

Social Engineering & Insider Threat

12th Vancouver International Security Conference

December 1st 2009

Peter Broznitsky



Agenda

- What is SE ?
- Risks, Methods, Mitigation
- What is InT ?
- Risks, Methods, Mitigation



The Usual Disclaimer

- The views and opinions expressed in this presentation are those of the author who is solely responsible for the content. The views expressed may not necessarily reflect the views of the R.C.M.P. or Reboot, which has not reviewed, authorized, or approved the contents either explicitly or impliedly.
- All data and information provided in this presentation is for informational purposes only. The author makes no representations as to accuracy, completeness, currentness, suitability, or validity of any information in this presentation and will not be liable for any errors, omissions, or delays in this information or any losses, injuries, or damages arising from its display or use. All information is provided on an as-is basis.
- In no event shall the R.C.M.P. or Reboot be liable for any damages whatsoever resulting from any action arising in connection with the use of this information or its publication, including any action for infringement of copyright or defamation.



Security & People

- Thinking about security is good for your business
- People are, and always have been, the most vulnerable aspect of any organization's security infrastructure



Security & People

- It is easy to take advantage of human goodwill. People want to trust those who appear courteous, helpful, or honest. People also want to help those in need.
- Unfortunately, **con artists** exploit these good qualities in people.



What is Social Engineering?

- The clever manipulation of the natural human tendency to trust
- The gathering of confidential information from unsuspecting citizens or your employees through lies, misrepresentation, pretext, or guise

What is SE ?

- A category of security attacks in which someone manipulates others into revealing information that can be used to steal data, give access to systems, access to cellular phones, money, or even a complete identity



What is SE ?

- "Many of the most damaging security penetrations are, and will continue to be, due to Social Engineering, not electronic hacking or cracking. . . Social Engineering is the single greatest security risk in the decade ahead." **The Gartner Group October 2004**



Three Types of SE

- Computer-based
- Human-based
 - Phone
 - In person

Computer-based SE

- Using computer software to attempt to retrieve the desired information



Today's News

- Spam
- 419
- Phishing / Spear Phishing
- Event Phishing
- SEO Poisoning
- Web 2.0

Spam

- Sophos 2009's Security Threat Report stated an incredible **97%** of business email is SPAM!!
- Affecting blogs and social networks
- What's your spam filter like?



FEDERAL MINISTRY OF JUSTICE

Authority to Pay Certificate



RC NO: 0387

Between **UNION BANK NIGERIA PLC**

And

GAYDAMASCHUK YURIY

This is to Certify on this day **28TH NOVEMBER** 20**03** that Union Bank (Nigeria) Plc, agrees to pay **GAYDAMASCHUK YURIY** and the nature of the payment of **NEXT OF KIN/BUSINESS PARTNER** to the **LATE ENGR. MARK ELHOURIY** for the value of **US\$6.000,00,00 MILLION DOLLARS**

DEEDS:

1. The Union Bank Nigeria Plc, through the Federal Ministry of Justice reserve the right to revoke this payment if the beneficiary fails to deliver the relevant documents when needed.
2. Every tax or taxes to any ministry of corporation here in Nigeria, e.g. Central Bank, Ministry of Justice, e.t.c must be paid upfront before funds will be transferred or deposited into the beneficiary's designated foreign account.
3. No matter the fluctuation in currency, the payment value cannot be amended or changed.

Having been cautioned in English Languages as the beneficiary has agreed and been abided by the above mentioned payment deeds.

Union Bank Nigeria Plc

Federal Ministry of Justice

Beneficiary



In This Issue

- . Keep Your Money Safe
- . Add Your Bank Account
- . How to Transfer Money
- . Online Buying Tip
- . Money Market Fund
- . Share Your Story
- . Special Offers

TIP**Know Who You're Buying From**

Before you buy, click the link under the seller's email address on the **Payment Details** page to see their account type and status, and length of time as a PayPal member.

For more online safety tips, [visit our Security Center](#).

Money Market Fund

Earn a competitive rate on your PayPal balance . enroll in the PayPal Money Market Fund. It's easy . [sign up now](#)

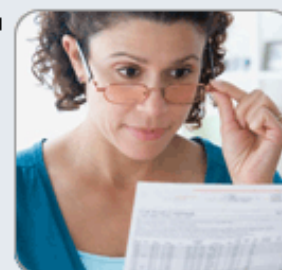
Share Your Story

Do you have an extraordinary PayPal story? Send an email to [paypal@paypal.com](#) and tell us all

Keep Your Money Safe

Dear Cusotmer,

As part of our security measures, we regularly screen activity in the PayPal system. We contacted you after noticing an issue on your account. We request information from you for the following reason:



A recent review of your account determined that we require some additional information from you in order to provide you with secure service.

Case ID Number: PP-178-257-467

This is a reminder to log in to PayPal as soon as possible. Once you log in, you will be provided with steps to restore your account access. We appreciate your understanding as we work to ensure account safety.

In accordance with PayPal's User Agreement, your account access will remain limited until the issue has been resolved. Unfortunately, if access to your account remains limited for an extended period of time, it may result in further limitations or eventual account closure. We encourage you to log in to your PayPal account as soon as possible to help avoid this.

To review your account and some or all of the information that PayPal used to make its decision to limit your account access, please visit the Resolution Center. If, after reviewing your account information, you seek further clarification regarding your account access, please contact PayPal by visiting the Help Center and clicking "Contact Us".

We thank you for your prompt attention to this matter. Please understand that this is a security measure intended to help protect you and your account. We apologize for any inconvenience.

Please follow the link below and renew your account information.
<https://www.paypal.ca/cgi-bin/webscr?cmd=login-run>

Spear Phishing

- Targeted
- Individually addressed to executives or other employees
- Embedded .PDF or .PPT or .XLS containing a Trojan or Keylogger

Event Phishing

- Elections, sporting events, natural disasters, war, economic recession, CRA, Tiger Woods' driving
- Embedded .url, document, or a video asking for a codec install
- CNN, MSNBC, Monster



SEO

■ Search Engine Optimization Poisoning

[Security Software - Free Software Downloads and Software Reviews ...](#) ✓

download security center. Your source for antispymware and **security** downloads ... Software maker will release its Microsoft **Security Essentials** "in the coming ... Vista and **Windows** Server 2008, but not the final version of **Windows 7**. ...

[download.cnet.com/windows/security-software/](#) - [Similar](#)

[Linda Chong's Blog : Download a free copy of Windows Security ...](#) ✓

30 Sep 2009 ... Microsoft **Security Essentials** is officially released in 8 languages and 19 countries around the world. You can **download** Microsoft **Security** ...

[blogs.msdn.com/.../download-a-free-copy-of-windows-security-essentials-to-protect-your-home-pc-and-laptop-today.aspx](#) - 9 hours ago - [Similar](#)

[Microsoft Security Essentials Download](#) ✓

29 Sep 2009 ... Free Microsoft **Security Essentials** available for **download** Microsoft has good reason to ensure **Windows** PCs are secure and malware-free. ...

[www. \[redacted\] security-essentials-download](#) - 16 hours ago - [Similar](#)

Web 2.0

follow us on twitter

Join our facebook Page

Read our blog

view our Video Channel

skobsie shadows grovee: You Blogniscient Tin FINGER shuttelli ZAZZLE Tailrank TagWorld INods Lulu R blish theadcloud rblog.com catépre garber Pexa browser oyogi WOLOOEC Frapp-L jakeey dabble tech memorandum Calendaris Suprgla pondo zigtag AllPrest arfb Zozolo niya Wordcast Opinky STREAMLOAD nativetext CONGOO PODZINGER flickr Ning Cokles Bloop FeedBurner gobbeom Gcast ritty chatsum PANDORA looklater WebFly PLAYS Noodly vizi digg TRUVEO eggSurf newsvine Clipfire Lexxealpha yelp! MusicSearch Meet With Approval HomePortals Spin messenger Megite Coca-Cola

Facebook, Twitter users beware: Crooks are a mouse click away

updated 4 hours, 59 minutes ago

- STORY HIGHLIGHTS**
- The FBI reports nearly
 - Online scam losses an
 - Facebook has automa
 - MySpace.com creates

[Next Article in Crime »](#)

By Stephanie Chen
CNN

TEXT SIZE  

(CNN) -- If you're on Facebook, Twitter or any other social networking site, you could be the next victim.



That's because more cyberthieves are targeting increasingly popular social networking sites that provide a gold mine of personal information, according to the FBI. Since 2006, nearly 3,200 account hijacking cases have been reported to the Internet Crime Complaint Center, a partnership between the FBI, the National White Collar Crime Center and the Bureau of Justice Assistance.

It starts with a friend updating his or her status or sending you a message with an innocent link or video. Maybe your friend is in distress abroad and needs some help.

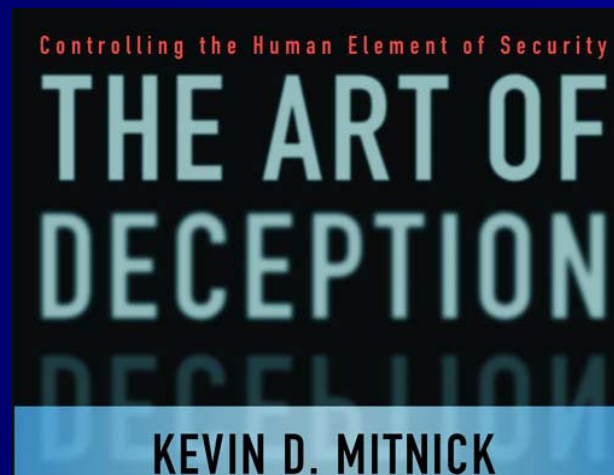
All you have to do is click.

When the message or link is opened, social network users are lured to fake Web sites that trick them into divulging personal details and

passwords. The process, known as a phishing attack or malware, can infiltrate users' accounts without their

Human-based SE

- Person-to-person interactions to retrieve the desired information



Human-based SE

- Usually conducted via the telephone
- Network reconnaissance



Methods: SE

- "Hi, this is the helpdesk, I need to fix your computer, what's your password?"
- "Hi, this is cyber security, there's a problem with your system, what's your password?"
- "Hi, this is travel, could you please read me your credit card number?"

Methods: SE

- "Hi, this is Bill in accounting, I'm looking for ..."
- "Hi, this is Mary in billing, can you help me ..."
- "Hi, this is Don in legal, I have a problem ..."

Methods: SE

- Was the caller really who you thought it was?
- Seemingly insignificant information can complete a Social Engineer's puzzle
- Data mining

What's your response?

- "Hello, can I speak with Tom Smith from R&D please?"
- "I'm sorry, he'll be on vacation until next Monday"
- "OK, who's in charge until he gets back?"
- "Robert Jones"

What's your response?

- Let's call another employee, Mike
- "Mike, just before Tom Smith went on vacation, he asked me to review the new design. I talked with Robert Jones and he said you should just fax it to me. My number is 555-1212. Could you do it as soon as possible? Thanks."



In Person SE

- The social engineer may enter the building and pretend to be an employee, guest, courier, or service personnel
- May be dressed in a uniform
- Becomes part of the cleaning crew
- Is she allowed to roam ?

War Stories



Methods: SE



- Morning giveaway in London's financial district
- Free vacation somewhere tropical
- Load a CD in your computer and access a website
- 75 of 100 were loaded into business computers that day; CD contained malware

Methods: SE

- 20 USB drives were left near the target building in the parking lot and smoking areas
- Employees picked up 15 of the 20 drives and installed them on their computers to see what they held
- A Trojan horse program gathered passwords, logins, and other data and emailed them back to the attacker



Methods: SE

- Conference attendees who are given USB thumb drives and CDs that supposedly contain just the conference papers, but increasingly also contain malicious software



 E-mail this to a friend

 Printable version

Parking ticket leads to a virus

Hackers have discovered a new way of duping users onto fraudulent websites: fake parking tickets.

Cars in the US had traffic violation tickets placed on the windscreen, which then directed users to a website.

The website claimed to have photos of the alleged parking violation, but then tricks users into downloading a virus.

Anti-virus firm McAfee says the Vundo Trojan then gets users to install a fake anti-virus scanner.

Vehicles in Grand Forks, North Dakota, were the targets for this new type of fraud.

Drivers found the following message on the yellow ticket on their windscreen: "PARKING VIOLATION This vehicle is in violation of standard parking regulations".

The ticket then instructed drivers to visit a website, where drivers could "view pictures with information about your parking preferences".

According to internet security watchdog The SANS Institute, the website then had photos of cars in various car parks around Grand Forks and instructed users to download a tool bar to find photos of their own vehicle.

But the tool bar was actually an executable file which installed a

[To view pictures of your or someone else's horrible parking or to upload pictures: CLICK ME FOR THE PICTURE SEARCH TOOLBAR](#)

[Install the toolbar to input details of your location and more to find your vehicle's pictures!](#)



Hackers are finding new ways of tricking potential victims

[To view pictures of your vehicle from Grand Forks, North Dakota download here: SEARCH TOOLBAR](#)



War Stories

- Spear phishing
- “IT Services Survey”
- Installing a sniffer or keylogger

Mitigating SE



- Become familiar with the techniques used
- Trust your instincts
- Provide notification to targeted groups during attempts
- Provide a coordinated response when scams are identified

Mitigating SE



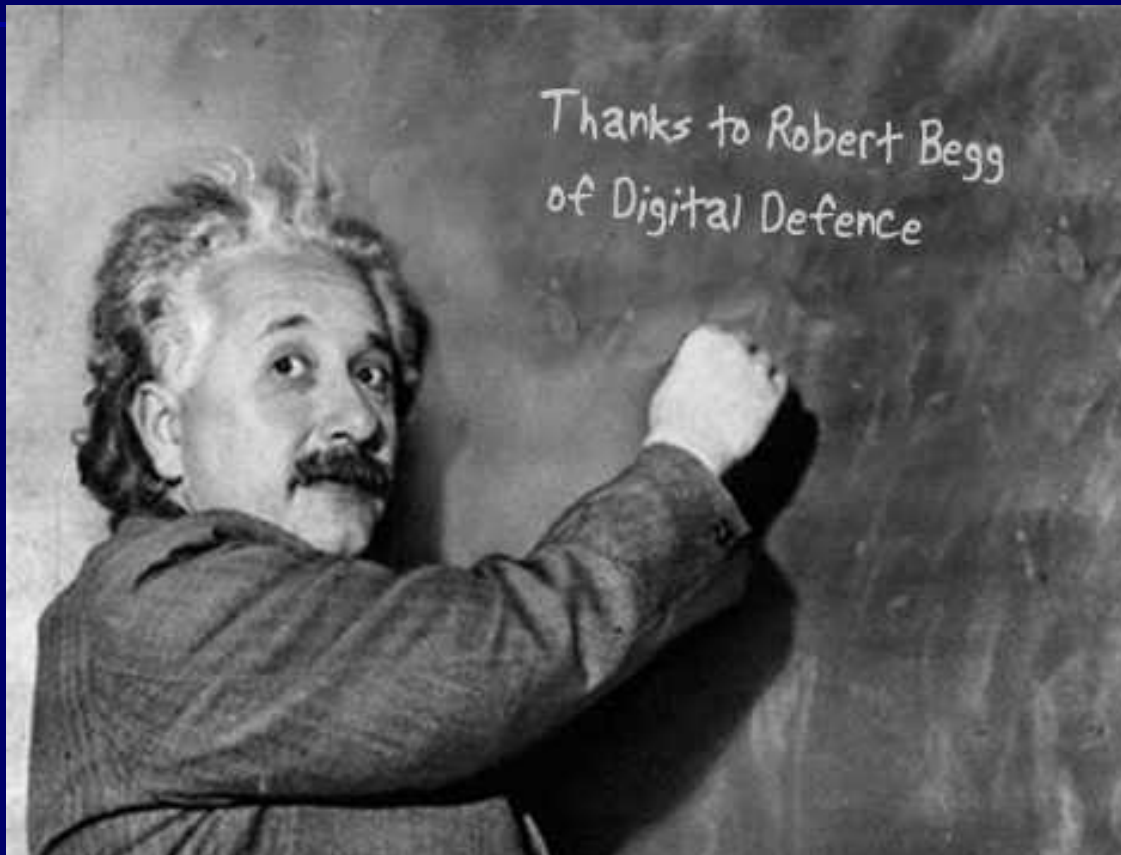
- Test your readiness
- Educate all employees - everyone has a role in protecting the organisation and thereby their own jobs
- If someone tries to threaten them or confuse them, it should raise a red flag

Mitigating SE



- Train new employees as they start
- Give extra security training to security guards, help desk staff, receptionists, telephone operators
- Keep the training up to date and relevant

Insider Threat (InT)



What is Insider Threat ?

- Using legitimate authority for illegitimate purposes
- Initiated by full or part-time employees, consultants, contractors, co-op students, partners, clients, hardware/software vendors, or even automated processes of an organization – **gone rogue**



What is InT ?

- Insider threat can also, unfortunately, be due to human error or from lack of due diligence
- Not malicious
- But very damaging, at all levels

Insider risk problem revealed

August 25th 2009

By Maggie Shiels
Technology reporter, BBC News, Silicon Valley

Security experts have turned the notion that so called "malicious insiders" are the biggest cyber security threat for companies on its head.

The security vendor RSA revealed that the majority of breaches are actually caused unintentionally by employees.

Its survey showed that firms believed 52% of incidents were accidental and 19% were deliberate.

"Unintentional risk gets overlooked, yet it's the most serious threat to business," said the RSA's Chris Young.

"The sexy incident where someone gets arrested for stealing records and selling them to a third party for a lot of money is the stuff that catches the attention of the media, the regulators, executives and Congress people.

"But this is not necessarily where organisations have 100% of the risk," said Mr Young, the RSA's senior vice president of products.

The study conducted by the RSA and IT analysts IDC looked at 11 different categories of risk ranging from malware and spyware to employees having excessive access to systems and from unintentional data loss to malicious acts for personal gain.

Accidental

- Incompetence is a bigger IT security threat than maligning insiders
- You'd do better to worry about Mr. Bean in Accounting

InT Tactics

- The recent economic downturn
- Inappropriately accessing internal information (e.g. celebrity medical records)
- Sabotaging data or network devices, denying businesses access to their data, including “logic bombs”

InT Tactics

- Stealing personal information for resale to identity thieves
- Stealing intellectual property or customer information for re-use, frequently when the employee leaves and goes to a competitor or starts his own business

Data Breaches

- Verizon's 2009 Data Breach Investigation Report
- 74% of breaches resulted from external sources, 32% were linked to business partners, and 20% were caused by insiders

InT Profile

- A profile of the malicious insider includes individuals with a strong sense of **entitlement** (usually based on their perceived value to the company, and how they are not fairly compensated in tough economic times), a sense of **frustration**, and a **lack** of corporate **loyalty**



InT Profile

- They are not necessarily skilled in the use of computers, but they compensate for this with extensive planning



InT Warning Signs



- Acting “above” the rules or outside information security policy
- Increased number of access violations (attempting to perform actions reserved for privileged users, such as installing software)

InT Warning Signs



- Reduction in the number and complexity of logical controls (passwords, network shares)
- Non-business applications installed on corporate resources, especially those used for unmonitored communication and remote access

InT Warning Signs



- Instant messaging, web conferencing, web mail, P2P file sharing, adware, spyware, anonymizers, RSS, and Skype™ and other VoIP services
- Access to, and storage of, non-business content (adult content, copyrighted software)

InT Warning Signs



- One negative incident can begin the spiral
- Changes in behaviour and inter-personal reactions
- Appears disgruntled or, paradoxically, overly enthusiastic

InT Warning Signs



- Hints of domestic turmoil or dependencies
- Hints of a change in spending patterns
- A project that fails
- Changes in associates, either internal or external

Mitigation - HR



- Malicious activities are largely a result of employees who are “disgruntled” - this speaks to the strong role that must be played by managers and HR in controlling this threat. Typical administrative controls include:

Mitigation - HR



- Recent and relevant background checks on insiders, especially those with privileged levels of access
- Enforce separation of duties and **least** privilege

Mitigation - HR



- Monitor, and respond to, suspicious or disruptive employee behavior; don't ignore the possible precursors to malicious activity

Mitigation - HR



- If employees must be terminated, ensure that it is fair, follows consistent practices, and that it minimizes the opportunity for privileged employees to access the network

Mitigation - HR



- Manage negative workplace events; ensure a consistent and fair approach in dealing with all employees
- Implement informal and formal grievance procedures, or other means for employees to voice their concerns

Mitigation - HR



- Ensure that there is a way for co-workers to report suspicious behavior to management; adopt a “whistle blower” policy
- Include insider threat as an element of regular security awareness training delivered to all employees

Mitigation - IT



- Ensure physical controls are in place and verified
- Implement rigid access control (local and remote access). Ensure access to the network is disabled following termination; monitor for access attempts

Mitigation - IT



- If privileged employees are terminated, passwords must be changed, and it is recommended that a penetration test be completed to look for remote access tools, malicious software, etc

Mitigation - IT



- Log and monitor employee activities ; consider the use of honeypots and honeytokens to identify inappropriate internal access attempts
- Consider encryption for critical data

Mitigation - IT



- Implement a program of “pro-active data forensics (design, construct, and configure data systems to support forensic investigations)”

Mitigation - IT



- Implement a documented change control process
- Implement and validate backup and recovery processes; ensure historical records are secure

Inside the Perimeter

- Portable Storage Devices
- USB Flash Drives
- Camera Memory Cards
- Ipods et al
- PDAs (Blackberries et al)
- Smart (Intenet) Phones
- Camera Phones

Social Engineering & Insider Threat

12th Vancouver International Security Conference

December 1st 2009

Peter.Broznitsky@rcmp-grc.gc.ca

