Creating smarter fish by customizing the pond
What application developers can do to stop phishing

12 July, 2006

Ron Ritchey
Chief Scientist
IATAC
703/377.6704
Ritchey_ronald@bah.com
Agenda

- Introduction
- Why phishing works
- Browser-based defenses
- Site customization
- Vendor Services
- Other approaches
Phishing and Pharming: Problems that are Only Getting Worse

- **Phishing** – an attack aimed at stealing personal identity data and/or financial account data. These attacks use a combination of social engineering and technological techniques centered around email.
- **Pharming** – an attack aimed at stealing personal identity data and/or financial account data that involves misdirecting users to fraudulent websites by compromising DNS servers.

- **May 06 Statistics**
  - Brands Hijacked: 137
  - # Brands in Top 80%: 20
  - Average time Online: 5 days
  - Max Time online: 31 days

Source: Anti-Phishing Working Group (www.antiphishing.org)
Current Trends in Phishing Attacks
Common Targets

- The most common phishing targets represent the Internet's largest online vendors and financial service institutions:
  - Citibank (highest volume)
  - Ebay/Paypal (highest merchant volume)
  - Foreign National who died, etc.

- Financial Services are major targets
  - Financial services comprise 92% of phishing targets
  - Online retailers make up 6% of those targeted

- According to Cyota, a leading anti-Phishing vendor recently acquired by RSA Security, phishers are beginning to target non-US banks
  - In April 2006 57% of banking brands that were used in phishing attacks were International brands
  - Mainly European financial institutions in the UK, Germany, and Spain
Current Trends in Phishing Attacks
New Targets

- In the last year several new phishing schemes have surfaced
- During the last tax filing season phishing heavily targeted US taxpayers by posing as the IRS
  - Huge target audience: all US taxpayers (100-130 Million people)
  - Probability of success is very high since taxpayers fear audits and other retribution for failure to provide records
- Research into domain name registrations has shown that fraudsters may target hurricane relief during this hurricane season
- Computer Security industry should look to similar sociological events that can trigger phishing scams
Current Trends in Phishing Attacks
Why Phishers Phish

- It is estimated that the average loss to a successful Phishing scheme is $1200
  - It is trivial to send millions of phishing emails
  - It is estimated that 3-5% of users targeted are duped in some way by phishing scams
    - This may seem small, but 3% of 1 million is still 30,000 people
    - If even 0.5% of those fully divulge information, the fraudsters stand to make thousands

- The net result?
  - Almost 2 million users divulged sensitive information in 2003 that results in nearly $1.2 Billion in losses
Phishing Life Cycle

1) Phisher copies site
2) Phisher sends email
3) Users receive email and visit phishing site
4) Phisher retrieves credentials and verifies account
5) Phisher sells credentials to buyer
6) Buyer uses “mules” to transfer money
7) Site is detected and taken down
8) Phisher, Buyer, and “Mules” all walk away

• This typically all happens in less than five days
Agenda

- Introduction
- Why phishing works
- Browser-based defenses
- Site customization
- Vendor Services
- Other approaches
Why Phishing Works
Lack of Knowledge

- Although the user community has begun to understand that email can be spoofed, they lack the knowledge to detect other phishing schemes.
- Recent studies have shown that 90% of users can be duped by a good phishing site.
- Users do not understand how to determine the security of sites;
  - Most are convinced a site is secure when security graphics are displayed on the page
    - Padlock icon
    - Tested secure by xxx…
  - Half of users do not understand the meaning of HTTPS and Certificates
  - 75% of users ignore all browser pop-up warning because they do not understand them
- A well executed phishing attack exploits user emotions
  - Fear of losing access to accounts, etc.
Why Phishing Works
Ineffective Browser Indicators
Why Phishing Works
Bad Practices

- Home page is insecure
- Security is indicated by a lock icon in the page
- Login data IS sent securely, however it trains users to trust icons in pages rather than their browser
- Similar sites are prime targets for a phishing attack
Why Phishing Works
Technological Deceptions

- Direct Data Collection
- “Typejacking”
  - Use of “cousin” domains
- JavaScript Redirection
- URL Encoding
- XSS Attacks
  - Extremely hard to detect when executed well
  - Usually executed as a pop-over
- Pharming
What’s wrong with this?

What’s RIGHT with this?

De Lotto Netherlands
41132, NL-1007 DB AMSTERDAM
www.deлотtonetherlands.net

FROM: THE DESK OF THE PROMOTIONS MANAGER,
INTERNATIONAL PROMOTIONS/PRIZE AWARD DEPARTMENT,
AB96532 AND BATCH NO: 57/1088/IBA.

RE: AWARD NOTIFICATION,

We are pleased to inform you of the announcement today, 23rd November, 2002, of
winners of the DE LOTTO NETHERLANDS SWEEPSTAKES LOTTERY / INTERNATIONAL
PROGRAMS held on 29TH September 2002 as part of our end of year bonanza.

You/your company, attached to ticket number 047-1776-1342-440, with serial
number 21564-07 drew the lucky numbers 01-77-13-55-38-11, and consequently
won the lottery in the 1st category (category 'A').

You have therefore been approved for a lump sum pay out of US$3,000,000.00 in
cash credited to file REF NO. AB96532. This is from total prize money of
US$6,000,000.00 shared among the two(2) international winners in this category. All
participants were selected through a computer balloting system drawn form 25,000
names from Middle East, Asia, Africa, Canada, Europe and North America as part our
International Promotions Program, which is conducted annually.

CONGRATULATIONS!

Your fund is now deposited with FIRST SECURITIES INC., Due to the mix up of some
numbers and names, we ask that you keep this award strictly from public notice until
your claim has been processed and your money remitted to your account. This is
part of our security protocol to avoid double claiming or unscrupulous acts by
participants of this program.

We hope with a part of you prize, you will participate in our end of year high stakes
US$1.3 billion International Lottery.

To begin your claim, please contact your claim agent;
Why Phishing Works
Example

Did you really sign up for an Ameritrade account?

The phishy “cousin” domain

Thank you for opening your Ameritrade® account!

Your account must be funded before you can begin trading. For details about your funding choices, log on at www.ameritrading.net and choose Help Center from the Help menu. Then click Managing your account and Deposits:

You can make the most of your Ameritrade experience by checking out Ameritrade Streamer® (TM), setting up your watch lists, and taking a look at everything available to you under the Research menu.

Again, thank you for choosing Ameritrade. We look forward to serving you for years to come.

Sincerely,
Kenneth I Feldman
President, Private Client Division
Ameritrade

Source: www.antiphishing.org
Why Phishing Works Example

A perfect copy of the real Ameritrade site

The phisy "cousin" domain

www.ameritrade.com vs.
www.ameritrading.net

Source: www.antiphishing.org
Why Phishing Works
Example

Dear PayPal,

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address.

If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you. However, if you did not initiate the log ins, please visit PayPal as soon as possible to verify your identity:


Verify your identity is a security measure that will ensure that you are the only person with access to the account.

Thanks for your patience as we work together to protect your account.

Sincerely,
PayPal

Actual Link: http://218.246.224.203/icons/.cgi-bin/paypal/cgi-bin/webscr?cmd=_login-run
Why Phishing Works Example

Spoofed Address Bar (actually an image)

Discrepancy (no lock icon in status bar)

Source: www.antiphishing.org
Why Phishing Works

Example

Full HTML email looks legit

Non-Threatening

Actual link:

IP address has been encoded

Source: www.antiphishing.org
Why Phishing Works

Example

Real Site

• Very sophisticated
• Non Threatening
• Used a flaw in BoA site to inject script

Source: www.antiphishing.org
Why Phishing Works Example

Specific user data gathered from database compromise

Obscured Link

Actual Link: http://www.chase.com @213659570/public.index.html

Dear Mr. Kough,

On April 12, 2006 our Online Banking Review Team identified some unusual activity in your savings account number XXXXXXXX12359. In accordance with Chase Bank’s User Agreement and Online Security Policies, and to ensure that your online account has not been compromised, access to your account has been temporarily restricted. Your account will remain restricted until this issue has been resolved. If you believe that this access was a security incident, please do not be alarmed, our security measures ensure that no funds are removed from your account until we have verified the authenticity of these actions. In order to review the actions in question, please log in and answer your security questions. Once verification has been complete normal account access will be restored immediately. If the verification procedure is not completed in 72 hours your online account access will be suspended and you will need to visit a branch location to restore access.

http://www.chase.com

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

Thank you for your prompt attention to this issue. We at JPMorgan Chase make your account security our number one goal and we apologize for the inconvenience.

Have a nice day,

JPMorgan Chase & Co., Online Account Support

©2006 JPMorgan Chase & Co.
Agenda

- Introduction
- Why phishing works
  - Browser-based defenses
- Site customization
- Vendor Services
- Other approaches
Browser based defenses
What the market leaders are proposing

- Internet Explorer 7 and Firefox 2.0 will both include anti-phishing features
  - IE7 will check websites against Microsoft's database of known phishing sites
  - Mozilla has partnered with Google to use Google Safe Browsing to verify sites against the Google list of known phishing sites.
  - It appears the lists will be built independently
  - Some heuristic detection capability is claimed but the algorithms have not been disclosed
Browser based defenses
What the market leaders are proposing

- **Google Safe Browsing**
  - Although details of Google’s method for identifying phishing sites is vague, some think it will mostly be based on user reporting.
  - This relies on basically a giant “neighborhood watch” for the internet
  - A downside being that each and every page visited results in an HTTP request being sent to Google
    - Google can store your browsing history
    - Can be a security issue if sensitive information is included in a GET request

- **IE7**
  - Site’s are checked against “whitelists” that are stored locally on the user machine and updated periodically
  - “Suspicious” sites are checked against “blacklists” that are stored on Microsoft machines and continuously updated
  - Has indicated partnerships with various security vendors to update blacklists
Browser based defenses
Some other proposed browser techniques

- Browser skins
  - Overlay a personal image on username and password fields to verify authenticity
  - Would help protect against pop-overs
  - Would require initial setup by user

- Automatic password hashing
  - Hash password with local key combined with identifying value from SSL cert
  - Real site gets consistently hashed password
  - Phishing site gets unusable password
Agenda

- Introduction
- Why phishing works
- Browser-based defenses
- Site customization
- Vendor Services
- Other approaches
Site customization
Passmark Sitekey

- Site personalization is a type of two-way authentication
- This can be a very defined authentication method such as PassMark Security’s (recently acquired by RSA Security) SiteKey product
- Uses client “fingerprinting” to verify that the user is signing in from a previously verified device
- If this is a new device then the user must pass a secondary authentication before their picture and phrase are displayed

Source: [http://www.passmarksecurity.com](http://www.passmarksecurity.com)
Site customization
Sitekey mechanics

Here's How SiteKey Works

By passing back and forth secret information that only you and Bank of America know, you can feel even more secure with your Online Banking experience. We recognize you and you recognize us.

1. Enter your Online ID.

2. Click Sign In using my SiteKey.

3. If we recognize your computer:
   We will show you your secret SiteKey. If you are vision-impaired, you can recognize your Sitekey by its specific name and message.
   Your SiteKey Image and Message:
   cute dog

4. If we don’t recognize your computer:
   We will ask you one of your secret SiteKey Confirmation Questions.
   After you answer your question correctly, we will show you your SiteKey.
   What was your high school mascot?
   * Answer: __________________________

5. Once you view your valid SiteKey, you can then safely enter your Passcode and continue onto your Online Banking account.
   Passcode: **********

Source: http://www.bankofamerica.com
Site customization
Can be worked into the look and feel

- Usage of site personalization as a security measure requires adding visual features that would be obvious when missing
- Users must be educated continuously for this to be effective
Site customization
Areas of potential customization

- In addition to authentication backgrounds, other personalization’s can help a user differentiate a legitimate site from a bogus one
  - “Welcome back Mr. Gibson (if you are not Mr. Gibson, click here)”
  - Let users choose graphics for landing page
  - Let users add stock tickers or calendars
  - Allow users to change color schemes

- User identity must be asserted before this authentication can take place.
  - Can be cookie based or user entered
  - User entered identity assertion means a two phase authentication
    - This is the SiteKey/Band of America model
  - Cookie based is less obvious to the user
Agenda

- Introduction
- Why phishing works
- Browser-based defenses
- Site customization
- Vendor Services
- Other approaches
Vendor services

- Many vendors offer Anti-Phishing and/or Brand Protection Services
  - Brandimensions
  - MarkMonitor
  - RSA Security (formerly Cyota)
  - VeriSign
  - Many more (full listing available at [www.antiphishing.org](http://www.antiphishing.org))

- Services offered include:
  - “Cousin” domain name monitoring
  - “Typo domain” registration
  - Site Blocking
  - Site Takedown
  - Honeypot Account Tracing
  - “Watermarking” of website content to trace attack origination
Vendor services
Domain services

- “Cousin” domain name monitoring
  - Vendor works with domain name registrars
  - Monitors domains that are registered that match certain criteria that could be used to infringe on a brand
  - Can provide a jump start on Phishing attacks by detecting brand infringement before emails are sent

- “Typo domain” registration
  - Vendor aids selection of domains that could be accessed accidentally and registers them with redirection to the real site.
    - [http://www.bank0famerica.com](http://www.bank0famerica.com)
Vendor services
Site removal

- **Site Blocking**
  - Works with Domain name registrars and ISPs to prevent access to phishing sites after an attack is launched
  - If DNS entry is referenced in phishing email that DNS entry is removed
  - If an IP address is referenced directly, that IP addresses is added to blacklists

- **Site Takedown**
  - The next step after a site is blocked is taking down the machine
  - Vendors work with ISPs globally to remove hosting machines from the web
  - Many times phishing sites are hosted on “owned” machines
  - Several of the largest vendors have shown ability to remove even international sites.
Vendor services
Phishing detection

- **Blacklist**
  - Collect large list of known phishing sites across all customers
  - Inbound requests are compared against list

- **Transaction profiling**
  - Rules-based or neural net models used to detect unusual transactions

- **“Honeypot” account tracing**
  - Many vendors recommend submitting honeypot accounts to phishing sites prior to takedown
  - These are “real” account credentials and/or credit card information that are closely monitored
  - Allows tracing of account credentials and money to guilty parties:
    - Phishers - execute attack
    - Those who verify credentials and account contents
    - Parties who purchase compromised credentials for “juicy” targets
    - “Mules” who transfer funds
  - Allows detection of other compromised accounts
Agenda

- Introduction
- Why phishing works
- Browser-based defenses
- Site customization
- Vendor Services
  - Other approaches
Other approaches

- **Consistent Branding**
  - All websites should have a specific brand
  - All correspondence should be consistent with the brand
    - From, Reply to, and To fields should be consistent

- **Continuously notify users of account credential policies**

- **Monitor email bounce back**
  - If consistent branding is used, phishers will be forced to use valid From and Reply fields
  - This will cause bounced email to be sent to the phishing target
  - Serves as an “early warning system”

- **Monitor referrer sites**
  - Once credentials are gathered users are usually sent to the real site
  - A sudden spike in referrals from an unusual host can help spot a phishing site
Other approaches

- Watermark content
  - Watermarked content can be used to set a timeline for the attack
  - It can also be used to trace back to the original machine or IP address that pulled images

- Provide formal method for phishing reporting
  - If all else fails, user will see fraudulent email and they should report it
  - Ensure links are clear and easy to access

- Adaptive authentication
  - Several vendors offer adaptive authentication solutions
  - Adaptive authentication allows additional security checks for high-risk or unusual activity
  - This is basically the old “mothers maiden name” knowledge based authentication
  - Additional authentication when client “fingerprint” changes
Other approaches

- Two factor authentication
  - Perhaps the most tried and true method of foiling phishing
  - Several vendors offer solutions
    - RSA Security, Verisign, Entrust, Vasco Data Security
  - Solutions vary from One Time Password to Challenge – Response
  - Hardware and software based solutions

- Secure Data Entry
  - Letters are randomized
  - Can be modified so only partial password or pin is entered (e.g. enter last three characters of password)
Other approaches
Defeating man in the middle

- Even two factor authentication can fail against m-in-m attacks
  - Phishing site acts as proxy until access is gained
- Transaction signing is being implemented by some banks to combat problem
  - Unique details of customer commanded transaction included in challenge value
  - Response computed by customer’s smartcard/token
  - Transparency of challenge creation to user critical
Questions?