Identity Fraud May Be Down But Your Guard Needs to Stay Up!

Fraud comes in many shapes and sizes and unfortunately, it will never go away. Nor will the money and time spent fixing it. That's why it's vital to ramp up your security arsenal.

While fraud operators are constantly developing new viruses, spyware and online fraud schemes, the good news is that you can take action to protect yourself against online fraud. Delve into this site to find out how.

TAKE THE KEYS TO CONSUMER CONTROL: PREVENTION AND DETECTION

Prevention stops identity theft at the source and protects your private data before it is compromised by fraudsters. Taking advantage of online bill pay and even good old fashioned paper-shredding contributes to your own online safety.

Early **Detection** is equally important. Successful detection includes records consolidation and the regular review of your financial accounts for unusual activity. Banking online gives you quick access to your accounts, so that you can detect fraudulent activity sooner.

FRAUD TACTICS

Different fraud tactics all share the same goal: to obtain your personal, confidential and financial information for fraudulent use.

From obtaining your information 'the old fashioned way' via discarded mail, to emails that ask you to verify personal information under the guise of a trusted source — like your financial institution — fraudulent activity comes in many different forms.

FRAUD TACTICS INCLUDE:

Adware: Software that displays advertising content on your computer. Like its cousin spyware, some adware runs with your full knowledge and consent, some doesn't. More often an annoyance than a security risk, adware may also monitor browsing activities and relay that information to someone else over the Internet.

Bot or Web bot: Derived from "robot." An automated program, such as a Web crawler, that performs or simulates human actions on the Internet. Used for legitimate purposes by search engines, instant message (IM) programs, and other Internet services. Web bot can also be used to take control of computers, launch attacks, and compromise data; may act as part of a blended threat.

Botnet or Zombie Armies: A group of computers that have been compromised and brought under the control of an individual. The individual uses malware installed on the compromised computers to launch denial-of-service attacks, send spam, or perpetrate other malicious acts.

Denial-of-Service (DoS). An attack on a computer or network in which bandwidth is flooded or resources are overloaded to the point where the computer or network's services are unavailable to clients. Can also be carried out by malicious code that simply shuts down resources

Dumpster Diving: Thieves rummage through trash looking for bills or other paper that includes your personal information.

Spam: Unsolicited email, usually sent in bulk to a large number of random accounts; often contains ads for products or services. Also used in phishing scams and other online fraud. Can be minimized using email filtering software.

Spim or Instant Spam: Unsolicited instant messages, usually sent in bulk to a large number of IM accounts; often contain marketing materials and links to product Web pages. May also be used in phishing scams or to spread malware. See also, *spam*.

Spoofing: Spoofing is when an attacker masquerades as someone else by providing false data. Phishing has become the most common form of Web page spoofing. Another form of spoofing is URL spoofing. This happens when an attacker exploits bugs in your Web browser in order to display incorrect URLs in your browser location bar. Another form of spoofing is called "man-in-the-middle". This occurs when an attacker compromises the communication between you and another party on the Internet. Many firewalls can be updated or configured to significantly prevent this type of attack.

Spyware: Loaded on to your computer unbeknownst to you, spyware is a type of program that watches what users do and forwards information to someone else. It is most often installed when you download free software on the Internet. Unfortunately hackers discovered this to be an effective means of sending sensitive information over the Internet. Moreover, they discovered that many free applications that use spyware for marketing purposes could be found on your machine, and attackers often use this existing spyware for their malicious means.

Keylogger: Software that monitors and captures everything a user types into a computer keyboard. Used for technical support and surveillance purposes. Can also be integrated into malware and used to gather passwords, user names, and other private information.

Malware: Also known as 'malicious software', malware is designed to harm, attack or take unauthorized control over a computer system. Malware includes viruses, worms,Trojan horses,some keyloggers, spyware, adware and bots. It's important to know that Malware can include a combination of the types noted.

Pharming: Pharming takes place when you type in a valid Web address and you are illegally redirected to a Web site that is not legitimate. These 'fake' Web sites ask for personal information such as credit card numbers, bank account information, Social Security numbers and other sensitive information.

Phishing: A scam that involves the use of replicas of existing Web pages to try to deceive you into entering personal, financial or password data. Often suspects use urgency or scare tactics, such as threats to close accounts.

Pop-Ups: A form of Web advertising that appears as a "pop-up" on a computer screen, pop-ups are intended to increase Web traffic or capture email addresses. However, sometimes pop-up ads are designed with malicious intent like when they appear as a request for personal information from a financial institution, for example.

RetroVirus: This virus specifically targets your computer defenses. It will look for vulnerabilities within your computer operating system or any third party security software. Most security vendors have some form of tamper-proof measure in place, so it is important to keep your patches up-to-date. Retro Viruses are usually combined with another form of attack.

Social engineering: A method of deceiving users into divulging private information, social engineering takes advantage of our natural tendency to trust one another rather than rely solely on technological means to steal information. Often associated with phishing, pharming, spam, and other Internet-based scams.

Trojans: A Trojan is malicious code that is disguised or hidden within another program that appears to be safe (as in the myth of the Trojan horse). When the program is executed, the Trojan allows attackers to gain unauthorized access to the computer in order to steal information and cause harm. Trojans commonly spread through email attachments and Internet downloads. A common Trojan component is a "keystroke logger" which captures a user's keystrokes in an attempt to capture the user's credentials. It will then send those credentials to the attacker.

Virus: A computer virus is a malicious program that attaches itself to and infects other software applications and files without the user's knowledge, disrupting computer operations. Viruses can carry what is known as a "payload," executable scripts designed to damage, delete or steal information from a computer.

A virus is a self-replicating program, meaning it copies itself. Typically, a virus only infects a computer and begins replicating when the user executes the program or opens an "infected" file.

Viruses spread from computer to computer only when users unknowingly share "infected" files. For example, viruses are commonly spread when users send emails with infected documents attached.

Vishing: Vishing is a type of phishing attack where the attacker uses a local phone number in the fake email as a means of obtaining your sensitive information. The goal is to fool you into believing the email is legitimate by instructing you that responding to the request by phone is safer than responding by email and shows authenticity. The unsuspecting caller is then tricked through an automated phone system to relinquish their sensitive information.

Worm: A worm is similar to a virus but with an added, dangerous element. Like a virus, a worm can make copies of itself; however, a worm does not need to attach itself to other programs and it does not require a person to send it along to other computers.

Worms are powerful malware programs because they cannot only copy themselves; they can also execute and spread themselves rapidly across a network without any help.

REPORT FRAUD

The impact of identity theft and online crimes can be greatly reduced if you can catch it shortly after your data is stolen or when the first use of your information is attempted. One of the easiest ways to get the tip-off that something has gone wrong is by reviewing your monthly statements provided by your bank and credit card companies for anything out of the ordinary.

If you know, or even think, you've been a victim of identity fraud, take immediate action and follow these five steps.

More specifics can be found on the FTC's Identity Theft Web site

1

Report the fraudulent activity. If the activity is related to our financial institution please contact us directly. If it is related to another financial institution, your credit card company, or any other organization contact them directly.

2

Contact one of the three consumer reporting companies and have a fraud alert placed on your credit report. This will help stop fraudsters from opening any additional accounts in your name. Contact only one of the following (the others are required to contact the other two):

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

3

Close any accounts that you know - or even think – might have been tampered with or opened fraudulently. Report the transgression to a security spokesperson at the relevant company. Ask them about any additional steps – they'll probably ask you to send relevant copies of the fraudulent activity.

You can also use the FTC Theft Affadavit ID Theft Affidavit (PDF, 56KB) as formal certification of your dispute.

4

File your complaint with the FTC. Use the online complaint form; or call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

5

Sharing your identity theft complaint with the FTC will help law enforcement officials track down identity thieves and stop them. Call or visit the local police or police in the community where the identity theft took place and file a

report. Have a copy of your FTC ID Theft complaint form available to give them. Obtain a copy of the police report and the police report number.

FRAUD PREVENTION

It's not always easy to identify online fraud but cybercrime prevention can be straightforward. When you're armed with a little technical advice and common sense, you can avoid many attacks. Remember that online criminals are trying to make their money as quickly and easily as possible. The more difficult you make their job, the more likely they are to leave you alone and move on to an easier target. The tips below provide basic information on how you can keep your computer and your identity safe.

SAFEGUARD YOUR EMAIL

Email is often a vehicle used to transmit malware and commit fraud. It is important to evaluate your email behaviors and develop good habits to help protect your computer and your identity.

In addition to viruses and worms that can be transmitted via email, phishing also threatens email users. A type of email fraud, phishing occurs when a perpetrator, posing as a legitimate, trustworthy business, attempts to acquire sensitive information like passwords or financial information.

TO SAFEGUARD YOUR EMAIL:

Never open or respond to SPAM (unsolicited bulk email messages).
Delete all spam without opening it. Responding to spam only confirms your email address to the spammer, which can actually intensify the problem.

Never click on links within an email.
It's safer to retype the Web address than to click on it from within the body of the email.

Don't open attachments from strangers.
If you do not know the sender or are not expecting the attachment, delete it.

Don't open attachments with odd filename extensions.
Most computer files use filename extensions such as ".doc" for documents or ".jpg" for images. If a file has a double extension, like "heythere.doc.pif," it is highly likely that this is a dangerous file and should never be opened. In addition, do not open email attachments that have file endings of .exe, .pif, or .vbs. These are filename extensions for executable files and could be dangerous if opened.

Never give out your email address or other sensitive or personal information to unknown web sites.
If you don't know the reputation of a Web site, don't assume you can trust it. Many Web sites sell email addresses or may be careless with your personal information. Be wary of providing any information that can be used by others for fraudulent purposes.

Never provide sensitive information in email.
Forged email purporting to be from your financial institution or favorite online store is a popular trick used by criminals to extract personal information for fraud. It is also a good idea not to send security passwords or one-time passcodes over email.

Don't believe the hype.

CHECKLIST

Protect your Privacy

- Don't include sensitive information in email.
- Never click on links within an email. Don't open SPAM or attachments from strangers.
- Be suspicious of emails asking for personal information.
- Be selective when providing your email address.
- Only open email and attachments from known senders.

Many fraudulent emails send out urgent messages that claim your account will be closed if sensitive information isn't immediately provided, or that important security needs to be updated online. Your financial institution will never use this method to alert you of an account problem.

Be aware of poor design, and/or bad grammar and spelling.
A tell-tale sign of a fraudulent email or Web site includes typos and grammar errors as well as unprofessional design layout and quality. Delete them immediately.

Backup your sensitive data records.
Consider backing up all sensitive files. This will not only help you restore damaged or corrupted data, but it will help protect against fraud attacks and help recover lost files if needed.

Safeguard your identity online
In addition to protecting your email, there are a number of guidelines to follow that will help safeguard your identity online. **Do not allow a Web site to keep sensitive information or credentials for future convenience.**

It is a common practice when registering for access to a Web site or making a purchase from a Web site to be asked if you want to keep your access credentials, credit card number or other sensitive information on file as a matter of convenience. This common request is referred to as "remembering" for the future use.

Be selective about where you surf.
Not all Web sites are benign. Sites that are engaged in illegal or questionable activities often host damaging software and make users susceptible to aggressive computer attacks.

Don't choose "Remember My Password."
You should never use the "remember password" feature for online banking or transactional Web sites.

Don't use public computers for sensitive operations.
Since you cannot validate the computer's integrity, there's a higher risk of fraud when you log in from a public computer.

Work on a computer you trust.
Firewalls, antivirus, anti-spyware and other protection devices help keep a computer properly monitored and provide peace of mind. These tools are important in order to protect your computer and data. A good firewall is critical if you commonly access the Internet via a wireless connection. It is also important to keep your computer up-to-date with patches to security tools as well as to the operating system and other programs on your computer. Make sure to configure your computer to update all security fixes.

Select a strong password.
The best password is an undetectable one. Never use birth dates, first names, pet names, addresses, phone numbers, or Social Security numbers. Use a combination of letters, numbers and symbols. Be sure to change your passwords regularly. Don't write down your passwords and try not to use the same password for every service you use online.

Use a secure browser.
Only use secure Web pages when you're conducting transactions online. Your online banking channel is secured with an Extended Validation SSL Certificate which provides an extra layer of protection to you by requiring third-party Certificate Authorities (CA) to follow a strict issuance and management process for certificate approval and delivery. This secure browser is recognizable because the browser

address bar (1) begins with ‘https’, (2) turns green (in high-security browsers) and (3) a special field appears to the right of the URL with a padlock and the name of the legitimate web site owner. If you click on this section, you can view the details of the Certificate.

Update security software often.
When you get notices from software vendors to update your software, do it. Most operating system and browser updates include security patches. Your name and email address may be all it takes for a hacker to slip through a security hole into your system. And it almost goes without saying, you should be protected by Internet security software, and it should always be up to date. Purchase a reputable brand of AntiVirus and be aware of fake anti-virus for “free.”

Avoid clicking on Ads.
Never click on Ads on social network sites. Sure these ads are there to assist in giving the website money, However these are one of the leading causes for Virus infections on systems today.

Sign off, shut down, disconnect.
Always sign off or logout from your online banking session or any other Web site that you’ve logged into using a user ID and password. When a computer is not in use, it should be shut down or disconnected from the Internet.

Lock your computer when it is not in use.
This helps protect you from unauthorized user access.

Beware of shoulder surfing.
This is a common tactic that happens in public places such as coffee shops, airports, libraries etc. where an attacker will look over your shoulder when you’re logged in to obtain your sensitive information. Be vigilant and aware of prying eyes.

Set up a timeout.
The Timeout feature is an additional safety check. It can prevent others from continuing your online banking session if you left your PC unattended without logging out. You can set the Timeout period in the User Options screen.

Enhanced Security Login
Online Security: Everyday, Everywhere

Never open or respond to SPAM (unsolicited bulk email messages).
Your online security has always been a top priority.

That's why Enhanced Login Security is so important. This security service is free, easy, and most importantly, gives you extra protection from fraud and identity theft.

CHECKLIST

Protect your Privacy

- Monitor your postal mail.
- Don't give out your personal information freely.
- Check your credit report annually.
- Shred documents containing personal information before discarding them