Accomplishing Risk-Based Decisions

CyberSecurity Risk Environment – 2013

Dave Hall
ESEP/CISSP
Hall Associates
301 641-1530
halld105048@yahoo.com
http://www.linkedin.com/pub/dave-hall/22/4b6/5a2

Why Do I Care About Cybersecurity?

Businesses and individuals increasingly work with and through the Internet and computers, making the risks inherent in these systems far more threatening than ever. **You are increasingly "connected"**.

There are more and more complex threats "in the wild", making Internet and IT security harder to accomplish. It's not a case of **IF**, but of **WHEN**. **NO** system or device can be made absolutely secure.

Internet and IT risks, when they occur, will cause 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 risks/threats you face, you will not be prepared for them.

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 and personnel have a responsibility to identify areas of risk 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 risks***. Individuals also have a responsibility to ***properly identify and respond to risks*** to maintain what they and their family has.

Why do I care? Failure to identify, assess, control and monitor risk sets both businesses and individuals up for serious security breaches and financial losses now and down the road.

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

Why Should Small Businesses Be Concerned?

Myth – **Small businesses are different than big businesses when it comes to Cyber risks. They are too small to be a target.** In 2011, malicious codes were inserted into 20,000 to 30,000 sites that small businesses use to conduct their business. These codes stole information from the small businesses when they used the site.

In one report – **24% of 2012 breaches occurred at retailers and restaurants**, 20% in manufacturing, transportation and utilities.

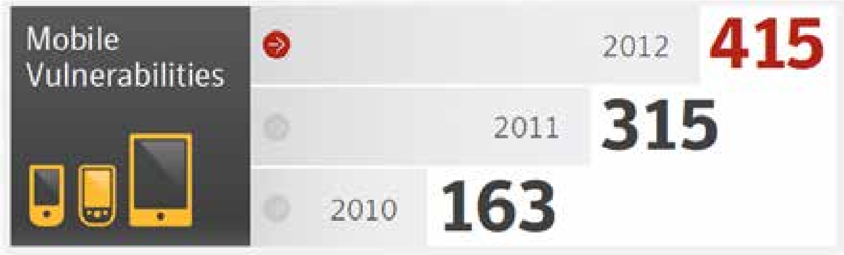
In a Symantec report - **40% of all cyber attacks are directed at small companies**. ***60% of small businesses closed within 6 months of a cyber attack.*** 59% of small businesses do not have a contingency plan for responding and report data breaches. 66% of small businesses are not concerned about cyber threats – either internal or external. **Attacks were up 18% from 2011.**

Verizon data breach investigations report notes that **small businesses continue to be the most victimized of all companies.** Of the 621 confirmed data breaches almost 50% occurred at companies with fewer than 1000 employees, including 193 incidents at companies with fewer than 100 employees.

Cybercriminals are using small businesses as stepping stones – they offer the path of least resistance into a major network.

2012 in Numbers

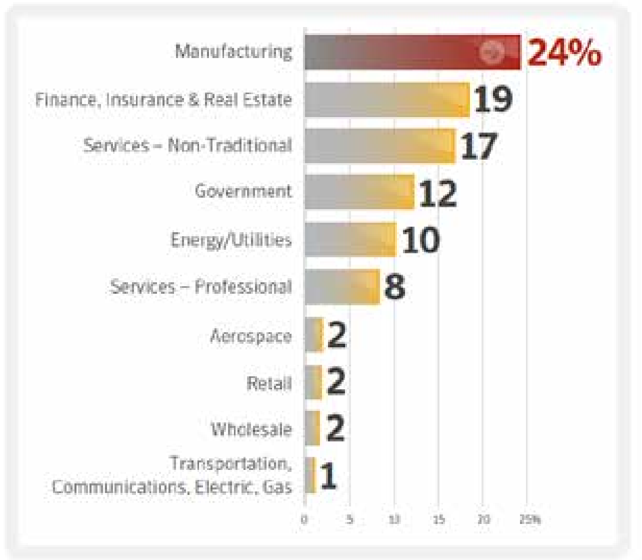
Targeted
Attacks
in 2012
42% INCREASE



Mobile Malware
Families Increase
2011–2012
58%

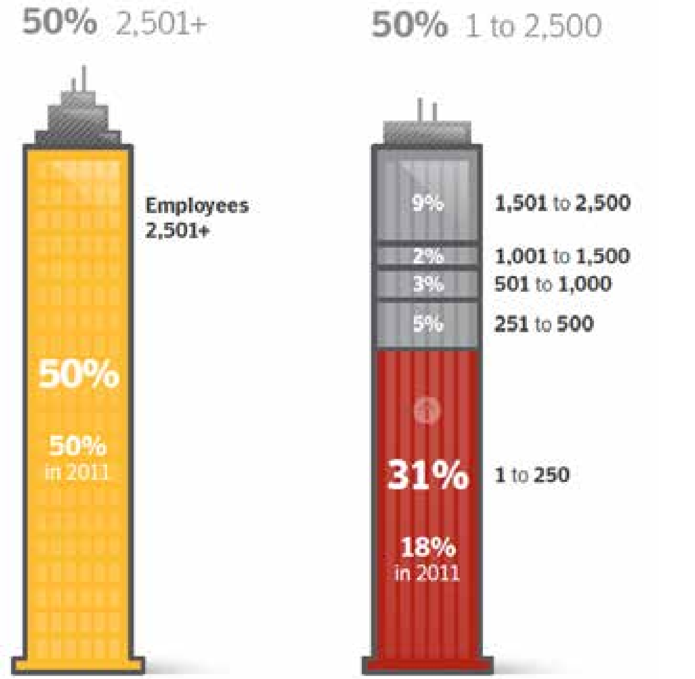
Top 10 Industries Attacked in 2012

Source: Symantec

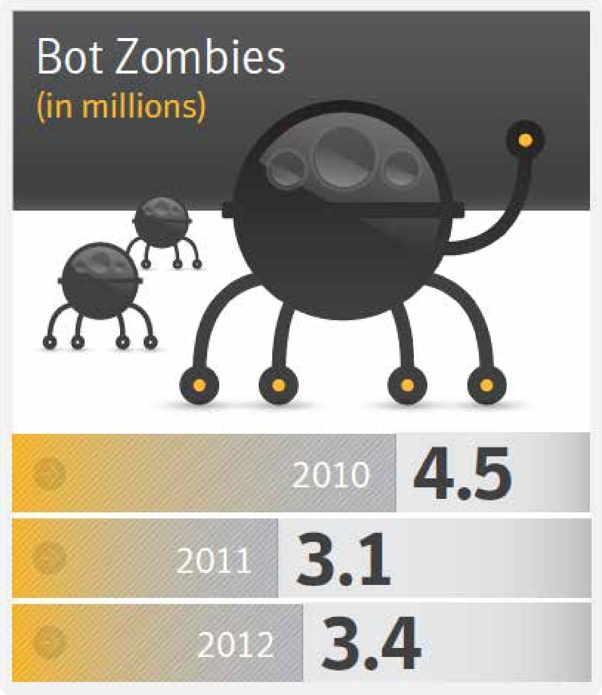


Attacks by Size of Targeted Organization

Source: Symantec

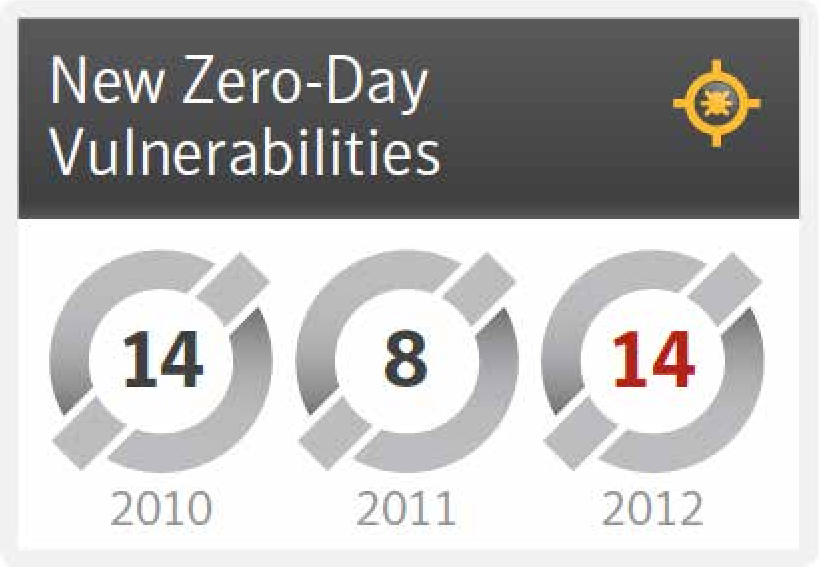


2012 in Numbers



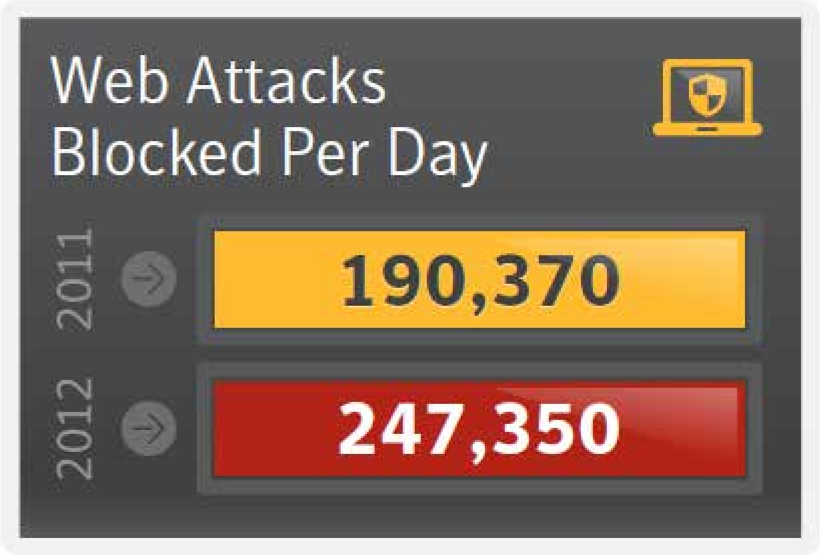
Bot Zombies
(in millions)

2010	4.5
2011	3.1
2012	3.4



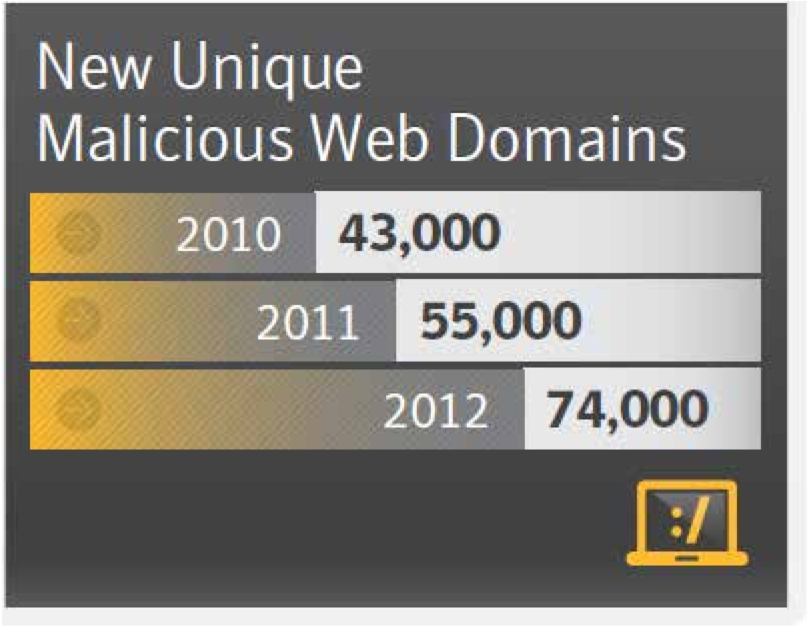
New Zero-Day Vulnerabilities

2010	14
2011	8
2012	14



Web Attacks Blocked Per Day

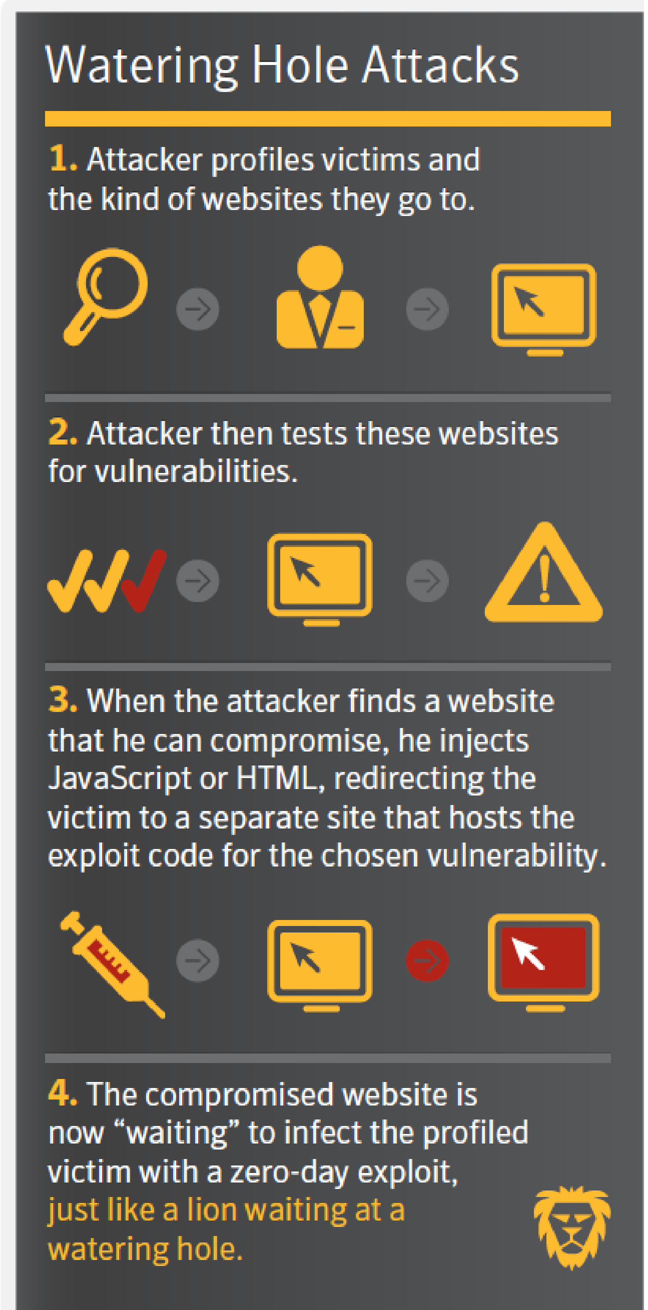
2011	190,370
2012	247,350



New Unique Malicious Web Domains

2010	43,000
2011	55,000
2012	74,000

2012 in Numbers



Watering Hole Attacks

1. Attacker profiles victims and the kind of websites they go to.

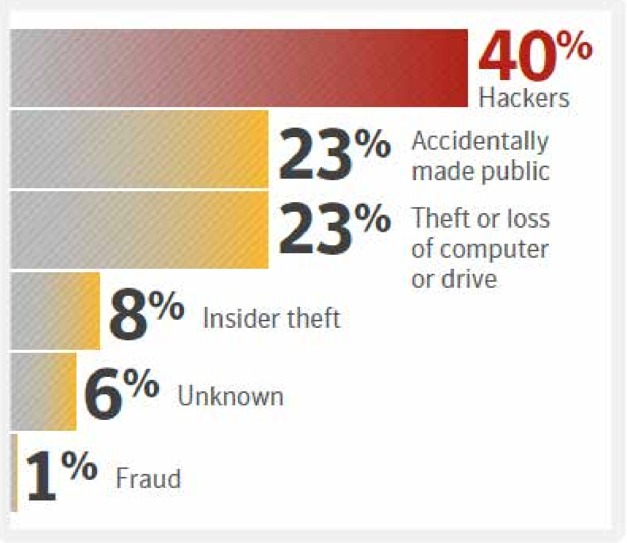
2. Attacker then tests these websites for vulnerabilities.

3. When the attacker finds a website that he can compromise, he injects JavaScript or HTML, redirecting the victim to a separate site that hosts the exploit code for the chosen vulnerability.

4. The compromised website is now “waiting” to infect the profiled victim with a zero-day exploit, just like a lion waiting at a watering hole.

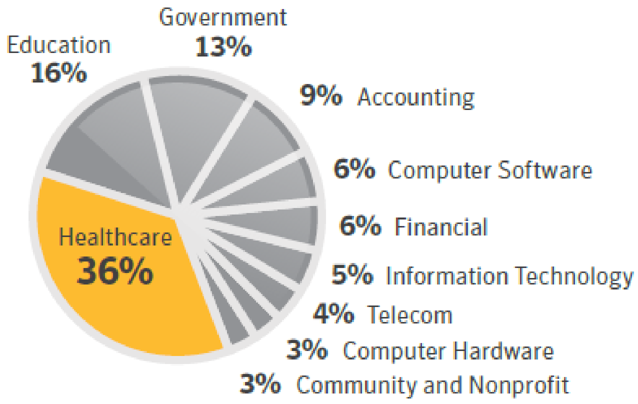
Top Causes of Data Breaches in 2012

Source: Symantec



Data Breaches by Sector in 2012

Source: Symantec

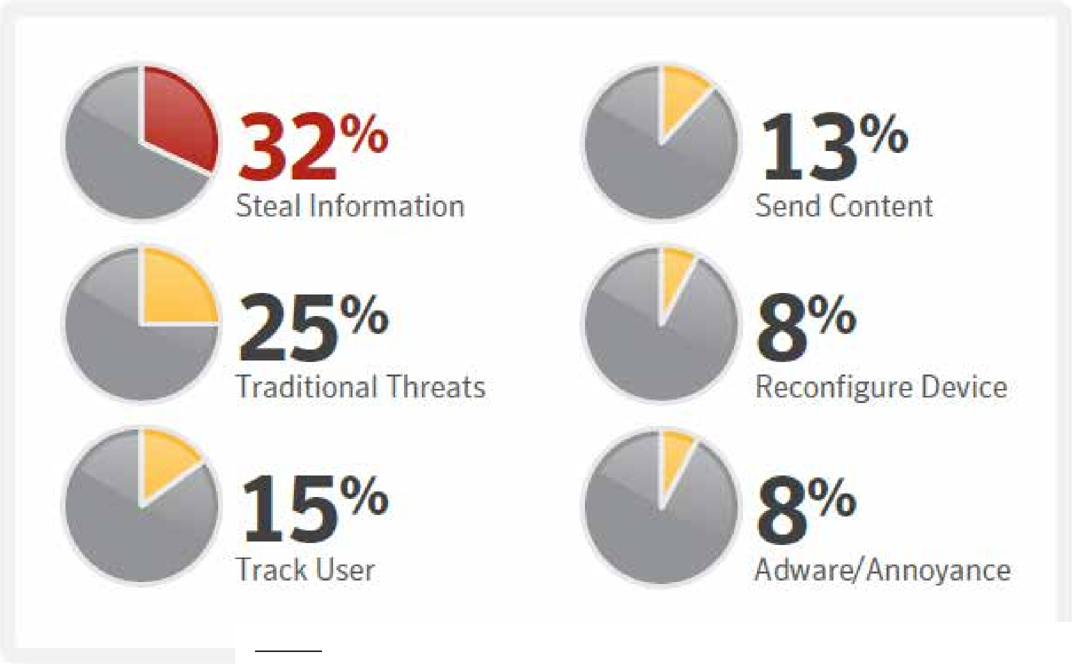


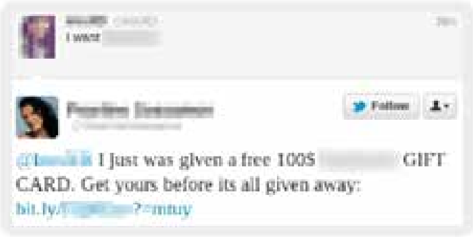
At 36 percent, the healthcare industry continues to be the sector responsible for the largest percentage of disclosed data breaches by industry.

2012 in Numbers

Mobile Threats in 2012

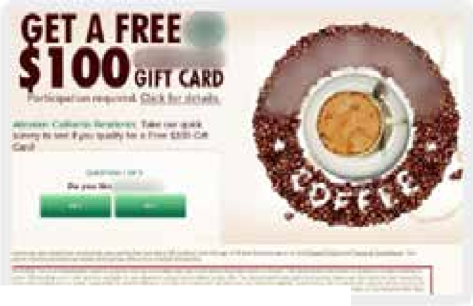
Source: Symantec





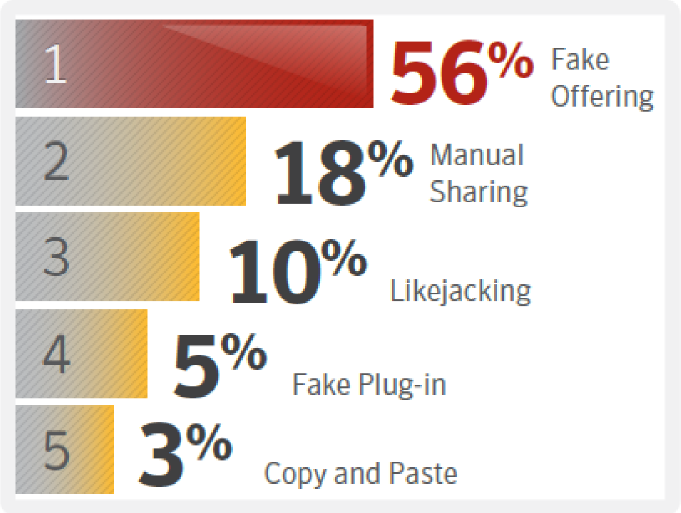
@[redacted] I Just was given a free 100$ [redacted] GIFT CARD. Get yours before its all given away: bit.ly/[redacted]?=mtuy

Typical social media scam.



Top 5 Social Media Attacks in 2012

Source: Symantec

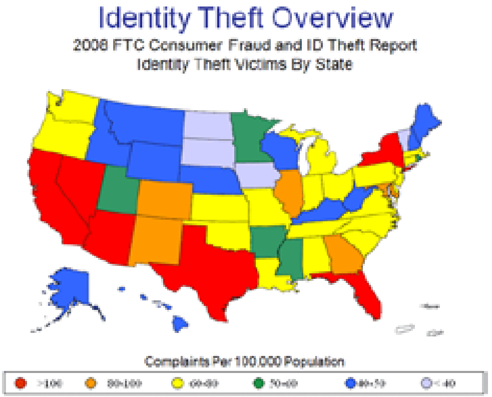


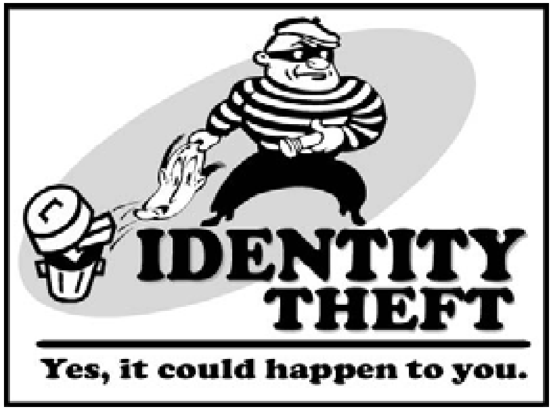
- **Fake Offering.** These scams invite social network users to join a fake event or group with incentives such as free gift cards. Joining often requires the user to share credentials with the attacker or send a text to a premium rate number.
- **Manual Sharing Scams.** These rely on victims to actually do the hard work of sharing the scam by presenting them with intriguing videos, fake offers or messages that they share with their friends.
- **Likejacking.** Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, spreading the attack.
- **Fake Plug-in Scams.** Users are tricked into downloading fake browser extensions on their machines. Rogue browser extensions can pose like legitimate extensions but when installed can steal sensitive information from the infected machine.
- **Copy and Paste Scams.** Users are invited to paste malicious JavaScript code directly into their browser's address bar in the hope of receiving a gift coupon in return.

Cybersecurity Risk – Identity Theft

More than 93 million identities were exposed in 2012 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-

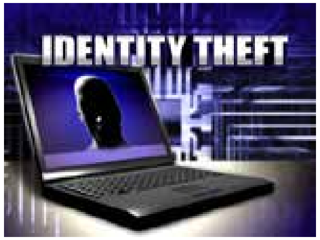
36% - Healthcare;
13% - Government;
16% - Education;
6% - Financial
9% - Accounting;
6% - Computer Software;
5% - IT;
4% - Telecom
3% - Computer Hardware;
3% - Community and Nonprofit


Identity Theft Overview
2008 FTC Consumer Fraud and ID Theft Report
Identity Theft Victims By State
Complaints Per 100,000 Population
● >100
● 80-100
● 60-80
● 50-60
● 40-50
● < 40



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 Alabamanoted. 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.

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 kid's 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.

IRS Overwhelmed by Tax Related Identity Theft

[Tax ID Theft]
1040
U.S. Individual Income Tax Return
Label
Presidential Election Campaign
Filing Status

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.

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.***

Cybersecurity Risk - Extortion

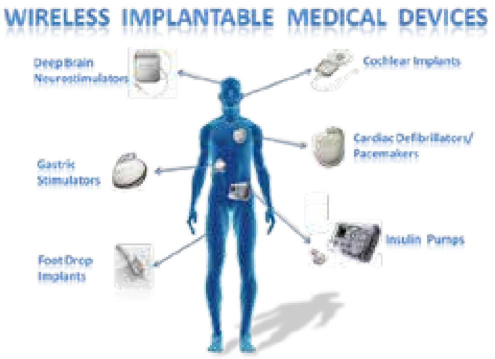
Scammers (extortionists) are requiring a payoff or discount from retail stores or restaurants or they will post a terrible rating on online review sites. Legal experts say that not to pay and not to file a lawsuit is wise. If a business is seen as litigious, it can be as bad for your reputation. The 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.

Cybersecurity Risk – Mobile Devices

Over half of consumers 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 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.**

Cybersecurity Risk – Mobile Devices

Interesting thought – some mobile devices are just now coming into widespread use – wireless medical devices both worn and implanted. These CAN be hacked.


WIRELESS IMPLANTABLE MEDICAL DEVICES
Deep Brain Neurostimulators
Cochlear Implants
Cardiac Defibrillators/ Pacemakers
Gastric Stimulators
Insulin Pumps
Foot Drop Implants

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".**

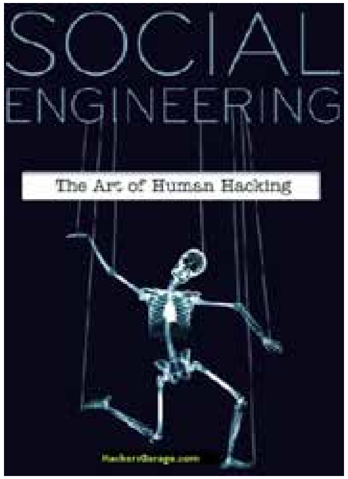
Laptops and PCs can be hacked and the webcam and microphone **turned on remotely**.

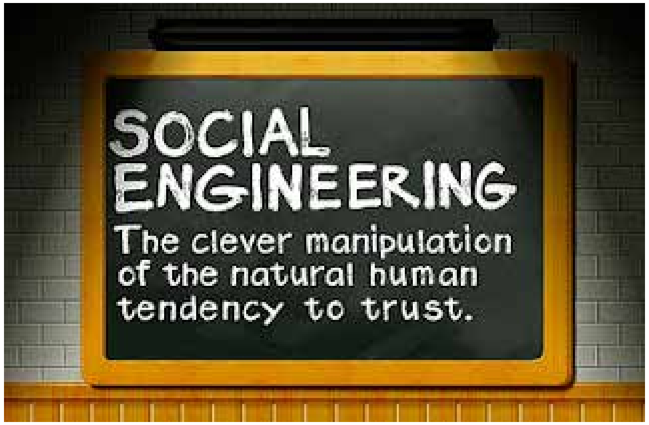
Over half of consumers using smart mobile devices employ location-based applications despite concerns about safety and 3rd party use of their personal information. Almost half state that **they don't read agreements** when downloading apps. Note that smart phone photos are imprinted with the current GPS coordinates **unless that feature is turned off.**

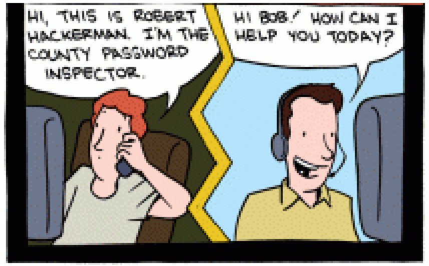
Cybersecurity Risk – Social Engineering

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.






HI, THIS IS ROBERT HACKERMAN. I'M THE COUNTY PASSWORD INSPECTOR.
HI BOB! HOW CAN I HELP YOU TODAY?

Cybersecurity Risk – 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 personal information.

Be leery of e-mails or text messages that indicate a problem or question regarding your financial accounts.

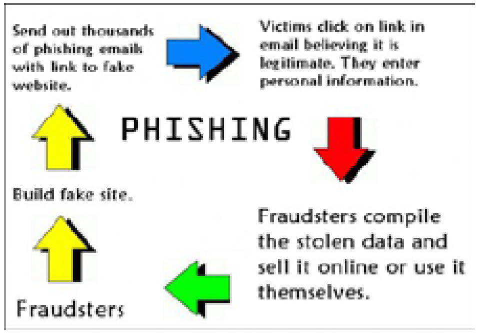
Phishing schemes related to deliveries are also rampant.

Phishing is difficult to detect

Most phishing e-mails include threats requiring immediate action.

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

Cybersecurity Risk – Fraud/Phishing



Send out thousands of phishing emails with link to fake website.

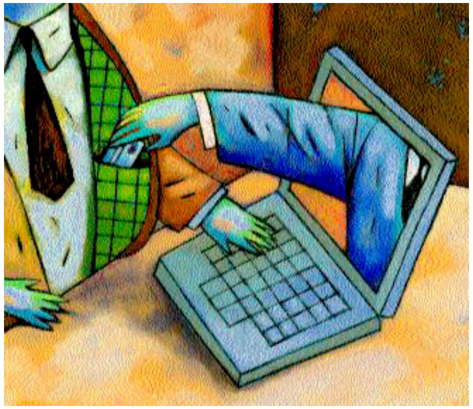
Victims click on link in email believing it is legitimate. They enter personal information.

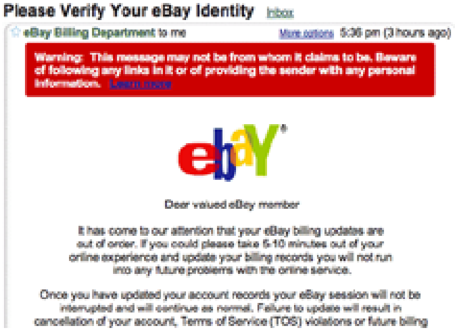
PHISHING

Build fake site.

Fraudsters compile the stolen data and sell it online or use it themselves.

Fraudsters





Please Verify Your eBay Identity

eBay Billing Department to me 5:36 pm (3 hours ago)

Warning: This message may not be from whom it claims to be. Beware of following any links in it or of providing the sender with any personal information. Learn more

Dear valued eBay member

It has come to our attention that your eBay billing updates are out of order. If you could please take 5-10 minutes out of your online experience and update your billing records you will not run into any future problems with the online service.

Once you have updated your account records your eBay session will not be interrupted and will continue as normal. Failure to update will result in cancellation of your account, Terms of Service (TOS) violations or future billing

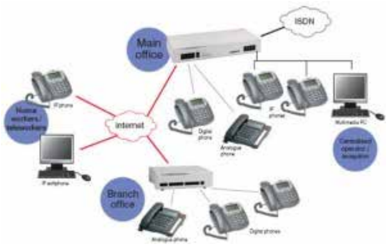
A massive phishing and fraud scheme that targeted Bank of America, Chase Bank and payroll processor ADP members defrauded them of $1.5 million. The phishing attacks directed users to spoofed or fake web pages designed to mimic legitimate sites. Once on the spoofed sites, users were conned into entering 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.***

Social Engineering – It Works!

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.

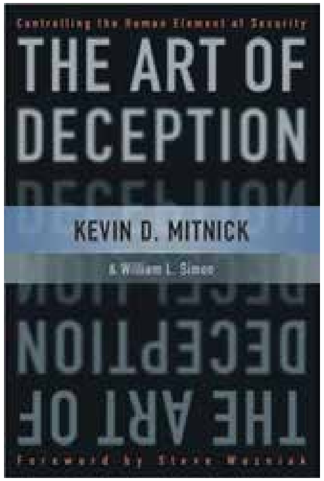
That job isn't fixing your computer. In fact, he's really just after your personal information. If you receive a call like this, hang up, call the company the bogus technician claimed to be from, and report the incident to a legitimate representative. If there really is a problem, they'll be able to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



Classic Examples of Social Engineering Attacks

Baiting - a bait disk or bait drive is left in the open for a target to find.
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.
Defense Against Phishing – Your password doesn’t get entered anywhere but your login page, and that page better have the right URL.


Controlling the Human Element of Security
THE ART OF DECEPTION
KEVIN D. MITNICK
& William L. Simon
Foreword by Steve Wozniak

Pretexting - The human equivalent of phishing, where someone impersonates an authority figure who is entitled to access your login information.
Defense Against Pretexting – ***Nobody needs your password, ever.***

Quid Pro Quo – A system that requests your password or personal information in exchange for some compensation.
Defense Against Quid Pro Quo – ***Nobody needs your password, ever.***

Classic Examples of Social Engineering Attacks

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.***

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.

Common Scams Used in Social Engineering

Auctions and Deals To 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.

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

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.

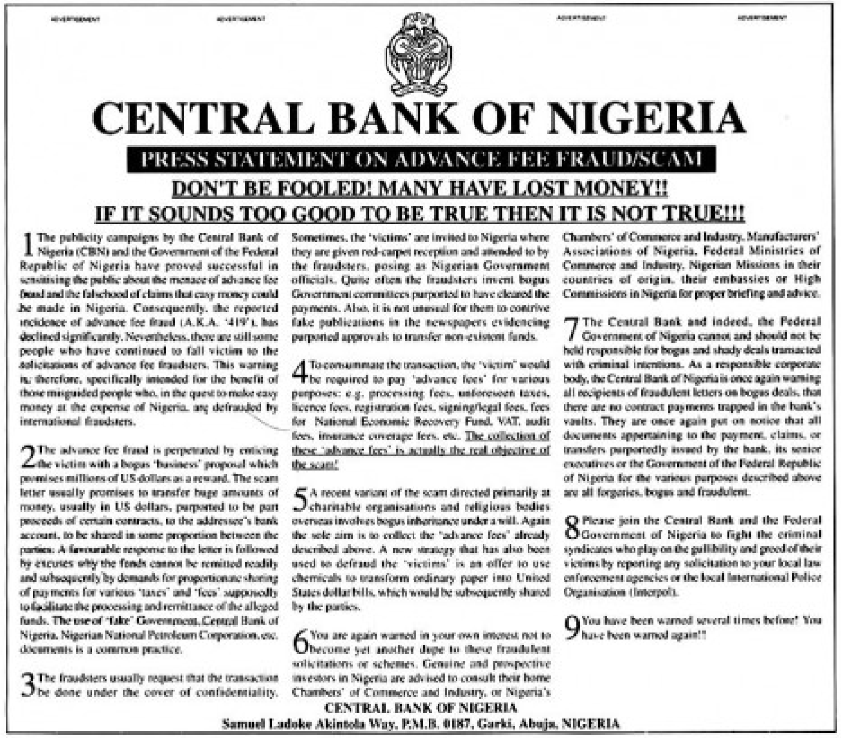
Vacation Homes (Not Really) For Rent – This up and coming scam is simple – a fraudster sets up a vacation rental site for a real home (complete with photos) and they rent it out for weekend and holiday getaways. The problem is that the scammer doesn't own the house, its not actually for rent, and when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

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.



ADVERTISEMENT ADVERTISEMENT ADVERTISEMENT ADVERTISEMENT

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 campaigns by the Central Bank of Nigeria (CBN) and the Government of the Federal Republic of Nigeria have proved successful in sensitising 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.K.A. '419'), 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. Sometimes, the 'victims' are invited to Nigeria where they are given red-carpet reception and attended to by the fraudsters, posing as Nigerian Government officials. Quite often the fraudsters invent bogus Government committees purported to have cleared the payments. Also, it is not unusual for them to contrive fake publications in the newspapers evidencing purported approvals to transfer non-existent funds.

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. <u>The collection of these 'advance fees' is actually the real objective of the scam!</u>

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 Chambers' of Commerce and Industry, Manufacturers' Associations of Nigeria, Federal Ministries of Commerce and Industry, Nigerian Missions in their countries of origin, their embassies or High Commissions in Nigeria for proper briefing and advice.

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 gullibility and greed of their victims by reporting any solicitation to your local law enforcement agencies or the local International Police Organisation (Interpol).

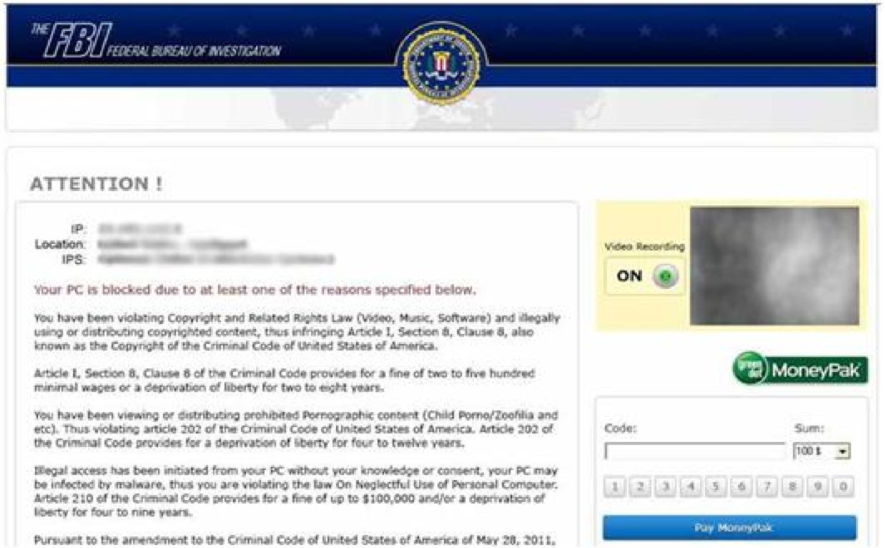
9 You have been warned several times before! You have been warned again!!

CENTRAL BANK OF NIGERIA
Samuel Ladoke Akintola Way, P.M.B. 0187, Garki, Abuja, NIGERIA

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.

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.



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,

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 on the compromised computer 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. Infected computers may not operate normally. You can file a complaint at **www.IC3.gov** . Seek out a local computer expert to assist with removing the malware.

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 – How Can You Lose Your Data?

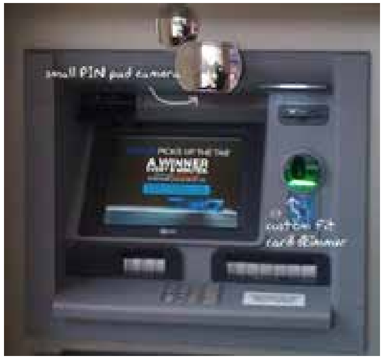
Credit/Debit Systems - Four Steps for Protecting Customer Data

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 – How Can You Lose Your Data?



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. He also 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.

Cybersecurity Risk – How Can You Lose Your Data?

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.

Cybersecurity Risk – How Can You Lose Your Data?

HEALTH INSURANCE PORTABILITY and ACCOUNTABILITY ACT

HIPAA

ADMINISTRATIVE SIMPLIFICATION: PRIVACY, SECURITY, TRANSACTIONS

How Much Protection Does Your Data Need?

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 are fully documented.

Annual Privacy Act Training
and
PPI / PII Training

User Name:
Password:
Domain: HQ

Data Protection Priorities –
ISO 27000 Compliant
Sarbanes Oxley Compliant –
HIPAA Compliant
Privacy Act Compliant

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.

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

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

- Do not respond to unsolicited (spam) e-mail.
- Do not click on links contained within an unsolicited e-mail.
- Don’t open e-mails that don’t have subjects.
- 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.
- Avoid filling out forms contained in e-mail messages that ask for personal information.
- 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.
- 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.

Tips From The Trenches

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

- Contact the actual business that supposedly sent the e-mail to verify if the e-mail is genuine.
- 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.
- Verify any requests for personal information from any business or financial institution by contacting them using the main contact information.
- Check your credit reports (and all of your families) at least once a year.
- Have someone continually checking the web for your SSN, credit card numbers, account numbers, etc. to show up.
- You should use a dedicated and locked down computer for all online financial transactions.
- Encryption of **ALL** data, regardless of where it is, remains the best prevention idea.
- 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

- **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.
- 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).
- Always have backups for any important data/applications.
- 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.
- Be cautious of E-mails Soliciting Donations FOR ANYTHING.
- 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.

What Can Technology Do? And How Effective is It?

Acquiring security wares gets more complicated every day – there are currently some 1000 vendors offering more than 150 categories of products. Is it reasonable to expect that even the most well-intentioned person to know everything about what vulnerabilities they "fix" and how to use them. Still, **it is your responsibility** to make smart decisions about what to acquire and how to use them.

Note that even if you hire a managed security services provider or get antivirus/antimalware apps you **can not** abdicate responsibility for what happens on your Network/on your Device. It has to be viewed as a partnership where **both work together** for optimum results.

Vendor (third party) data security polices and practices **must be** consistent with those of your company. Failure to make prompt disclosure of data breaches to affected individuals increases the risk of class action litigation.

Summary and Conclusions

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