WHY HACKERS LOVE END USERS

Chad Todd

CEH, CEI, MCSE:Security

chad@trainingconcepts.com

WHAT IS SOCIAL ENGINEERING?

- What is Social Engineering?
  - The art of manipulating people into performing actions or divulging confidential information.

  - Social Engineers influence victims to perform actions desired by the attacker. Social Engineers depend on the fact that people are unaware of their valuable information.

  - Trickery or Deception for the purpose of information gathering, fraud, or computer systems access.

Outsider → Insider

WHY SOCIAL ENGINEERING WORKS!

- There is no patch for STUPID!
- People want to trust people.
- People believe what they read.

WHY SOCIAL ENGINEERING WORKS!

- There is no specific software or hardware for defending against a social engineering attack
- There is no method to ensure complete security from social engineering attacks
- It is difficult to detect social engineering attempts
- Security policies are as strong as their weakest link, and humans are the most susceptible factor

IMPACT ON THE ORGANIZATION

- Damage of Goodwill
- Economic Loss
- Loss of Privacy
- Dangers of Terrorism
- Temporary or Permanent Closure
- Lawsuits and Arbitrations
- Identity Theft

PRETEXTING

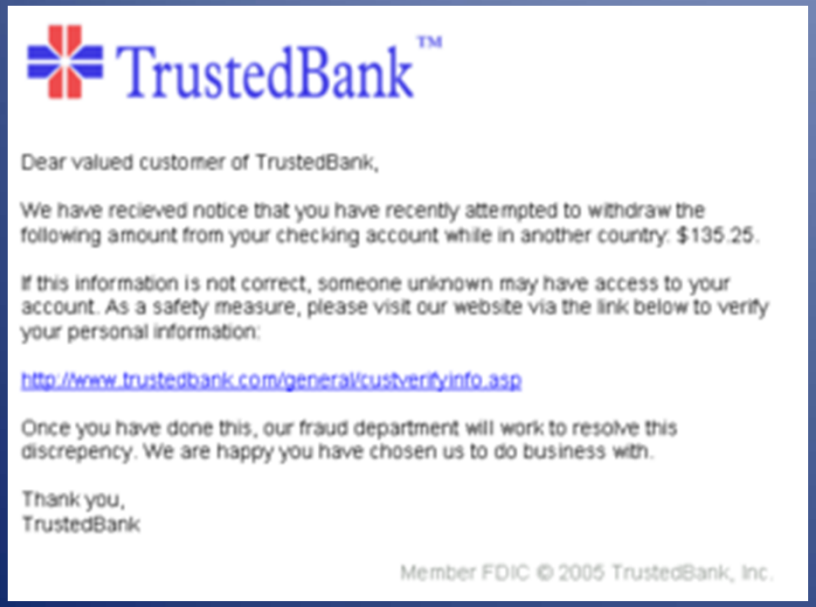
- Pretexting is the act of creating and using an invented scenario (the pretext) to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances. An elaborate lie, it most often involves some prior research or setup and the use of this information for impersonation (*e.g.*, date of birth, Social Security Number, last bill amount) to establish legitimacy in the mind of the target.
- This technique can be used to blame a business into disclosing customer information as well as by private investigators to obtain telephone records, utility records, banking records and other information directly from company service representatives.
  - Microsoft co-founder Paul Allen victim of ID theft - Computerworld http://bit.ly/LnH4TA
  - Wired writer Matt Honan had all his electronic devices wiped http://bit.ly/ToEL4x
- Pretexting can also be used to impersonate co-workers, police, bank, tax authorities, clergy, insurance investigators — or any other individual who could have perceived authority or right-to-know in the mind of the targeted victim. The pretexter must simply prepare answers to questions that might be asked by the victim. In some cases all that is needed is a voice that sounds authoritative, an earnest tone, and an ability to think on one's feet.

RESEARCH AND RECON

- Finding the Targets
  - Spokeo - http://www.spokeo.com/
  - People Search - http://pipl.com/
  - Peek You - http://www.peekyou.com/
  - Internet Archive - http://archive.org/
  - Social Networking Sites - Facebook, LinkedIn, or Twitter

PHISHING

- Phishing is a technique of fraudulently obtaining private information. Typically, the phisher sends an e-mail that appears to come from a legitimate business—a bank, or credit card company—requesting "verification" of information and warning of some dire consequence if it is not provided. The e-mail usually contains a link to a fraudulent web page that seems legitimate—with company logos and content—and has a form requesting everything from a home address to an ATM card's PIN.



TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

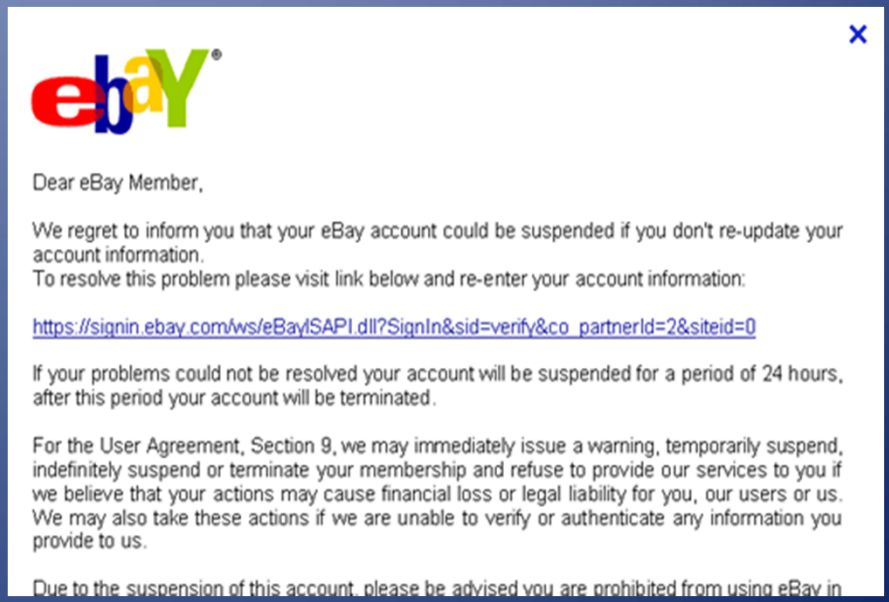
If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.



eBay

Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-update your account information.
To resolve this problem please visit link below and re-enter your account information:

https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0

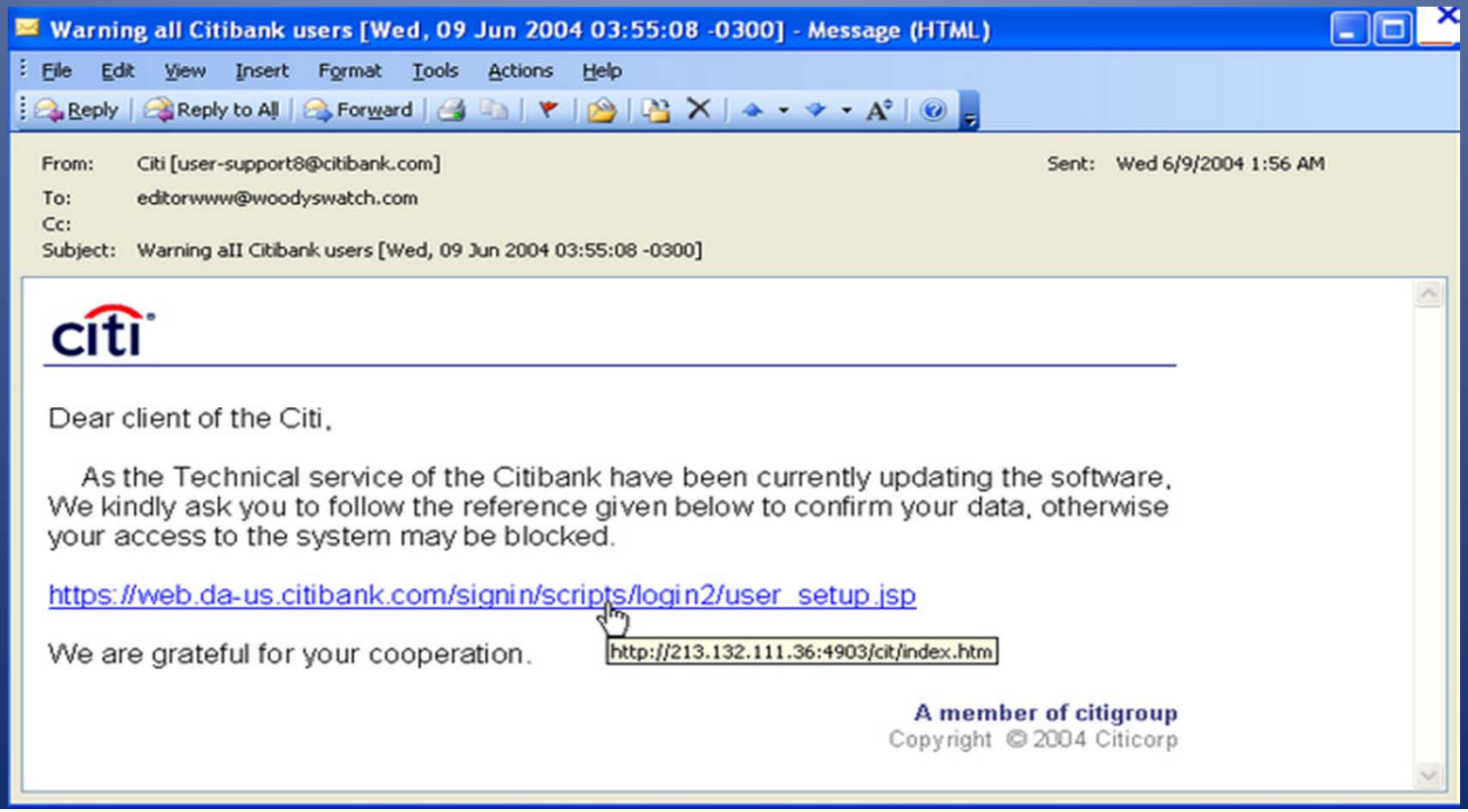
If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

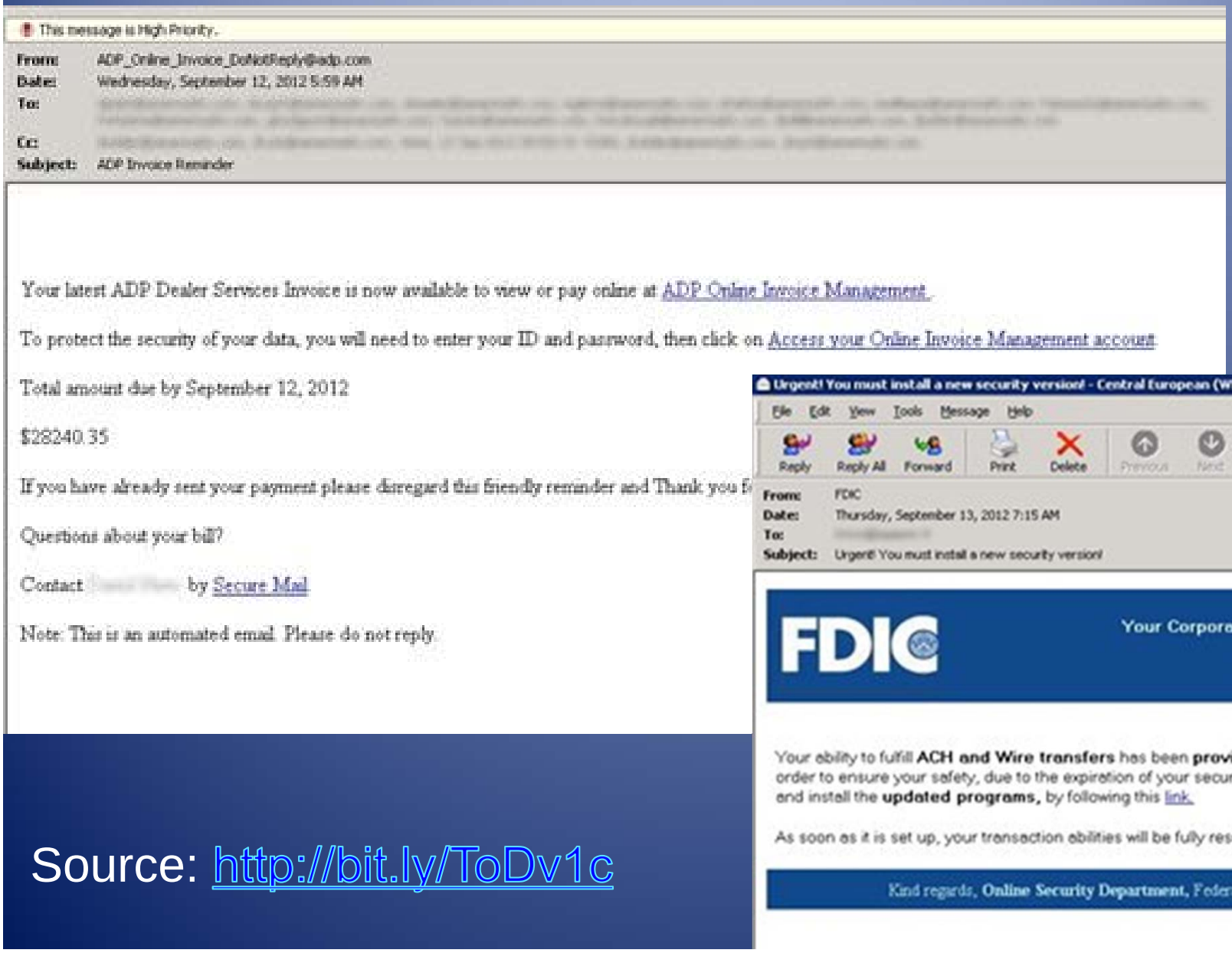
Due to the suspension of this account, please be advised you are prohibited from using eBay in

MALWARE SPOOFED E-MAIL

- "Unfortunately we were not able to deliver the postal package …. Please print out the invoice copy attached and collect the package at our department."
  - Source: Webroot Threat Blog http://bit.ly/LdyjeC



FAKE ADP AND FDIC



This message is High Priority.

From: ADP_Online_Invoice_DoNotReply@adp.com
Date: Wednesday, September 12, 2012 5:59 AM
To:
Cc:
Subject: ADP Invoice Reminder

Your latest ADP Dealer Services Invoice is now available to view or pay online at ADP Online Invoice Management.

To protect the security of your data, you will need to enter your ID and password, then click on Access your Online Invoice Management account.

Total amount due by September 12, 2012

$28240.35

If you have already sent your payment please disregard this friendly reminder and Thank you f

Questions about your bill?

Contact by Secure Mail.

Note: This is an automated email. Please do not reply.

Urgent! You must install a new security version! - Central European (Windows)

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

From: FDIC
Date: Thursday, September 13, 2012 7:15 AM
To:
Subject: Urgent! You must install a new security version!

FDIC

Your Corporated and Business Banking
Federal Deposit
Insurance Corporation

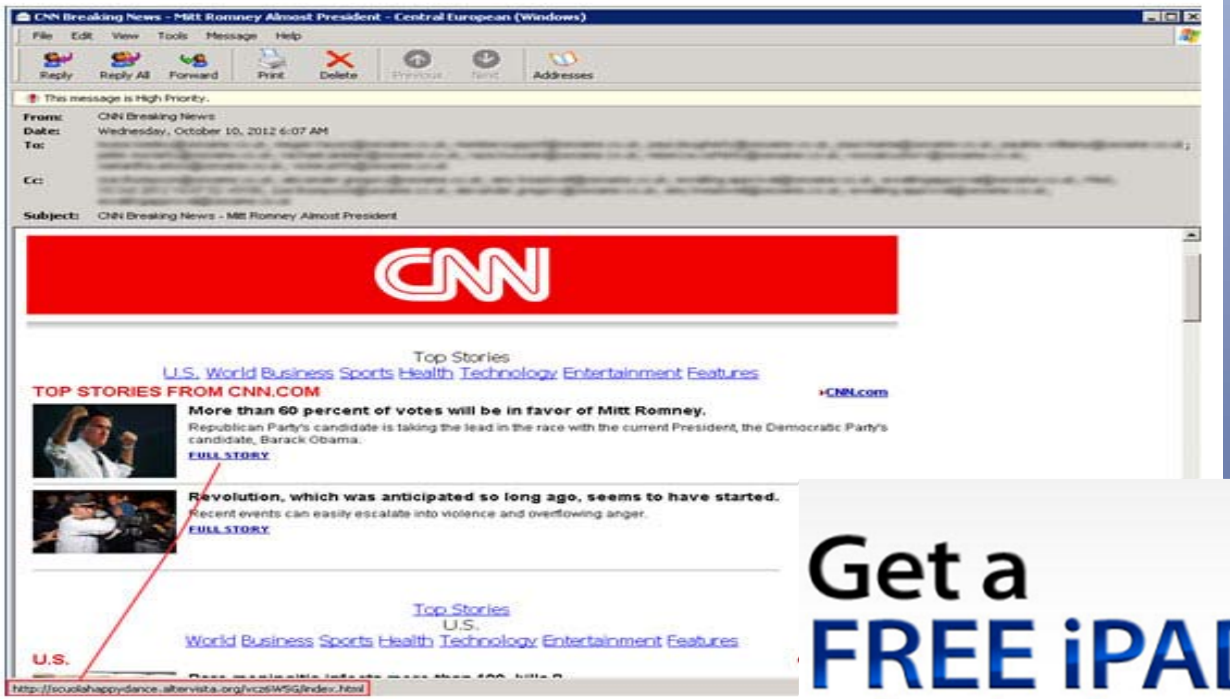
Your ability to fulfill **ACH and Wire transfers** has been **provisionally suspended** in order to ensure your safety, due to the expiration of your security version. Please download and install the **updated programs,** by following this link.

As soon as it is set up, your transaction abilities will be fully resumed.

Kind regards, **Online Security Department,** Federal Deposit Insurance Corporation.

Source: http://bit.ly/ToDv1c

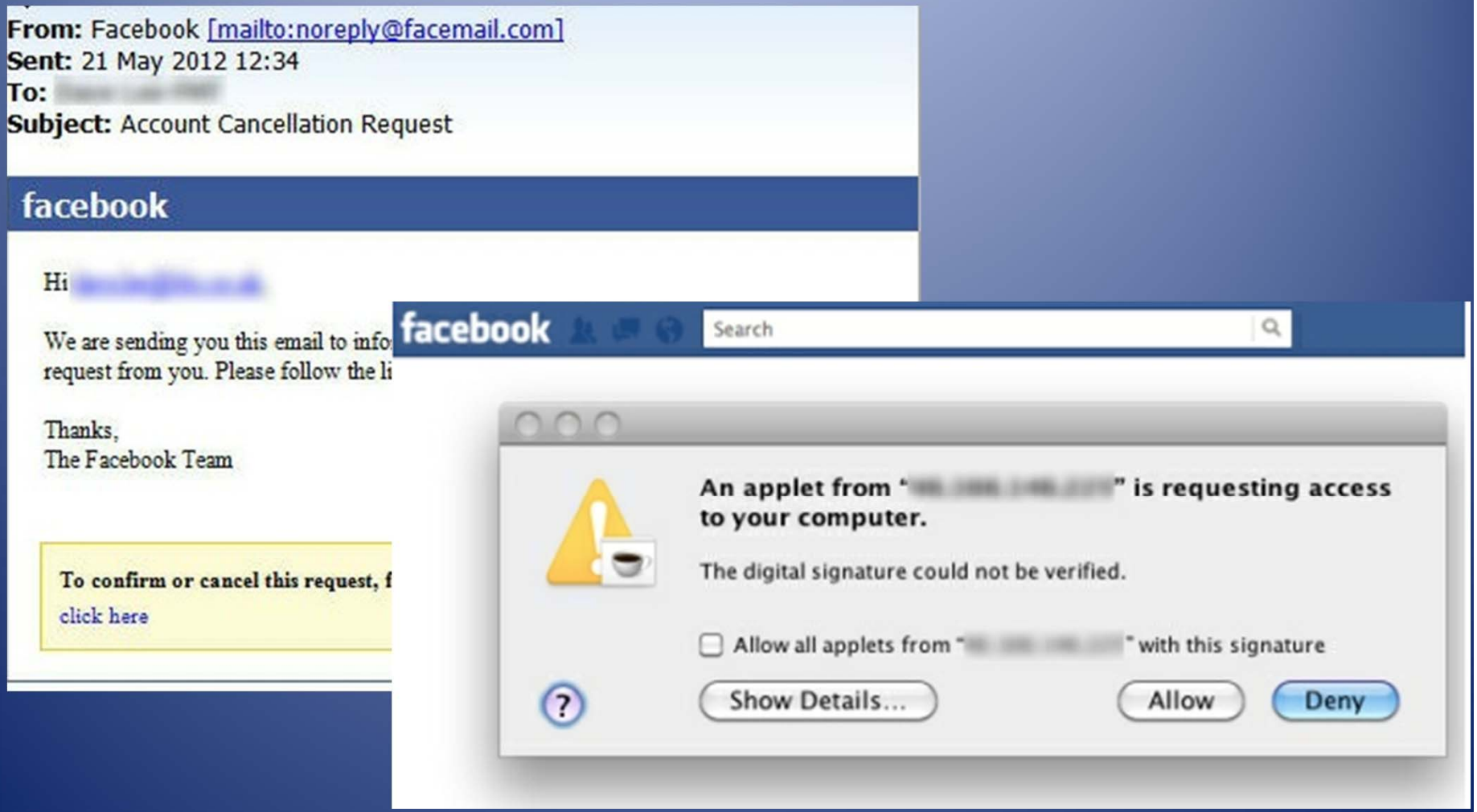
PHISHING EXAMPLES



PHISHING EXAMPLES

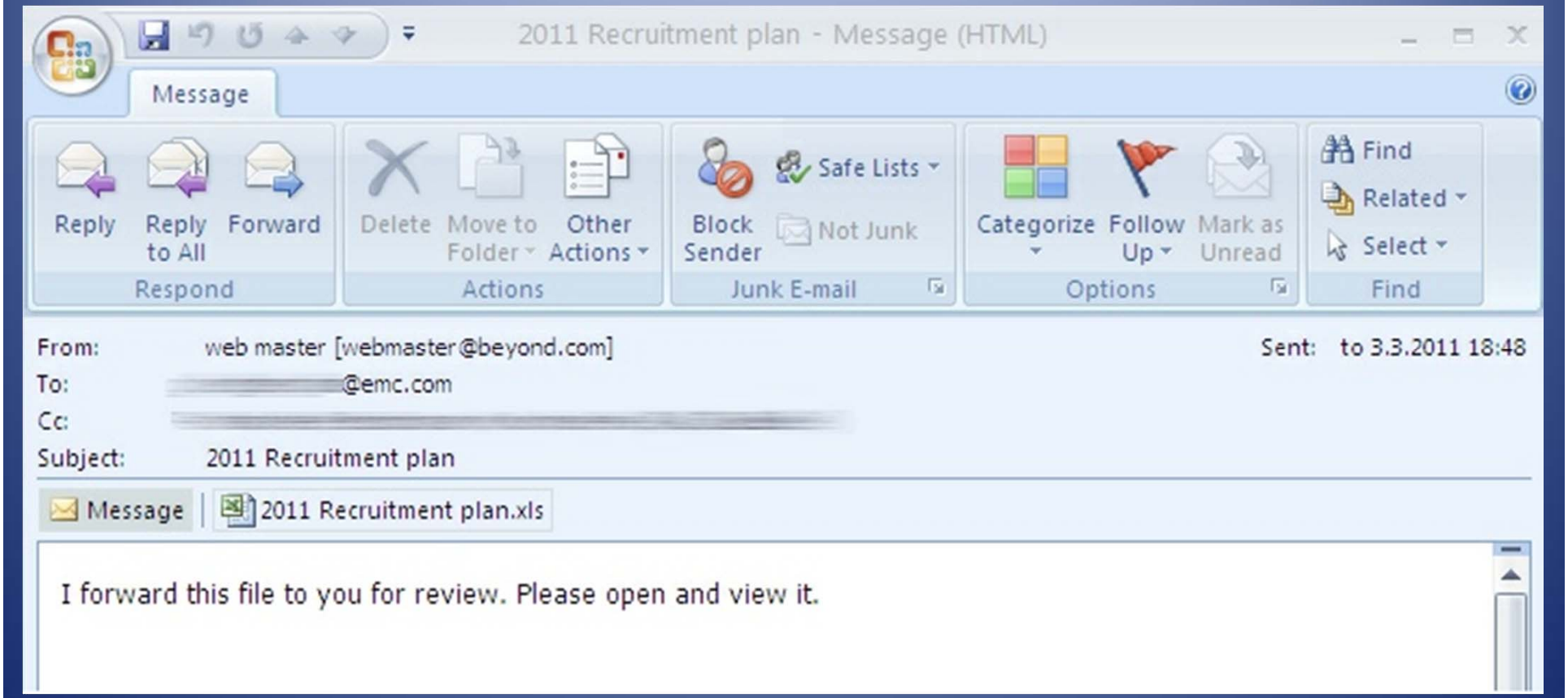
- Phishing scam directed the target to a phone number.
  - "Your card has been suspended because we believe it was accessed by a third party. Please press 1 now to be transferred to our security department." - BankInfoSecurity http://j.mp/3Gj0AA
- Bogus Pinterest Pins Leads to Survey Scams
  - Trend Micro http://bit.ly/MsDkke
- Vishing attack directed users to visit malicious websites.
  - "The recorded message tells me to go to www.helphs.com."
    - ZDNet Blog http://zd.net/Jet7oA

FACEBOOK PHISHING



Source: Sophos http://bit.ly/La67e8

HOW RSA GOT HACKED!



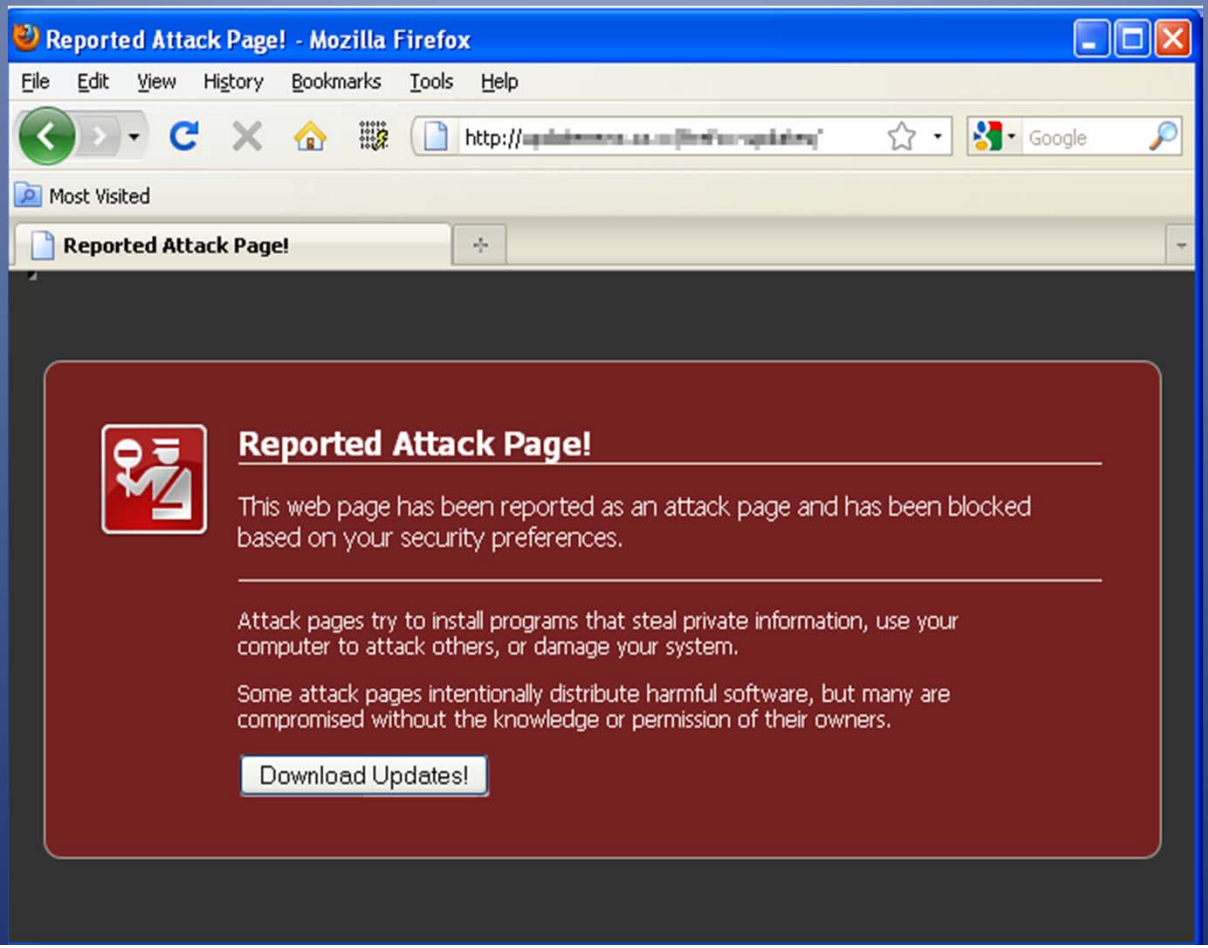
Sources:
http://m.wired.com/threatlevel/2011/08/how-rsa-got-hacked/
http://blogs.rsa.com/rivner/anatomy-of-an-attack/

RANSOMWARE

- What is Ransomware?
  - A class of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator of the malware in order for the restriction to be removed.
- Malware Poses as US Department of Justice Violation Notice
  - Source: Threat Post http://bit.ly/KqOm60
- Fake Antivirus Lives On, Now Infecting 200K WordPress Pages
  - Source: Threat Post http://bit.ly/J35B0q
- Scammers call users to help disinfect their Computers
  - Source: Yahoo! UK & Ireland Answers http://yhoo.it/J37UR6
  - Source: Symantec http://j.mp/jSjWBD
  - Source: Computer Repair Tips http://bit.ly/IUHlzc

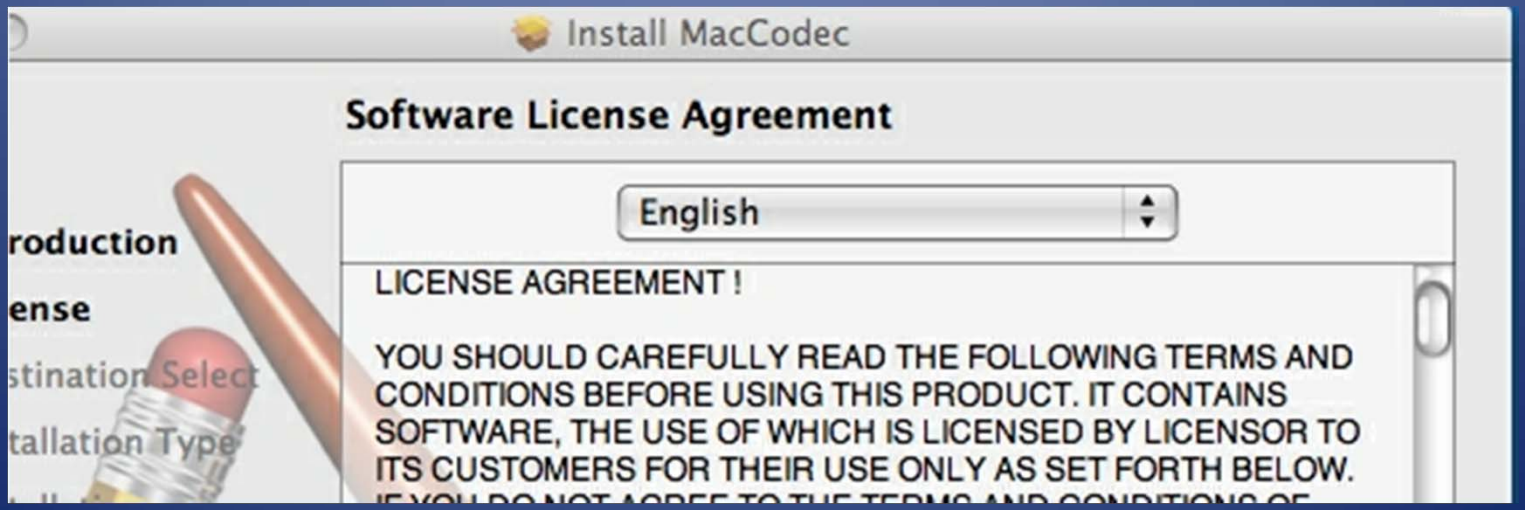
DRIVE-BY DOWNLOADS

- Malicious websites presented a security warning to the users, asking to download an update. Source: http://bit.ly/LeAKO3



TRICKED TO DOWNLOAD

- Fake Downloads lead to malicious downloads.
  - Source: F-Secure Weblog http://bit.ly/LdQ3qf
- DNS Changer Trojan leads users to download a fake codec
  - Source: http://bit.ly/KzVQDr



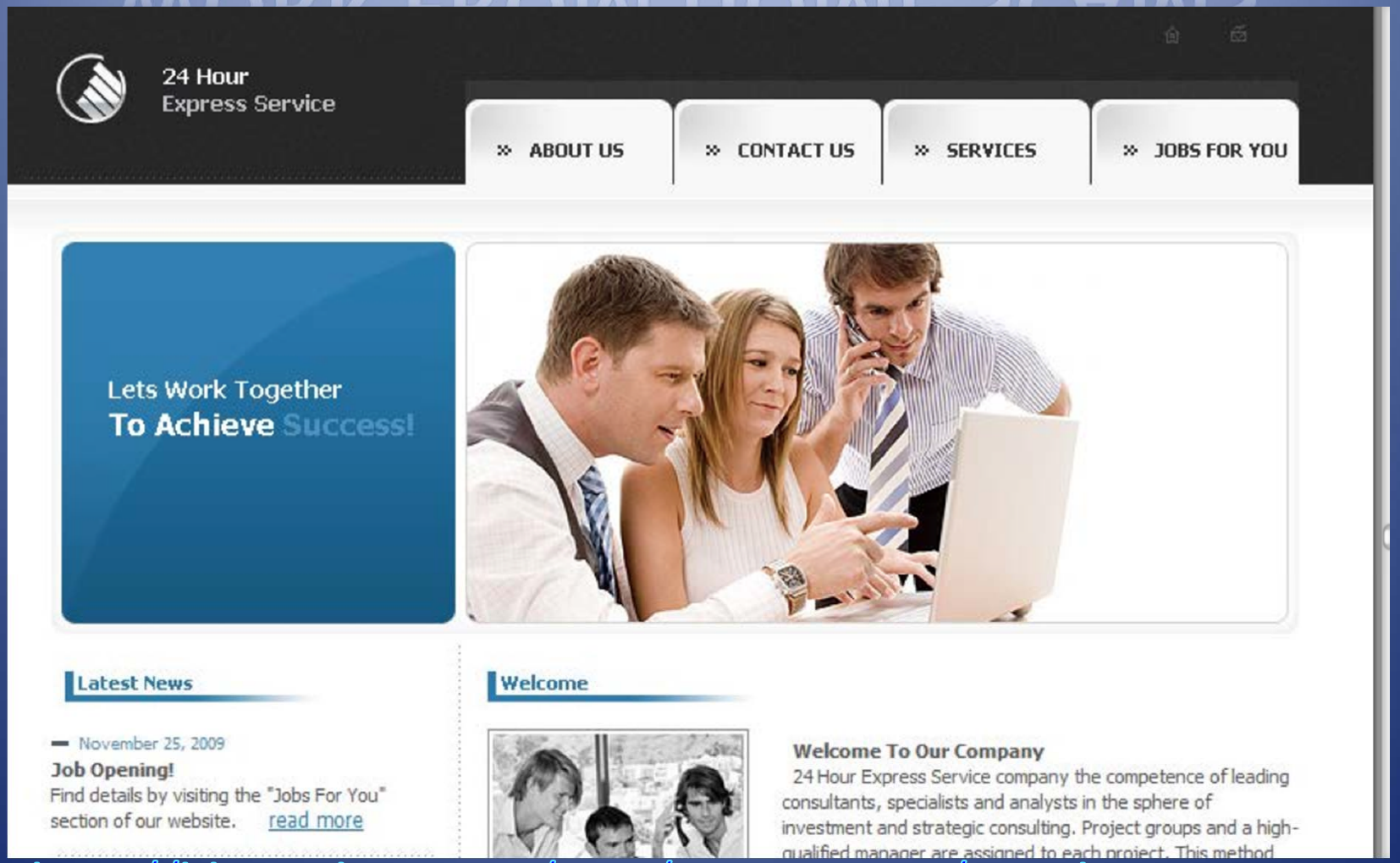
SOCIAL SITE SCAMMING

- Facebook Chat Scam asking for money
  - Source: http://bit.ly/LdHR9A
- Koobface Social Network Botnet
  - Source: NYTimes http://nyti.ms/KzWxN9

CLICKJACKING

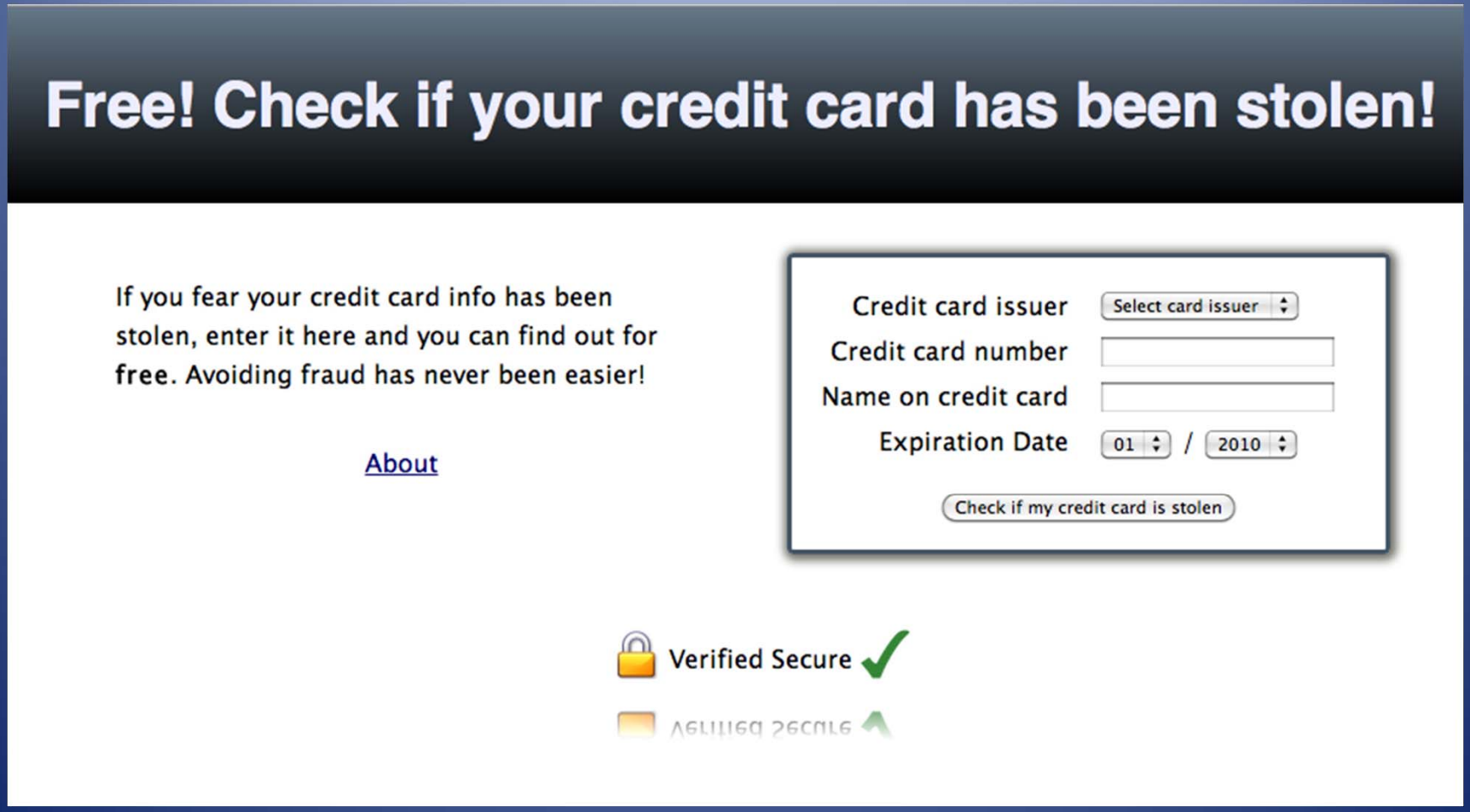
- What is ClickJacking?
  - A malicious technique of tricking a user into clicking on something different to what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.
    - Source: SecTheory - Internet Security http://bit.ly/IUDmTb
  - Countermeasures:
    - No Script - http://noscript.net/
    - Ghostery - http://www.ghostery.com/
    - GuardedID - http://www.guardedid.com/default.aspx

WORK FROM HOME SCAMS



- http://blog.zeltser.com/post/2685898823/social-engineering-in-online-scams

PHISHING EDUCATION



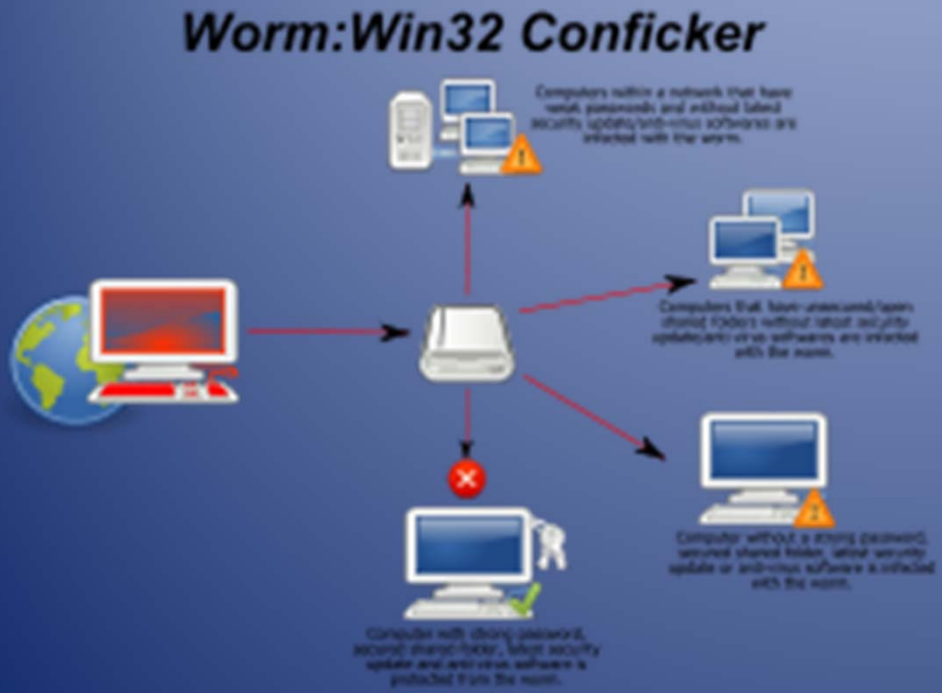
Source: ismycreditcardstolen.com

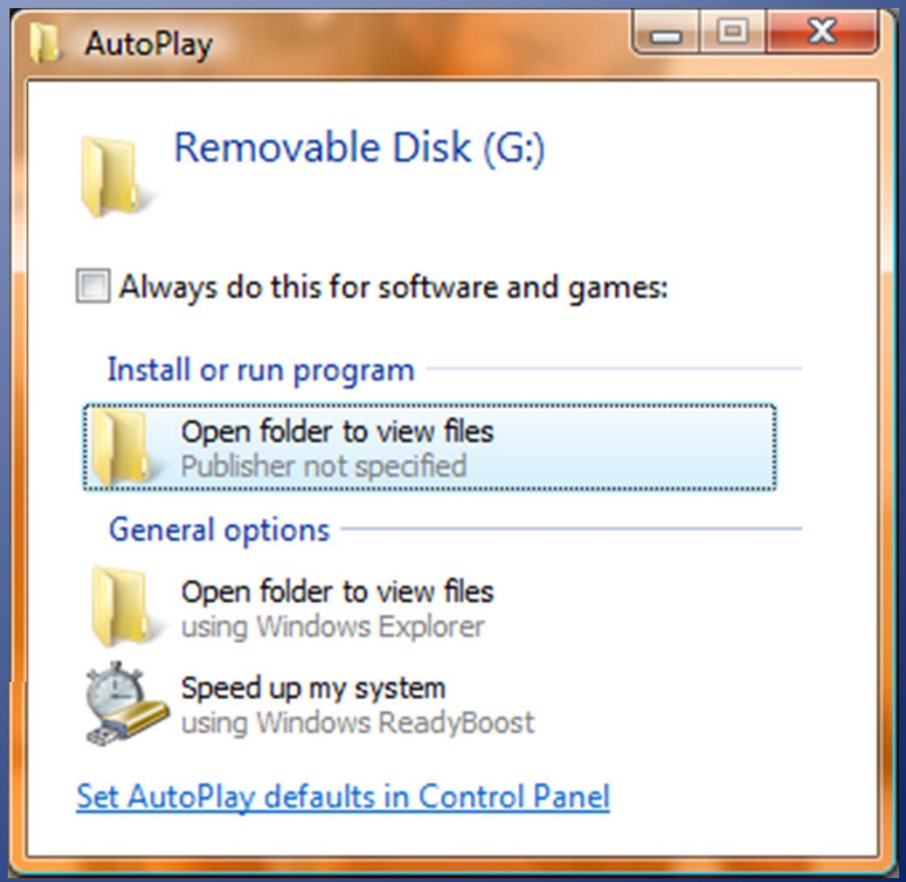
BAITING

- Baiting is like the real-world Trojan Horse that uses physical media and relies on the curiosity or greed of the victim.
- In this attack, the attacker leaves a malware infected floppy disk, CD ROM, or USB flash drive in a location sure to be found (bathroom, elevator, sidewalk, parking lot), gives it a legitimate looking and curiosity-piquing label, and simply waits for the victim to use the device.
- For example, an attacker might create a disk featuring a corporate logo, readily available from the target's web site, and write "Executive Salary Summary Q2 2012" on the front. The attacker would then leave the disk on the floor of an elevator or somewhere in the lobby of the targeted company. An unknowing employee might find it and subsequently insert the disk into a computer to satisfy their curiosity, or a good samaritan might find it and turn it in to the company.
- In either case as a consequence of merely inserting the disk into a computer to see the contents, the user would unknowingly install malware on it, likely giving an attacker unfettered access to the victim's PC and perhaps, the targeted company's internal computer network.
- Unless computer controls block the infection, PCs set to "auto-run" inserted media may be compromised as soon as a rogue disk is inserted.
- More attractive than memory, hostile devices can also be used. For instance, a "lucky winner" is sent a free digital audio player that actually compromises any computer it is plugged to. Technology security company HBGary has sold such devices to the US government

BAITING EXAMPLE

- USB Keys used as an infection vector.

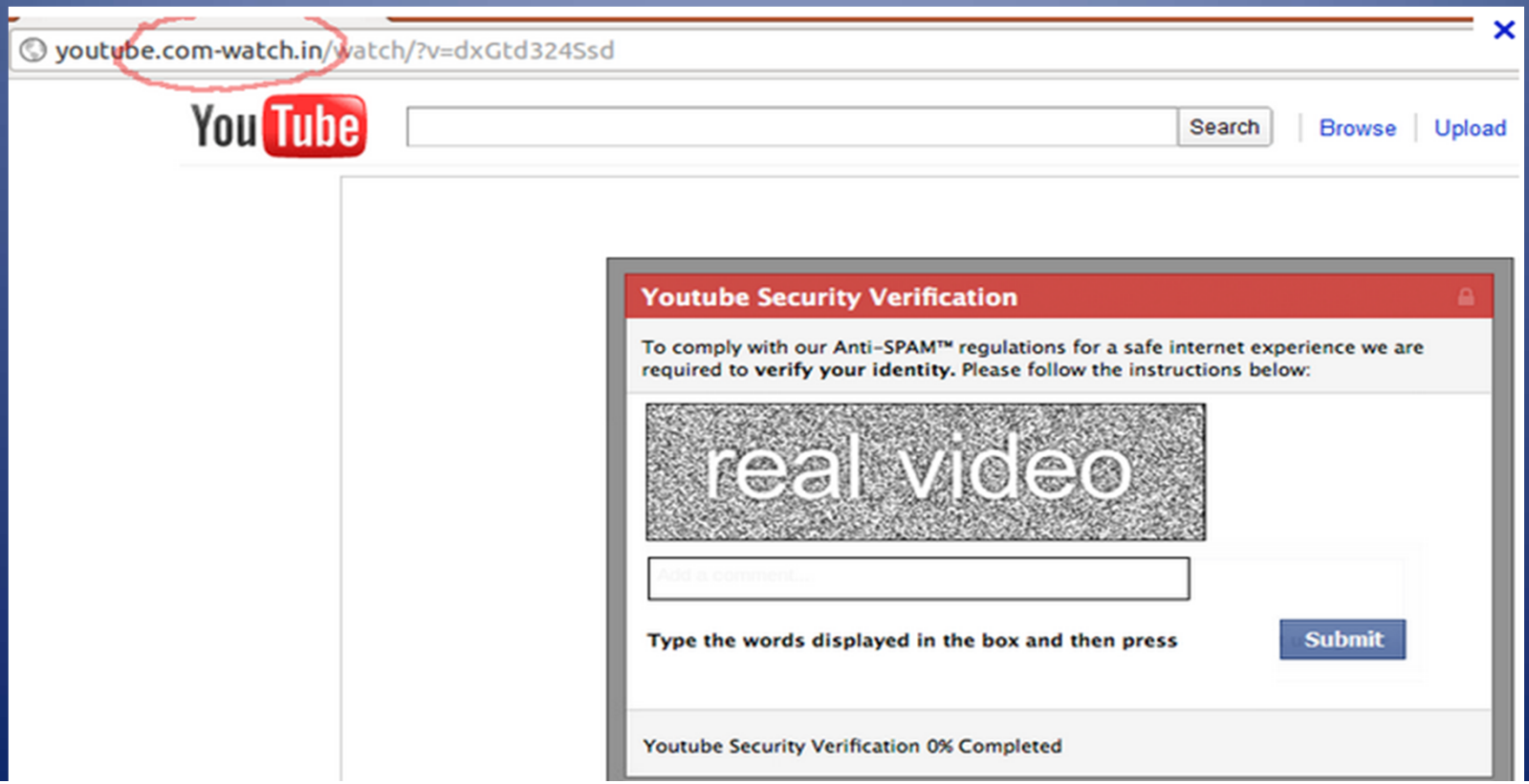




Source: Internet Storm Center
http://j.mp/HGTgRX

DOMAIN KITING

- What is Domain Name Kiting?
  - The method of exploiting loopholes in domain name registers registration procedures in order to earn money from temporary domain registration.



PHYSICAL SOCIAL ENGINEERING

Malware infection that began with windshield fliers

Published: 2009-02-03,
Last Updated: 2009-02-04 02:05:38 UTC
by Lenny Zeltser (Version: 1)

3 comment(s)

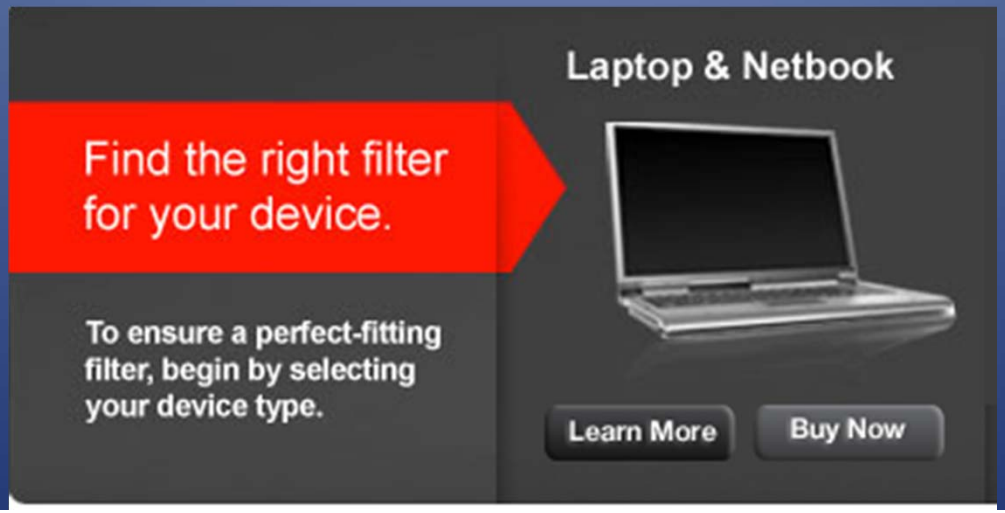
I had the opportunity to examine malware whose initial infection vector was a car windshield flier with a website address. The malicious programs were run-of-the-mill; however, the use of fliers was an innovative way of social-engineering potential victims into visiting a malicious website.

Several days ago, yellow fliers were placed on the cards in Grand Forks, ND. They stated:

> PARKING VIOLATION This vehicle is in violation of standard parking regulations. To view pictures with information about your parking preferences, go to website-redacted

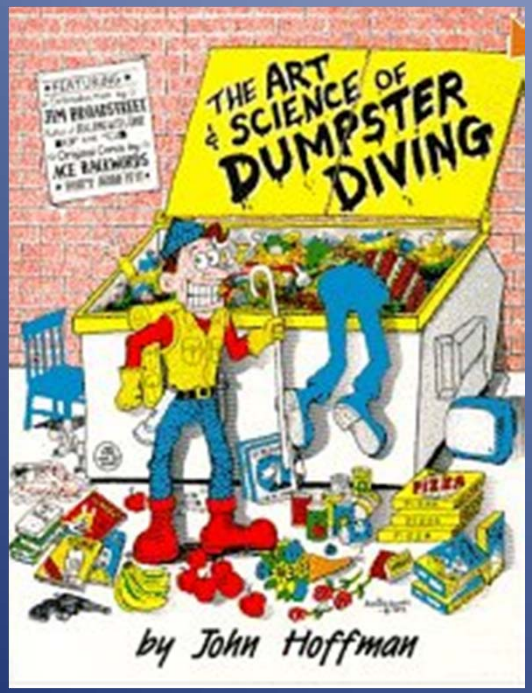
If you went to the website, you'd see several photos of cars on parking lots in that specific town, including:

SHOULDER SURFING



DUMPSTER DIVING

- Dumpster diving is looking for treasure in someone else's trash.(Phone Bills, Contact Info, Financial Info)



TAILGATING

- An unauthorized person, wearing a fake ID badge, enters a secured area by closely following an authorized person through a door requiring key access.
- “I forgot my ID badge at home. Please help me.”
- Fake Name Generator

http://bit.ly/Ldrk5r

COUNTERMEASURES

- Organizations must, on an employee/personnel level, establish frameworks of trust. (i.e., When/Where/Why/How should sensitive information be handled?(Data Classification))
- Organizations should perform background checks and proper termination processes
- Organizations must establish security protocols for the people who handle sensitive information. (i.e., Paper-Trails for information disclosure and/or forensic crumbs)
- Employees must be trained in security protocols relevant to their position. (e.g., employees must identify people who steer towards sensitive information.) (also: In situations such as tailgating, if a person's identity cannot be verified, then employees must be trained to politely refuse.)
- An Organization's framework must be tested periodically(pentest), and these tests must be unannounced.
- Dumpster Security by using a waste management service that has dumpsters with locks on them, with keys to them limited only to the waste management company and the cleaning staff. Also making sure the dumpster is located in a place where it is not out of view, and trying to access it will carry a risk to being seen or caught or behind a locked gate or fence where the person must trespass before than can attempt to access the dumpster.

COUNTERMEASURE PART 2

- Organizations must implement strong password policies(Multi-Factor Authentication)
- Organizations must implement anti-virus and anti-phishing defenses using multiple layers of defense(Mail Filter and Client-Side Anti-Virus)
- Secure and Shred all documents containing private or sensitive information
- Users never give out sensitive information over the phone or email.(Passwords, SSN#’s, etc..)
- Implement Data Reminisce policies for outdated hardware that may contain sensitive information.

ONE LAST THING!!!

Report anything unusual. If it sets off a warning in your mind, it just may be a problem. Don't ignore it!!!!!

WHAT ARE THE STEPS INVOLVED WITH HACKING?

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Covering Tracks

WHAT IS RECONNAISSANCE?

- Passive Reconnaissance
- Active Reconnaissance
- www.archive.org, physical security, wireless

WHAT IS SCANNING?

- Finding information about networks by probing resources.
- Utilizes dialers, port scanners, network mapping, vulnerability scanning, etc.
- Demo: SuperScan

HOW DO HACKERS GAIN ACCESS?

- Gaining access refers to the actual penetration of the network.
- Accomplished by exploiting vulnerabilities.
- Enumeration – comprising user names and passwords.
- Demo – Null Connection, DumpSec, NAT, PWDUMP3E, John the Ripper

HOW DO HACKERS MAINTAIN ACCESS?

- Hackers utilize backdoors, rootkits, and Trojans.
- These allow hackers to retain ownership of the system without anyone knowing.

HOW DO HACKERS COVER THEIR TRACKS?

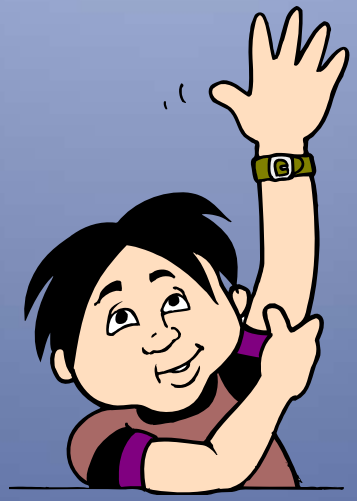
- Hackers utilize steganography, tunneling, and altering log files.

- Demo – Alternate Data Streams (ADS)

CLASSES OFFERED IN SECURITY

- Security Awareness Training - One Day
- CompTIA Security+ - Five Days
- CompTIA Advanced Security Practitioner – Five Days
- ISC^2 CISSP - Five Days
- Certified Ethical Hacker - Five Days
- Certified Hacking Forensics Investigator – Five Days
- Certified Security Analyst - Five Days

QUESTIONS AND ANSWERS



chad@trainingconcepts.com

803.772.6441

Training CONCEPTS