Microsoft

Q4 – CY2012

Trustworthy Computing

Microsoft Scam Defense Survey

More than half of U.S. Adults have encountered online fraud and scams

There's a good chance you've received an email today saying, "Congratulations, you've won!" or that "Your friend has tagged a photo of you" on a social networking site and you need to check it out now. As online scams shift from exploiting vulnerabilities in software to tricking users into downloading viruses or divulging personal informtion, they are becoming more creative, sophisticated and targeted.

According to a new Microsoft Scam Defense Survey, the top five most commonly encountered scams are:

1. Lottery or "Congratulations, you've won!" scams promising free things or coupons (44%);
2. Fake antivirus alert scams that imitate real programs (40%);
3. Phishing scams using official-looking, yet fake, emails that encourage people to click them (39%);
4. Advance fee scams. For instance, someone like a "foreign prince" needs your bank account information because he wants to send you money (39%);
5. Work from home scams to "help you start your own business" (38%).

A wide array of scams continues to proliferate highlighting the growing nature of the threat. On average, adults have encountered roughly eight different types of online scams. While that mail from a "foreign prince" may seem routine, individuals are now most vulnerable to risks such as fraudulent and malicious links, online identity theft, and exposing sensitive personal information. The types of deceptive tactics used are becoming ever more effective at tricking even the most aware.

Percentage of U.S. Adults that Report Encountering the Following Scams (by category)

Impersonation - 55%	General - 54%	Shopping/Auction - 53%	Advance Fee, Job - 51%
Fake antivirus alert - 40%	Phishing scams – 39%	Lottery or 'you've won' - 44%	Advance fee fraud - 39%
Scams impersonating people you know - 22%	Fraudulent websites - 32%	Unsecured shopping websites - 21%	Work from home scams - 38%
Facebook friend added a new photo of you scam - 17%	Shortened URL scams - 18%	Email shopping - 20%	Money laundering job - 18%
FBI-related scams - 16%	SMS phishing scams - 17%	Auction scams - 15%	Postal forwarding or reshipping scams - 18%
Online dating scams - 16%	Spear phishing scams - 15%	Wrong transaction scams - 15%	

Only a handful of adults feel fully protected

- Nearly three quarters of respondents (72%) rated their own actions to help safeguard themselves from online fraud and scams to be excellent or above average, grading themselves an "A" or a "B" on an A-to-F grading scale.
- As a result, 62% of adults feel they are extremely (14%) or very (48%) unlikely to become a victim of an online fraud or scam.
- Yet, the survey found that only 12% say they feel fully protected. Furthermore, over half of the U.S. adults surveyed report that they are very or somewhat concerned about various types of online scams, such as general scams (54%), shopping and auction scams (54%) and impersonation scams (52%).

Help protect yourself from online scams & identity theft

- **Be defensive with sensitive information**
  - Avoid sharing it in email, instant (IM) or text messages. They may not be secure.
  - Save banking, shopping, and other financial transactions for your secured home computer.
  - Before entering sensitive info, look for signs a webpage is secure: "https" in the address and a closed padlock.

- **Boost your computer's security**
  - Keep all software (including your browser) current with automatic updating.
  - Install legitimate antivirus and antispyware software.
  - Protect your wireless router with a password, and use flash drives cautiously.
  - Think before you click links or call a number in a message, even if you know the sender. If you're unsure, make contact on a different device or account.

- **Create strong passwords or phrases**
  - Mix capital and lowercase letters, numbers, and symbols; keep them secret.
  - Don't reuse passwords.

- **Watch out for scams**
  - Be wary of alarmist messages with urgent requests for personal information.
  - Look out for misspellings and grammatical errors, or deals and prizes that sound too good to be true.

For more tips on protecting your information, family, and devices:

Microsoft.com/Security
Facebook.com/SaferOnline
Twitter.com/Safer_Online
YouTube.com/MSFTOnlineSafety

Glossary of Frauds and Scams

General Scams:

- **Phishing scams:** Phishing is a virtual trap set by cyber thieves that uses official-looking email messages, instant messages and posts on social networks to lure you to fake websites and trick you into revealing your personal information.
- **Spear-phishing scams:** Spear-phishing is a highly targeted phishing scam that seeks unauthorized access to confidential data—typically conducted by perpetrators out for financial gain rather than "random hackers." It targets select groups of people with something in common (e.g., you work at the same company, bank at the same financial institution, attend the same college, or order merchandise from the same website.)
- **SMS phishing or "SMiShing" scams:** SMiShing is a security attack in which you are tricked into downloading a Trojan horse, virus, or other malware onto your cellular phone or other mobile device. SMiShing is short for "SMS phishing."
- **Fraudulent websites:** These sites are often set up by phishers and other scammers as the destination for a phishing attack. These sites look legitimate, often impersonating your bank, credit card company, or other trusted institution. The sites are designed to trick you into either providing your sensitive personal information or downloading malicious software onto your computer.
- **Major event scams:** These scams try to lure you into clicking links to fraudulent websites, or downloading malware through email, social networks, or text messages. The scammers use the draw of current events or other popular topics, preying on your need to be "in the know" or up to speed on what "everybody's talking about" to lure you to a fraudulent website that downloads malware onto your machine. Common topics are natural disaster relief for tragedies like the 2011 tsunami in Japan, links to celebrity videos everyone's talking about such as the Erin Andrews "peep hole" video scandal, and supposed cheap tickets to high-demand sporting events such as the Olympics.
- **Shortened URL scams:** Given the demand for shortened URLs driven by social networks like Twitter, scammers are now using these shortened URLs to trick you into clicking links that otherwise might appear suspicious to you. Many of us now know how to spot a suspicious URL in a link, but if the URL is shortened using one of the common URL shorteners like bit.ly or owl.y, it may not be so obvious. Scammers are now disguising their links to fraudulent websites or malware downloads by first converting them to shortened URLs before sending them in tweets, social networking posts, or other communications.

Advance Fee Fraud and Job Scams:

- **Advance fee fraud (e.g., "foreign dignitary") scams:** These email scams seek to trick you into wiring money, or try to gain access to your bank account or debit card, by asking you to be an accomplice who will help the sender—often some "foreign dignitary"—to transfer large sums of money into their account for a cut of the total. You may be asked to travel overseas to meet with the scammers and complete the necessary paperwork. But before the transaction can be finalized, you must pay thousands of dollars in "taxes," "attorney costs," "bribes," or other advance fees.
- **Money laundering job scams:** Money launderers often create job postings on popular sites like Monster.com that say they're recruiting American citizens to "process payments" or "transfer funds," because as foreign nationals, they can't do it themselves. When you respond to the ad, you're offered a "job" and asked to provide personal and bank account information. You then find your accounts have been wiped out. Or, even worse, if you cooperate, you'll be asked to use your personal bank accounts to move stolen or bad checks on the scammers' instructions and keep a percentage as your pay. You may then be liable to your own bank for depositing the scammer's rubber checks, and you could even find yourself implicated in the crime.
- **Work-from-home scams:** These take on various forms, but typically fall into two categories: 1) asking you to work from home stuffing envelopes, assembling crafts, etc., or 2) "helping" you start your own home-based business (e.g., mystery shopper, network marketer, etc.)—but the only money anyone sees is the money the scammer pockets from the "start-up costs" you send them.
- **Postal forwarding or reshipping scams:** These begin with online ads seeking a "correspondence manager" for an offshore corporation that lacks a U.S. address or bank account, and needs someone—like you—to accept goods and reship them overseas. Or you may be asked to accept wire transfers into your bank accounts and then transfer the money to your "new boss's" account. In each case, you are promised a percentage of the goods or amount transferred. Products are purchased online using stolen credit cards—often with identities that have been purloined by phishers—and shipped to your address. You then reship the goods to the

thieves, who fence them overseas. Or, you transfer stolen funds from one account to another, obscuring the money trail. Either way, you can end up with your bank accounts drained, and you may even be implicated in the criminal operation.

Shopping and Auction Scams:

- **Lottery or "Congratulations, you've won!" scams:** These scams seek to trick you into wiring money, or try to gain access to your bank account or debit card, by informing you that you've won a lottery or a particular item—typically the hot gadget *du jour* like an iPod or Xbox. But, before you can receive the winnings or prize, you're asked to send money in advance to cover processing fees or taxes, etc.
- **Auction scams:** Auction scams list items on the most common auction sites, like eBay. When you "win" the auction and send your money, you never get the product promised, or the promises don't match the product. Descriptions may be vague, incomplete, or completely fake.
- **Wrong transaction scams:** Scammers send an email from a hotel or airline that you recently patronized, citing an incorrect charge to your credit card. They then ask you to go to a (fraudulent) website and complete a form for a refund.
- **Email shopping scams:** In a form of phishing scam that's prevalent during the holidays, scammers send an email from your favorite store offering a huge discount. The link takes you to a fraudulent site that can install malware on your computer or access sensitive personal information.
- **Unsecured shopping websites:** An unsecured website does not use encryption technology to protect information being sent to and from the site. While unsecured websites are not scams themselves, they are common targets for fraud, so if you enter sensitive information there, it can easily be stolen and used for identity theft. You can distinguish secure websites from unsecure ones by looking for "https://" vs. "http://" at the beginning of a sites URL. The 's" indicates the site is secure. You can also look for a closed padlock either next to the web address or in the lower right corner of the window.
- **Auto fraud scams:** Scammers attempt to sell you a car online that they do not own. Often the reason stated is an impending move, which the scammer uses as a reason to rush the sale and avoid meeting in person. The scammer then asks you to wire money to a third party who will hold the money in "escrow" until the car is delivered. The scammer takes the money and doesn't deliver a vehicle.
- **Overpayment scams:** In these scams, a buyer "overpays" you for something you may be selling online—either through a popular auction site or classified ads service. The scammer overpays with a money order that looks real, but is fake. He or she then asks you to send or wire back the difference. You are out the money you send and if you provided the scammer with any account information to "refund" the money, you could lose the money in your bank account as well.

Impersonation Scams:

- **Tech support scams:** These begin with a scammer posing as a tech support person from a respected company, like Apple, Dell, or Microsoft. They call you on your phone to tell you your computer is infected with a virus or has some technical problem, and attempt to trick you into installing malicious software that could capture sensitive data, such as online banking user names and passwords. The thieves might also try to charge you to remove this supposedly harmful software.
- **FBI-related scams:** In these scams, a caller claims that you are delinquent on your taxes or some government loan or subsidy and must repay the money owed to avoid legal action. The callers purport to be FBI, IRS, or other government agents, or representatives of law firms or collection agencies. You are then directed to a fraudulent website to pay your "debt" online.
- **Loan intimidation scams:** Similar to FBI-related scams, a caller claims you are delinquent on your loan and must repay it to avoid legal consequences. The callers purport to be representatives for legitimate-sounding agencies or companies, collecting debts for various companies. You are then directed to a fraudulent website to pay your "debt" online.
- **Traffic ticket scams:** Similar to FBI-related scams, an email claims that you were issued a traffic ticket and must pay the fine to avoid legal action. Callers purport to be agents of legitimate-sounding agencies, collecting debts for various jurisdictions. You are then directed to a fraudulent website to pay your "fine" online.
- **Live chat scams:** Through malicious code already installed on your machine, scammers generate a "live chat" pop-up when you visit your bank's website. (The bank's website has not been hacked—the pop-up is generated from your own, already compromised computer.) The pop-up impersonates a bank service rep who tells you that the bank system doesn't recognize you and asks you to

provide information to confirm your identity. This scam is particularly effective because it occurs while you are visiting a site that you know is secure and authentic.

- **Political survey scams:** The fake political survey scam is phone- and Internet-based. Initially, you receive a telephone call from an organization purportedly conducting a political survey. After answering a few questions, you are told that you have won a prize of some sort and told you must pay a processing fee to receive your prize. You are given a website address to verify the legitimacy of the call and then are asked for your credit card information.
- **Online dating scams:** Scammers pose as people looking for dates, but are not potential dates at all. A scammer will pose as an online love interest that likes you and asks you for your email address, at which point you get marketing email or other spam. Or, the scammer asks you to send money to pay for a trip to visit you or to help them deal with some personal "family emergency."
- **Fake antivirus alert scams:** These scams try to trick you into downloading malware onto your computer by delivering a fake alert that tells you your computer is infected with a virus. Fake virus alerts are usually generated by a Trojan—a program that takes control of your computer after you open an email attachment, click on a pop-up advertisement, or visit a particular website.
- **Scams impersonating people you know (e.g., fraudulent requests to wire money):** These scams typically start when a friend or family member's email or social networking account has been compromised. The scammer, now in control of the account, impersonates your friend or family member and sends you a message or email detailing some crisis (e.g., having been robbed while travelling overseas), and asks you to wire money.
- **Facebook friend added a new photo of you scam:** This scam sends you a fake email from Facebook claiming a close friend has tagged you in a photo. It asks you to click on the attachment to see the photo. Clicking on the attached ZIP file releases malware in the form of a Trojan — a program that takes control of your computer after you open an email attachment.