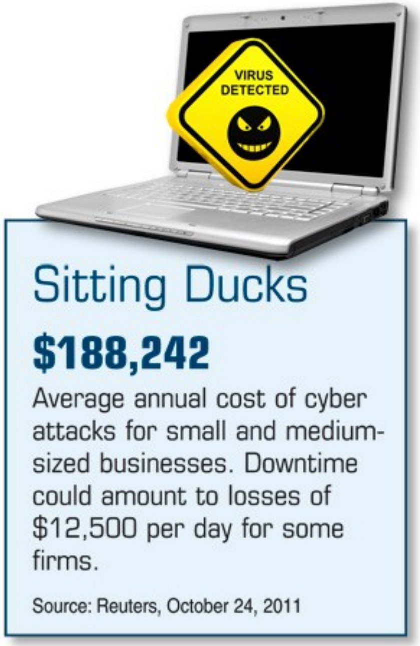


Sitting Ducks

$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 Concerns and Compliance for Small Business

Dave Hall
ESEP/CISSP
Hall Associates

Why Should I Care About Cybersecurity?

Because the Internet is not a very safe place and is getting worse.

June, 2012 2,405 millions 34.3 % of World Population is connected to the Internet

Being one of a numberless crowd is the prevailing idea. Being lost in the herd will keep me/my family/my business safe. Wrong idea!

Cybercriminals, Cybergangs, individual hackers, hacker groups, Governments all have *automated* scan, search and data mining capabilities.

The automated scans are looking for unprotected/unshielded computers.

Lists of such computers, lists of personal information, lists of business information are for sale.

Exploit kits, social engineering kits, automated scan software are for sale or rent on the internet.

What is Cybersecurity Risk?

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

Why? ***Because they 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 accessing (stealing) this type of information, these people (**no matter where they are in the world!!!**) can get and use YOUR ideas, your money and your identity, your business' ideas, money and identity 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 !!!

What is Cybersecurity Compliance 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.

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.***

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?

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.

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.

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.

It's hard to enforce social engineering policy and to limit what web sites are accessed on personal devices.

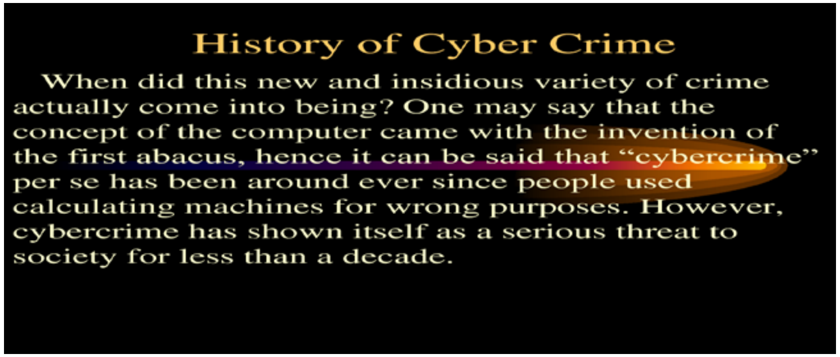
Cybersecurity Risk – Mobile Devices

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.**

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.

Just realize that there are bad things out there and do things to shield yourself.

.



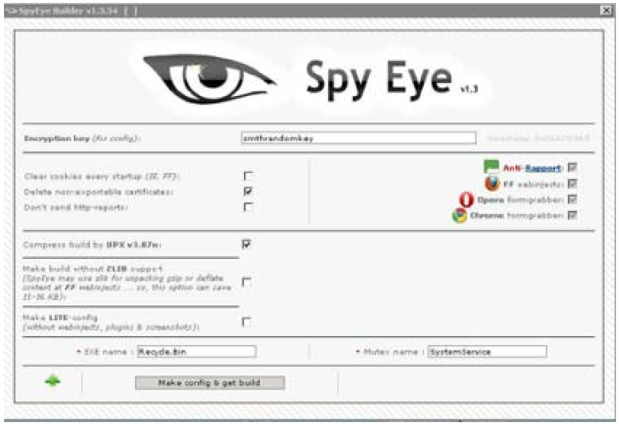
History of Cyber Crime

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 – 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.



SpyEye Builder v1.3.34 [ ]

Spy Eye v1.3

Encryption key (for config): smithrandomkey

Clear cookies every startup (IE, FF): □
Delete non-exportable certificates: ☑
Don't send http-reports: □

Anti-Rapport: ☑
FF webinjects: ☑
Opera formgrabber: ☑
Chrome formgrabber: ☑

Compress build by UPX v3.07w: ☑

Make build without ZLIB support (SpyEye may use zlib for unpacking gzip or deflate content at FF webinjects ... so, this option can save 11-16 KB): □

Make LITE-config (without webinjects, plugins & screenshots): □

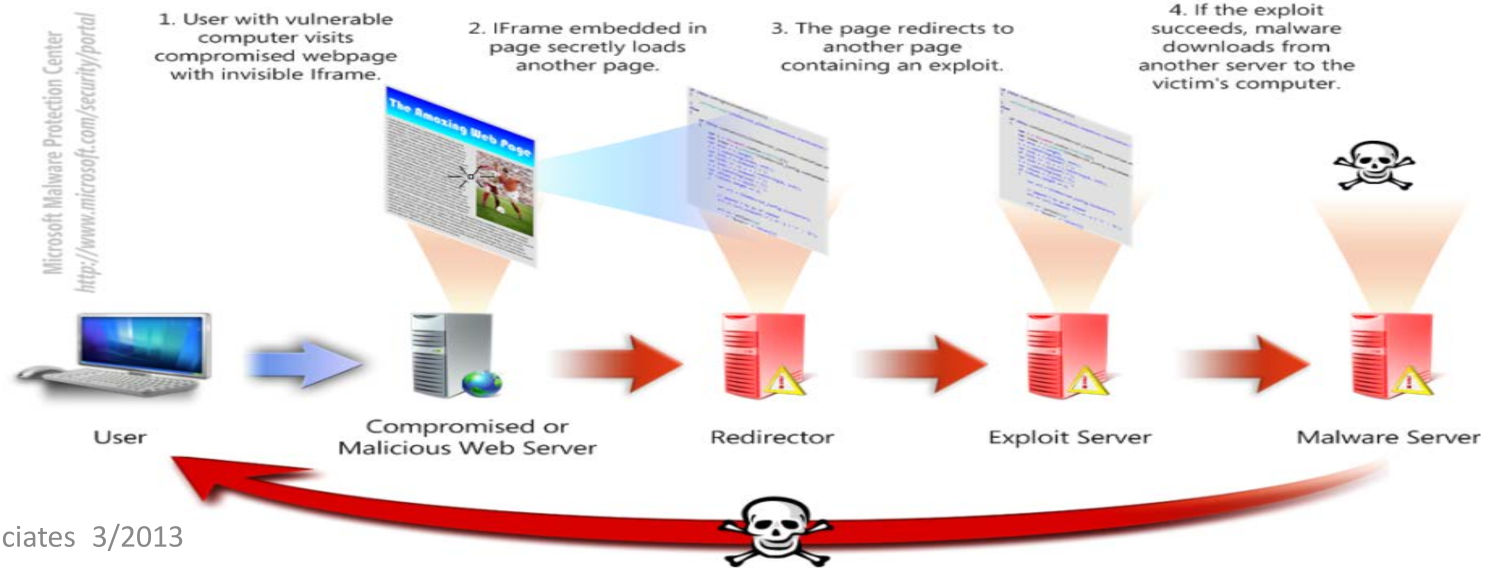
* EXE name : Recycle.bin
* Mutex name : SystemService

Cybersecurity Risk – Drive-By Malware Download

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

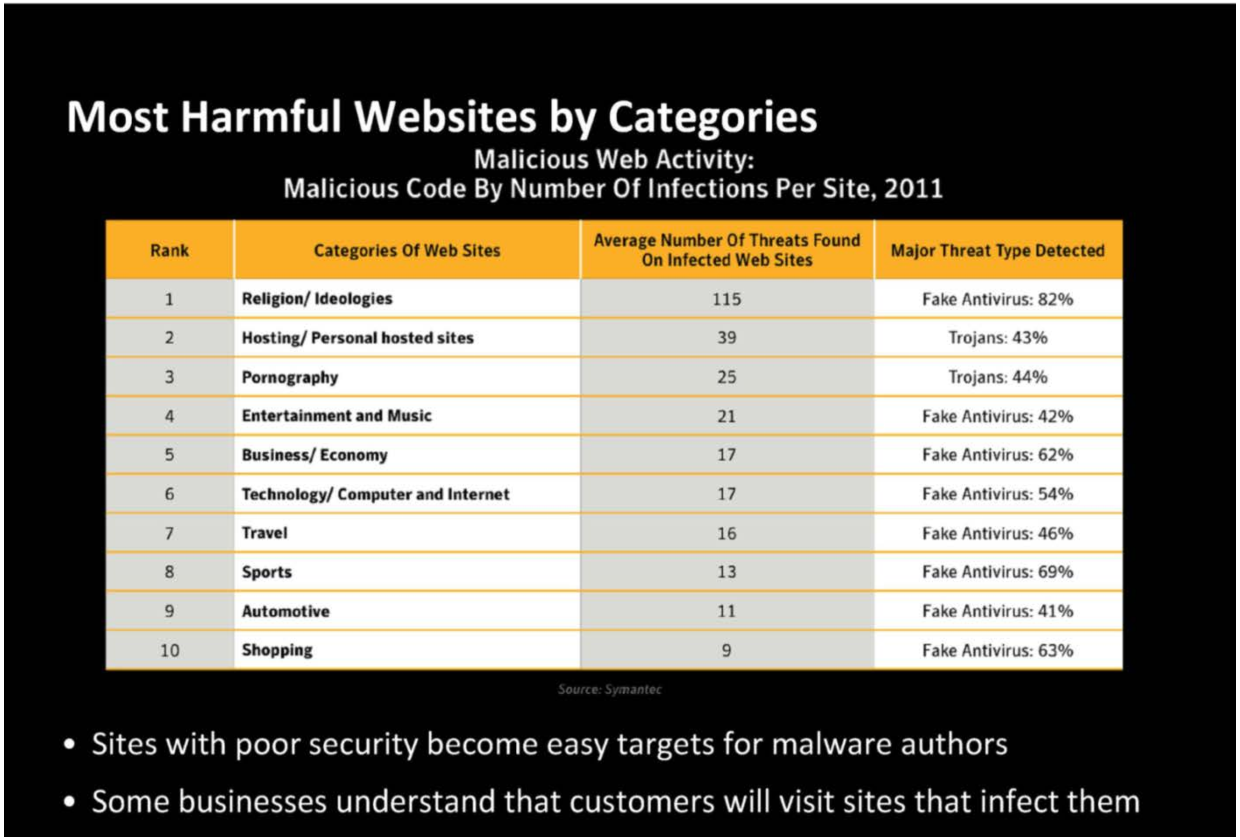
1. Downloads which a person authorized but without understanding the consequences (e.g. downloads which install an unknown or counterfeit executable program, ActiveX component, or Java applet).
2. Any download that happens without a person's knowledge, often a computer virus, spyware, malware, or crimeware.

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.


Microsoft Malware Protection Center
http://www.microsoft.com/security/portal
1. User with vulnerable computer visits compromised webpage with invisible Iframe.
2. IFrame embedded in page secretly loads another page.
3. The page redirects to another page containing an exploit.
4. If the exploit succeeds, malware downloads from another server to the victim's computer.
The Amazing Web Page
User
Compromised or Malicious Web Server
Redirector
Exploit Server
Malware Server

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

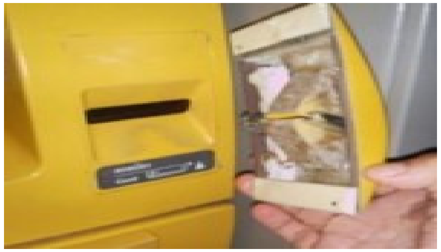
Identity thieves are targeting children – it's the crime of opportunity and is often committed by someone in the family. Children are targeted 35 times more than adults, with 15% under the age of 5. This crime tends to go undetected until victims turn 18 and try to get a student or car loan and discover 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.**

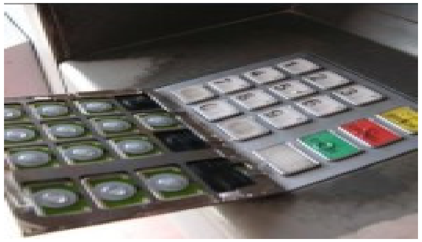
Approximately ***15 million United States residents*** have their identities used fraudulently each year with financial losses totaling upwards of $50 billion. On a case-by-case basis, that means approximately 7% of all adults have their identities misused with each instance resulting in approximately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

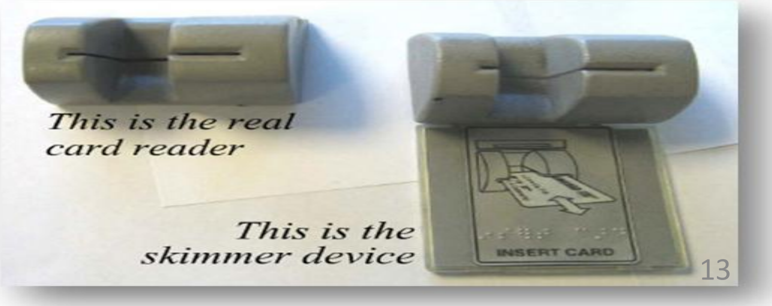
Cybersecurity Risk – Pin Skimming

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.







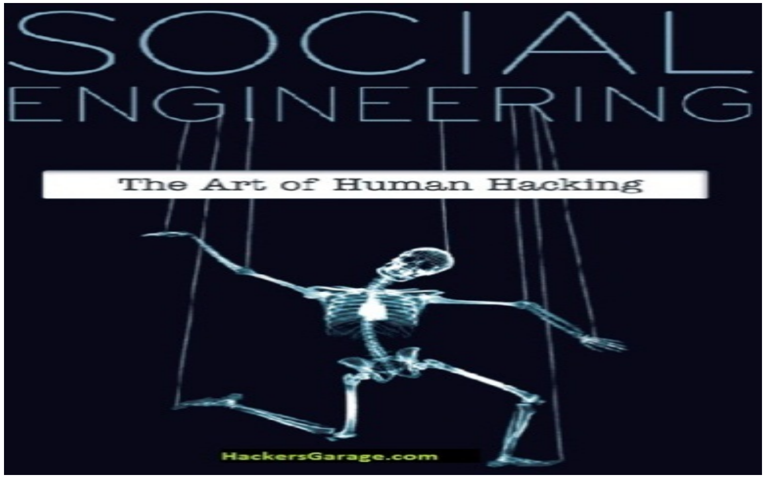
Cybersecurity Risk – Pin Skimming

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.

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.

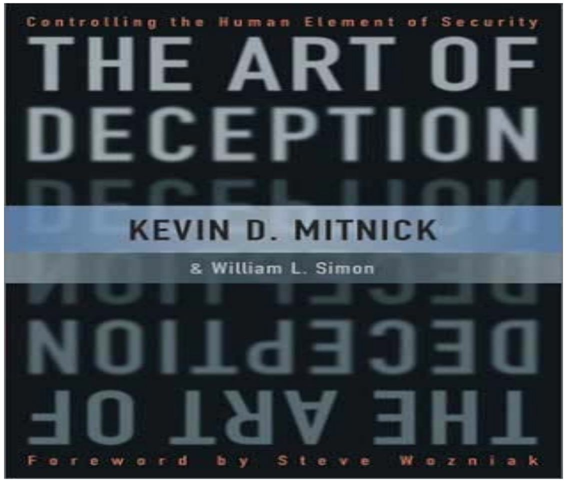
Fraudsters are perfecting their abilities to target and manipulate people. Well-crafted social engineering schemes take advantage of common user behavior. Don’t click on unknown links or provide personally identifiable information to someone you don’t positively know. A call from “the IT department”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



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.

Phishing/Smishing/Whaling – 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.

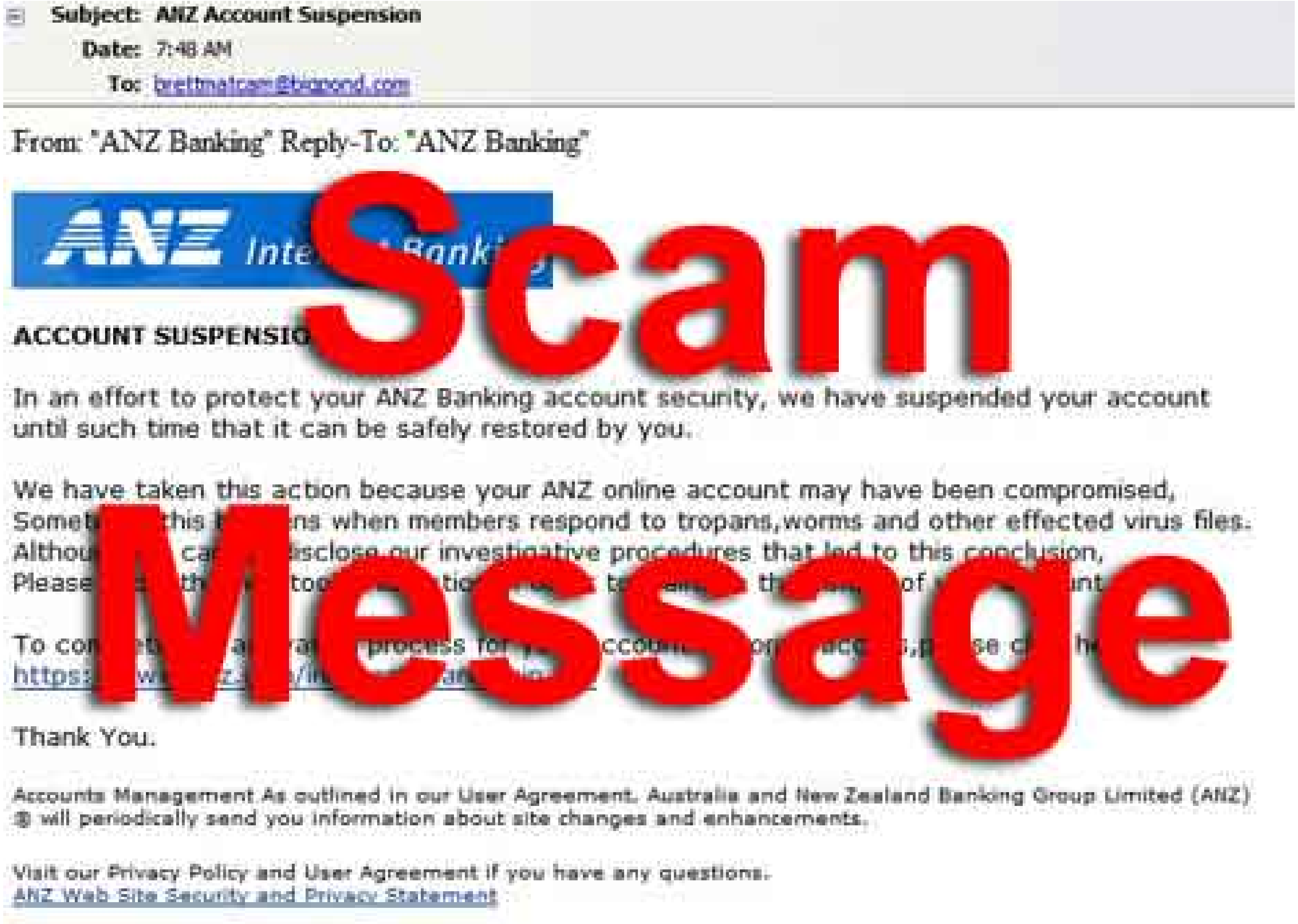

Controlling the Human Element of Security
THE ART OF DECEPTION
KEVIN D. MITNICK
& William L. Simon
Foreword by Steve Wozniak

Pretexting - The human equivalent of phishing, where someone impersonates an authority figure who is entitled to access your login information. 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.

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.

Cybersecurity Risk – Fraud/Phishing



Subject: ANZ Account Suspension
Date: 7:48 AM
To: brettmalcom@bigpond.com

From: "ANZ Banking" Reply-To: "ANZ Banking"

ACCOUNT SUSPENSIO

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,
Someti [illegible] this h [illegible] ns when members respond to tropans,worms and other effected virus files.
Althou [illegible] ca [illegible] isclose our investigative procedures that led to this conclusion,
Please [illegible] th [illegible] too [illegible] tio [illegible] t [illegible] th [illegible] of [illegible] nt

To co [illegible] a [illegible] process for [illegible] ccoun [illegible] ac [illegible] ,p [illegible] se c [illegible] h
https: [illegible] w [illegible] z [illegible] /i [illegible]

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.

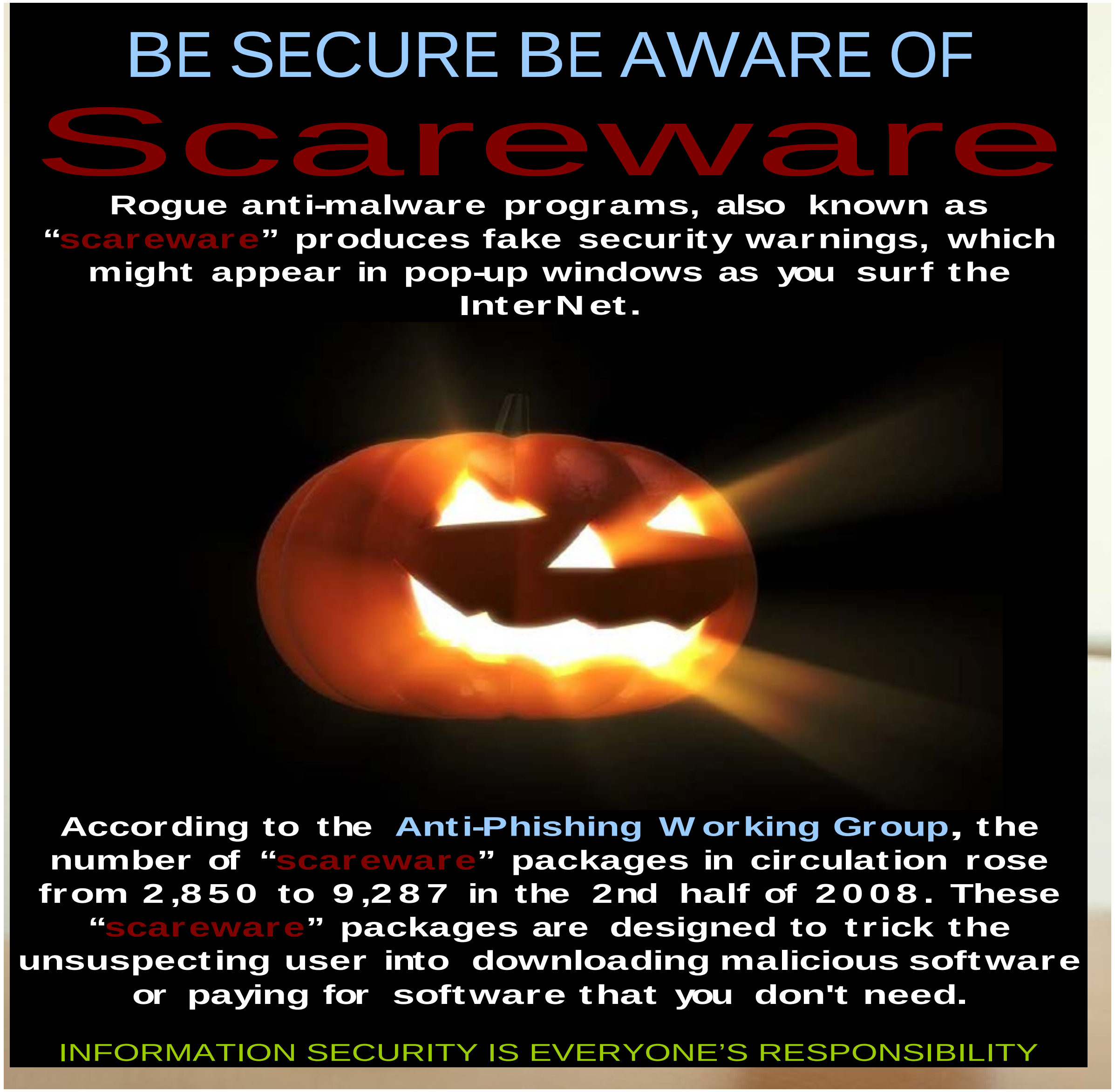
Visit our Privacy Policy and User Agreement if you have any questions.
ANZ Web Site Security and Privacy Statement

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 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.***

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.

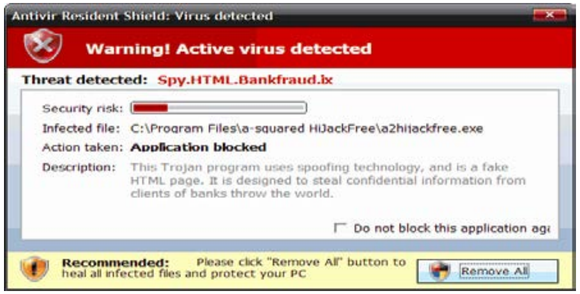
INFORMATION SECURITY IS EVERYONE'S RESPONSIBILITY

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.

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



Antivir Resident Shield: Virus detected

Warning! Active virus detected

Threat detected: Spy.HTML.Bankfraud.lx

Security risk:

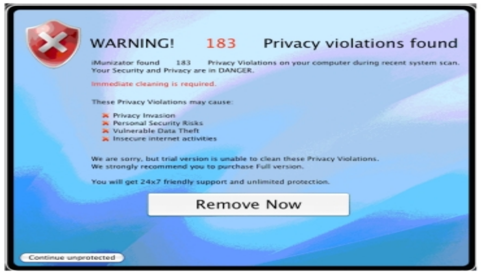
Infected file: C:\Program Files\a-squared HiJackFree\a2hijackfree.exe

Action taken: **Application blocked**

Description: This Trojan program uses spoofing technology, and is a fake HTML page. It is designed to steal confidential information from clients of banks throw the world.

□ Do not block this application ag

Recommended: Please click "Remove All" button to heal all infected files and protect your PC



WARNING! 183 Privacy violations found

iMunizator found 183 Privacy Violations on your computer during recent system scan. Your Security and Privacy are in DANGER.

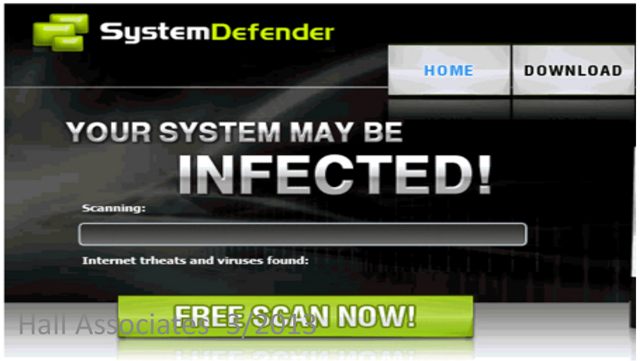
Immediate cleaning is required.

These Privacy Violations may cause:

- Privacy Invasion
- Personal Security Risks
- Vulnerable Data Theft
- Insecure internet activities

We are sorry, but trial version is unable to clean these Privacy Violations. We strongly recommend you to purchase Full version.

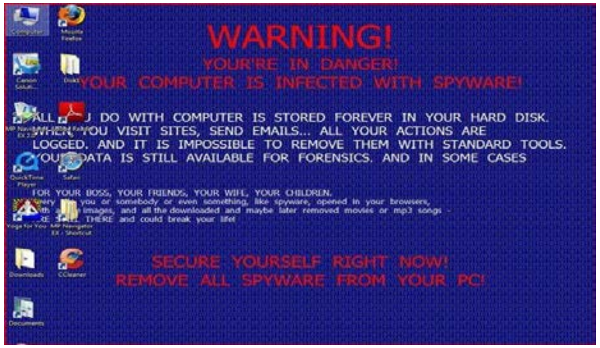
You will get 24x7 friendly support and unlimited protection.



YOUR SYSTEM MAY BE INFECTED!

Scanning:

Internet trheats and viruses found:



WARNING!

YOUR'RE IN DANGER!

YOUR COMPUTER IS INFECTED WITH SPYWARE!

ALL [illegible] U DO WITH COMPUTER IS STORED FOREVER IN YOUR HARD DISK. WHEN YOU VISIT SITES, SEND EMAILS... ALL YOUR ACTIONS ARE LOGGED. AND IT IS IMPOSSIBLE TO REMOVE THEM WITH STANDARD TOOLS. YOU[illegible] DATA IS STILL AVAILABLE FOR FORENSICS. AND IN SOME CASES FOR YOUR BOSS, YOUR FRIENDS, YOUR WIFE, YOUR CHILDREN.

[illegible]ery [illegible] you or somebody or even something, like spyware, opened in your browsers, [illegible]th [illegible] images, and all the downloaded and maybe later removed movies or mp3 songs - [illegible]E [illegible] THERE and could break your life!

SECURE YOURSELF RIGHT NOW!

REMOVE ALL SPYWARE FROM YOUR PC!

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…

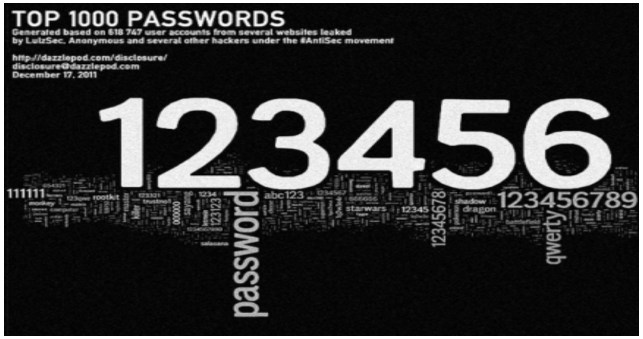
Cybersecurity Risk – Data Breach

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. ***babygir***l 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.***

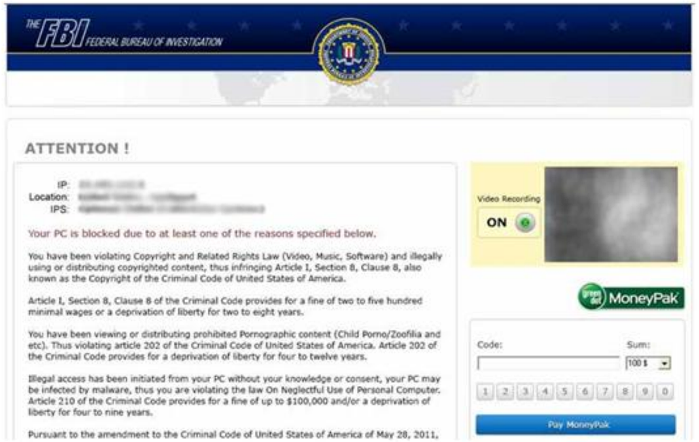
Get in control of your online privacy.


TOP 1000 PASSWORDS
Generated based on 618 747 user accounts from several websites leaked
by LulzSec, Anonymous and several other hackers under the #AntiSec movement
http://dazzlepod.com/disclosure/
disclosure@dazzlepod.com
December 17, 2011
123456
111111
abc123
password
starwars
12345
12345678
shadow
dragon
123456789
qwerty

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 tho your screen does not show it and can be used to commit online banking and credit card fraud.



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

Code:
Sum: 100 $

Latest Incidents

Thrift Savings Plan

Federal employees can manage their accounts on the Thrift Savings Plan website.

The Federal Government's Thrift Savings Plan (TSP) warns participants against free iPhone app from Apple store

The Thrift Savings Plan has warned its participants against using a free iPhone app being offered through the Apple store, saying it is not an official offering of the 401(k)-style program for federal employees.

The app, called TSP Funds, asks account holders for their account login information, but providing that information "could result in a security risk to your account," the TSP said.

The TSP last year disclosed that a 2011 hacking incident had been discovered in which Social Security numbers and other personal information on more than 120,000 account holders were compromised.

View the TSP warning at:
https://www.tsp.gov/whatsnew/plan/planNews.shtml#iPhoneApp

Latest Incidents

U.S. Army
Criminal Investigation
Command (CID)

CID Warns of Email Scam, Criminals Posing as Police

Cyber-criminals are attempting to impersonate members of the U.S. Army Criminal Investigation Command via email, stating that they are from the "Office of the Division of Criminal Investigation (DCI)," when no such organization exists within Army CID.

In the email, the perpetrators state that they have discovered fraudulent activities with a company that the targeted victim had contact with. The cyber-criminals then ask the potential victim to acknowledge the email and provide financial and personal information.
The ability of law enforcement to identify these perpetrators is very limited, so individuals must stay on the alert and be personally responsible to protect both themselves and their loved ones.
CID strongly recommends that Soldiers, civilians and family members who receive any suspicious and/or unsolicited emails should delete them immediately without response. However, if you receive an email claiming to be from "Office of the Division of Criminal Investigation (DCI)", to take the following steps:

- DO NOT RESPOND TO THE EMAIL - STOP all contact if you have responded to the email and report it to CID.

Latest Incidents

Facebook users unwittingly revealing intimate secrets, study finds

Researchers were able to accurately infer a Facebook user's race, IQ, sexuality, substance use, personality or political views using only a record of the subjects and items they had "liked" on Facebook – even if users had chosen not to reveal that information. The researchers used computer software to predict personality traits, but said the same information could be collected by anyone with training in data analysis. They were able to draw "surprisingly accurate" findings about people by aggregating swaths of seemingly innocuous "likes", such as TV shows and movies.

http://www.guardian.co.uk/technology/2013/mar/11/facebook-users-reveal-intimate-secrets

Social Media Landscape
Social Media
Publish
Share
Discuss
Social Networks
Microblog
Lifestream
Livecast
Virtual Worlds
Social Games
MMO
wikia
digg
YouTube
slideshare
flickr
last.fm
Crowdstorm
phpbb
PHORUM
meebo
skype
talk
myspace.com
facebook
Bebo
orkut
hi5
LinkedIn
Ning
twitter
Pownce
PLURK
twitxr
tweetpeek
socializr
FriendFeed
socialthing!
ustream
livecastr
justin.tv
Qik
Second Life
HABBO
CLUB PENGUIN
doof
POGO
KONGREGATE
KARTRIDER
FredCavazza.net

Latest Incidents

Protect Yourself from Email Tax Scams

It’s tax season and criminals are seizing the opportunity for scams. Don’t become the next victim.

They may offer seemingly legitimate “tax services” designed to steal your identity and your tax refund, sometimes with the lure of bigger write-offs or refunds. Scams may include mocked up websites and tax forms that look like they belong to the IRS to trick you into providing your personal information.

Scam artists can prey on users by promising refunds that are fraudulent, a scam the IRS says has been rampant in previous years. In these scams, notices are posted on bulletin boards, in libraries, and at other community sites where people visit either in person or online.

For More Information: For additional information about tax related scams and identity theft, please visit:

- Taxpayer Guide to Identity Theft: www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft
- Tax Scams/Consumer Alerts: www.irs.gov/uac/Tax-Scams-Consumer-Alerts
- IRS Releases the Dirty Dozen Tax Scams for 2012: www.irs.gov/uac/IRS-Releases-the-Dirty-Dozen-Tax-Scams-for-2012
- What’s Hot – IRS: www.irs.gov/uac/What's-Hot
- Report Phishing: www.irs.gov/uac/Report-Phishing

Latest Incidents

Internet Perverts Called 'RATters' Are Hacking Into Women's Webcams

A RAT is a Remote Administration Tool that was developed to allow IT to look inside computers as a diagnostic tool. It's software that tech sections in corporations sometimes use to get remote control of a desktop for troubleshooting purposes. RATers have co-opted this software to hijack women's systems without their knowledge. And it is being used to spy on many others – like Syrian rebels.

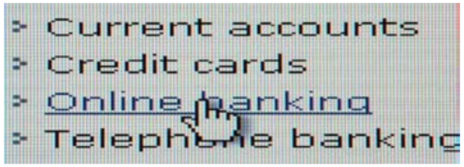
Things that popular RAT Tool DarkComet software can do.

- Find out all system information, including hardware being used and the exact version of your operating system, including security patches
- Control all the processes currently running on your system
- View and modify your registry
- Modify your Hosts file
- Control your computer from a remote shell
- Modify your startup processes and services, including adding a few of its own
- Execute various types of scripts on your system
- Modify/View/Steal your files
- Put files of its own on your system
- Steal your stored password
- Listen to your microphone
- Log your keystrokes
- Scan your network
- View your network shares
- Mess with your MSN Messenger / Steal your contacts / Add new contacts
- Steal from your clipboard (things you've copied)
- Control your printer
- Lock/Restart/Shutdown your computer
- Update the implant with a new address to beacon to or new functionality
- Watch your webcam
- Use your computer in a denial of service (DOS) attack

Ever faced a situation where you have a FUD server, but cannot get victims? Or maybe you're getting a lot less installs compared to the amount of work you are putting in?

This guide is specifically for you. The eBook includes 3 original methods you can use. The eBook comes with the tools and resource files you'll need to implement it. This completely private method is written by me after 2 years worth of research and spreading and after the release of v6 of my eBook which was the most sold eBook to ever hit the Hackforums eBook Bazaar. Using this method can easily get you around 500-3k installs a day and the methods are very easy to implement. The eBook includes many screenshots which makes it newbie friendly.

Summary and Conclusions


- Current accounts
- Credit cards
- Online banking
- Telephone banking

Cyber fraud is one of the greatest risks facing the nation's (and your) 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.**

Connections abound and are increasing – and each presents additional vulnerabilities and threats.

Everyone needs an understanding of how best to 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 help protect you and your business/family.