



Sitting Ducks

\$188,242

Average annual cost of cyber attacks for small and medium-sized businesses. Downtime could amount to losses of \$12,500 per day for some firms.

Source: Reuters, October 24, 2011



Cybersecurity Risks, Scams, Frauds, Crimes – 2012

Dave Hall
ESEP/CISSP
Hall Associates
301 641-1530

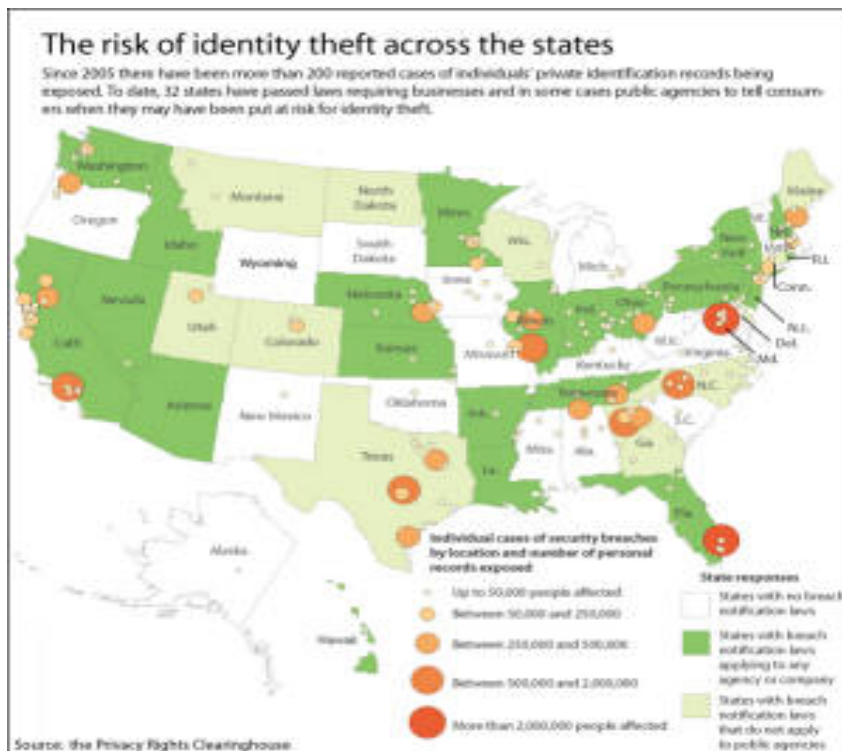
halld105048@yahoo.com

<http://www.linkedin.com/pub/dave-hall/22/4b6/5a2>



Contents

- **Why Do I Care About Cybersecurity?**
- **Cybersecurity Statistics**
- **Tips From The Trenches**
- **Interesting Occurrence Descriptions**
- **Summary and Conclusions**



Graphic by Danny Dougherty - StateLine.org

Why Do I Care About Cybersecurity?

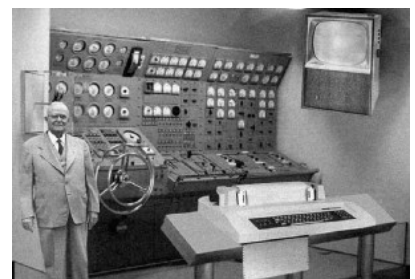


Because the Internet is not a very safe place.

There are cybercriminals trying to access your computer/network/mobile device, worms trying to infect you, malicious Trojans disguised as helpful programs, and spyware that reports your activities back to their makers. In many cases those who become infected unknowingly become a breeding ground for unwanted programs and criminal activity.

Your experiences in your business and personal life do not have to be this way. With proper education and smart computing the Internet can be a safe and useful place, without having to worry as much about what is lurking around the virtual corner.

This document was created to provide information on the threats “in the wild” you need to be aware of as well as providing tips and techniques for smarter and safer computing. If you use these tips and techniques you will be able to better protect your business and personal lives from cybercriminals. The advice in this document applies to all computer/network/mobile device users and all operating systems. It is impossible to completely secure any computer or network, but you can make it much harder for cybercriminals to get and use your information.



Why Do I Care About Cybersecurity?

You, your family, your business increasingly works with and through the Internet , computers and mobile devices, **making the vulnerabilities of and the threats inherent in these systems and devices far more menacing than ever. You are increasingly “connected” to the world and all of its cybercriminals.**

5 years ago people’s reactions were “I don’t want to do more. Get away from me. I feel like I am a slave to my computer. It’s taking away my life. Now people say “My device is part of who I am. It enriches my life. It helps me live on the edge.”. We have gone, in a VERY short time, from people being fearful of technology to being fearful of being without it. There is a new term – nomophobia – the fear of not being with your phone. Its derived from no mobile phone phobia.

Cybercrime today represents a primary threat on both a global , business and a personal scale. It is a rapidly growing industry impacting every sector of our society – causing serious financial losses. Cybercriminals are developing new methods and implementing new and sophisticated frauds, scams and schemes. And every day, there are more and more complex threats “in the wild”, making you and your business more and more vulnerable and more and more likely to become a victim. It’s not a case of IF you will be attacked, but of WHEN. **No system or device can be made absolutely secure. Knowledge is our only security, so read this document and learn to recognize scams, frauds, attacks and what to do to minimize your vulnerabilities.**

Cybercrimes, when they occur, will cause serious business and individual losses - lost resources, lost revenue, lost customers, lost reputation, lost personnel effectiveness, lost productivity - lost money, lost identity, lost credit, lost reputation.

And if you don’t know what threats you face, you will not be prepared for them.



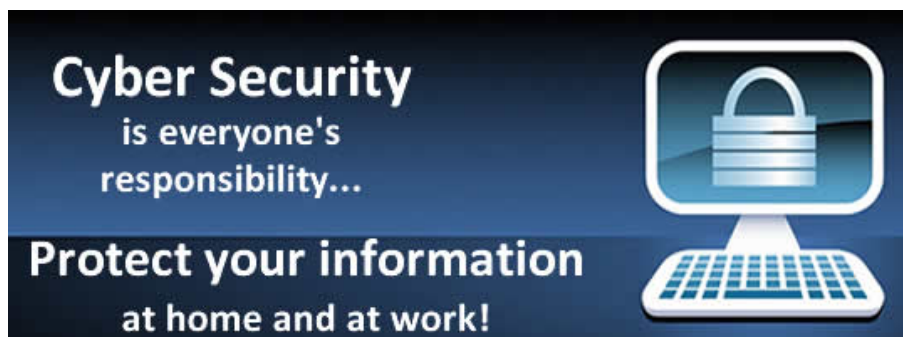
12/2012 Peacock Map – An Impression of What the Internet Looks Like

What is at Risk? From Where?

Your personal/business information, from wherever it is at is at risk from anywhere in the entire world!

Where is your information? Have you ever thought about that?

- Social; Networking sites (Facebook, MySpace, Blogs)
- Location-Based Social Networking Sites (Foursquare)
- Search Engines (www.popl.com and others) Look yourself or your business up!
- Resume Websites (Monster, ClearanceJobs, etc.)
- Official Websites/Medical Systems/School Systems
- Associations/Professional/Hobbies Websites (LinkedIn, Ancestry.com)
- In Cell Phones, PDAs, Smartphones (GPS capable, GPS coordinates on all JPEGs)
- E-Mail (official and personal), E-mail servers
- Cars (What is in your glove box?)
- Homes/businesses (Where is your personal/business information (electronic and hard copy) located?)



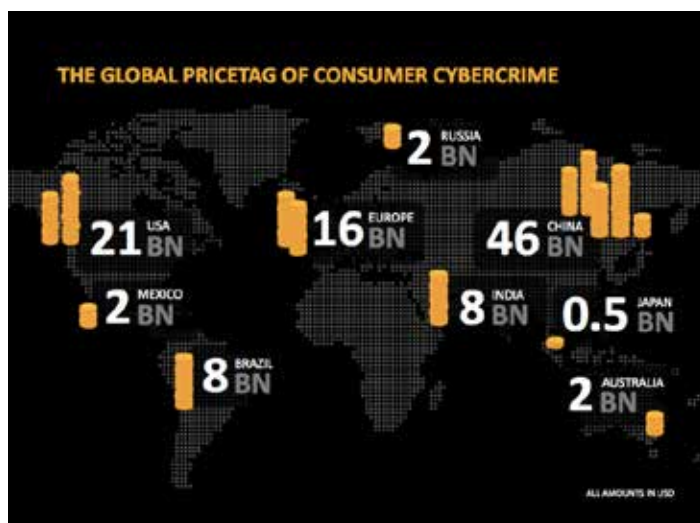
What is Cybersecurity Risk?

Cybersecurity risk definition: Any threat to your *personal or business information, critical systems/devices* and *business processes*.

Why me? Business management, employees and individuals have a responsibility to identify vulnerabilities and threats and respond in a timely fashion to these by improving processes, augmenting controls and requiring testing to ensure that the business is properly identifying and responding to these threats. Individuals also have a responsibility to properly identify and respond to these threats to maintain what they have. Now no other organization or person will replace funds you lose to a cybercrime. if the loss was due to your ignorance of a threat.

Why do I care? Failure to identify, assess, control and monitor these threats sets both businesses and individuals up to be serious cybercrime victims and financial/personal losses now and down the road. You can get cybercrime insurance, but it is extremely specific and costly. Current liability and errors/omissions insurance DOES NOT cover cyber.

What is the main issue? The challenge for most businesses and individuals is to determine what threats pertain to them and to identify a repeatable process to identify, assess, control and monitor these threats without interrupting their business or personal activities.



The Big Numbers for 2011

5.5B Attacks blocked by Symantec	↑	+81%
403M Unique variants of malware	↑	+41%
4,595 Web attacks per day	↑	+36%
4,989 New vulnerabilities	↓	-20%
8 Zero-day vulnerabilities	↓	-43%
315 New mobile vulnerabilities	↑	+93%
75% Spam rate	↓	-34%

What is Cybersecurity Risk?

Both business and home computers and mobile devices (phones, PDAs, tablets, etc.) are targets for the ever increasing number of cybercriminals.

Why? Because cybercriminals want what you've stored there! They look for credit card numbers, social security numbers, bank account information, and anything else they can find. By stealing this type of information, cybercriminals (no matter where they are in the world, can get and use YOUR money and your identities, your businesses money to buy themselves goods and services.

The above statement, while appearing self-evident, is really overlooked or ignored by most of the general population and business population and even by many of the computer-savvy population. **It seems that "...It won't happen to me or to my business." is a very common belief. A wrong common belief!.**

Not only are increasing numbers of cybercriminals attacking your existing computers and mobile devices, but also attacking any new and unprotected computers and mobile devices in increasingly shorter periods of time. **As a result, the average time to exploitation on some networks for an unprotected computer is measured in minutes.** This is especially true in the address ranges used by cable modem, DSL and dial-up providers, So your new home computer or mobile device is very vulnerable as soon as you connect it to the Internet.

This occurs because cybercriminals know the common broadband and dial-up IP address ranges and scan them regularly using automated scan applications. Also, most computers and mobile devices default configurations (how they are in the box) are really insecure. Numerous worms are already circulating continuously on the Internet scanning for new computers and mobile devices to exploit.



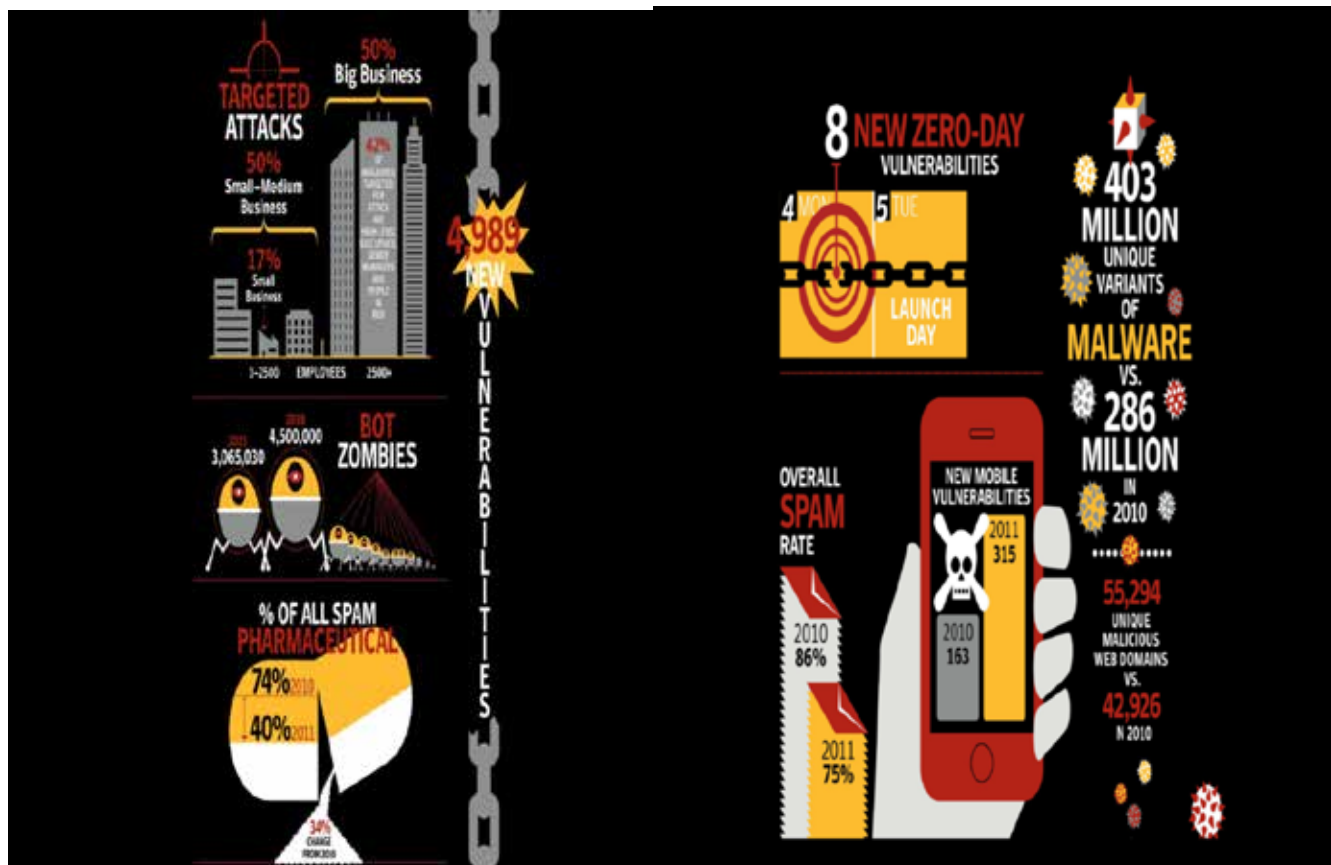
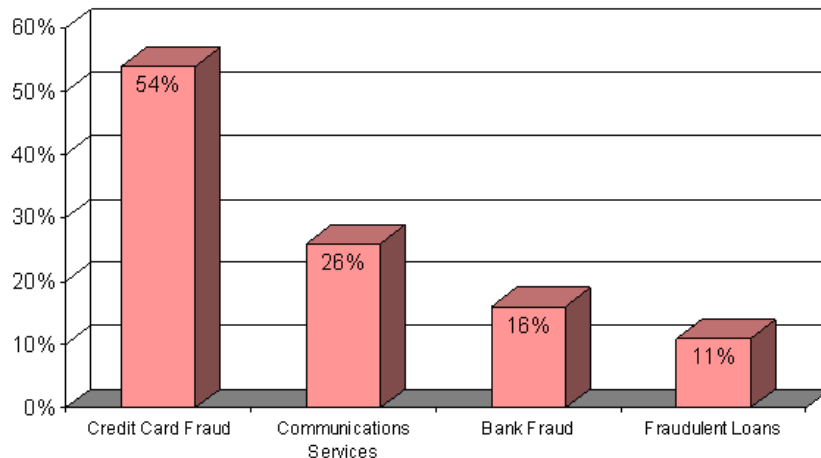
How to minimize the severity of security incidents.

- Outline clear course of action within the first 72 hours.
 - One early misstep can destroy crucial evidence, delay an effective response, and trigger government penalties or class-action lawsuits.
- Define responsibilities of a coordinated incident response team.
- Track fast changing data breach laws, privacy regulations, and notification mandates before a breach should occur.
- A comprehensive preparedness plan can promote better efficiencies when a breach threatens an organization.



Why Do I Care About Cybersecurity?

Most Common Forms of ID Theft

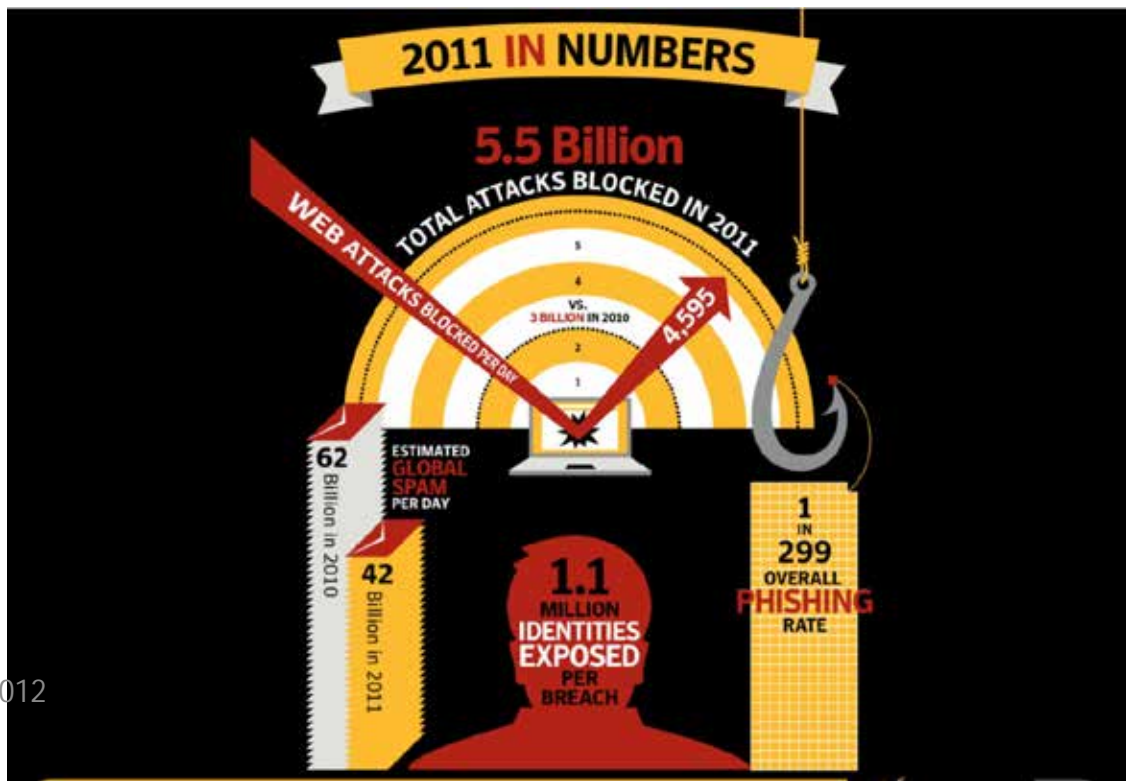


Why Do I Care About Cybersecurity?

The Federal Trade Commission's Identity Theft Clearinghouse collects and consolidates identity theft complaints. Their basic complaint data show that the most common forms of identity theft reported during the first seven months of operation were:

- ✓ Credit Card Fraud - Approximately 54% of consumers reported credit card fraud - i.e., a credit card account opened in their name or a "takeover" of their existing credit card account;
- ✓ Communications Services - Approximately 26% reported that the identity thief opened up telephone, cellular, or other utility service in their name;
- ✓ Bank Fraud - Approximately 16% reported that a checking or savings account had been opened in their name, and/or that fraudulent checks had been written; and
- ✓ Fraudulent Loans - Approximately 11% reported that the identity thief obtained a loan, such as a car loan, in their name.

The states with the largest populations account for the largest numbers of complainants and suspects. California, New York, Florida, Texas, and Illinois, in descending order, represent the states with the highest number of complainants.. About 55% of victims calling the identity theft hotline report their age. Of these, 40% fall between the 30 and 44 years of age. Approximately 26% are between age 45 and 64, and another 25% are between age 19 and 29. About 7% of those reporting their ages are 65 and over; and slightly over 2% are age 18 and under.

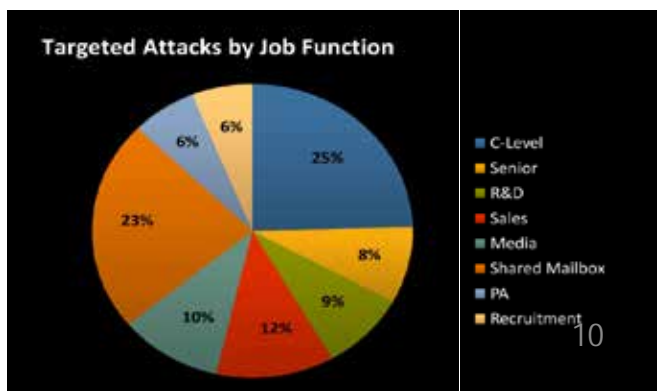
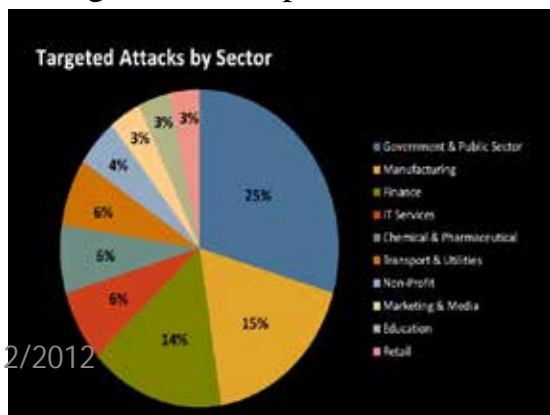


Cybercriminals Are Targeting Small Businesses And Individuals

Small businesses and individuals are now more at risk than large companies or government organizations. Large businesses and most government organizations can afford to hire IT professionals that focus solely on security while small businesses and individuals don't even know what vulnerabilities exist. While many small businesses and individuals think that their small size means that they are not on a cybercriminal's radar screen, the existence of holes in their systems and lack of social engineering methods and scams is exactly what is attracting the cybercriminals. **Cybercriminals use automated tools to search the internet and look for vulnerable businesses and individuals.**

The main defense against this is making sure that your computer systems and mobile devices are safe and secure and ensuring that you understand the potential social engineering methods being used. Make sure that all software is updated and all patches are installed properly, have policies in place to not visit dubious web sites, click on e-mail links or inadvertently share information with the wrong person. Have strong passwords on all devices and make sure all your data (no matter where stored) is encrypted. Encryption is the simplest and most powerful security measure. **Training is the best key to stopping these attacks.** At a minimum, you need an annual security training course that updates each year to include the new schemes and provide a refresher on long-term attacks like phishing.

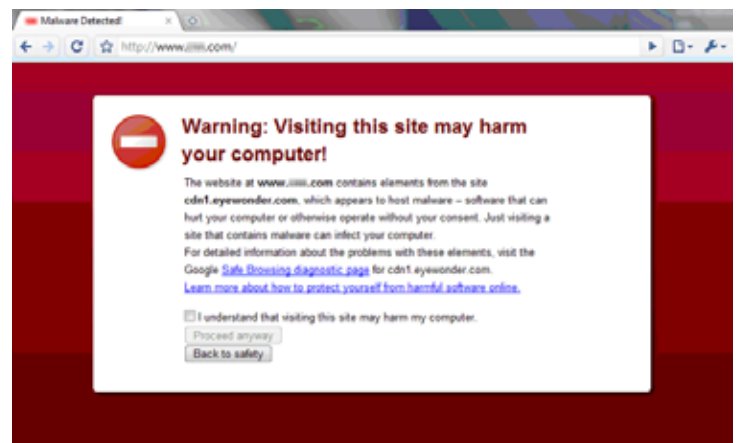
If you are infiltrated or breached, and important business and/or personal data falls into the wrong hands, how you respond makes a world of difference. For businesses, you should notify law enforcement about the breach immediately and notify customers/other businesses that are impacted to give them the chance to reduce potential misuse of their information. For individuals, you should notify law enforcement immediately and work to change accounts, passwords, etc. on ALL your accounts.



Cybersecurity Risk – What is Malware?

Viruses and Worms

Malware is short for malicious software – that is software that is used or created to disrupt computer operations, gather sensitive information or to gain unauthorized access to private computers or networks. It can appear in the forms of code, scripts, active content or other software types. Malware is the general term used to refer to a variety of forms of hostile or intrusive software. Malware includes worms, viruses, Trojan horses, spyware, adware, and numerous other malicious programs. In the legal code of some US states malware is known as a computer contaminant. A lot of malware is disguised as genuine software and some may come from an official company website. An example of this is software used for normal purposes that is packed with additional tracking capabilities that gathers marketing statistics.



Malware has caused the rise in protective software such as anti-virus, anti-malware and firewalls. The best known types of malware, viruses and worms, are named for the manner in which they are spread rather than any specific type of behavior. A virus is a program that infects some executable software and, en run, allows the virus to spread to other executable programs. A worm is a program that actively transmits itself over a network to infect other computers. These definitions lead to the observation that a virus requires user intervention to spread, but a worm spreads itself automatically.

Cybersecurity Risk – What is Malware?

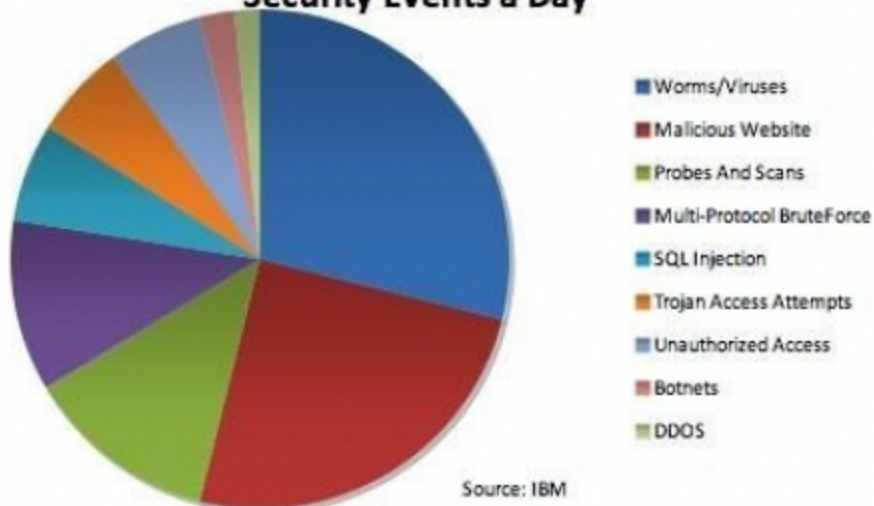


Trojan Horse

For a malicious program to accomplish its objective, it must be able to run without being detected, shut down or deleted. When a malicious program is disguised as something normal or desirable, users will willfully install it without realizing its malicious. This is the techniques used by Trajan Horses or simply Trojans. A Trojan is any program that invited the user to run it, while concealing harmful or malicious code. The harmful code may take effect immediately and will lead to numerous undesirable effects – such as deleting user files, installing additional software or sending your files to its creator.

One of the most common types of spyware is distributed as a Trojan, bundled with a piece of desirable software you download. When the desirable software is installed, the Trojan is installed with it. Some spyware actually pops up an end-user license agreement that states what it does (loosely) and most users never take the time to read these, simply clicking on **'I agree'** without understanding what they just agreed to.

Top Cyber Threats in 2011
Based on IBM Monitoring on Average 13 Billion
Security Events a Day



Cybersecurity Risk – What is Malware?



Rootkits

Once a malicious program is installed in your system, it is essential that it stays concealed and avoid detection. Techniques known as Rootkits allow this concealment by modifying your operating system so that the malware is hidden from the normal user. Rootkits can prevent a malicious program from being visible in your system's list of processes or keep its files from being read.

Some malicious programs contain routines to defend against removal, not just to hide themselves but to actually resist efforts to delete/remove them. AN early example of this behavior is in the Jargon file tale of a pair of programs infesting a Xerox CP-V timesharing system. Each ghost job (Malicious program) would detect that another had been detected and would start a new copy of the recently deleted program within a few milliseconds. The only way to kill all the ghost programs was to kill them simultaneously (very difficult) or to deliberately crash/wipe the entire system.



Trojan Horse Backdoors

Type of Trojan horse backdoor	Characteristics	Analogy	Example tools in this category
Application-Level Trojan Horse Backdoor	A separate application runs on the system	An attacker adds poison to your soup.	Sub7, BOZK, Tati, etc.
Traditional RootKit	Critical Operating System components are replaced	An attacker replaces your potatoes with poison ones	Lik6, T0nk1t, etc.
Kernel-Level RootKit	Kernel is patched	An attacker replaces your tongue with a poison one	Kaard, adore, Kernel Intrusion System, rootkit.com, etc.



Backdoors

A backdoor is a method of bypassing normal authentication procedures. Once a system has been compromised by a worm or Trojan, one or more backdoors may be installed automatically to allow easy entry in the future. Backdoors may also be installed by insiders before they are let go so that they can get into the system later and wreak havoc. There are indications that computer equipment from some foreign manufacturers may contain backdoors that allow foreign entities access to running computer systems.

Cybersecurity Risk – Credit/Debit Card Fraud



Credit card fraud is **up 87 percent since 2010**, resulting in a total loss of \$6 billion. Last year, about 8.6 million U.S. households, or 7 percent, experienced some form of identity theft, up from the 6.4 million that fell victim to identify thieves in 2005, according to Bureau of Justice Statistics estimates. The total financial losses for those households totaled \$13.3 billion. In most cases, identity thieves obtained victims' existing credit card information. The data includes both attempted and successful use of the stolen information.

The U.S. currently accounts for 47 percent of global credit and debit card fraud even though it generates only 27 percent of the total volume of purchases and cash,

Credit/Debit Systems - Four Steps for Protecting Customer Data

The Payment Card Industry Security Standards Council released a set of security standards to be followed by any business accepting credit and debit card payments. If a small business owner is not able to prove that they are PCI compliant by these standards and there is a data breach, **then the small business can be fined for each instance of the breach.** The fines can be extremely excessive and for some businesses they could put them out of business.

1. Visit PCISTandards.org and determine your merchant level.
2. Identify your validation type.
3. Pass a vulnerability scan. You must have proof of this scan in order to be compliant.
4. Obtain a certificate of Attestation. Once all else is done, you need to obtain a certificate from the PCI Security Standards Council. This must be done yearly.

And remember, this is an ongoing process. As your credit processing increases or you add new methods of payment your standards will change.

Cybersecurity Risk – Mobile Devices

The growth of cybercrimes targeting new social media platforms and mobile devices is really impressive. Cybercriminals love mobile devices due to their wide audience and almost complete lack of awareness of cyber risks.

BYOD – Bring Your Own Device to Work

More and more companies are allowing their employees to use their personal smartphones, tablets and computers for work, logging the devices on their business networks and databases. But without significant upfront planning and using the appropriate tools, **this can introduce significant risks to your business and even to the employees.** This risk is to your corporate data and employee personal information.

The biggest risk is that each of these devices has its own operating system. Hackers can go after different OSs differently since **all OSs have different vulnerabilities.** In a survey by Search Mobile Computing, 70% of businesses indicated that loss or theft of mobile devices was the top security concern. Yet, **only half** of companies participating in the survey had a policy requiring power-on passwords, and **just 41%** enforced the policy.

Hackers can find it easier to introduce malware onto employees devices because it is hard to enforce company security software on something not the company's property. Patching their software with the latest security patches is also questionable since the company IT folks can't look into personal devices. **It's hard to enforce social engineering policy and to limit what web sites are accessed on personal devices.**

Also, we are seeing attacks on mobile devices that enable conversations to be listened to and recorded even **if the mobile device is not "on"**. Note that smart phone photos are imprinted with the current GPS coordinates **unless that feature is turned off.**



Cybersecurity Risk – Mobile Devices

Think of how many individual mobile devices are now being used and who is using them. Over half of the people using smart mobile devices employ location-based applications despite concerns about safety and 3rd party use of their personal information. Almost half state that they don't read agreements when downloading apps. Add that to the fact that few organizations keep track of what type of devices access their organizational resources. More than 60% of organizations surveyed allow their personnel to bring their own smart devices to work and access organizational IT infrastructure. So organizations are allowing access to their IT infrastructure by mobile devices used by employees who download applications without understanding their consequences.

Google's Android is the most heavily targeted mobile operating system by malware since it is an open platform where malicious apps can make easy way to users' devices.



Cybersecurity Risk – Mobile Devices

In Q2 2012 5,033 pieces of malicious Android software were received by one security company, which represented a massive **64% increase** of Android malware over **Q1 2012**. This figure placed Android at the top of the list of the highest targeted mobile platforms at present. Most of these are coming from third-party Android markets. Out of the 5033, this company identified 19 new families and 21 new variants of existing families.

To protect your phone, use common sense. If you're downloading applications, look at the info you have available — user ratings, the developer, the number of downloads. If there's an app with few user comments and few total downloads, and it's released by a developer you never heard of, steer clear. If you see a free game or entertainment app that collects phone call, location and contact data, you should skip it. For Android, the danger is downloading apps outside of Google's App Market (or other reputable app stores such as Amazon's). If you're off somewhere getting apps from sources you don't know or trust, there could be consequences. For iPhone users, the line really is whether you jailbreak or not. Jailbreaking can be pretty easy, and getting pirated or bootlegged apps can seem like a great way to save money, but in doing so, you're basically handing out the smart phone equivalent of a front door key to someone .

Just realize that there are bad things out there.

History of Cyber Crime

When did this new and insidious variety of crime actually come into being? One may say that the concept of the computer came with the invention of the first abacus, hence it can be said that "cybercrime" per se has been around ever since people used calculating machines for wrong purposes. However, cybercrime has shown itself as a serious threat to society for less than a decade.

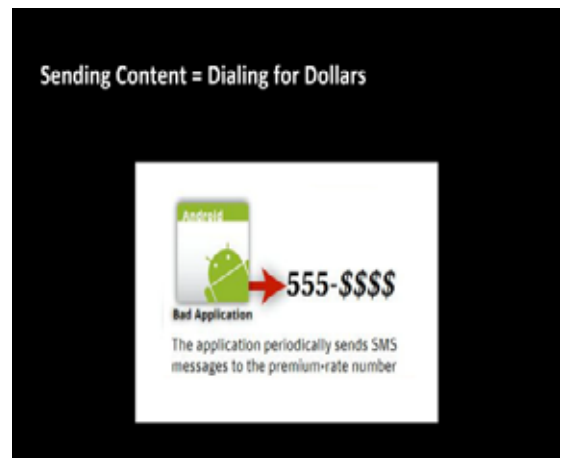


Cybersecurity Risk – Mobile Devices

Though they use different methods, Apple and Google are pretty good about monitoring what goes into their app stores. You should worry most if you're seeking ways to try to download premium apps without paying, trying to score bootleg apps available for "jailbroken" iPhones, or visiting any shady alternative Android app markets.

Geinimi Trojan - Hackers attach this to established apps and cutesy casual games such as "Monkey Jump 2" — over 30 apps so far. Then they redistribute the corrupted software in back-alley Android app stores. When people download the game or app, their whole phone gets taken over. Text messages, contacts and location information can be sent to a remote server, and evil-doers can even take over your phone, downloading files, placing phone calls and sending SMS messages.

SMS Android Trojan - This Trojan makes use of premium text messages. Once you download the seemingly harmless "Movie Player" app that it was hidden inside, it starts sending text messages to premium-rate numbers, each one levying a several-dollar charge to your phone bill. Though it's only surfaced on Android phones in Russia, it's probably worth keeping a close eye on your phone bill.



3D Anti-terrorist - This one was a game that was posted all around the Internet on download sites specializing in Windows Mobile apps. Much like the SMS Trojan, this one got hold of the phone and made premium-rate international calls, jacking up your phone bill in all kinds of ways. Windows Mobile was known for being wide open.



Examples of Cell Phone Malware

TapSnake - A supposed Snake game clone, the app would track your GPS coordinates and upload them to a remote server. If that wasn't bad enough, it would then download a premium app called GPS Spy, which would steal additional data from the phone. This malware made its way to Google's Android App Market before it got yanked.

Android.Opfake - Symantec has identified a trojan horse that affects Android users via SMS. It is a malware already known for years for desktop computers and laptops, but that has only recently been discovered for mobile operating systems. Certain parts of the malicious code changes every time it is downloaded, thus making each download unique. Although the origin of this “viral technology” was Russia, the trojan automatically sends text messages to phone numbers all over Europe, expanding the possible scope of action of the virus.

There are two new Android Trojans – **Loozfon and FinFisher**. Loozfon has the ability to steal a mobile user's phone number as well as contact details. It is promoted through work-at-home ads pushing users to websites designed to download Loozfon. FinFisher is spyware that targets Android Smart Phones hijacking specific components that enable criminals to remotely control and monitor the device regardless of its location. This is transmitted to your phone by clicking infected web links or by opening SMS messages sent directly to you. These SMS messages usually appear to provide links to system updates. In both of these, login credentials (username and password) for online banking access can be stolen. So mobile users that access online accounts through mobile browsers or those who save online banking credentials somewhere on their mobile devices are at serious risk. In addition, any online purchase made through an e-commerce site on a compromised mobile device exposes credit and debit details, including your three digit security codes.



Cybersecurity Risk – Mobile Devices

Navigation-and-emergency-services company OnStar is notifying its six million account holders that it will keep a complete accounting of the speed and location of OnStar-equipped vehicles, even for drivers who discontinue monthly service.

OnStar does not currently sell anonymized customer data, but it reserves that right. Both the new and old privacy policies allow OnStar to **chronicle a vehicle's every movement and its speed**. “What’s changed [is that if] you want to cancel your OnStar service, we are going to maintain a two-way connection to your vehicle unless the customer says otherwise. Canceling customers must opt out of the continued surveillance monitoring program, according to the privacy policy.”

An example of how the data might be used would be for a Department of Transportation “to get a feel for traffic usage on a specific section of freeway.” The policy also allows the data to be used for marketing purposes by OnStar and vehicle manufacturers.

Collecting location and speed data via GPS might also create a treasure trove of data that could be used in criminal and civil cases.



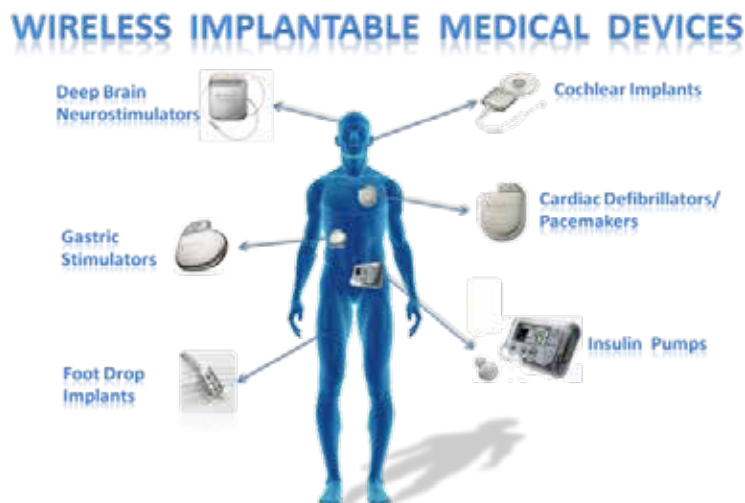
Cybersecurity Risk – Medical Devices

Over the past decade, there's been an explosion of tiny networked devices that manage a variety of health maladies, from regulating the beating of the human heart to controlling serious diabetic conditions. Allowing the devices to connect wirelessly to computers or other devices saves money and can eliminate the number of invasive surgeries needed to keep them in working order. But it also comes with a catch: researchers have devised proof-of-concept hacks that can disable or sabotage electronic pacemakers or deliver fatal insulin dosages over the air. In the case of wearable devices, it's crucial that they also authenticate the identity of the person who's using it.

This isn't the first time the issue has come up. A study in 2008 from a consortium of academics found that a popular pacemaker-defibrillator could be remotely reprogrammed to deliver deadly shocks. Now a way has been discovered to scan a public space from up to 300 feet away, find vulnerable pumps made by Minneapolis-based Medtronic Inc., and force them to dispense fatal insulin doses.

The U.S. Food and Drug Administration has said that electronic eavesdropping is a concern for any medical device with wireless communication components, and that device makers are responsible for making sure their equipment can be updated after it's sold. For many devices, that's not possible without a recall.

Medical malware is rampant in hospitals because of medical devices using unpatched operating systems. Under current law, software used to run medical devices in hospitals, once approved, must remain static. So manufacturers cannot provide updates to fix security flaws.



Cybersecurity Risk – Banking Trojans

The ZeuS Trojan and its rival SpyEye take advantage of security holes in your Internet browser to "piggyback" on your session when you log in to your bank's website. They avoid fraud detection using caution, calculating inconspicuous amounts of money to transfer out of your account based on your balance and transaction history.

While financial institutions continue to increase the layers of security involved in large transactions, such as requiring confirmation through "out-of-band" communications — such as your mobile device — digital crooks have lost no time adapting to the changes, with **banking Trojans able to change the mobile number tied to your account and intercept that confirmation request.** Who exactly is a target for these? **Basically anyone who does not have up-to-date anti-virus or anti-spyware software running on their PC.** Zeus is known to spread through spam emails, infected websites and even downloaded files.

How To Beat The Banking Trojans

Though banking Trojans are getting more sophisticated, you can keep them off your system by running regular scans with up-to-date security software. Don't click links in emails that claim to be from your bank, and when you go to your bank's website, use the latest version of your browser and enter the URL manually. If your bank offers extra security tools, use them. In the case of fraud, the bank is less likely to hold you liable if you have used its protection.



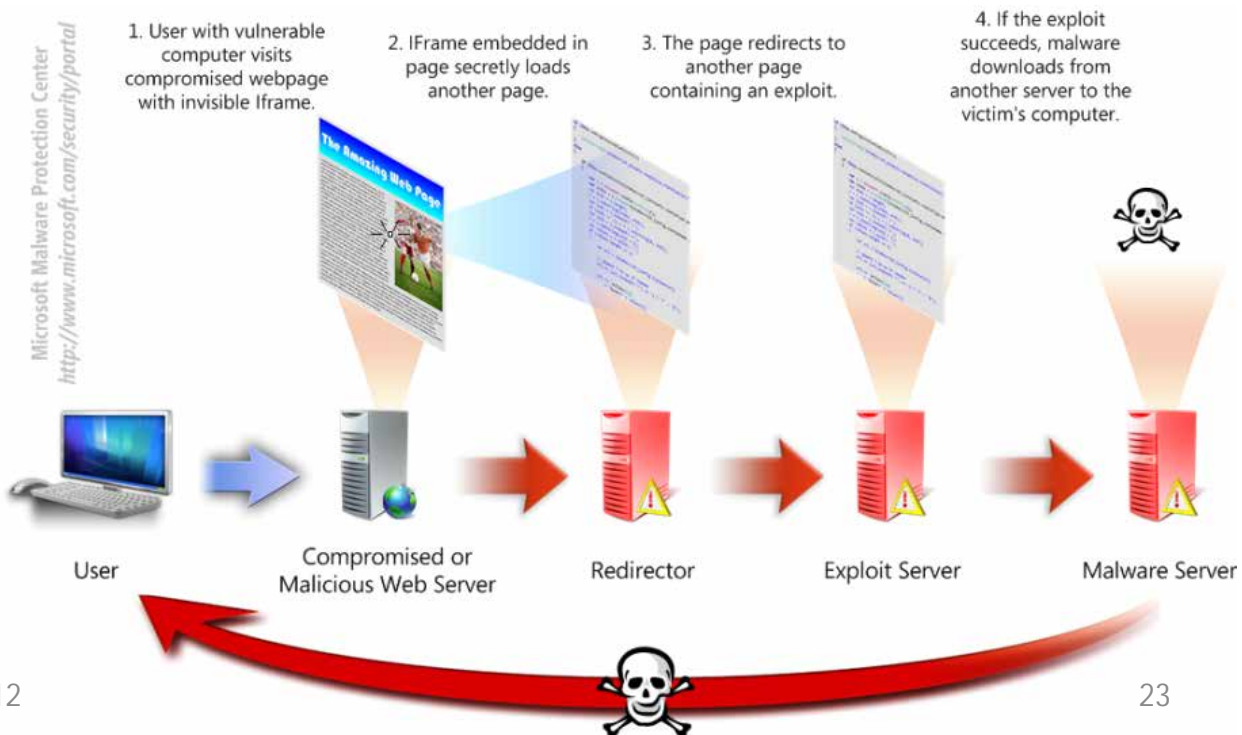
Cybersecurity Risk – Drive-By Malware Download

Drive-by download means two things, each concerning the unintended download of computer software from the Internet:

1. Downloads which a person authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet).
2. Any download that happens without a person's knowledge, often a computer virus, spyware, malware, or crimeware.

Drive-by downloads may happen when visiting a website, viewing an e-mail message or by clicking on a deceptive pop-up window: by clicking on the window in the mistaken belief that, for instance, an error report from the computer's operating system itself is being acknowledged, or that an innocuous advertisement pop-up is being dismissed. In such cases, the "supplier" may claim that the person "consented" to the download although actually unaware of having started an unwanted or malicious software download.

A detailed statistical analysis from Barracuda Labs shows the extent of drive-by downloading on the internet: more than 10 million users were exposed to drive-by exploits in February 2012 alone.



Cybersecurity Risk – Drive-By Malware Downloads

There are several sophisticated cybercriminal operations **that plant malware on news and other websites – but interestingly only on pages that contain specific articles/photos/etc.** that would interest the kind of people the cybercriminal wants to target. This kind of social engineering does a lot of the cybercriminal's work on winnowing down the universe of targets to just those of interest.

Most Harmful Websites by Categories

Malicious Web Activity:
Malicious Code By Number Of Infections Per Site, 2011

Rank	Categories Of Web Sites	Average Number Of Threats Found On Infected Web Sites	Major Threat Type Detected
1	Religion/ Ideologies	115	Fake Antivirus: 82%
2	Hosting/ Personal hosted sites	39	Trojans: 43%
3	Pornography	25	Trojans: 44%
4	Entertainment and Music	21	Fake Antivirus: 42%
5	Business/ Economy	17	Fake Antivirus: 62%
6	Technology/ Computer and Internet	17	Fake Antivirus: 54%
7	Travel	16	Fake Antivirus: 46%
8	Sports	13	Fake Antivirus: 69%
9	Automotive	11	Fake Antivirus: 41%
10	Shopping	9	Fake Antivirus: 63%

Source: Symantec

- Sites with poor security become easy targets for malware authors
- Some businesses understand that customers will visit sites that infect them

Cybersecurity Risk – Identity Theft

More than 187.2 million identities were exposed in 2011 by data breaches, but most of the breaches are linked to *old-fashioned theft (like a stolen laptop) and/or sloppy security* rather than to hacking. Top ten sectors for data breaches in 2011-

- 43% - Healthcare;
- 14% - Government;
- 13% - Education;
- 8% - Financial
- 5% - Arts and media;
- 5% - Computer Software;
- 4% - Retail;
- 3% - Hospitality
- 3% - Insurance;
- 3% - Information Technology



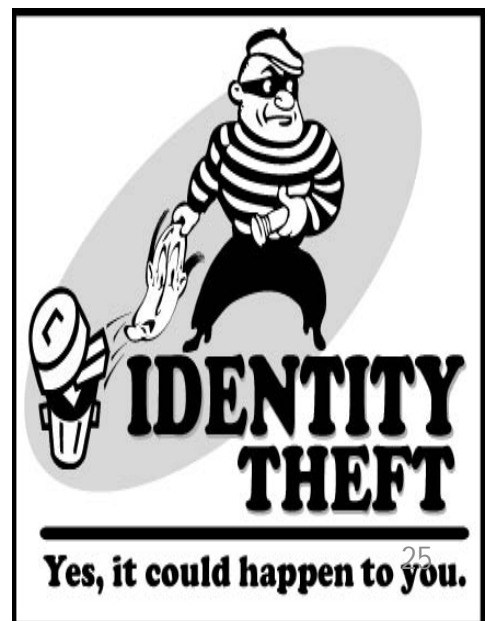
A scam that hit much of the country in June has now reached utility customers in Alabama, natural gas company Alagasco and the Better Business Bureau of Central Alabama noted. Scammers have been going door-to-door and using text messages, social media and handbills to solicit personal data such as social security numbers. The scammers claim that a grant program authorized by President Barack Obama will pay their utility bills, if they provide the personal data.

Identity Theft Overview

2008 FTC Consumer Fraud and ID Theft Report
Identity Theft Victims By State



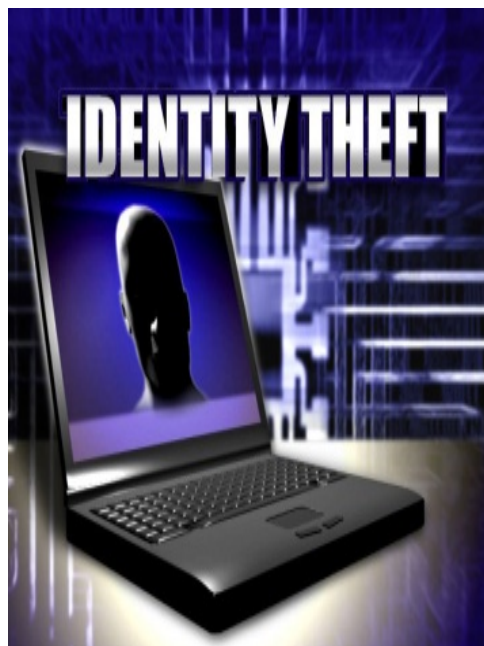
Complaints Per 100,000 Population



Cybersecurity Risk – Identity Theft

Identity thieves are targeting children – it's the crime of opportunity and is often committed by someone in the family. Children are targeted 35 times more than adults, with 15% under the age of 5. This crime tends to go undetected until victims turn 18 and try to get a student or car loan and discover they already have a credit file. All that is required is an SSN, birthday, addresses and parent's names. Since the Social Security verification service can only be used for W-2 reporting purposes, banks verify SSNs, names and birthdates with credit bureaus. **So keep your kids' SSNs, birthdates, etc. information close hold, DON'T put it on Facebook or MySpace.**

Approximately **15 million United States residents** have their identities used fraudulently each year with financial losses totaling upwards of \$50 billion. On a case-by-case basis, that means approximately 7% of all adults have their identities misused with each instance resulting in approximately \$3,500 in losses. These alarming statistics demonstrate identity theft may be the most frequent, costly and pervasive crime in the United States.



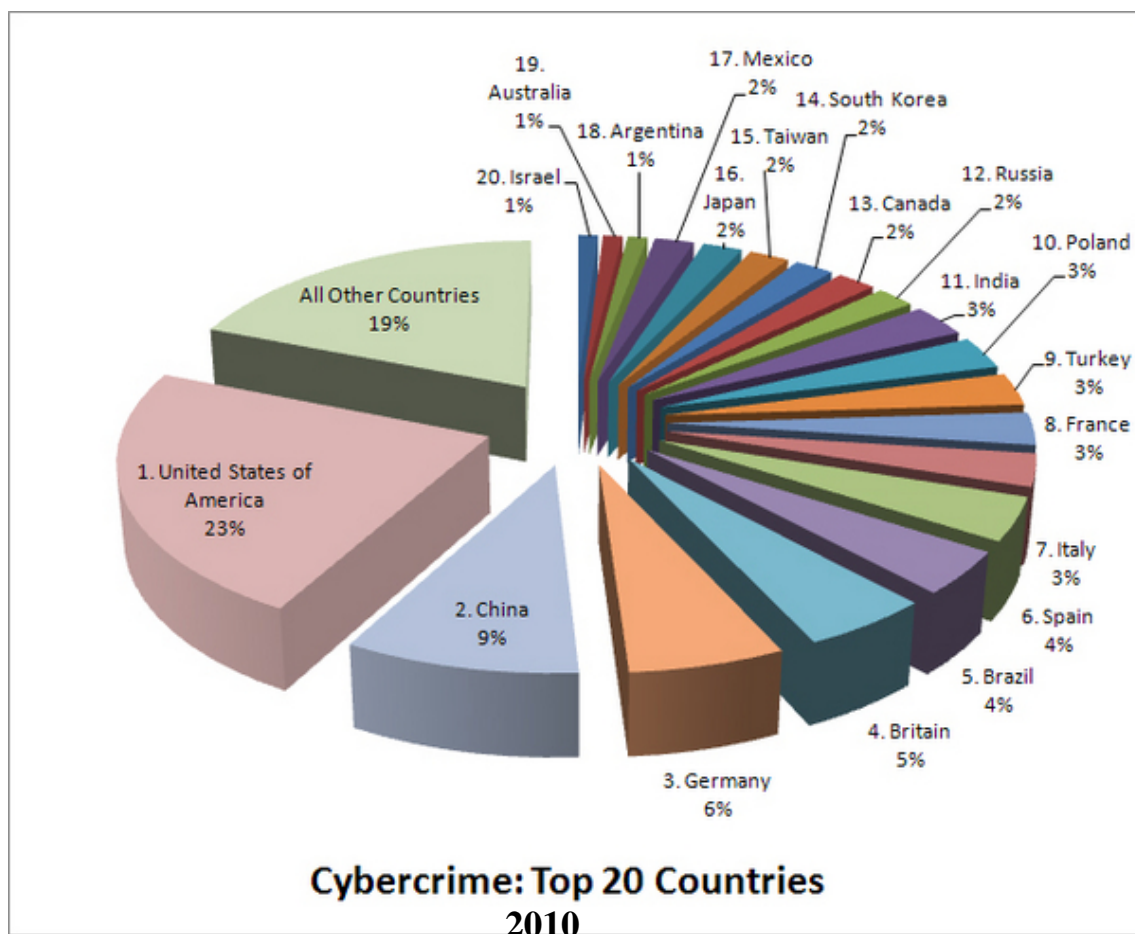
Cybersecurity Risk – Identity Theft

Identity Theft Assistance Center Victim Survey Says.....

A survey of more than 1,500 identity theft victims shows that approximately three out of four, or 72%, do not know the source of the crime, according to ITAC, the Identity Theft Assistance Center.

Your best bet is to treat your personal information as you do your personal safety – like buckling your seat belt. Keep data in your home and workplace in a secure location, keep your anti-virus software, browser and operating system updated, and monitor your accounts online for unusual activity..

We will see these anonymous sources grow since criminals use stolen consumer data as currency and are becoming more targeted and organized.



Cybersecurity Risk – Identity Theft

A total of 111 people have been indicted in an identity-theft scheme that originated largely in the back rooms of Queens restaurants and then mushroomed into a worldwide network of counterfeiters, hackers, fences and thieves who made off with an estimated \$13 million in fraudulent purchases. *Often, the police said, the criminals obtained victims' credit card information from restaurant employees who used hand-held skimming machines.*

The police and prosecutors said that early in their investigation, they received no tips from credit card companies or retail businesses even though balances on stolen accounts were skyrocketing. The Queens Police Department's Identity Theft Squad said that law enforcement *had been urging the business community to take greater security measures.*

Social Media Platforms (Facebook, MySpace, Twitter)

Cybercriminals view these sites as a great venue for finding victims. As a result, security stories about Twitter and Facebook have dominated the headlines in the past 12 months. In one high-profile story from 2009, hackers managed to hijack the Twitter accounts of more than 30 celebrities and organizations, including President Barack Obama and Britney Spears. Hacked accounts had been used to send malicious messages, many of them offensive. According to Twitter, the accounts were hijacked using the company's own internal support tools. Twitter has also had problems with worms as well as spammers who open accounts and then post links on popular topics that actually link to porn or other malicious sites. Facebook, too, is regularly chasing down new scams and threats.



Bank account identity theft --
medical identity theft -- tax
refund fraud -- social security
theft -- child identity theft --
social network identity theft -
- credit card fraud --
employment identity theft --
email scams -- WiFi hacking --
computer virus threats --
password hacking And
that's just the start.

Cybersecurity Risk – Identity Theft


FEDERAL TRADE COMMISSION ESPAÑOL

CONSUMER INFORMATION

MONEY & CREDIT HOMES & MORTGAGES HEALTH & FITNESS JOBS & MAKING MONEY PRIVACY & IDENTITY [BLOG](#) [VIDEO & MEDIA](#)






Protecting Your Identity

MAKE IT PART OF YOUR ROUTINE!



SCAM ALERTS

STAY CONNECTED






-  [Get Email Updates](#)
-  [Blog Feed](#)
-  [Facebook](#)
-  [YouTube](#)
-  [Twitter](#)

New on the Blog

- [Welcome to the FTC's Home for Consumer Information](#)
- [6 Timely Tips for Using Apps with Kids](#)
- [Snuffing Undisclosed History Sniffing](#)
- [Steering clear of a storm-damaged car](#)


[More >](#)

Take Action

-  [File a Consumer Complaint](#)
-  [Register for Do Not Call](#)
-  [Report Identity Theft](#)
-  [Get Your Free Credit Report](#)
-  [Order Free Resources](#)


JUST FOR YOU...


- [Looking for a Refund?](#)
- [Consumer Advocates](#)
- [Military Families](#)



The Federal Trade Commission (FTC) is the nation's consumer protection agency. The FTC works to prevent fraudulent, deceptive and unfair business practices in the marketplace.

[Privacy Policy](#)
[About Us](#)
[Contact Us](#)

 [Share Our Resources. Here's How >](#)

 [File a Complaint with the FTC >](#)

IRS Overwhelmed by Tax Related Identity Theft



The IRS increasingly struggles to control taxpayer identity theft. Since 2008, the IRS has identified 470,000 incidents of identity theft affecting more than 390,000 taxpayers. “Victims of tax-related identity theft are the casualties of a system ill-equipped to deal with the growing proficiency and sophistication of today’s tax scam artists” said Sen. Bill Nelson, who chairs the newly formed Subcommittee on Fiscal Responsibility and Economic Growth.

Identity theft harms innocent taxpayers through (1) employment and (2) refund fraud, according to the GAO. In refund fraud, an identity thief uses a taxpayer’s name and Social Security number to file for a tax refund, which the IRS discovers after the legitimate taxpayer files. In the meantime, the victim is out the money due him/her. You must painstakingly prove your identity to the IRS, normally time after time over a several-month period, often 10 -15 months. **For many people this has happened more than once.**

Phoebe Putney Memorial Hospital in Albany is warning patients that their personal information might have been accessed by a former nurse accused of identity theft. Melody Milton was charged in April with stealing the identities of people and filing more than \$1 million worth of false tax returns.

How do you know if your tax records have been affected?

Usually, an identity thief uses a legitimate taxpayer’s identity to fraudulently file a tax return and claim a refund. Generally, the identity thief will use a stolen SSN to file a forged tax return and attempt to get a fraudulent refund early in the filing season. You may be unaware that this has happened until you file your return later in the filing season and discover that two returns have been filed using the same SSN.

IRS Overwhelmed by Tax Related Identity Theft

Be alert to possible identity theft if you receive an IRS notice or letter that states that:

- More than one tax return for you was filed,
- You have a balance due, refund offset or have had collection actions taken against you for a year you did not file a tax return, or
- IRS records indicate you received wages from an employer unknown to you.

What to do if your tax records were affected by identity theft?

If you receive a notice from IRS, respond immediately. If you believe someone may have used your SSN fraudulently, please notify IRS immediately by responding to the name and number printed on the notice or letter. You will need to fill out the IRS Identity Theft Affidavit, Form 14039. For victims of identity theft who have previously been in contact with the IRS and have not achieved a resolution, please contact the IRS Identity Protection Specialized Unit, toll-free, at 1-800-908-4490.

How can you protect your tax records?

If your tax records are not currently affected by identity theft, but you believe you may be at risk due to a lost/stolen purse or wallet, questionable credit card activity or credit report, etc., **contact the IRS Identity Protection Specialized Unit at 1-800-908-4490.**




Cybersecurity Risk – Pin Skimming

Pin Skimming

At Chase Bank in Manhattan, East Village a customer inserted his ATM card into one of two side-by-side automatic teller machines. When the machine told him it could not read his card, it took him a bit of jiggling to get his card back. He tried it a couple more times and got the same results. Before trying the other machine, he inspected the slot of the current ATM he was using and realized that it had a false plastic cover attached to the slot.





The amazing thing about the cover was that the translucent green plastic matched the card reader slot perfectly, meaning that it was made specifically for Chase ATMs. After snapping a few photos with his iPhone, he alerted the branch manager and explained what happened. The customer went back to the ATM to inspect, which is where he found an extra mirror attached to the vandalized machine that the other ATMs didn't have. Drilled into the mirror was a tiny pinhole with a camera inside, directed at the PIN pad. The customer asked Chase why they hadn't inspected the ATM. Chase honestly replied that they hadn't thought of it because they had never encountered that sort of thing before.



What do skimming devices look like?

Spot the difference...Can you tell now?



- Top photo shows an unadulterated ATM fascia. The flashing lead-through entry indicator is easily observed.
Note: Most skimming devices when fitted will obscure the flashing entry indicator. This should be a vital clue to any suspect tampering.
- A skimming device has been placed in or near the card reader slot. Although the device has been given the appearance of being a standard part of the terminal it is in fact an additional fitted piece and is clearly different from the above photo.
Note: No flashing lead-through light can be seen and the shape of the bezel is clearly different.

Spot the difference in the next photo.



Cybersecurity Risk – Pin Skimming



Lax security makes non-banking ATM sites prime targets for pin skimming attacks. One attack hit eight hospitals. Over the past six months (2012) these hospitals were targeted because of the traffic and high-volume cash dispensers and because they are easy targets. Note that a gas station pump is equivalent to an ATM and many have hosted pin skimmers.

ATM placement in hospitals and non-banking businesses seems to have security as an afterthought. The ATMs are mostly installed in remote or low travel areas of the buildings, where skimmers can easily tinker with the skimming device placement and retrieval without much threat of notice. Beyond remote locations, hospital and other business staffers are not usually trained in what to look for when it comes to ATM tampering. So a skimming device could go undetected for weeks or months before it is found. Today, skimming devices match the color of the ATM making them look like they are part of the ATM. Also note that for non-banking ATMs, few are screened for clearance or facility access and few have cameras.

Whether or not you're using a bank machine that's familiar to you, it's never a bad idea to somehow cover your hand as you're typing your PIN into the keypad. It's the combination of the information on your card's magnetic strip and the PIN a camera records that gives the thieves complete access to your bank account, so without your PIN they'll have a much bigger hurdle to climb over to get at your money. Using cash machines in very public areas can be a good way to avoid machines that are targets for skimmers in the first place, as they offer less opportunity for thieves to install and later remove the skimmers without being seen. When in doubt, these machines are a better bet simply because there's always someone "watching" them. Finally, even when you're traveling it's a good idea to check in with your bank account online every so often if you can. **But DON'T do so over a public or hotel Wi-Fi!** So a day or so after each transaction, log into your account to find out if anything other than your withdrawals are showing up, it may give you enough of a heads-up to stop any further theft. And in any situation, if you have one of those "funny feelings" about a bank machine, don't put your card in it – find another machine and use it instead.

Cybersecurity Risk – Pin Skimming

HOW IT WORKS

Skimming is an illegal activity that involves the installation of a device, usually undetectable by automated teller machine users, that secretly records bank account data when the user inserts an ATM card into the machine. Criminals can then encode the stolen data onto a blank card and use it to loot the customer's bank account.

- 1 Hidden camera**
A concealed camera is typically used in conjunction with the skimming device in order to record customers typing their personal identification number (PIN) into the ATM keypad. Cameras are usually concealed somewhere on the front of the ATM — in this example, just above the screen in a phony ATM part — or somewhere nearby (like a light fixture).
- 2 Skimmer**
The skimmer, which looks very similar to the original card reader in color and texture, fits right over the card reader. The original card reader is usually concave in shape (curving inward), while the skimmer is more convex (curving outward). As customers insert their ATM cards, bank account information on the card is “skimmed,” or stolen, and usually stored on some type of electronic device.
- 3 Keypad overlay**
The use of a keypad overlay — placed directly on top of the factory-installed keypad — is a fairly new technique that takes the place of a concealed camera. Instead of visually recording users punching in their PINs, circuitry inside the phony keypad stores the actual keystrokes.



SOURCE: FBI

THE BLADE

Cybersecurity Risk – Pin Skimming

So how can you spot a skimmer? If it looks like something's been attached, snapped or glued onto the ATM, that's a warning sign. ATMs are pretty straightforward, so if something looks physically wrong, it probably is.

Be vigilant at ATMs. Visually and physically check the machine. Most skimmers, key pad overlays, and cameras will be recognizable to the typical ATM user. In particular, users should pay attention to the card reader and anything that protrudes from the machine, such as a mirror or pamphlet-holder—these are prime hiding places for tiny cameras. It can't hurt to give any of these items a quick tug to make sure they weren't glued or taped into place. Another red flag: any machine in a row of ATMs that looks different from the others.



Skimming device removed from ATM



Skimming device and mirror removed from ATM



Skimming Pad on top of legitimate Pin Pad



Cybersecurity Risk – Pin Skimming

Pay-at-the-pump terminals and ATMs also rank high in the skimming chain because they are unattended. They are usually a fraudsters' easiest target. Pay-at-the-pump has proven vulnerable because of easy accessibility. **Default codes** used to open gas pump enclosures have been exploited by criminals posing as technicians, for instance. Once inside, the criminal can install a skimming device and connect it directly to the terminal's key pad and card reader. It's undetectable from the outside, giving the device ample opportunity to collect card data in real-time, as the card is swiped and PIN entered.

Chase Bank branches in and around Las Vegas have found card skimmers *on their doors*, enabling thieves to capture bank card info without tampering with the ATM at all. At the cash machines, all the thieves need are pinhole cameras to record the PINs.



Cybersecurity Risk – Reputation

Extortion

Storefront Extortion

Scammers (extortionists) are requiring a payoff or discount from retail stores or restaurants or they will post a terrible rating on online review sites. Legal experts say that not to pay and not to file a lawsuit is wise. If a business is seen as litigious, it can be as bad for your reputation. The best course is to use the same social media to explain your side of the story and work for more positive reviews. Victims of cyber extortion can't blame the online sites. Review sites are not legally responsible for what their users do.

Data Held Hostage

Holding data hostage can be as simple as stealing the most recent backup and wiping the original version from the corporate servers. Or it may be as complex as changing the encryption key (similar to a complex password) within a database and holding the new key hostage. However the data is held hostage, the victim's company may be put into data limbo while it negotiates with the cyber-criminal.

Release of Protected or Personal Data

One of the biggest financial and reputation fears of businesses and organizations is the compromise of protected information such as medical, identity, or credit card information. Such a compromise and public disclosure may result in huge government or industry fines, a flight of customers from an embarrassed or perceived technically incompetent business, or both.

Rather than use this stolen information for direct identity or financial theft, cyber-criminals will sometimes threaten the breached corporation with the disclosure that the information has been stolen. The payment of ransom may be a lot less expensive and damaging than the resulting cost and company-customer relationship fallout that a disclosure would cause.



Cybersecurity Risk – Reputation

Extortion

Release of Private Business or Personal Information

We only need to look back at the last year to ask the question ‘What were they thinking?’, as we consider the stream of dumb emails, texts, pictures and tweets from people who should know better – celebrities, athletes. Corporate C-Levels, and government officials. And this was the information that people went out of their way to make public. One can only imagine the really damaging information that could be found on the personal computers and corporate IT systems that people thought were hidden from public view.



With many home computers compromised by malware and corporate IT systems being breached at an alarming rate, we can only speculate on the depth and breadth of extortion-worthy information in the hands of hackers.

Distributed Denial of Service (DDoS)

There are massive numbers of compromised personal computers (reported to be 50 percent of all home computers) that can each be directed to send an unlimited number of communication requests to any web site in the world. These malicious personal computer bots are managed by bot herders from cyber-crime tolerant countries around the world.

As the recent and successful DDoS on the CIA website has shown, an energized botnet (herd of bots) can easily wreak havoc on almost any commercial or government web site – overloading the site to the point where it gives up in cyber exhaustion. Imagine the fear within an e-commerce dependent company should a plausible DDoS threat be received. Even an hour of DDoS imposed downtime might cost the targeted company millions in on-line sales revenues, let alone the creditability and future sales the company might lose.

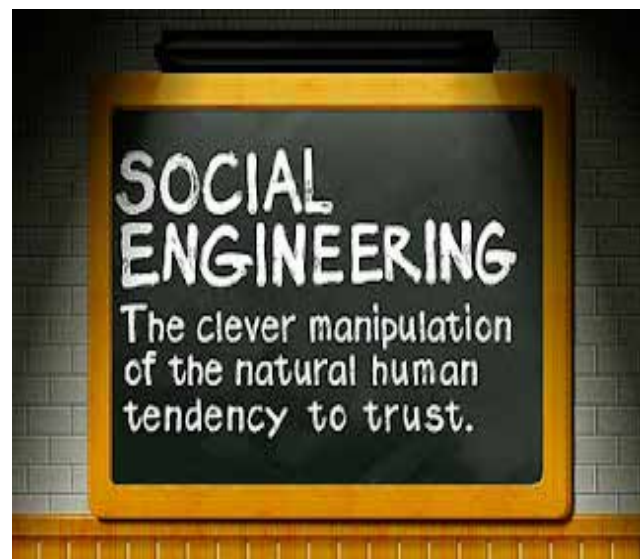
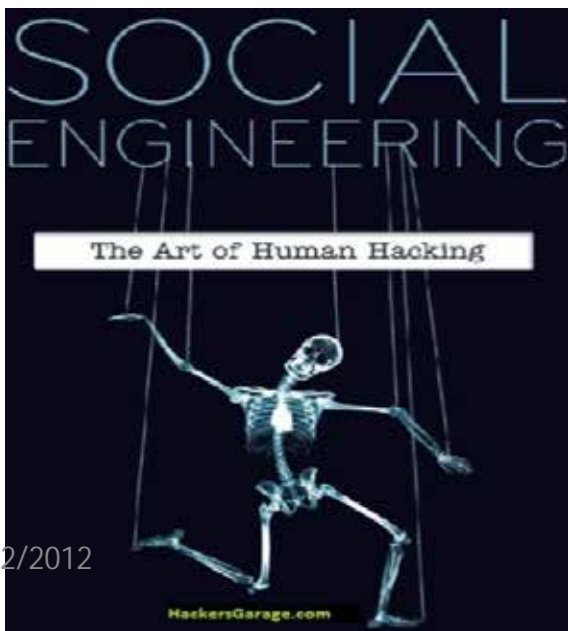


Cybersecurity Risk – Social Engineering

Social engineering is the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

Fraudsters are perfecting their abilities to target and manipulate people. Well-crafted social engineering schemes take advantage of common user behavior. Don't click on unknown links or provide personally identifiable information to someone you don't positively know. A call from "the IT department" asking for your password to check some obscure area of the computer system works wonderfully well.

IN 2011, the Department of Homeland Security ran a test where staff secretly dropped USB drives and CDs in the parking lots of government buildings and private contractors. Of those people who picked up the drives or CDs, fully 60% plugged them into office computers to see what they contained. IF the CD had an official logo, 90% were plugged in. **Have you warned your employees or your family NOT to use "found" digital media or any digital media given tot hem by unknown persons?** This is an easy way for a cybercriminal to install malware on your computers.



Classic Examples of Social Engineering Attacks

Baiting - Much like a bait car is used to attract automobile thieves, a bait disk or bait drive is left in the open for a target to find. Succumbing to curiosity, the target attempts to read the disk and thereby infects his computer with malware.

Defense Against Baiting - Don't access that disk, you don't know where it's been.

Phishing – False emails, chats or websites designed to impersonate real systems with the goal of capturing sensitive data. The classic examples are a mocked-up login page that steals your username and password, or an email requesting you reply to confirm your personal information.

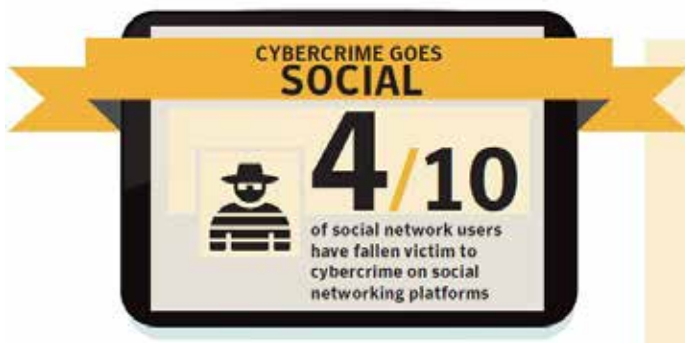
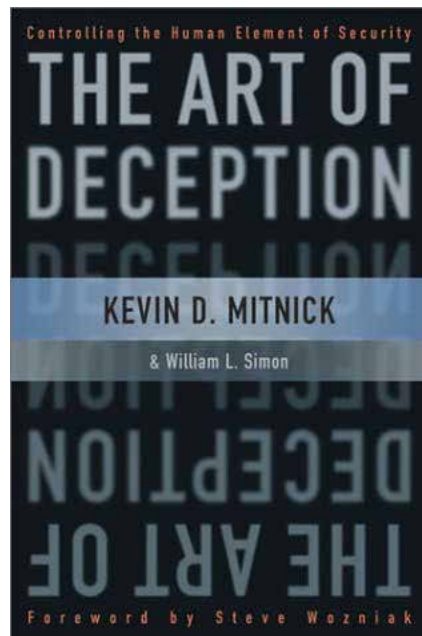
Defense Against Phishing – Your password doesn't get entered anywhere but your login page, and that page better have the right URL.

Pretexting - The human equivalent of phishing, where someone impersonates an authority figure who is entitled to access your login information. The fake IT staffer asking for your password to do system maintenance, or the false investigator performing a company audit are two typical pretexting examples.

Defense Against Pretexting – ***Nobody needs your password, ever.***

Fake Tech-Support Calls

You might get an unsolicited phone call from a tech-support representative claiming to be from Microsoft or another big-name IT corporation. But the caller won't be who he claims to be. After warning you that "**suspicious activity**" has been detected on your computer, he'll offer to help — once you give him the personal information he requires to get his job done.



Classic Examples of Social Engineering Attacks

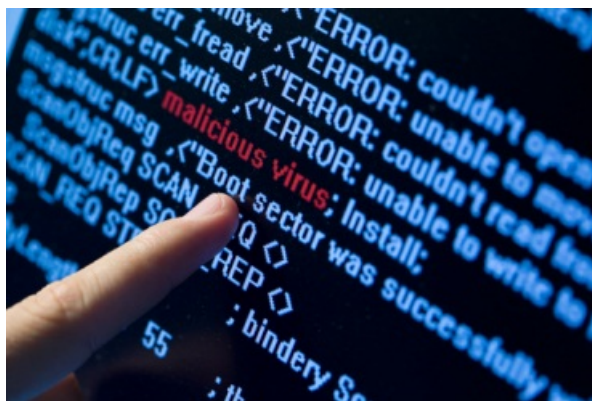
Defense Against Fake Calls - That job isn't fixing your computer. In fact, he's really just after your personal information. If you receive a call like this, hang up, call the company the bogus technician claimed to be from, and report the incident to a legitimate representative. If there really is a problem, they'll be able to tell you; if not, you just thwarted a data thief.

Quid Pro Quo – A system that requests your password or personal information in exchange for some compensation. Previously, these took the form of contests — share your password to win a free t-shirt — but increasingly resemble application install or download forms where the user is prompted to share login credentials to access an online game or service.

Defense Against Quid Pro Quo – *Nobody needs your password, ever.*

Tailgating – Following someone into a restricted area or system. In physical attacks, this could simply mean passing through a security door at the same time as a legitimate entrant, as in “can you hold the door?” or similar exploitations of courtesy. In the context of the cloud, this typically means using a device that is already logged into an online app, such as when an attacker asks to borrow a phone or laptop to “check email” but surreptitiously performs malicious acts instead.

Defense Against Tailgating – *Nobody other than you uses your computer (or tablet, or phone) while you're logged in, ever.*



Common Scams Used in Social Engineering

1. **Quizzes, polls and contests** – The promise of something for nothing is a classic scam. One promises that the first 20 responders will receive \$1,000 gift cards to a popular electronics store if they “like” the store on Facebook. Clicking on the link in the e-mail will take you to a bogus page that asks for numerous personal details – basically identity theft – and there is no gift card.

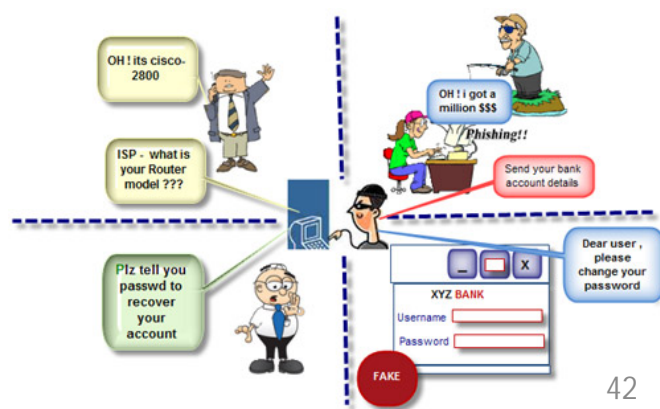
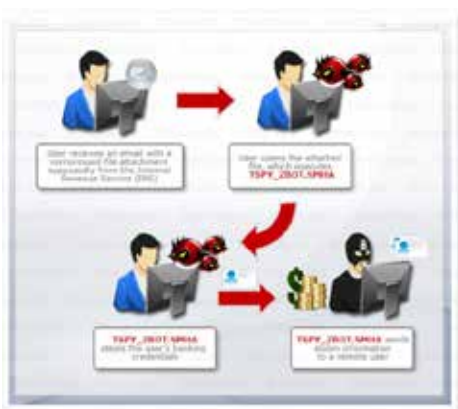
To protect yourself **IGNORE** these kinds of offers or **go directly** to a company’s Facebook page or website to verify that the offers are legitimate.

2. **Auctions and Deals Too Good To Be True** – Shopping at online auctions and classified ad sites can be useful, but **NOT** if the seller wants you to wire money in advance.

To protect yourself remember the old sayings “If it’s too good to be true, it probably is”. Thoroughly check out a seller’s ratings and reviews before you bid on any online auction. Some fraud sites actually imitate a BBB seal or offer phony positive reviews to throw you off. Verify BBB approval at BBB.org. Whatever you do, **NEVER** pay by wire transfer as this is a surefire indication of a fraudulent sale.

3. **Phony Do-Gooders** – After any disaster, scammers try to take advantage of our good nature and generosity by asking for donations via a website or text message and then keeping the money for themselves.

To protect yourself **CHECK** if a charity is legitimate at the BBB Wise Giving Alliance or American Institute of Philanthropy websites. Or **donate directly** through a known charity’s web site.



Common Scams Used in Social Engineering

4. **Malware-ridden e-cards and Programs** – Animated cards, games and screen savers never go out of style. Scammers take advantage of user's boredom and trick them into downloading applications laden with spyware and other malware.

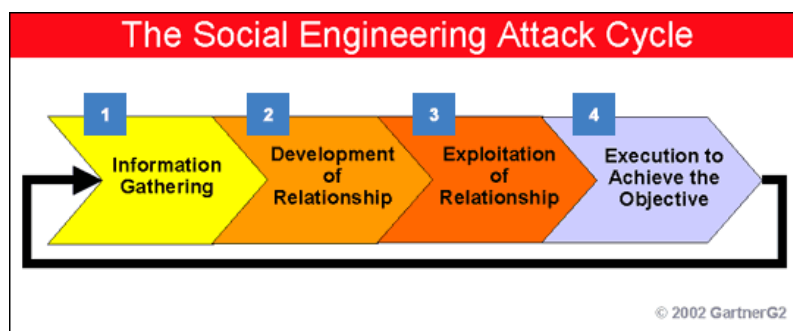
To protect yourself, use a strong anti-malware product. That will usually stop malware in its tracks. But your best bet is **not to open any e-mail attachment** – even from someone you know – if you aren't certain it is legitimate. **Check before you click.**

5. **Vacation Homes (Not Really) For Rent** – This up and coming scam is simple – a fraudster sets up a vacation rental site for a real home (complete with photos) and they rent it out for weekend and holiday getaways. The problem is that the scammer doesn't own the house, its not actually for rent, and when you get there, the owner doesn't know anything about it.

To protect yourself **use only trusted** travel sites and rental agencies when booking. Low-resolution photos of the home and super-low rental prices are giveaways that something is fishy.

6. **Fake E-Mails and Phishing Trips** – A common trick is an e-mail that “confirms” an order, payment or shipment you know nothing about. The e-mail, which may appear to be from a reputable company, advises you to click on a link or attachment to view the status of the order or shipment. When you click you are routed to a fake website that asks you to enter your personal information – identity theft.

To protect yourself **avoid opening** e-mails from people and companies you don't recognize or trust. Permanently delete those e-mails. Don't click on links or attachments. Type the web address into your address bar so you go directly to the site. If you are not expecting a shipment, delete the e-mail. If you receive an order or payment contact the company directly.



Social Engineering– Fraud/Phishing

Phishing and Smishing Schemes

In **Phishing** schemes, a fraudster poses as a legitimate entity and uses e-mail and scam websites to obtain victims' personal information, such as account numbers, user names, passwords, etc.

Smishing is the act of sending fraudulent text messages to bait a victim into revealing business or personal information.



Be leery of e-mails or text messages that indicate a problem or question regarding your financial accounts. In this scam, fraudsters direct victims to follow a link or call a number to update an account or correct a purported problem. The link directs the victim to a fraudulent website or message that appears legitimate. Instead, the site allows the fraudster to steal any personal information the victim provides.

Phishing is difficult to detect because it contains official-looking logos and other identifying information from legitimate organizations. A phishing e-mail normally starts with a generic greeting, such as “Dear Customer” or “To our valued client.” Phishers send out millions of messages to randomly generated e-mail addresses hoping that people who can relate to the message would reply to them. Banks personalize their greetings and indicate your full name when sending official correspondence.

Most phishing e-mails include threats requiring immediate action. They contain phrases such as “Verify your account,” “Update your account,” and “Failure to do so will result in account suspension.” Mainly all phishing scams will request your personal information. Most legitimate banks will not demand this information online or through e-mail. If you receive an e-mail or pop-up message from your bank or credit card company or from businesses that you regularly transact with such as eBay or Amazon and you suspect it is a phishing scam, do not reply to it.

Just ignore and delete the message.

The primary way to avoid phishing scams is to educate yourself.



Only YOU can prevent social engineering!

Social Engineering– Fraud/Phishing

Phishing and Smishing Schemes

Current **smishing** schemes involve fraudsters calling victims' cell phones offering to lower the interest rates for credit cards the victims do not even possess. If a victim asserts that they do not own the credit card, the caller hangs up. These fraudsters call from TRAC cell phones that do not have voicemail, or the phone provides a constant busy signal when called, rendering these calls virtually untraceable.



Another scam involves fraudsters directing victims, via e-mail, to a spoofed website. A spoofed website is a fake site that misleads the victim into providing personal information, which is routed to the scammer's computer.

Even seemingly rudimentary attacks may be just the first in a series of advanced, coordinated and devastating crimes. Advanced targeting attacks against low level personnel/resources without particularly sensitive roles or permissions can still open the door to vital information and have huge consequences.

The best way to avoid phishing is by knowing what to look for and to NOT give out any personal information to anyone unless you absolutely know who you are giving your information to.



Spoofted Website

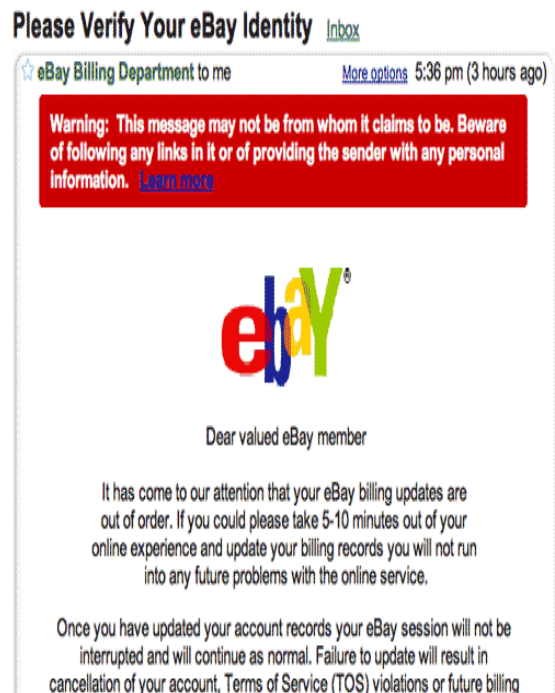
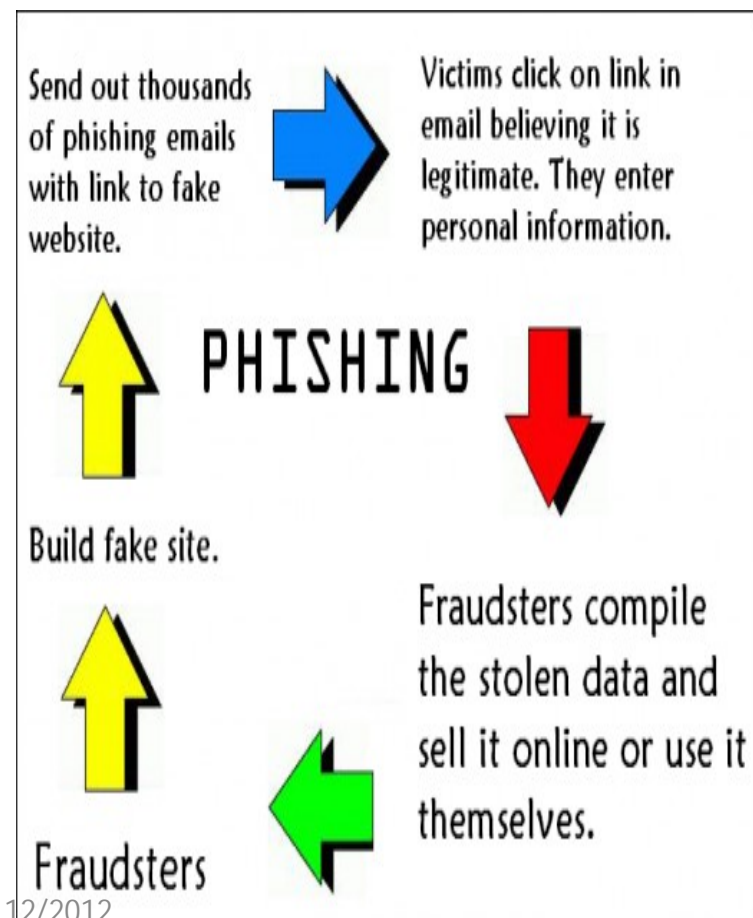
A Spoofted Website is site which is similar to a real website - usually joined with phishing scams. There are ways to determine a spoofted website.

1. The best way to find out a Spoofted Website is checking the websites' certificate. Update your web browser regularly, older versions of browsers can be easily hacked. New browsers are very secure which can avoid scams, viruses, spoofted Websites, etc
2. Be aware of cybersquatting. Cyber criminals open a website similar to a real website for earning cash through advertisements. These kind of websites are illegal and normally contain viruses.
3. Bookmark websites you go to often and avoid opening them from e-mails or possible mistyping.
4. Always use an antivirus program to alert you if a site may contain malicious programs or virus.
5. Check if a website is secure by checking if the URL begins with an "https" and if a closed padlock icon is displayed on the browser's status bar. To confirm authenticity of the site, double-click on the lock icon and review the security certificate information it will display.



Cybersecurity Risk – Fraud/Phishing

A massive phishing and fraud scheme that targeted Bank of America, Chase Bank and payroll processor ADP defrauded them of \$1.5 million. The phishing attacks directed users to spoofed or fake web pages designed to mimic legitimate sites. Once on the spoofed sites, users were conned into entering confidential personal and financial information. These stolen usernames and passwords were used to hack and compromise accounts as well as initiate unauthorized transactions and withdrawals. The phishers also created fake drivers licenses, access online accounts (viewed online checks to find out how to forge signatures) and access payroll accounts at ADP. They added fake employee accounts to company payrolls and had paychecks issued to the fake employees. *Social engineering schemes are getting much more sophisticated.*



Cybersecurity Risk – Fraud/Phishing

Subject: ANZ Account Suspension

Date: 7:48 AM

To: bretmalcom@diamond.com

From: 'ANZ Banking' Reply-To: 'ANZ Banking'



ACCOUNT SUSPENSION

In an effort to protect your ANZ Banking account security, we have suspended your account until such time that it can be safely restored by you.

We have taken this action because your ANZ online account may have been compromised. Sometimes this happens when members respond to trojans, worms and other effected virus files. Although we can't disclose our investigative procedures that led to this conclusion, Please be aware that too often, scammers use the name of ANZ to gain the trust of members.

To complete a re-activation process for your account, please click on the following link:
<https://www.anz.com/online/secure/activation>

Thank You.

Accounts Management As outlined in our User Agreement, Australia and New Zealand Banking Group Limited (ANZ) will periodically send you information about site changes and enhancements.

Visit our [Privacy Policy](#) and [User Agreement](#) if you have any questions.
[ANZ Web Site Security and Privacy Statement](#)

Cybersecurity Risks- The Nigerian E-Mail Scam

You've seen the e-mail – some terminally ill Nigerian prince or General or the Director of a large corporation contacts you urgently asking you to move a large sum of money, promising you a share. All they need are your credit card number or bank account info.

But who on earth actually believes these e-mails? Doesn't matter. Those of us who wonder are not the target. A recent study found that the scammers aren't interested in being too believable because it would be too expensive if everyone fell for it. *So the e-mail is designed to eliminate anyone intelligent*, leaving only the most gullible to hit. It works, last year one Nigerian man was jailed after scamming \$1.3 million.

A Kauai woman received several e-mails as part of a Nigerian scam attempting to obtain large sums of money from her. The e-mails contained a photo of a Hawaii County police officer, a Police Department logo and other information that had been cut-and-pasted from the Hawaii Police Department's website in an apparent attempt to mimic official letterhead and impersonate a police officer.

CENTRAL BANK OF NIGERIA
PRESS STATEMENT ON ADVANCE FEE FRAUD/SCAM
DON'T BE FOOLED! MANY HAVE LOST MONEY!!
IF IT SOUNDS TOO GOOD TO BE TRUE THEN IT IS NOT TRUE!!!

- 1 The publicity campaign by the Central Bank of Nigeria (CBN) and the Government of the Federal Republic of Nigeria have proved successful in scolding the public about the menace of advance fee fraud and the falsehood of claims that easy money could be made in Nigeria. Consequently, the reported incidence of advance fee fraud (A.F.F.) has declined significantly. Nevertheless, there are still some people who have continued to fall victim to the solicitations of advance fee fraudsters. This warning is, therefore, specifically intended for the benefit of those misguided people who, in the quest to make easy money at the expense of Nigeria, are defrauded by international fraudsters.
- 2 The advance fee fraud is perpetrated by enticing the victim with a bogus "business" proposal which promises millions of US dollars as a reward. The scam letter usually promises to transfer huge amounts of money, usually in US dollars, purported to be part proceeds of certain contracts, to the addressee's bank account, to be shared in some proportion between the parties. A favourable response to the letter is followed by excuses why the funds cannot be remitted readily and subsequently by demands for proportionate sharing of payments for various "taxes" and "fees" supposedly to facilitate the processing and remittance of the alleged funds. The use of "fake" Government, Central Bank of Nigeria, Nigerian National Petroleum Corporation, etc. documents is a common practice.
- 3 The fraudsters usually request that the transaction be done under the cover of confidentiality.
- 4 To consummate the transaction, the "victim" would be required to pay "advance fees" for various purposes: e.g. processing fees, unforeseen taxes, licence fees, registration fees, signing/legal fees, fees for National Economic Recovery Fund, VAT, audit fees, insurance coverage fees, etc. The collection of these "advance fees" is actually the real objective of the scam.
- 5 A recent variant of the scam directed primarily at charitable organisations and religious bodies overseas involves bogus inheritance under a will. Again the sole aim is to collect the "advance fees" already described above. A new strategy that has also been used to defraud the "victims" is an offer to use chemicals to transform ordinary paper into United States dollar bills, which would be subsequently shared by the parties.
- 6 You are again warned in your own interest not to become yet another dupe to these fraudulent solicitations or schemes. Genuine and prospective investors in Nigeria are advised to consult their home Chambers of Commerce and Industry, or Nigeria's CENTRAL BANK OF NIGERIA.
- 7 The Central Bank and indeed, the Federal Government of Nigeria cannot and should not be held responsible for bogus and shady deals transacted with criminal intentions. As a responsible corporate body, the Central Bank of Nigeria is once again warning all recipients of fraudulent letters on bogus deals, that there are no contract payments trapped in the bank's vaults. They are once again put on notice that all documents appertaining to the payment, claims, or transfers purportedly issued by the bank, its senior executives or the Government of the Federal Republic of Nigeria for the various purposes described above are all forgeries, bogus and fraudulent.
- 8 Please join the Central Bank and the Federal Government of Nigeria to fight the criminal syndicates who play on the pithiness and greed of their victims by reporting any solicitation to your local law enforcement agencies or the local International Police Organisation (Interpol).
- 9 You have been warned several times before! You have been warned again!!

Samuel Ladake Akintola Way, P.M.B. 0187, Garki, Abuja, NIGERIA

SOCIAL ENGINEERING SPECIALIST
Because there is no patch for human stupidity

Citadel Malware Continues to Deliver Reveton Ransomware in Attempts to Extort Money

A new Citadel malware platform used to deliver ransomware named Reveton. The ransomware lures the victim to a drive-by download website, at which time the ransomware is installed on the user's computer. Once installed, the computer freezes and a screen is displayed warning the user they have violated United States federal law. The message further declares the user's IP address has been identified by the Federal Bureau of Investigation as visiting websites that feature child pornography and other illegal content.

To unlock the computer, the user is instructed to pay a fine to the U.S. Department of Justice using a Prepaid money card service. The geographic location of the user's IP address determines what payment services are offered. In addition to the ransomware, the Citadel malware continues to operate in the background even though your screen does not show it and can be used to commit online banking and credit card fraud.

This is an attempt to extort money with the additional possibility of the victim's computer being used to participate in online bank fraud. If you have received this or something similar, do not follow payment instructions. Turn off your computer and unhook from the internet immediately. Seek out a local computer expert to assist with removing the malware. You can file a complaint at www.IC3.gov.

THE FBI FEDERAL BUREAU OF INVESTIGATION

ATTENTION !

IP: [REDACTED]
Location: [REDACTED]
IPS: [REDACTED]

Your PC is blocked due to at least one of the reasons specified below.

You have been violating Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted content, thus infringing Article I, Section 8, Clause 8, also known as the Copyright of the Criminal Code of United States of America.

Article I, Section 8, Clause 8 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child Porno/Zoofilia and etc). Thus violating article 202 of the Criminal Code of United States of America. Article 202 of the Criminal Code provides for a deprivation of liberty for four to twelve years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the law On Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of up to \$100,000 and/or a deprivation of liberty for four to nine years.

Pursuant to the amendment to the Criminal Code of United States of America of May 28, 2011.

Video Recording
ON

MoneyPak

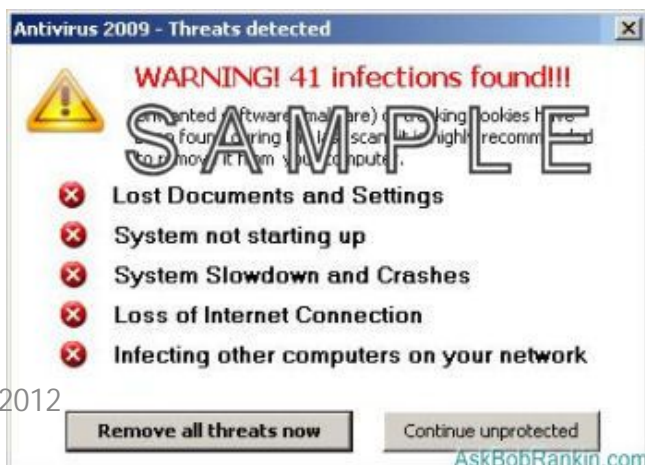
Code: [REDACTED] Sum: [100 \$]
1 2 3 4 5 6 7 8 9 0
Pay MoneyPak 50

Malware Installed on Travelers' Laptops Through Software Updates on Hotel Internet Connections

Recently, there have been instances of travelers' laptops being infected with malicious software while using hotel Internet connections. In these instances, the traveler was attempting to set up the hotel room Internet connection and was presented with a pop-up window notifying the user to update a widely used software product. If the user clicked to accept and install the update, malicious software was installed on the laptop. The pop-up window appeared to be offering a routine update to a legitimate software product for which updates are frequently available.

Anyone who believes they have been a target of this type of attack should immediately get their laptop cleaned and contact their local FBI office to report it. The FBI's complaint database links complaints together to refer them to the appropriate law enforcement agency for case consideration. The complaint information is also used to identify emerging trends and patterns.

The FBI recommends that all government, private industry, academic personnel and individuals who travel abroad **take extra caution** before updating software products through their hotel Internet connection. Checking the author or digital certificate of any prompted update to see if it corresponds to the software vendor may reveal an attempted attack. The FBI also recommends that travelers perform software updates on laptops immediately before traveling, and that they download software updates directly from the software vendor's website if updates are necessary while abroad.



E-Mails Containing Malware Sent to Businesses Concerning Their Online Job Postings

Recent FBI analysis reveals that cyber criminals engaging in ACH/wire transfer fraud have targeted businesses by responding via e-mail to employment opportunities posted online. Recently, more than \$150,000 was stolen from a U.S. business via unauthorized wire transfer as a **result of an e-mail the business received that contained malware**. The malware was embedded in an e-mail response to a job posting the business placed on an employment website and allowed the attacker to obtain the online banking credentials of the person who was authorized to conduct financial transactions within the company. The malicious actor changed the account settings to allow the sending of wire transfers, one to the Ukraine and two to domestic accounts. The malware was identified as a Bredolab variant, svrwsc.exe. This malware was connected to the ZeuS/Zbot Trojan, which is commonly used by cyber criminals to defraud U.S. businesses.

The FBI recommends that potential employers **remain vigilant in opening the e-mails of prospective employees**. Running a virus scan prior to opening any e-mail attachments may provide an added layer of security against this type of attack. The FBI also recommends that businesses **use separate computer systems to conduct financial transactions**.



Cybersecurity Risks – Employment Scams (Job Scams)

What are Job Scams and how do they work?

Employment Scams (Job Scams) are just one more way scammers separate hard-working people from their money. There are many variations and the Internet has been a God-send to these leeches, but almost all of them use some form of check fraud, whether it's receiving ('processing') counterfeit or redirected checks, forwarding stolen goods or the proceeds from selling stolen goods to a third party.

Most Internet jobs are advertised as Work From Home or Work At Home (WAH) and are intended to target home makers, retired people, disabled people, students and other people who just want to make a little extra cash, while staying at home. Transaction Processing Assistant, Reshipping Agent, Goods Forwarding Executive, Processing Online Auction Listings are all job descriptions that are being used. The scammers haunt online job and classified ad websites (Monster.com, Craigslist.com, Dice.com etc) and forums where they use people to scatter bomb links to their worthless websites.

If you are thinking that you have nothing to lose, you may be wrong. If your address is used as a receiving address for counterfeit checks or stolen products and you forward money/goods from your home address, you could be prosecuted for Money Laundering, Possession of Stolen Goods or Trafficking in Stolen Goods.



Cybersecurity Risk – Employment Scams (Job Scams)

In most cases, they use Spam to deliver their message. The website names change, often monthly, as their website gets blacklisted. The websites are enticing, always seem to take the same format which should ring alarm bells:

1. Lots of Graphics, pictures of money, cars, holiday destinations etc.
2. Shouty text, imperatives, exclamation marks, colored, large point size text.
3. Very Very long pages - you scroll down and down and it never seems to end - then, at the very bottom, there's the deal.
4. Lots and lots of testimonials
5. They almost always tell you that the jobs are 'scam-free', or 'totally legitimate'. Some Work at Home (WAH) sites even use the fact that there are a lot of scammers out there to promote their own (presumably non-scam) WAH jobs.
6. Extremely low qualifications required, almost always demand you have access to an Internet connected computer.
7. Payment of a fee may be required for 'training materials' or some magic list (companies, people, products etc.).
8. Pay is fantastically great! \$100/hour, \$9,000 a week, etc., etc.
9. Very scant details of location of the 'employer' - no address, phone number (beyond the 1-800 number). Domain name will have existed for a very short time - Check with domainwhitepages.com. Type in the domain name and look at the 'Creation Date' on the Domain Whois Record. If it's less than six months ago, forget it!.



Cybersecurity Risk – Employment Scams (Job Scams)

Making Money with Google?

If you've seen those spam ads about making a fortune with Google then you should be aware that this is a complete scam. The (Domain) names change but the scam continues, whether it's called '*Google Money Tree*', '*Fast Google Profits*' or '*I bought the Brooklyn Bridge with my Profits from Google*', the scam is the same one. You sign up for a service, your credit card is abused and you receive a CD full of worthless articles - then the next month, you get abused again.

Google has had enough of this scam and has filed suit against the 'Google Money' scammers. Google says that the fraudulent websites have been using Google's good name without its permission or endorsement. Misleading ads try to take advantage of consumers in the midst of a difficult economy, and as the economic situation has worsened, the problem has only grown. As far as we can tell, thousands of people have been tricked into sending payment information and being charged hidden fees by questionable operations.

Work from Home

There are some valid, profitable work-from-home Internet-based opportunities out there and they include such work as Processing Rebate checks, Filling Surveys, Drop-Shipping, Auction Selling, Product Testing and even Blogging. Sometimes there is an investment to be made, eg in Drop-Shipping but it should be low to start - ***beware of investing any money*** in an on-line business

The important thing is to do your research to avoid getting stung. A pretty good rule is this: ***If you get an unsolicited email offering you 'work-from-home', hit the 'delete' key- it's almost certainly a scam!***



Cybersecurity Risks – Protect Personal Information When Seeking Employment

Phishbucket.org – an online clearinghouse of job scam information – states that *the number of reported job scams tripled between 2008 and 2010*. Protect yourself by:



1. Never put the following on your resume if you intend to post it – SSN, driver's license number and date of birth. Also don't put it on job applications. Consider writing "prefer to provide this information during the interview".
2. Not all career websites are created equal. Be sure that you review the privacy policy and user terms and agreements before you post your resume. If in doubt check with The World Privacy Forum's Consumer's Guide to Online Job Sites. You might be looking at a fake job ad if it offers considerable pay with few to no duties, promises payment of wages in cash, contains no physical address or contact person and/or requires you to open a new bank account or accept company checks to "test" a wire transfer service.
3. Carry good data security practices with you offline – other vulnerable situations include phone interviews, job fairs and e-mail and phone conversations with recruiters. As long as someone thinks an offer is genuine, they are **more likely to provide sensitive information. Know who you are talking to. Virtually all legitimate businesses or recruiters will NOT ask for your SSN or other personal information until after you have begun a formal interview process.** A legitimate company should not ask for you to divulge personal identifiers via e-mail as e-mail is not secure.



Cybersecurity Risk – Protect Personal Information When Seeking Employment

4. Think before you post to a social media site. The more you reveal online, the greater the chance of having the information accessed by identity thieves. *Remember this* – if you wouldn't give this information to a stranger on the street, you probably don't want to put it online for the world to see.
5. Secure your delivery channels. Make sure your computer or other device you use is equipped with antivirus and antimalware programs. And *don't use a Public or hotel WI-FI to transmit data.*
6. It's important to remember that no matter how credible the job site or how well it safeguards the data it keeps, no one can guarantee what happens to your resume after it has been downloaded.

need-a-job
find
careers
employment
job
seek
find-a-job
work-at-home
get-a-job
search



Apartment Rentals, Home Rentals, Vacation Rentals Scams



It's never a good idea to wire money to someone you've never met for an apartment, home or vacation rental you haven't seen.

In your search for an apartment, a rental home or a vacation rental, you find a great prospect at a great price. It can be yours if you wire money – for an application fee, security deposit, first month's rent, etc. The “owners might say they are out of the country (or somewhere away from you) but they use an agent or lawyer to get you the key and documentation. However, once you've wired the money, it's gone and when you get to the “rental”, there is no rental.

A scammer hijacked a legitimate rental listing by changing the contact information and placing the altered ad on other sites or there never was a rental and the scammer made up the listing for a place that isn't for rent or doesn't exist.

If you have a rental property, watch out for the reverse – a potential renter who says he wants to cancel his deposit and asks you to wire the money back – before you realize the original check was a fake.

There have also been fraudulent sales of new homes and foreclosed homes. Here are what I consider to be some red flags that a rental property or home may really be a vehicle for a scam:

You cannot go and see the inside of the property, the rent/price is very low compared to the rest of the area, the landlord/owner cannot meet you in person at the property and the landlord/owner wants you to send the money out of state or out of the country



What You Can Do:

Never wire money to cover a security deposit, an application fee or a first month's rent. If you can't visit the rental or home yourself, as someone you trust or a real estate agent **You Find** in the area to see it for you. **Be skeptical** of owners or agents who say they are out of the country. **Don't** wire money to someone overseas. **Do a search** to see if the same listing is listed elsewhere with a different name or phone number.. **If you are the target of a rental scam, report it to local law enforcement, the FTC at www.ftc.gov/complaint and the FBI at www.ic3.gov/.**

Rental Scam Targets Aqualane Shores Home

COLLIER COUNTY, Fla - A scam targets a high end home in one of Naples most expensive neighborhoods. The crooks take listings off legitimate real estate websites and re-post them for a fraction of the price. The Collier County Sheriff's Office gets rental scam reports on a weekly basis, but this was the first time they saw a listing on a legitimate rental website.

WINK News found a three bedroom, 2,000 square foot home in the prestigious Aqualane Shores neighborhood on Trulia.com last week. The advertisement describes an updated beach cottage, with a pool, walking distance to the beach and downtown Naples all for \$800/month with a \$400 deposit. Anyone who knows the town would know it really didn't make sense, but someone who is not in town wouldn't necessarily know right off the bat that's way out of line for the area. This listing that really rents out for \$10,000/month fell victim to the scam.

The current renter declined an interview, but says people have been stopping by all week long to look at the property and all had received the same email from someone using the name John Larson. The email says, "you are welcome to rent and stay for any period of years as you wishes. You can drive by my house today, then get back to me so we can proceed with the rental plan."

Lt. Chad Parker with the Collier County Sheriff's Office says the scams usually come from overseas, meaning their hands are tied. "In this case we tried calling the number and it says out of service already so they use the phone temporarily to commit a bunch of scams in a short period of time and they get rid of the phone and the phone number."

The full article is at <http://www.winknews.com/Local-Florida/2012-09-07/Rental-scam-targets-Aqualane-Shores-home->



Social Engineering – It Works!

BE SECURE BE AWARE OF **Scareware**

Rogue anti-malware programs, also known as “**scareware**” produces fake security warnings, which might appear in pop-up windows as you surf the InterNet.



According to the [Anti-Phishing Working Group](#), the number of “**scareware**” packages in circulation rose from 2,850 to 9,287 in the 2nd half of 2008. These “**scareware**” packages are designed to trick the unsuspecting user into downloading malicious software or paying for software that you don't need.

Social Engineering - Scareware



Scareware or Fake Security Software

Security intelligence gathered by Microsoft Corp shows a significant increase in rogue security software or 'Scareware' that lures people into paying for protection that, unknown to them, is actually malware often designed to steal personal information.

Individuals are warned not to follow advertisements for unknown software that appears to provide protection and should avoid opening attachments or clicking on links to documents in e-mail or instant messages that are received unexpectedly or from an unknown source.



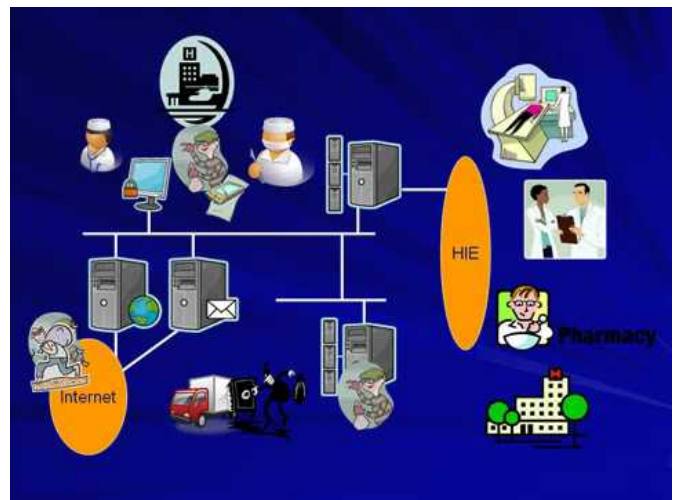
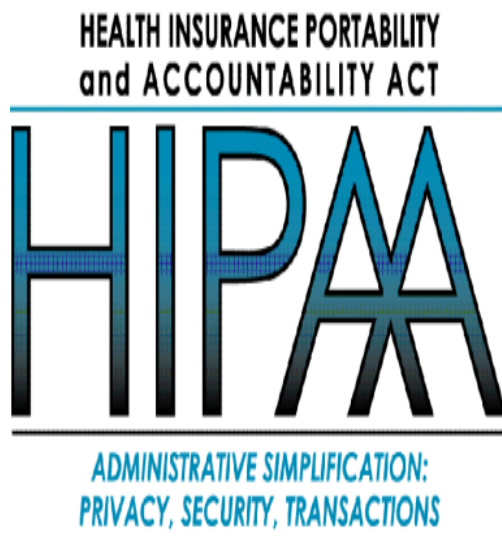
Cybersecurity Risk – Medical/Health-Related Information

HIPAA compliance requires training of almost all individuals who work for a healthcare organization – even those who may only be incidentally exposed to such information. Examples of people who should be trained in the HIPAA regulations (in the basics of patient privacy and confidentiality including concepts such as "Protected Health Information" (PHI) and the "Minimum Necessary" principle) include:

- ✓ physicians, chiropractors, nurses, technicians, administrators, clerks, order processing staff, staff employees such as custodians, transportation, security, volunteers, independent contractors, consultants and vendors

And the rules also require that these training programs be fully documented.

Top HIPAA Security Rule compliance issues are: inadequate user activity monitoring; inadequate contingency planning; insufficient authentication and integrity of data; media reuse and destruction; not conducting regular risk assessments and inadequate monitoring of granting or modifying user access. (Dept of Health and Human Services Office for Civil Rights audit effort, May 2012)



Cybersecurity Risk – Medical/Health-Related Information

Anyone can order the Federal Trade Commission's consumer brochure on Medical Identity Theft from

www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt.10.shtm.

It explains medical identity theft and offers tips on how to minimize the risks and how to recover from a theft.

The latest updates on major health information breaches confirms that the loss and theft of **UNENCRYPTED** devices is one of the major reasons for such breaches. The HITECH Act (Electronic Health Record Incentive Program) contains encryption provisions in the Stage 2 rules, but they are not expected to go into effect until 2014.

Breaches involving unencrypted devices are common because many healthcare providers are reluctant to invest in encryption. Many people have the misperception that encryption costs a lot and impacts their computer's operation. The latest encryption technology has dramatically lowered the costs and no longer significantly affects a computer's performance.



Cybersecurity Risk – Data Breach

London NHS trust fined £90,000 for data breach

An NHS trust has been fined £90,000 after 59 patients' details were sent to the wrong person. Personal data, including diagnoses, was faxed to a member of the public 45 times for three months from last March. *The Central London Community Healthcare NHS Trust did not have sufficient checks in place.*



University of Nebraska Working to Fix Major Security Breach

A forensics team worked through the holiday weekend to find out how someone breached the computer system at the University of Nebraska. *The breach was discovered in 2011 and could affect up to 640,000 current students and alumni dating back to 1985.* Whoever hacked into the electronic database had access to the personal records of students, alumni and applicants at all four university campuses.



Federal Worker Savings Plan Computers Hit in Cyber-Attack

Earlier this year the FBI notified the Thrift Savings Plan, the contribution retirement savings plan for Federal employees, that *a contractor's computer systems had been breached in a complex cyber-attack* with 123,000 Social Security numbers being compromised. The hacking was targeted against computers of Serco Inc., the company that runs the computer systems for the TSP. Initial information indicates that *the hacking incident took place in July 2011.*



Cybersecurity Risk – Data Breach

Reading Hospital's medical records system was breached recently by an employee who **copied sensitive patient information and used it for training purposes**. Medical test results, diagnoses, prescribed medications and other data legally classified as Protected Health Information on 12 patients was made public without the hospital's knowledge or the patients' consent.



Thousands of passwords and credit card details have been exposed online after social engineers breached popular hosting billing platform WHMCS. **Attackers obtained the data after masquerading as the platform's lead developer, Matt Pugh. Attackers managed to con the company's hosting provider to release administrator credentials.**

Pugh's details were then used to access WHMCS' database and steal hashed customer credit card numbers and passwords, usernames and support tickets. That data along with the WHMCS control panel and web site information was dumped online in a 1.7 gigabyte cache. Links to the cache and other, smaller files were tweeted under the WHMCS Twitter account, which the attackers also hijacked.



Almost a day's worth of data was erased from the compromised servers, including "any tickets or replies submitted within the previous 17 hours."

A Northwestern Memorial Hospital employee has been charged with identity theft after she allegedly **used the personal information of hospital patients to pay her bills.** She has worked at Northwestern Memorial Hospital for the last four years. Matteson police began investigating Golden after village officials spotted "suspicious credit card activity" involving payments for her home water bill. Police said they identified the actual owners of credit cards she was using to pay her bills. And they learned from credit companies that all of the cards had been used at a laboratory at Northwestern Memorial. During a search of her home, Matteson police found credit card numbers, birth dates and Social Security numbers from more than 50 patients.

Massive new data breach: Was your email part of the “Epsilon Data Breach”? Should you care?

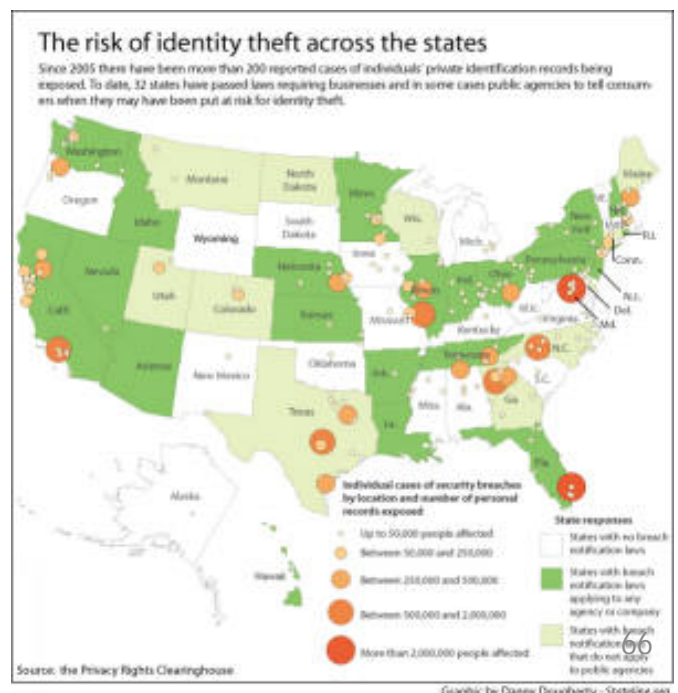
Recently, an email marketing company you’ve never heard of called Epsilon had a data breach where someone (presumably a hacker but they’re not sure) got all the names and emails in their database. Why is this a big deal?

Well, Epsilon just happens to send emails on behalf of lots of companies you have heard of:

- Citibank
- Best Buy
- Walgreens
- Capital One
- Patagonia
- The College Board
- And more.



Do the companies above have any information that might be important to you? About your finances? Health? School records? Of course they do. But do you have to worry? The hackers only got the names and email address, right? What can be done with just knowing your name and email address? Well...



Cybersecurity Risk – Data Breach

What we've learned from other data breaches where hackers got into company databases is that you re-use your passwords a lot. Here were the most common passwords:

1. 123456
2. 12345
3. 123456789
4. Password
5. iloveyou
6. Princess
7. rockyou
8. 1234567
9. 12345678
10. abc123
11. Nicole
12. Daniel
13. babygirl
14. monkey
15. Jessica
16. Lovely
17. michael
18. Ashley
19. 654321
20. Qwerty



But even if your password isn't on the list, the online privacy and identity theft problem here is **DATA MINING**. Hackers are good at cross-referencing data. They can take 50 million names and emails from Epsilon, compare that with 32 million emails and passwords from Rockyou (and other breaches and fake phishing sites), and get hundreds of thousands of online accounts with which they can commit fraud.

It's basically child's play.

This is why everyone needs to take care not to get too angry at Epsilon, *but get in control of your online privacy.*

Cybersecurity Risk – Data Losses

A class action lawsuit was filed against Durham Region Health after a nurse lost a USB key laden with the unencrypted personal information of 83,524 people in December 2009.

The Public Employees Retirement Association of New Mexico is notifying approximately 100,000 members of a breach involving a stolen laptop, containing personal information on its members. The device was taken from the car of an employee of Atkinson & Co., which the pension plan hired to perform its annual audit.

Memorial Sloan-Kettering Cancer Center is notifying 880 patients that some of their personal information may have been exposed when it was inadvertently embedded in PowerPoint charts posted on two websites. In April, the Center discovered 5 incidents involving patient information that was hidden behind graphs in PowerPoint presentations on the websites of 2 professional medical associates. Patient names, clinical information and in some cases SSNs were embedded in the charts. (Find out where your data is or can be!)

The Dumfries and Galloway Council, the governing body for the Dumfries and Galloway region in Scotland, is investigating a data breach involving confidential social work files that were lost after being dropped in a parking lot in Dumfries. According to the BBC, the social work files were found by tourists who brought them to the police. The incident was reported to Scotland's information commissioner, the report says.



**Malware Delivery Device
and Data Losing Device**

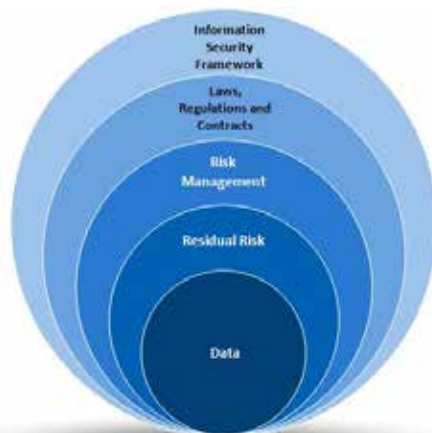


Cybersecurity Risk – Embedded Data In Electronic Files

Note that simply deleting a file or a part of a file does not render the data “gone”. To securely delete a file, it must be wiped using a wiping utility. However, doing this does not ensure that all data contained in the file is removed. Modern operating systems store data in multiple locations and make use of the registry, temp file, cookies, metadata and other forms of data storage to perform task requested. If such data is left intact, it provides a trail of information that renders wiping an obstacle, but not a barrier, to reading that data. Let’s look at some types of data the Windows Operating System leaves behind:

Web Browser – when you search the Internet, your browser creates a complete picture of where you have been and what you have done. Such data is stored in cookies, the cache (temp internet files), the location bar history , the browser history, the autocomplete memory, downloaded program files and the Index.dat files.

E-Mail programs – MS Outlook stores e-mail in personal folders in a PST file. When an e-mail is deleted it is still present and can be retrieved from the PST file. You can permanently delete an e-mail **FROM YOUR COMPUTER** (can’t delete it from the e-mail server, tho) by compacting the PST file and using a wipe utility. However, note that the MS Exchange Server sometimes stores deleted e-mails so that e-mail administrators can undelete in the event of user error.



Cybersecurity Risk – Embedded Data In Electronic Files

Word Processors and other applications – (MS Word is typical)

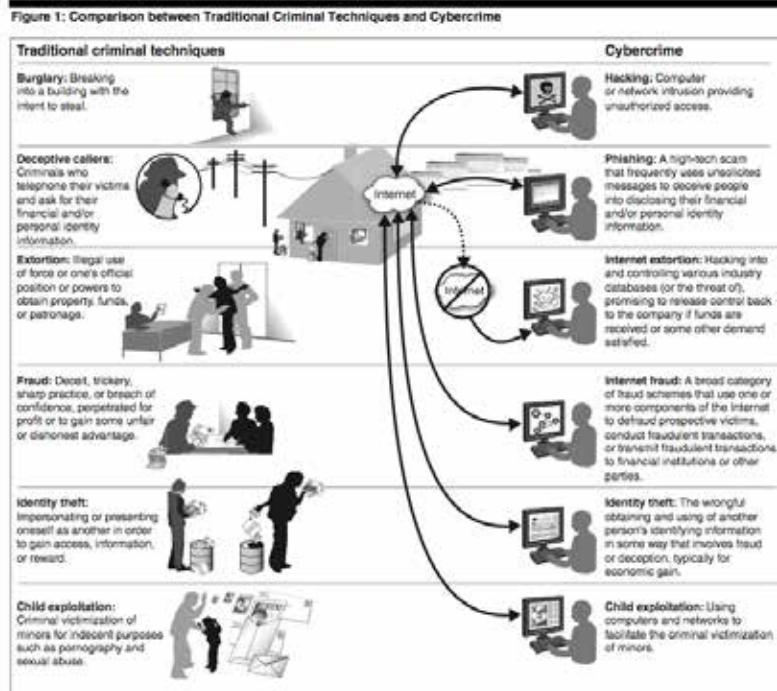
MS Word produces hidden temp files that can maintain copies of any file you are working on. A search of the Windows system for files with a *.tmp extension will show hundreds of Temp files that contain data from every application you have been working on. Additionally, Microsoft uses OLK directories that may contain a complete copy of files that have been viewed.

Metadata

Metadata is data about data. MS Office applications store metadata with the actual file. For example, a 1 character Word document is actually 19 kilobytes versus a 1 character Notepad document is 1 byte. This metadata lists potentially sensitive information about the user and the user's business.

Swap File

The most important storing of hidden data is the Windows Swap file. This file can potentially store any information that has ever been used in a system in plain text – even encrypted information. Like Index.Dat, the Swap file is locked and cannot be deleted. It can be wiped, but not easily. Note that data on the Swap file can appear as plain text both before and after it has been encrypted. It may be useful to use Swap file encryption for important files.

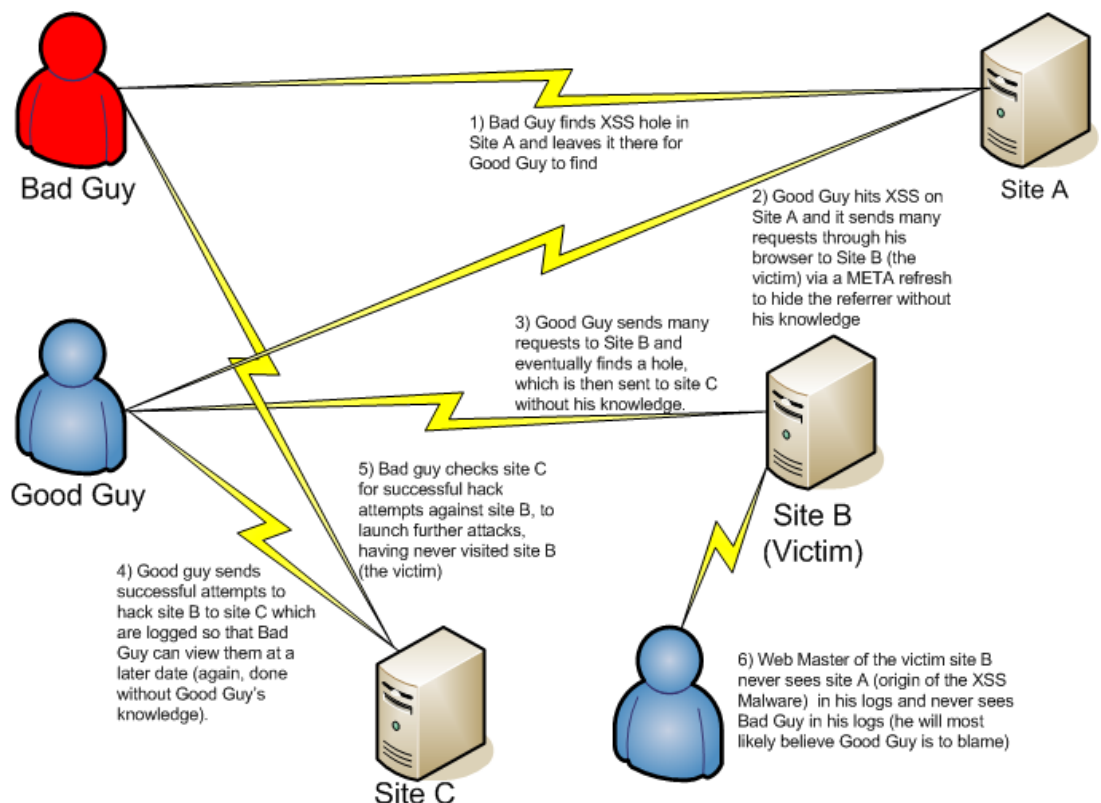


Cybersecurity Risk – Embedded Data In Electronic Files

Hibernation File

When a computer transitions from an active state to a sleep (hibernation) state, the contents of the RAM is immediately copied into a Hibernation File. This file needs to be wiped to remove any data remaining.

It is nearly impossible to completely remove all the information stored on a computer hard drive. The only way to remove all data stored in a computer is to use an approved wiping method on the entire hard drive or a highly rated degausser. After performing these actions, you should still shred and burn the hard drive. **Be aware of this difficulty in removing information from your hard drive if you ever donate your computer to anybody. Recommend taking the hard drive out and destroying it BEFORE donating it.**



Tips From The Trenches

Protecting Business and Personal Information

First and most importantly, you need to assess what information you have and identify who has access to it. Understanding how information moves into, through and out of your business or personal life – and who does or could have access to it – is essential to successfully avoiding cybercrime. Here are some steps you can take for protecting your business/family/group:

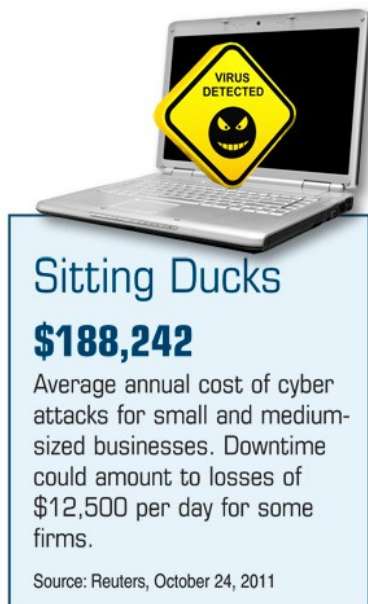
1. Inventory all files, computers, mobile devices, removable media, networks and any other equipment (like copiers and printers) to find out exactly where your business/family stores important information. Don't forget that you can have information stored in e-mail attachments, archives, download folders, caches, with outside service providers (cloud storage), customers, other family sites and your vendors.
2. Track each type of important information (business, personal, family, health, etc.) through its travels. Get a complete picture of who receives, stores, uses and sends all information.
3. Determine how important information comes in – through a web site? Via e-mail? Through the regular mail? Input locally? Note what type of information is collected at each entry point.
4. Determine who has – or can have – access to this important information. Who actually has permission/authority to look at and use this information? Determine if anyone else can get at this information and how.
5. Determine the legal and regulatory requirements for protecting each type of information.
6. Develop an Information Security Plan for your business or group that is integrated with your existing/required physical, administrative and technical safeguards.
7. Create a culture of information security by implementing a regular schedule of training for everyone.



Tips From The Trenches

Avoiding Credit/Debit Card Fraud

1. Keep an eye on your credit card every time you use it, and make sure you get it back as quickly as possible. Try not to let your credit card out of your sight whenever possible.
2. Be very careful to whom you give your credit card. Don't give out your account number over the phone unless you initiate the call and you know the company is reputable. Legitimate companies don't call you to ask for a credit card number over the phone.
3. Never respond to emails that request you provide your credit card info via email -- and don't ever respond to emails that ask you to go to a website to verify personal (and credit card) information. These are 'phishing' scams.
4. Never provide your credit card information on a website that is not a secure site.
5. Sign your credit cards as soon as you receive them.
6. Shred all credit card applications you receive.
7. Don't write your PIN number on your credit card -- or have it anywhere near your credit card (in the event that your wallet gets stolen).
8. Never leave your credit cards or receipts lying around.
9. Shield your credit card number so that others around you can't copy it or capture it on a cell phone or other camera.



Tips From The Trenches

Avoiding Credit/Debit Card Fraud

10. Keep a list in a secure place with all of your account numbers and expiration dates, as well as the phone number and address of each bank that has issued you a credit card. Keep this list updated each time you get a new credit card.

11. Only carry around credit cards that you absolutely need. Don't carry around extra credit cards that you rarely use.

12. Open credit card bills promptly and make sure there are no bogus charges. Treat your credit card bill like your checking account -- reconcile it monthly. Save your receipts so you can compare them with your monthly bills.

13. If you find any charges that you don't have a receipt for -- or that you don't recognize -- report these charges promptly (and in writing) to the credit card issuer.

14. Always void and destroy incorrect receipts.

15. Shred anything with your credit card number written on it.

16. Never sign a blank credit card receipt. Carefully draw a line through blank portions of the receipt where additional charges could be fraudulently added.

18. Never write your credit card account number in a public place (such as on a postcard or so that it shows through the envelope payment window).

20. Never lend a credit card to anyone else.

21. If you move, notify your credit card issuers in advance of your change of address.



Photo credit: [Kiyoshi Takahase Segundo](#)



Tips From The Trenches

Here are some tips against Social Engineering Attacks

Warn (And Train) Your Employees (And Your Family)– You’d be surprised how few people even consider the possibility of someone posing as an IT staffer to steal a password, or dropping a bait disk into an elevator. ***Forewarned is forearmed.*** An employee/individual that knows what proper security procedures are is much more likely to spot and thwart social engineering attacks.

Have A Clear Password Security Policy – A social engineering attacker’s greatest asset is uncertainty. If you have a clear “never give out your password” policy, your employees are bound to be more suspicious when someone asks for their credentials. More to the point, virtually all cloud applications give the administrator the ability to reset a password without knowing the existing credentials, so it should be clear to end-users that no IT administrator will ever need their password.

Create A “Culture of Ask” – A culture of double- and triple-checking access requests is always a good idea. Support and security staff should encourage employees to check in whenever access is requested.

Remember, you are the weakest link in your cybersecurity. Unless and until you treat social engineering attacks with the same seriousness as conventional security threats, you put your data, your organization and your family at risk. Train people, be smart about whom you give access to sensitive information and — as always — have a good backup plan.



Tips From The Trenches



Organizationally, there are things you can do to help avoid becoming a Phishing victim, and to minimize damage if you are victimized:

1. Using dedicated systems for payment requests and approval processes. Disable email access on any system involved with payment processing. If an attacker cannot compromise the systems in payment processing, he will have a harder time obtaining payment usernames and passwords, and a harder time actually requesting/approving a transfer.
2. Use a strong authentication mechanism on all payment processing systems. This would include replacing or augmenting username/password combinations with a hardware token and PIN, or with biometrics such as a fingerprint reader. An attacker will be unable to copy and reuse strong authentication such as a token or biometrics.
3. Block Internet access for systems involved in payment processing. If the system genuinely has no Internet access, malware would be unable to talk back to its controlling systems and attacker.
4. Disable the use of USB flash drives in payment processing systems. In some circles USB flash drives are often referred to as “malware delivery devices.”
5. Use tools available in your email client. Outlook, for instance, has the ability to help filter potentially harmful links.
6. Be diligent in your use of anti-virus and anti-malware software, including regular updates and scans. Most of the malware used as part of a phishing attack is not detected by standard anti-virus software, but some of it is. Some malware indicators may not be changed before an anti-virus update is available, and sometimes older versions of malware are distributed. Additionally, anti-virus software can help identify secondary infections that may be related to an attack.
7. Use reputation-based website, IP address, and URL filtering to help ensure that any systems accessed from within the company are not considered “bad” sites.

Tips From The Trenches

Phishing Tips Continued

8. Consider enforcing time-of-day login and payment processing. Many fraudulent transactions occur after normal working hours.
9. Do not allow access to payment processing systems from mobile devices, laptops, and systems based in home offices.
10. Do not allow access to any internal organization system, especially payment processing systems, from a personally owned home computer.
11. Conduct employee security awareness sessions to instruct employees on how to identify phishing emails and avoid falling victim to them.
12. Explicitly communicate to employees, partners and clients that you will never solicit account information via email, or send a link to update account information.



Individually, there are things employees can do to help avoid becoming a victim and compromising the integrity of organizational operations:

1. Never open attachments or links in unsolicited emails.
2. In general, be suspicious of all emails containing links. If you get an email with a link for you to click, do not click it. Navigate independently to the destination site (for example, by typing www.mybigbank.com into a new browser window) and find the referenced location without using the conveniently included link.
3. Do not respond to suspicious emails in any manner.
4. Do not access emails on the same computers used to initiate or approve payments.
5. Make management aware when you receive a suspicious email.

PASSWORDS...

Keys to
Information Security



**Teach Someone to Phish and
They Can Feed Themselves
Forever...**

Tips From The Trenches



Avoiding problems with mobile devices:

1. Turn off additional mobile features, even those set up in default setting, that are not being used.
2. Encrypt mobile operating systems
3. Install mobile malware and anti-virus applications
4. Use passcodes to protect mobile devices and enable the screen-lock feature.
5. Turn off your Geo-Location feature
6. Be aware that jail-breaking or rooting increases your risks as any time an application or service can run in unrestricted or system level, it allows and compromise to take full control of your device
7. Reset and wipe devices before they are sold or traded
8. Keep your software patches and upgrades up-to-date
9. Avoid links or software downloads from unknown sources
10. Before downloading ANY application or game, read the reviews about the app/game developer or company publishing the app/game and understand user app/game permissions.
11. Be able to remotely wipe devices in case of loss or theft
12. Encrypt all data maintained on the device
13. Do not allow data to move between applications
14. Ensure that there is strong authentication and authorization for device access to enterprise applications and resources



12/2012



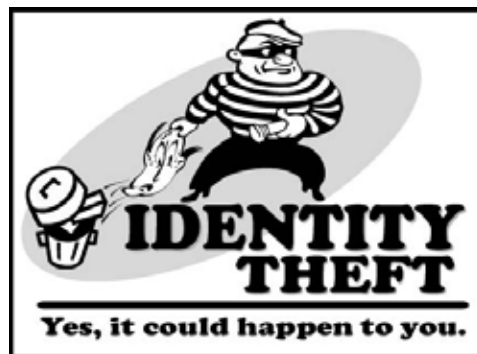
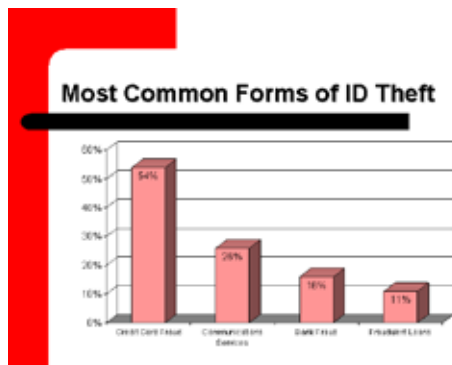
Tips From The Trenches

Here are some tips you can use to avoid becoming a victim of cyber fraud:

1. Do not respond to unsolicited (spam) e-mail.
2. Do not click on links contained within an unsolicited e-mail.
1. Don't open e-mails that don't have subjects.
2. Be cautious of e-mail claiming to contain pictures in attached files, as the files may contain viruses. Only open attachments from known senders. Scan the attachments for viruses and other malware.
3. Avoid filling out forms contained in e-mail messages that ask for personal information.
4. Always compare the link in the e-mail with the link to which you are directed and determine if they match and will lead you to a legitimate site.
5. Log directly onto the official website for the business identified in the e-mail, instead of "linking" to it from an unsolicited e-mail. If the e-mail appears to be from your bank, credit card issuer, or other company you deal with frequently, your statements or official correspondence from the business will provide the proper contact information.
6. Contact the actual business that supposedly sent the e-mail to verify if the e-mail is genuine.
7. If you are asked to act quickly, or there is an emergency, it may be a scam. Fraudsters create a sense of urgency to get you to act quickly.
8. Verify any requests for personal information from any business or financial institution by contacting them using the main contact information.
9. Check your credit reports (and all of your families) at least once a year.
10. Have someone continually checking the web for your SSN, credit card numbers, account numbers, etc. to show up.
11. You should use a dedicated and locked down computer for all online financial transactions.
12. Encryption of **ALL** data, regardless of where it is, remains the best prevention idea.
13. Always **KNOW WHO** you are talking/e-mailing/messaging to and don't provide ANY important information over the phone unless you have initiated the call. The HelpDesk, IT department, IT vendor, phone company, bank, etc. won't call.



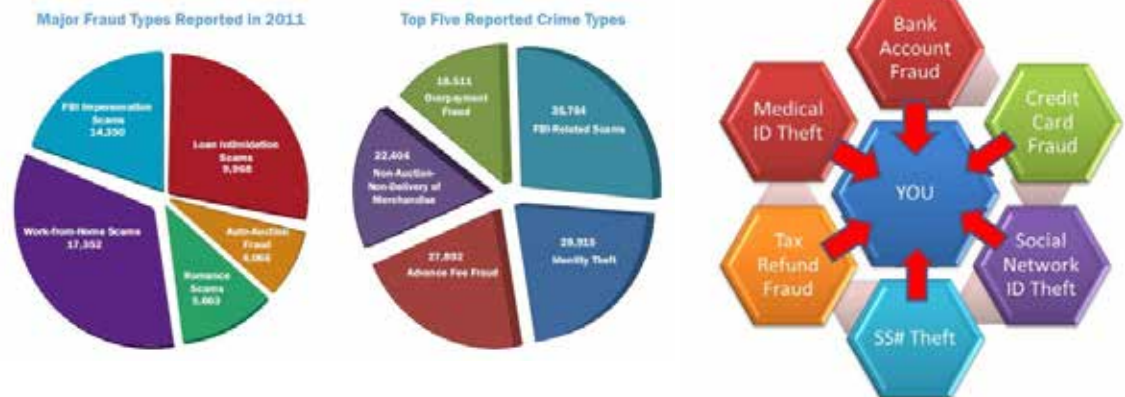
Tips From The Trenches



Ways to Protect Your Identity in 2013

1. Memorize your social security number and remove the card from your wallet
2. Write **"See ID"** in ink on the back of your credit card next to your signature
3. Where possible, use credit cards and gift cards instead of debit cards
4. Physically shake card readers at gas stations and ATMs to make sure ID thieves have not placed a "skimmer" on those machines
5. Accompany waiters\waitresses to the register and watch them run your credit or debit card
6. Don't give out personal information over email
7. Avoid shopping on public Wi-Fi networks and shared computers
8. Make sure your computer is updated and protected from viruses and malware
9. Beware of anyone looking over your shoulder when you're at the checkout line
10. Create a monthly inventory of bills, bank and credit account statements and expenses
11. When purchasing online, make sure the URL includes "https://" and check for a locked key logo at the bottom of the page
12. Don't swipe your credit card at the checkout, hand it to the cashier to run through the register
13. Carry only the credit cards you need while traveling
14. When traveling, only include first initial, last name and mobile number on luggage tags
15. As tempting as it may be, avoid putting details of your trip on social media and avoid uploading photos while on your trip
16. Pay for your downloaded music and avoid downloading peer-to-peer software
17. Type in the address of websites you want to visit instead of clicking on a pop-up or a hyperlink
18. Place fraud alerts with the three Major Credit Bureaus.
19. Periodically request a credit report and look it over carefully for any suspicious activity

Tips From The Trenches



How can you minimize the chance of becoming an Identity Theft victim?

1. Don't carry your Social Security card or any document(s) with your SSN on it.
2. Don't give a business your SSN just because they ask. Give it only when legitimately required.
3. Protect your financial information.
4. Check your credit report every 12 months.
5. Secure personal information in your home.
6. Protect your personal computers by using firewalls, anti-spam/virus software, update security patches, and change passwords for Internet accounts.
7. Don't give personal information over the phone, through the mail or on the Internet unless you have initiated the contact or you are sure you know who you are dealing with.
8. Don't leave personal information: in your car - When you go through the bank drive thru, a toll booth, or even a fast food drive thru, it is habit to through your credit cards, identification, bank statements and money into your center console or glove box. Take the time to properly put your identification, bank cards, and money in your wallet or purse.
9. keep your kids' birth certificates, passports and social security cards locked up in a safe place at home.
10. Every time somebody (a hospital or at a business) asks for your child's social security number, remember to ask why they need first and if the reason is valid then don't forget to write who you gave it to. This is done so that in case something out of the ordinary happens and your child's social security number is involved, all you need to do is produce the names of people you gave it out to and the relevant authority will handle the issue.

Tips From The Trenches

11. Most parents do not see the need in checking credit reports because they know their children do not have any credit. This is what identity thieves know and take advantage of. So ensure that you check it periodically.

12. Keep Travel Plans Private - People increasingly broadcast their travel and dinner places on Facebook or Twitter, making thieves aware of empty homes. According to recent surveys, nearly 50% of travelers between the ages of 18 and 34 post their whereabouts as social media updates. Many identity thieves know peak travel or go to dinner times and simply **break into empty homes in search of bank statements, SSN cards, and other important account information.** *So where is your important information and is it easy to find?* If it is not secure, you are at higher risk for identity theft. Don't write about where you are or post photos of a trip until you return.

13. Just remember – *Most legitimate businesses or government organizations* will **NEVER** ask you for personal information or business information over e-mail or telephone call (if you did not initiate it).

14. Always have backups for any important data/applications.

15. The biggest cause of data breaches as lost and stolen computer equipment, so maintain knowledge of your equipment and be able to remotely wipe it.

16. Be cautious of E-mails Soliciting Donations **FOR ANYTHING.**

17. Be cautious of e-mails and messages - Facebook /Twitter discussions - with links purporting to blog/discuss/show pictures of the latest person, place or thing.

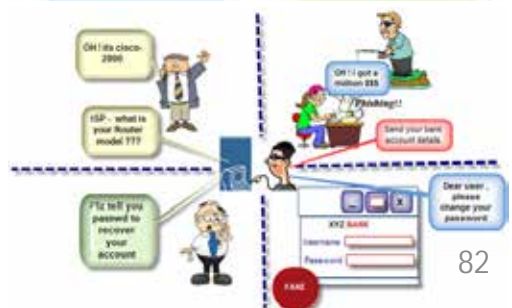


Top 10 passwords

123456 = 1666 (0.38%)
password = 780 (0.18%)
welcome = 436 (0.1%)
ninja = 333 (0.08%)
abc123 = 250 (0.06%)
123456789 = 222 (0.05%)
12345678 = 208 (0.05%)
sunshine = 205 (0.05%)
princess = 202 (0.05%)
qwerty = 172 (0.04%)

Top 10 base words

password = 1373 (0.31%)
welcome = 534 (0.12%)
qwerty = 464 (0.1%)
monkey = 430 (0.1%)
jesus = 429 (0.1%)
love = 421 (0.1%)
money = 407 (0.09%)
freedom = 385 (0.09%)
ninja = 380 (0.09%)
writer = 367 (0.08%)



Tips From The Trenches



Avoiding Online Scams

1. Know who you are dealing with – find a seller’s physical address (not just a P.O. Box) and phone number. Do an internet search for the company name and website and look for negative reviews.
2. Understand that wiring money is like sending cash. It’s nearly impossible to reverse such a transaction or trace the money, especially out o the country.
3. Don’t wire money to strangers, to sellers who insist on wire transfers for payment, or anyone who claims to be a relative or friend in an emergency who wants to keep the request a secret or for you to respond immediately.
4. Read your monthly statements or check online daily. If you see charges you didn’t authorize, contact your bank, card issuer or other creditor immediately.
5. Give only to established charities after a disaster. Don’t give to those that have sprung up overnight. For donating tips, check out www.ftc.gov/charityfraud.
6. Don’t agree to deposit a check and wire money back. Uncovering a fake check can take weeks and you are responsible for any check you deposit.
7. Don’t reply to messages asking for personal or financial information.
8. Don’t play a foreign lottery. Messages saying you have already won are scams. You will most likely be asked to pay “taxes”, “fees” or “customs duties” to collect your prize.
9. Report online scams – file a complaint with the Federal Trade Commission (<http://www.ftc.gog/complaint>) and your state Attorney General (<http://www.naag.org/current-attorneys-general.php>). For lottery material from a foreign country, give that to your local postmaster.

Tips From The Trenches



Avoiding/Reacting to Malware

1. Keep your security software updated. At a minimum, your computer and mobile device should have a firewall, antivirus and antispyware applications that update automatically.
2. Don't click on any links or open any attachments in e-mails unless you know who sent it and you know what it is.
3. Download and install software only from websites you have verified that know and trust.
4. Make sure your browser security settings are high enough to detect unauthorized downloads.
5. Use a pop-up blocker and don't click on any links within pop-ups.
6. Do not buy or download any software in response to unexpected pop-up messages or e-mail.
7. Talk with your family/employees/friends about safe computing and actions that put your/their computers and mobile devices at risk.
8. Back up your data regularly.
9. Monitor your computer and mobile device for unusual behavior. Does it slow down, crash, display repeated error messages, won't shut down or restart, serves up a barrage of pop-ups, displays web pages you didn't intend to visit, ends e-mails you didn't write.
10. Other warning signs: new and unexpected toolbars, new and unexpected icons in your shortcuts or on your desktop, a sudden or repeated change in your internet home page, a laptop battery that drains more quickly than it should.
11. If you think you have malware on your computer or mobile device, stop shopping, banking or doing any online activities that involve user names, passwords, or other personal information. Disconnect from the internet or turn off the mobile device.
12. Work with a computer specialist to get the malware removed **before** you go back on the internet. The malware may be running in the background and passing your personal information to another site.

Let the FBI (<http://www.ic3.gov>) know and file a complaint with the Federal Trade Commission (<http://www.ftc.gov/complaint>).

Tips From The Trenches

Securing a Wireless Network

Unless you take certain precautions, anyone nearby with a wireless-ready computer or mobile device can use your network. That means anyone nearby can piggyback on your network and access information in your computer or connected mobile device. Also, if an unauthorized person uses your network to commit a crime or send spam, the activity can be traced back to your account/network.



1. Use encryption. Use WPA2 if you have a choice. You must turn on your network's encryption feature.
2. Use a firewall, anti-virus and anti-spyware applications and keep them updated.
3. Change the name of your router from the default to something unique that only you know.
4. Change your router's preset password. The longer the password, the tougher it is to crack.
5. Turn off your wireless network when you know that you aren't using it.



To secure a network that allows mobile device connections:

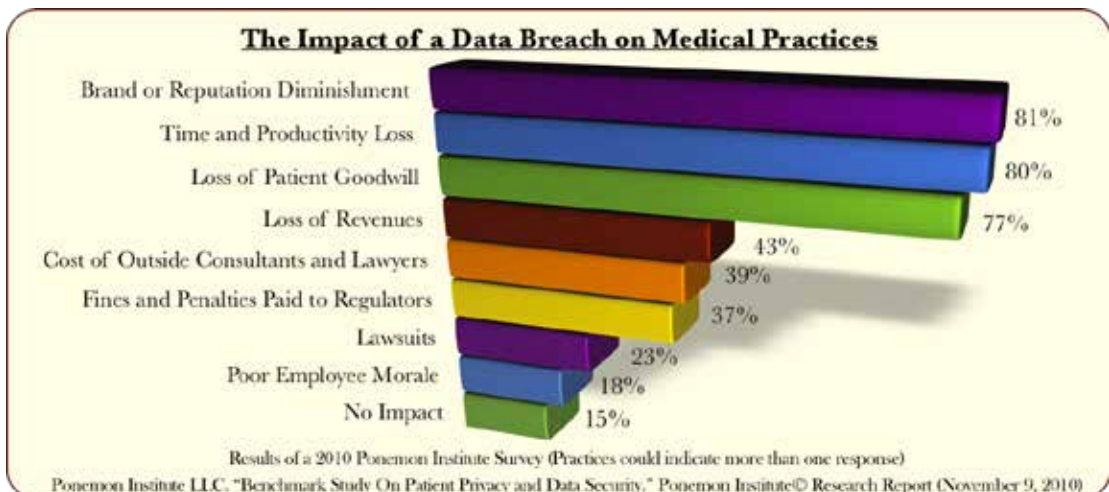
- q **Require strong password**
- q Have a Password history check
- q Ensure that Passwords expire
- q Inactivity time out
- q Lock out after 7 failed attempts to log in
- q Remote wipe if device is compromised or on lock out
- q Encryption on the mobile device

Tips From The Trenches

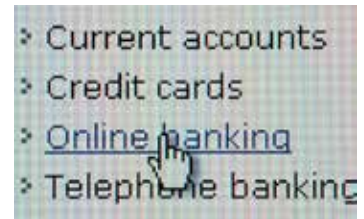
Health/Medical Information Protection

How to protect your health, medical, billing and financial records and correct them if they are compromised:

1. Make sure you have a copy of your health professional's Notice of Privacy Practices to have contact information about whoever is responsible for responding to questions or concerns about the privacy of health/medical information.
2. Make sure you are advised of your rights under HIPPA Privacy Rule - you are entitled to a copy of all of your records.
3. Note that the Originator of the information must correct any inaccurate/incomplete information and notify other parties (like labs) that they know received the incorrect/inaccurate information.
4. You must notify your health plan provider if you suspect or know that your medical information has been compromised or is being used fraudulently.
5. You should file a complaint with your local police and send copies of the complaint to your health care provider ;s fraud department, your health care provider and the three credit reporting agencies.
6. You can (and are encouraged to) file a complaint with the Federal Trade Commission at www.ftccomplaintassistant.gov or 1-877-IDTHEFT (1-877-438-4338);



Summary and Conclusions



Cyber fraud is one of the greatest threats facing the nation's economic future.

Everyone is in the front lines in terms of protecting their business and their family.
They need to feel this and act in accordance with it.

5 – 10 years ago many people were fearful of technology. Today they are fearful of being without it. The fear of not being without your phone – nomophobia. Connections abound and are increasing – and each presents additional vulnerabilities and threats.

Everyone needs an understanding of how best to capitalize on your investments, manage relationships and achieve compliance with ever-increasing cyberspace rules, regulations and laws.

Knowledge of the risk environment enables you to minimize business and personal losses - lost revenue, lost customers, lost reputation, lost personnel effectiveness, lost productivity, lost money, lost credit, lost reputation.

Remember if it looks too good to be true, it probably is.

Knowledge and awareness, combined with appropriate technology, will protect you and your business/family.

**Start using Risk-Based Decision Making,
Fire Prevention rather than Fire Fighting**



References and Links for Cybersecurity

Taxpayer Guide to Identity Theft

ID Theft Tool Kit

Are you a victim of identity theft?

If you receive a notice from the IRS, please call the number on that notice. If not, contact the IRS at 800-908-4490

Fill out the IRS Identity Theft Affidavit, Form 14039

The IRS does not initiate contact with taxpayers by email to request personal or financial information. The IRS does not ...

... request detailed personal information through email.

... send any communication requesting your PIN numbers, passwords or similar access information for credit cards, banks or other financial accounts.

How to handle and report phishing:

<http://www.irs.gov/privacy/article/0,,id=179820,00.html>

Report suspicious online or emailed phishing scams to: phishing@irs.gov

For phishing scams by phone, fax or mail, call: 1-800-366-4484

Useful IRS Publications:

Tax Scam Warning: Beware of Phony Refund Scheme Abusing Popular College Tax Credit; Senior Citizens, Working Families and Church Members Are Targets

IRS Releases the Dirty Dozen Tax Scams for 2012

IRS Alerts Public to New Identity Theft Scams

IRS Warns of New E-Mail and Telephone Scams Using the IRS Name; Advance Payment Scams Starting

IRS Warns of E-mail Scam Soliciting Donations to California Wildfire Victims

IRS Warns of New E-mail Scam Offering Cash for Participation in "Member Satisfaction Survey"

IRS Warns Taxpayers of New E-mail Scams

IRS Warns of Phony e-Mails Claiming to Come from the IRS

Electronic Federal Tax Payment System Cited in New E-mail Scam

References and Links for Cybersecurity

Alabama Cybersecurity Links

<http://www.idtheftcenter.org/artman2/publish/states/Alabama.shtml>

<http://alabamaidtheft.com/>

<http://www.ftc.gov/bcp/edu/microsites/idtheft/reference-desk/index.html>

Credit Bureaus

Equifax www.equifax.com 1-800-525-6285

Experian www.experian.com 1-888-397-3742

TransUnion www.transunion.com 1-800-680-7289

Anti-Phishing Working Group: reportphishing@antiphishing.org

- Better Business Bureau (investigates disagreements between businesses and customers; www.bbb.org/consumer-complaints/file-a-complaint/get-started)
- CyberTipLine, operated by the National Center for Missing & Exploited Children (investigates cases of online sexual exploitation of children; 1-800-843-5678 or www.cybertipline.com)
- Electronic Crimes Task Forces and Working Groups (www.secretservice.gov/ectf.shtml)
- The Secret Service (investigates fraudulent use of currency; www.secretservice.gov/field_offices.shtml)
- StopFraud.Gov Victims of Fraud Resources (www.stopfraud.gov/victims.html)
- U.S. Computer Emergency Readiness Team (www.us-cert.gov)
- U.S. Department of Justice (www.justice.gov/criminal/cybercrime)
- U.S. Postal Inspection Service (investigates fraudulent online auctions and other cases involving the mail; postalinspectors.uspis.gov/contactus/filecomplaint.aspx)

References and Links for Cybersecurity

OnGuardOnline.gov is the federal government's website to help you be safe, secure and responsible online. The Federal Trade Commission manages OnGuardOnline.gov, in partnership with the federal agencies listed below. OnGuardOnline.gov is a partner in the Stop Think Connect campaign, led by the Department of Homeland Security, and part of the National Initiative for Cybersecurity Education, led by the National Institute of Standards and Technology.

<http://www.onguardonline.gov>

Looking for consumer resources from the Federal Trade Commission? They're at consumer.ftc.gov, a new URL for information from the nation's consumer protection agency.

<http://www.consumer.ftc.gov/>

National Cyber-Forensics & Training Alliance

<http://www.ncfta.net/Index.aspx>

Multi-State Information Sharing and Analysis Center: The mission of the MS-ISAC is to improve the overall cyber security posture of state, local, territorial and tribal governments. Collaboration and information sharing among members, private sector partners and the U.S. Department of Homeland Security are the keys to success.

<http://msisac.cisecurity.org/resources/guides/>

Homeland Security Department – Reporting Cyber Incidents:

<http://www.dhs.gov/how-do-i/report-cyber-incidents>

<http://www.dhs.gov/stophinkconnect-cyber-tips>

Other Resources

Visit the Federal Trade Commission or call the FTC toll-free identity theft helpline: 1-877-ID-THEFT (1-877-438-4338)

FBI Internet Crime site - www.IC3.gov

References and Links for Cybersecurity

Malware Info Resource Center

Malware is the industry term used to generally describe malicious software, i.e., software that is designed to compromise the confidentiality, integrity or availability of computer systems. The term "Malware" is broader than the better known expression "Virus" as it also encompasses Worms, Trojan Horses, Rootkits, Spyware, Adware, Crimeware, Robot (botnet) Clients, etc. A detailed discussion of these specific terms is beyond the scope of this document. For more information refer to Wikipedia's malware page.

<http://www.malware-info.com/>

Maryland Cyber Security Center provides education programs to prepare the future cybersecurity work force, and develop new, innovative technologies to defend against cybersecurity attacks.

<http://doit.maryland.gov/cybersecurity/Pages/CyberSecurityHome.aspx>