Phishing

Spoofed emails

1

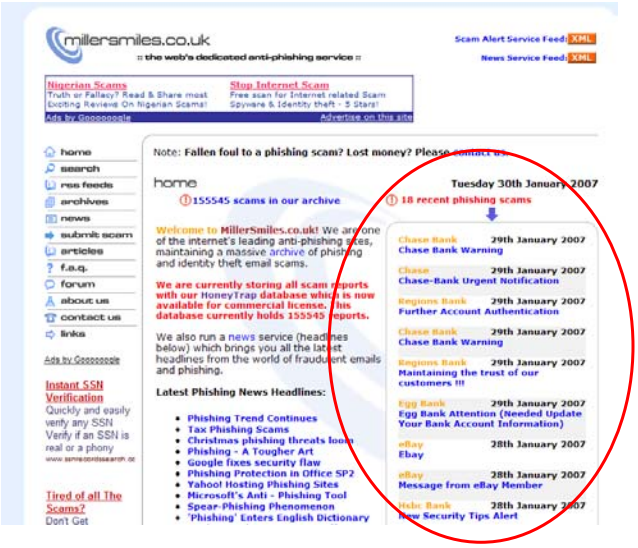
A Few Headlines

- "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"

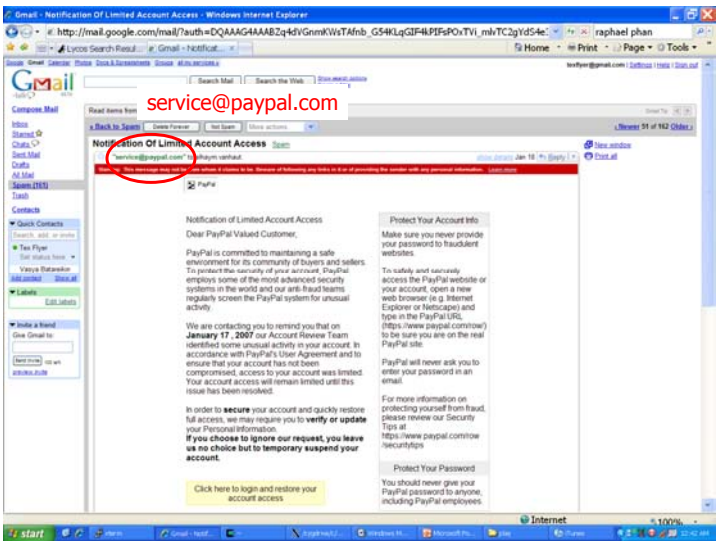
2

MillerSmiles.co.uk



3

A Snapshot of a Friends Mailbox

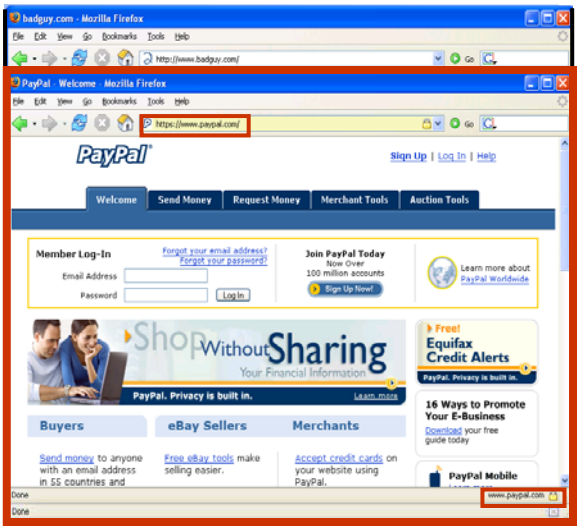


4

Typical Phishing Page

5

Or Even Like This



6

A Closer Look

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

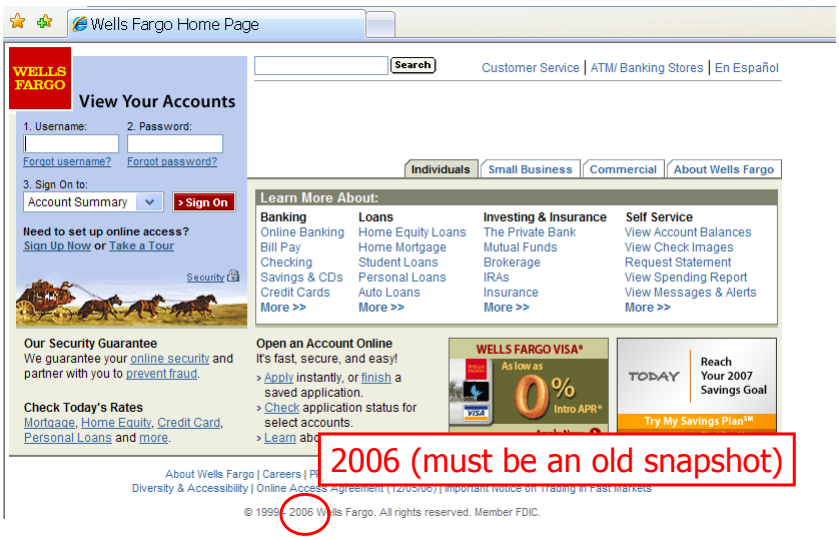
What you'll see on the page

Where the link actually goes

<a target="_blank"
href="**http://www.members.axion.net/~rod/.Wells.Fargo.com**" >
https://online.wellsfargo.com/signon?LOB=CONS

7

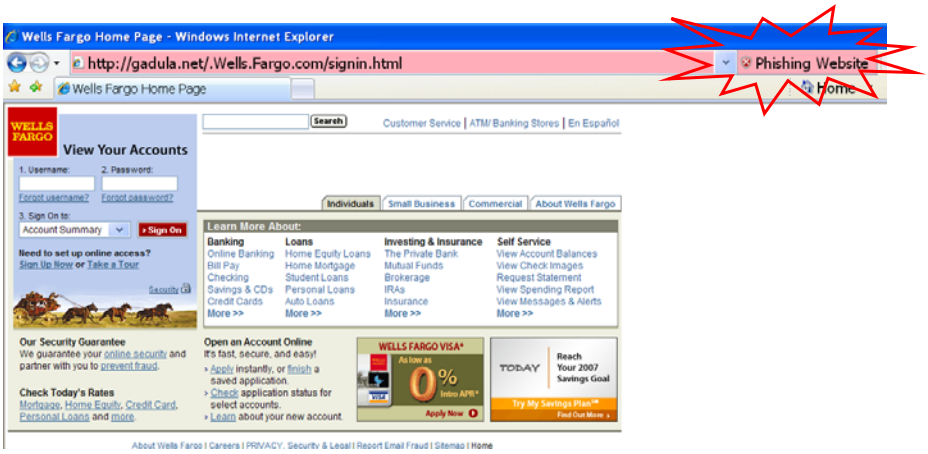
And You End Up Here



2006 (must be an old snapshot)

8

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"
- 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="spoof"
    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)

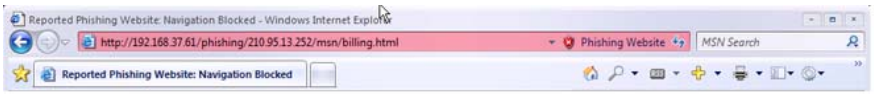
[Jagatic et al.]

- 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

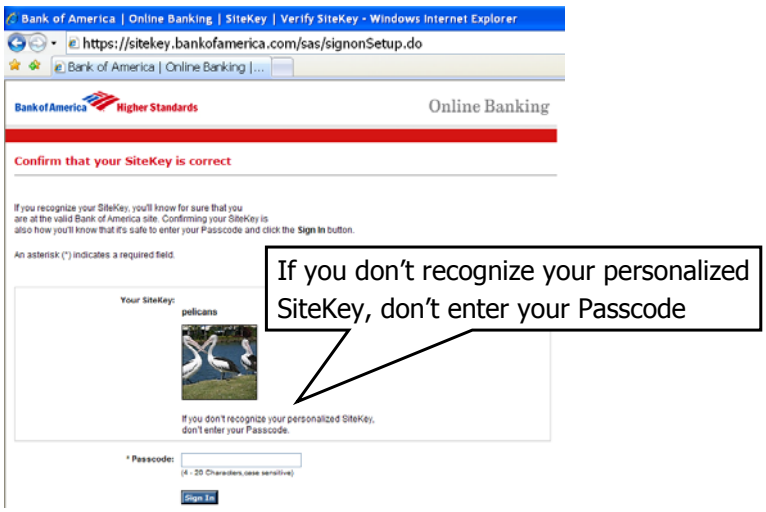
Defense #1: Internet Explorer 7.0

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



19

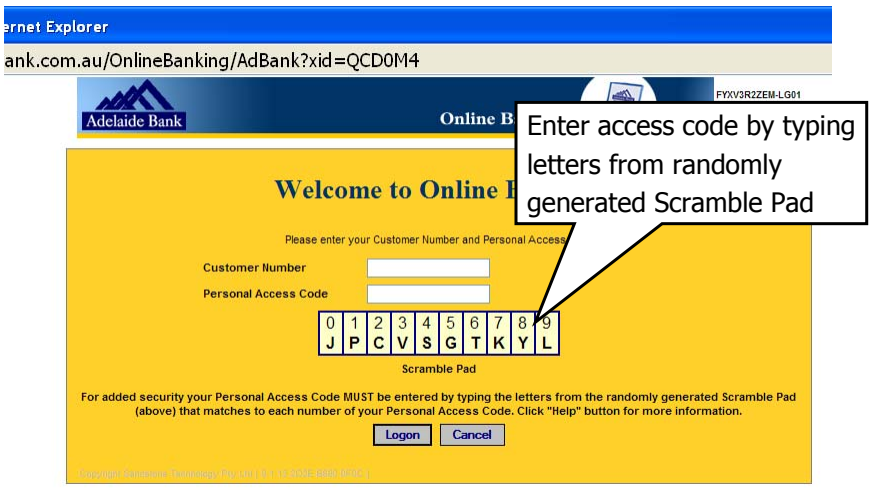
Defense #2: PassMark / SiteKey



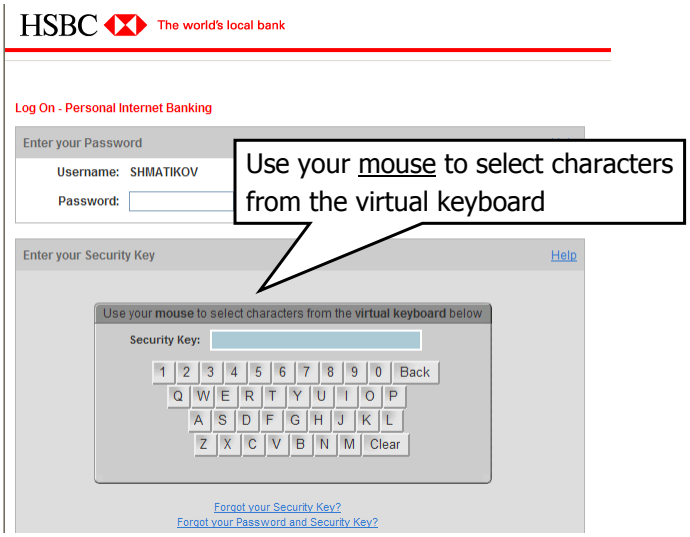
20

Defense #3: PIN Guard

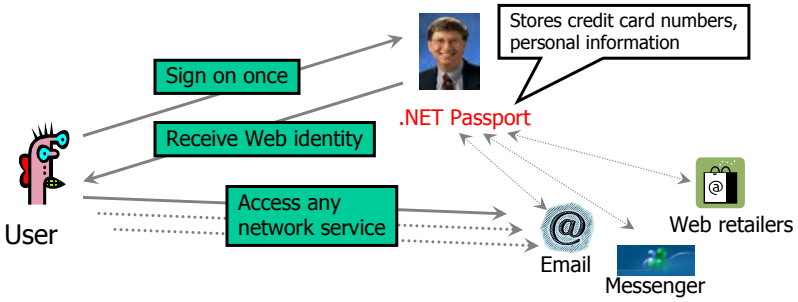
Defense #3A: Scramble Pad



Defense #4: Virtual Keyboard



Microsoft Passport



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

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

27