arrive. This could be a sign that someone has hijacked your account and redirected the statements elsewhere.

RECOVERY:
What to do if you are a victim of online fraud

Report suspicious or fraudulent incidents to the service provider. For example, in Microsoft services or software, contact us at www.microsoft.com/reportabuse. In addition, take these to help minimize any damage and protect your identity:

Restoring your computer

If you think your computer is infected with malware, here's what you can do:

Scan your computer. Use your antivirus software or the free Microsoft Safety Scanner, which checks for and removes viruses (working with your existing antivirus software), eliminates junk on your hard drive, and improves your PC's performance: www.microsoft.com/security/scanner.

Get help. If you have trouble restoring your computer so it works properly:

- Microsoft can help you diagnose and solve the problems that you find on your computer: www.consumersecuritysupport.microsoft.com.
- You can enter your zip code to find Microsoft-certified experts in your area: www.microsoft.com/security/partner-search-results.aspx.

Restore your data. After you've removed the virus or other malware, you may need to retrieve the data you backed up.

Recovering from identity theft

If you suspect that you are the victim of identity theft or you responded to a scam with personal or financial information, act immediately. Document your efforts as you go: make copies of all email messages and letters and keep detailed notes of phone calls.

Close credit card or other financial accounts that were accessed or opened fraudulently. Speak with the fraud department of each of those companies, and follow up with a letter.

Change the passwords or PINs on all other online accounts (email, social network, etc.) that are related or share the same password. (When you open new accounts, make sure to use new passwords and PINs.)

File a police report. Keep a copy to show your bank and other financial institutions that you're a crime victim, not a credit abuser.

Put a fraud alert on your credit reports. When you do this with one of the major U.S. credit bureaus, no financial institution will grant new credit without your approval.

Report the theft. In the United States, contact the Federal Trade Commission at ftc.gov/idtheft, or call toll-free (877) 438-4338.

Tip

Contact the major U.S. credit bureaus:

- **Equifax.** Answers to questions and phone numbers: www.equifax.com/cs/Satellite?pagename=contact_us
- **Experian.** www.experian.com or (888) 397-3742
- **TransUnion.** www.transunion.com or (800) 680-7289

MICROSOFT HELPS FIGHT ONLINE FRAUD

Microsoft aggressively fights online fraud through technology, anti-fraud teams, education and guidance, and partnerships with government, industry, law enforcement, and others.

Free security tools. We offer many online safety tools to help you fight online fraud, including Microsoft Security Essentials, the Microsoft Security Scanner, and our SmartScreen filter.

The SmartScreen filter in the Windows operating system and Windows Internet Explorer 9 and 10 warn you about potentially unsafe websites and helps protect you against downloading malware. Hotmail also uses SmartScreen technology to filter email, helping to separate phishing threats and other spam from legitimate email messages.

Dedicated anti-fraud teams. The Microsoft Digital Crimes Unit (DCU) is a team of lawyers, investigators, technical analysts, and other specialists from around the world. The DCU works to disrupt some of the most difficult cyber threats facing society today, particularly the sexual exploitation of children.

Education and guidance. The Microsoft Safety & Security Center provides guidance for safer Internet use, including tips on how you can secure your computer, help protect your children online, secure mobile devices, and avoid, block, and report inappropriate behavior.

Global partnerships. Microsoft works with governments around the world and with non-governmental organizations on issues of online fraud and abuse. With one such partner, National Cyber-Forensics & Training Alliance, Microsoft co-developed the Internet Fraud Alert, which allows participating researchers to report stolen account credentials to the appropriate institution when the theft is discovered online.

More helpful information

Microsoft Safety & Security Center
It provides guidance for safer Internet use: www.microsoft.com/security.

Microsoft Safer Online
Get regular safety tips via:

Facebook:
www.facebook.com/SaferOnline

Twitter:
www.twitter.com/Safer_Online

STOP | THINK | CONNECT™

This Microsoft-supported campaign aims to raise awareness of Internet safety risks and to promote strategies to help keep you safer online: www.stopthinkconnect.org.


Microsoft