

RKL Consulting Group Internet Security

Security Tip #1:

Smooth Operators: Fraudsters and Hackers

Fraudsters and hackers are constantly thinking of new ways to obtain information and enter a system. Below are some tactics that fraudsters and hackers may use:

They might call the authorized employee with some kind of urgent problem; as fraudsters and hackers often rely on the natural helpfulness of people as well as on their weaknesses. Appealing to your vanity, authority, and old-fashioned eavesdropping are typical fraudster and hacker techniques.

Fraudsters and hackers may rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it.

Fraudsters and hackers will search dumpsters for valuable information. This activity is known as dumpster diving. Make sure that you and your company shred all documents that are important, confidential and contain sensitive information.

Fraudsters and hackers will also memorize access codes by looking over someone's shoulder. This is known as "shoulder surfing". Make sure when entering private codes, whether at your computer or withdrawing money from an ATM that you do not have a shoulder surfer behind you.

Fraudsters and hackers also take advantage of people's natural inclination to choose passwords that are meaningful to them but can be easily guessed. LexisNexis will be distributing documents to help you choose a password.

Security experts propose that as our culture becomes more dependent on information, fraudsters and hackers will remain the greatest threat to any security system.

Prevention of fraudsters and hackers includes educating people about the value of information, training them to protect it, and increasing people's awareness of how fraudsters and hackers operate.

Security Tip #2:

Understanding Malware

Malware

Malware is any software program developed for the purpose of causing harm to a computer system, similar to a virus or trojan horse.

Malware can be classified based on how it is executed, how it spreads, and/or what it does. The classification is not STRICTLY DEFINED SINCE groups often overlap and the difference is not always obvious. It is very common for people to use the words adware, spyware, and malware interchangeably. To help protect your systems from Malware it's critical that you install and use anti-virus programs. Most products that call themselves spyware or adware removers will actually remove all types of malware.

Here are a few types of Malware:

Keylogger

A keylogger is software that copies a computer user's keystrokes to a file, which it may send to a hacker at a later time. Often the keylogger will only "awaken" when a computer user connects to a secure website, such as a bank. It then logs the keystrokes, which may include account numbers, PIN numbers and passwords, BEFORE they are encrypted by the secure website.

Spyware

Spyware is a piece of software that collects and sends information (such as browsing patterns in the more benign cases or credit card numbers in more malignant cases) about users or, more precisely, the results of their computer activity, typically without explicit notification. They usually work and spread like Trojan horses. The category of spyware is sometimes taken to include adware of the less-forthcoming sort.

Adware

Adware is the class of programs that place advertisements on

your screen. These may be in the form of pop-ups, pop-unders, advertisements embedded in programs, advertisements placed on top of ads in web sites, or any other way the authors can think of showing you an ad. The pop-ups generally will not be stopped by pop-up stoppers, and often are not dependent on your having Internet Explorer open. They may show up when you are playing a game, writing a document, listening to music, or anything else. Should you be surfing, the advertisements will often be related to the web page you are viewing.

Hijackers

Hijackers take control of various parts of your web browser, including your home page, search pages, and search bar. They may also redirect you to certain sites should you mistype an address or prevent you from going to a website they would rather you not, such as sites that combat malware. Some will even redirect you to their own search engine when you attempt a search. NB: hijackers almost exclusively target Internet Explorer.

Toolbars

Toolbars plug into Internet Explorer and provide additional functionality such as search forms or pop-up blockers. The Google and Yahoo! toolbars are probably the most common legitimate examples, and malware toolbars often attempt to emulate their functionality and look. Malware toolbars almost always include characteristics of the other malware categories, which is usually what gets it classified as malware. Any toolbar that is installed through underhanded means falls into the category of malware.

Dialers

Dialers are programs that set up your modem connection to connect to a 1-900 number. This provides the number's owner with revenue while leaving you with a large phone bill. There are some legitimate uses for dialers, such as for people who do not have access to credit cards. Most dialers, however, are installed quietly and attempt to do their dirty work without being detected.

E-mail Scams: Phishing

All Internet users should be aware of the online scam known as "phishing" (pronounced "fishing"). Phishing involves the use of e-mail messages that appear to come from your bank or another trusted business, but are actually from imposters.

Phishing e-mails typically ask you to click a link to visit a Web site, where you are asked to enter or confirm personal financial information such as your account numbers, passwords, Social Security number or other data. Although these Web sites may appear legitimate, they are not. Thieves can collect whatever data you enter and use it to access your personal accounts.

Other sites appear non-functional or temporarily out of service, this may be deceiving and in reality, the site may be downloading a virus and/or other ill-intended software to your computer.

How can I spot a phishing scam?

Look for these warning signs:

Language and tone. The message you receive may urge you to act quickly by suggesting that your account is threatened or will expire soon. It may say that if you fail to update, verify or confirm your personal or account information, access to your accounts will be suspended. The wording **may** also be sloppy and contain misspellings and or grammatical errors.

Requests for personal information. Scam e-mails typically ask for personal or account information such as:

- Account numbers and passwords
- Credit and check card numbers
- Social Security numbers
- Online banking user IDs and passwords
- Mother's maiden name
- Date of birth
- Other confidential information

E-mailed instructions to download software. All your

online business web access should be done through our secure Web site, and businesses will not send you e-mail instructions to download any software to your computer. Do not install software downloads directly from e-mail messages, or from companies or Web sites you do not recognize. When in doubt, contact the company directly.

Non-secure Web pages. Clever thieves can build a fake Web site that looks nearly identical to an authentic one. They can even alter the URL (the Web address) that appears in your browser window address field on the top. Watch out for non-secure Web pages that ask for sensitive information (secure sites will typically display a lock in the status bar at the bottom of your browser window).

How can I decrease my risk of being a phishing victim?

Here are some safety tips:

Be suspicious of demanding messages. Messages threatening to terminate or suspend your account without your quick response should be treated as suspicious. A legitimate business should not request personal information from you over an unsecured Web site. When in doubt, call the business' customer service number (available on your account statement) to confirm the status of your account. Do not use telephone numbers found on the suspected Web site or email.

Be cautious of downloads. Installing unknown software on your computer can put your personal information at risk and potentially harm your computer's hard drive. Make sure the software comes from a legitimate Web site, not an e-mail message. If you are not sure whether you should download a program, contact a customer service representative for more information.

Always type in the URL of the Web page you need.

Phishing scams rely on embedded links that take you to fake Web sites. It is safer to type your intended Web address directly into your browser so you know you are visiting the legitimate site.

Protect your password. Do not write down sensitive personal information such as your login ID, password or Social Security number.

Keep your computer up-to-date. Industry best practices

recommend that you install anti-virus and firewall programs to help keep your computer safe and that you keep updated with the latest Security improvements of your software providers.

Report an online scam

Call your local police

Learn more about phishing

To learn more about phishing, review the suggested materials below:

[phishing brochure](#) provided by The Office of the Comptroller of the Currency (OCC).

www.antiphishing.org

"How Not to Get Hooked by the 'Phishing' Scam," available at:

<http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm>,

"ID Theft: When Bad Things Happen to Your Good Name," available at:

<http://www.ftc.gov/bcp/edu/microsites/idtheft/>.

Recent phishing scam

Some customers have recently received e-mail messages thanking them for their order and advising them their credit card has been charged. The email directs them to login to their account and shows an invoice for 500 Look-Up Credits and mentions an amount of \$499.99

This e-mail message includes a link that **appears** to take customers to a Web site—however; the Web pages they go to are not legitimate. They actually take customers to fake Web pages where the scammers may collect login ID, password and account information, they can also install malicious software (also known as spyware, malware, keyloggers, virus, etc. on your computer). **If you receive a suspicious e-mail message, please do not open the email or click on any links it may have.**

General Security Tips

While anyone can fall prey to fraud and identity theft, many ways exist to minimize your risk. RKL Consulting provides these

security tips so you can guard against fraud and identity theft.

Privacy

Never give out personal information online or over the phone unless you have initiated the contact. Avoid using easily guessed or learned information for as your online password

Avoid writing down passwords

Personal Computer Security

Introduction

One way a thief can get personal information about you is from your home computer. The following tips detail how you can add to the security of personal information on your home computer.

Passwords and User IDs

For each computer or online service you use, you should have a user ID and password. Try to create the most unique password, and protect it. Commit your password to memory and do not share it with anyone.

The following easily identifiable items should be avoided when creating passwords:

Your birth date or a family member's birth date

Names of family members or pets

Social Security number

Phone numbers

Dates of important events, such as anniversaries

Your login ID

Tips for creating strong passwords:

Use a combination of numbers, letters and punctuation.

Longer passwords are better.

Make sure it is something you can remember without writing it down.

Enable IP Restrictions for your email Account

System administrators can prevent unauthorized access by restricting their account to a specific IP address or range of IP addresses.

Install and Use Anti-Virus Programs

Viruses can infect a home computer in many ways: through floppy disks, CDs, e-mail, Web sites and downloaded files. Anti-virus programs help protect your computer against most viruses, worms, Trojans and other unwanted invaders that can make your computer "sick." Viruses, worms and the like often perform malicious acts, such as deleting files, accessing personal data or using your computer to attack other computers. If a file is infected with a virus, most anti-virus programs provide you with options of how to respond, such as removing the harmful item or deleting the file. Installing an anti-virus program and keeping it up-to-date is the best defense for your home computer.

Firewalls: What Are They and How Do I Use Them?

Before you connect your computer to the Internet, you should install a firewall. A firewall can be generally described as a security guard for your home computer. The guard is a piece of software or hardware that helps protect your PC against hackers and many computer viruses and worms. With a firewall, you define which connections between your computer and other computers on the Internet are allowed and which are denied. There are firewall programs, both free and available for purchase that provides the capabilities you need to help make your home computer more secure.

E-mail Attachments

E-mail viruses and worms are fairly common. Here are steps you can use to help you decide what to do with every e-mail message attachment you receive. You should only open and read a message that passes all of these tests:

The know test—is the e-mail from someone you know?

The received test—have you received e-mail from this person before?

The expect test—were you expecting e-mail with an attachment from this sender?

The sense test—does the e-mail subject make sense based on who is sending the e-mail? Would you expect this type of attachment from this person?

The virus test—does this e-mail contain a virus? To determine this, you need to install and use an anti-virus program.

Purchasing and Installing Programs

Apply these practices when you select software for your home computer.

Learn as much as you can about the product and what it does before you purchase it.

Understand the refund/return policy before you make your purchase.

Buy from a local store that you already know or a national chain with an established reputation.

Keep Your System Up-to-Date

Most software vendors provide free patches to fix problems in their products. You can usually download these patches from the vendor's Web site. When you purchase a program, it is a good idea to find out how the vendor provides customer support.

Backups: How Important?

It is a good practice to back up important files and folders on your computer. To back up files, you can make copies onto media that you can safely store elsewhere, such as CDs or floppy discs.