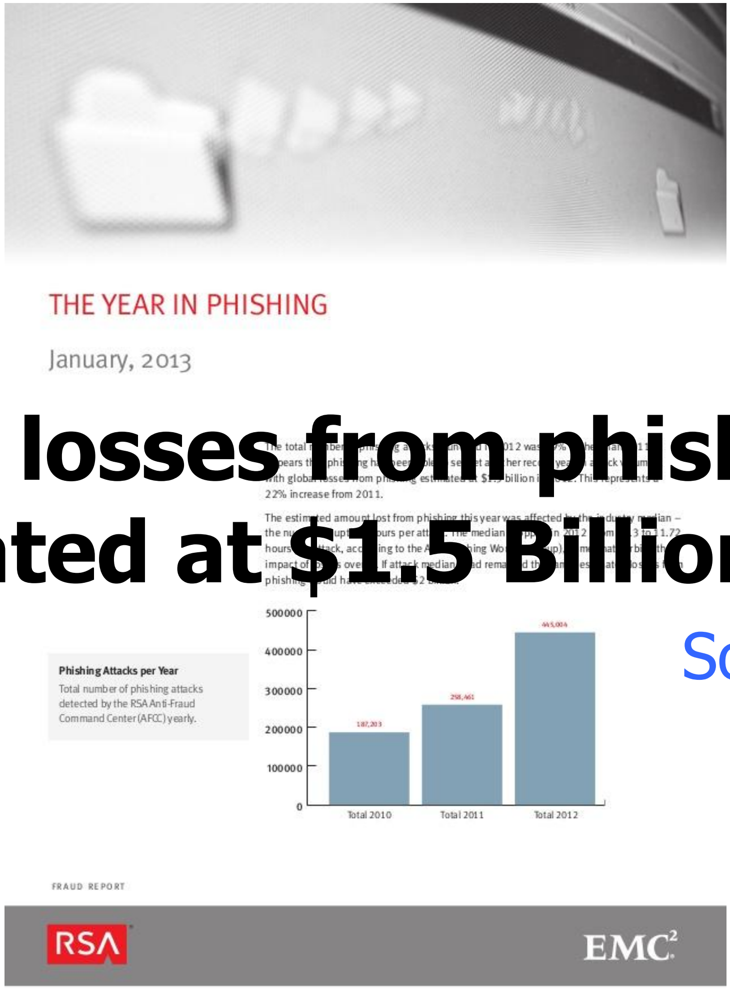
CS 361S

Phishing

Vitaly Shmatikov

$1,500,000,000



THE YEAR IN PHISHING

January, 2013

The total n[illegible]ber [illegible] phis[illegible]g a[illegible]cks [illegible]un[illegible]d i[illegible] 2012 was [illegible]9% [illegible]he[illegible] [illegible]an [illegible]11 [illegible]pears th[illegible] phis[illegible]ng ha[illegible] been [illegible]ble [illegible] se[illegible]t a[illegible]ther rec[illegible] yea[illegible] a[illegible]ck v[illegible]um[illegible] with global losses from phishing estimated at $1.5 billion i[illegible] 2012. This represents a 22% increase from 2011.

The estimated amount lost from phishing this year was affected by the industry median – the nu[illegible] [illegible]upt[illegible] [illegible]ours per att[illegible]. The median [illegible]pp[illegible] in 2012 [illegible]om [illegible]3 to 11.72 hours [illegible]ttack, acc[illegible]ing to the A[illegible]hing Wo[illegible]up), [illegible]me[illegible]at[illegible]r[illegible]bi[illegible] th[illegible] impact of [illegible]s over[illegible]. If attack median[illegible]ed rema[illegible]d th[illegible] [illegible]am[illegible] [illegible]es[illegible]at[illegible] los[illegible] from phishing [illegible]uld have exceeded $2 billion.

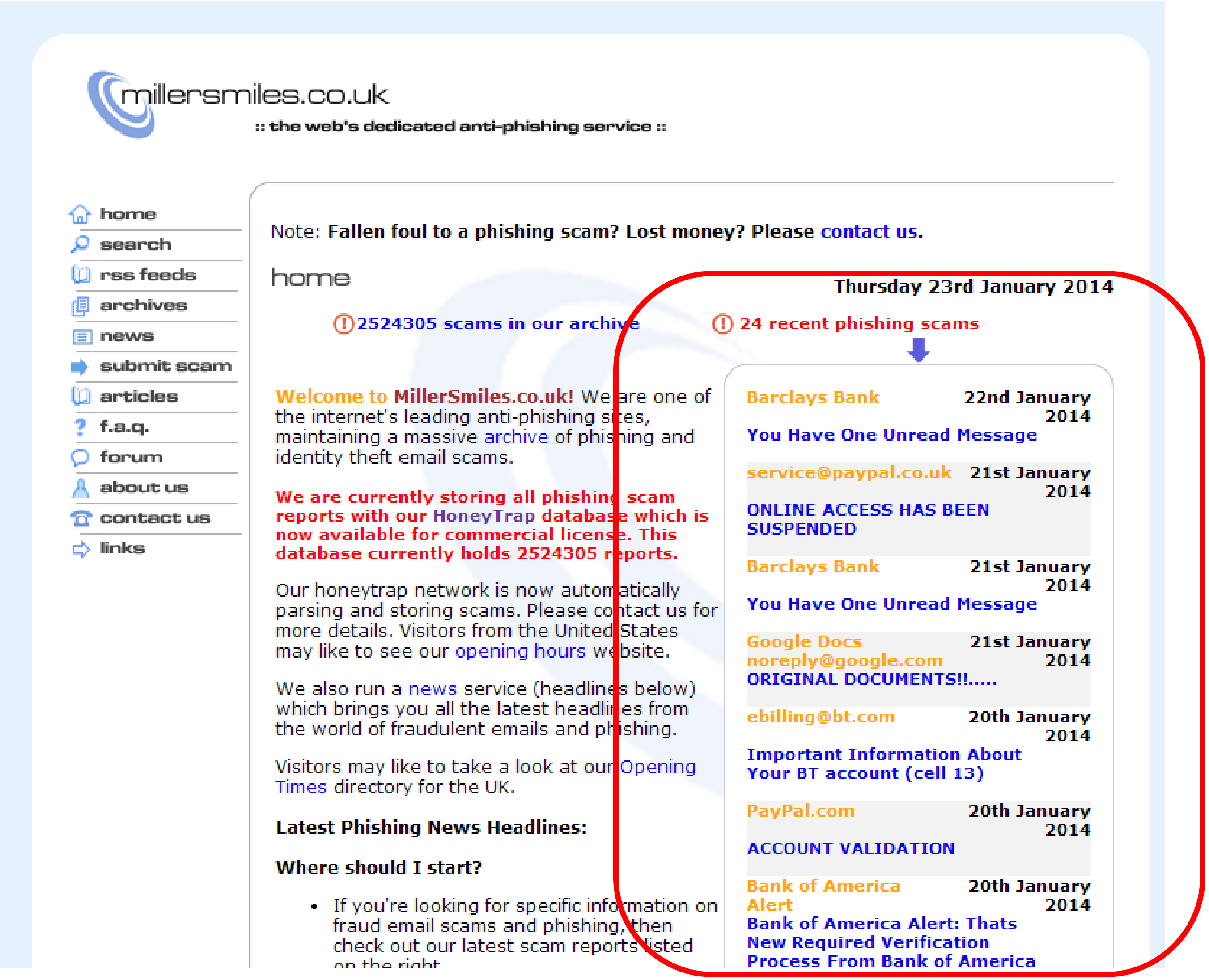
Phishing Attacks per Year

Total number of phishing attacks detected by the RSA Anti-Fraud Command Center (AFCC) yearly.

Global losses from phishing in 2012 estimated at $1.5 Billion

Source: RSA Fraud Report

MillerSmiles.co.uk



Note: **Fallen foul to a phishing scam? Lost money? Please contact us.**

home

Thursday 23rd January 2014

2524305 scams in our archive

24 recent phishing scams

Welcome to MillerSmiles.co.uk! We are one of the internet's leading anti-phishing sites, maintaining a massive archive of phishing and identity theft email scams.

We are currently storing all phishing scam reports with our HoneyTrap database which is now available for commercial license. This database currently holds 2524305 reports.

Our honeytrap network is now automatically parsing and storing scams. Please contact us for more details. Visitors from the United States may like to see our opening hours website.

We also run a news service (headlines below) which brings you all the latest headlines from the world of fraudulent emails and phishing.

Visitors may like to take a look at our Opening Times directory for the UK.

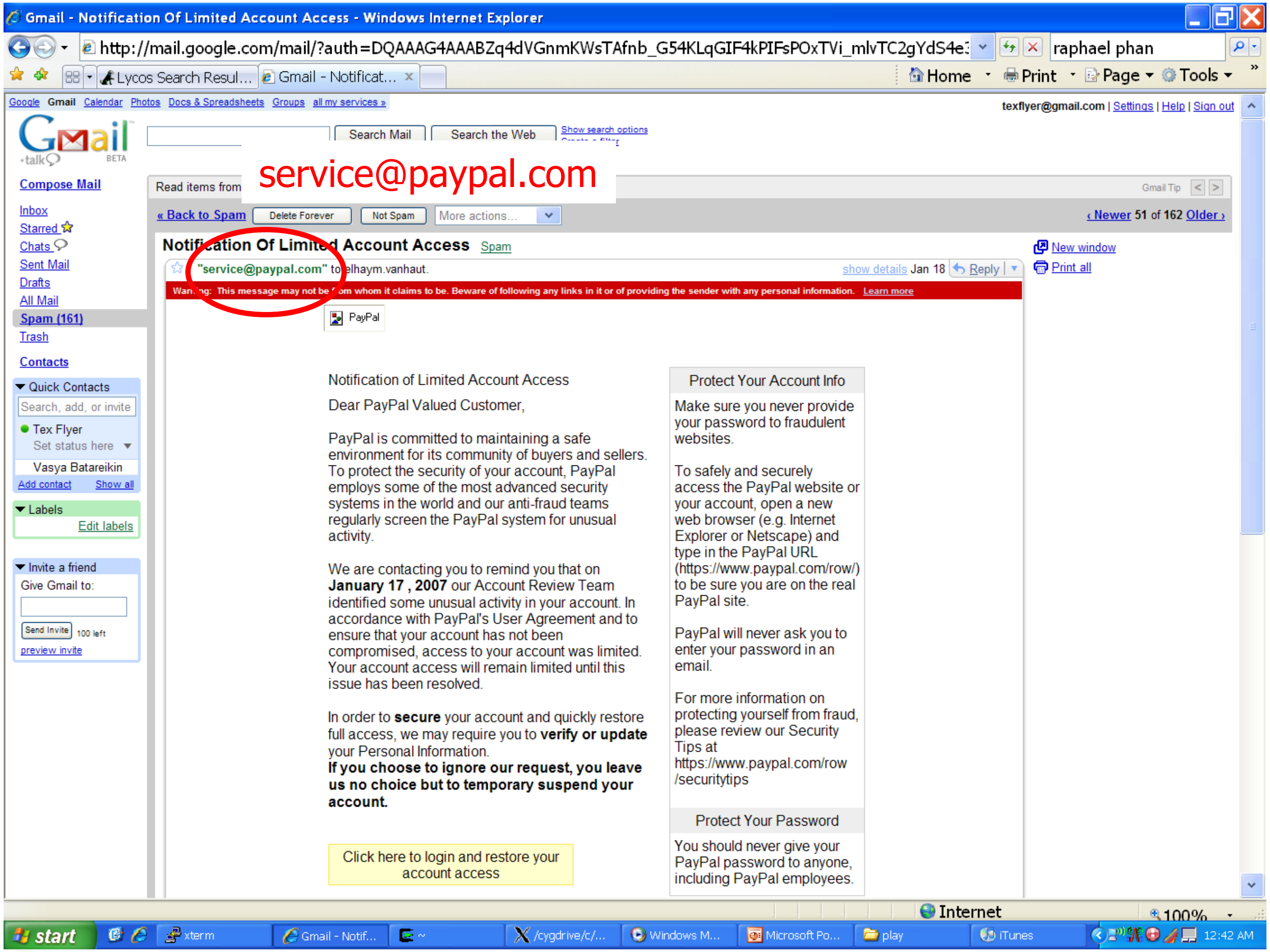
Latest Phishing News Headlines:

Where should I start?

- If you're looking for specific information on fraud email scams and phishing, then check out our latest scam reports listed on the right

Barclays Bank	**22nd January 2014**
You Have One Unread Message	
service@paypal.co.uk	**21st January 2014**
ONLINE ACCESS HAS BEEN SUSPENDED	
Barclays Bank	**21st January 2014**
You Have One Unread Message	
Google Docs noreply@google.com	**21st January 2014**
ORIGINAL DOCUMENTS!!.....	
ebilling@bt.com	**20th January 2014**
Important Information About Your BT account (cell 13)	
PayPal.com	**20th January 2014**
ACCOUNT VALIDATION	
Bank of America Alert	**20th January 2014**
Bank of America Alert: Thats New Required Verification Process From Bank of America	

A Snapshot of My Mailbox



service@paypal.com

Notification Of Limited Account Access

"service@paypal.com" to elhaym.vanhaut.

Warning: This message may not be from whom it claims to be. Beware of following any links in it or of providing the sender with any personal information. Learn more

PayPal

Notification of Limited Account Access

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 temporary suspend your account.**

Click here to login and restore your account access

Protect Your Account Info

Make sure you never provide your password to fraudulent websites.

To safely and securely access the PayPal website or your account, open a new web browser (e.g. Internet Explorer or Netscape) and type in the PayPal URL (https://www.paypal.com/row/) to be sure you are on the real PayPal site.

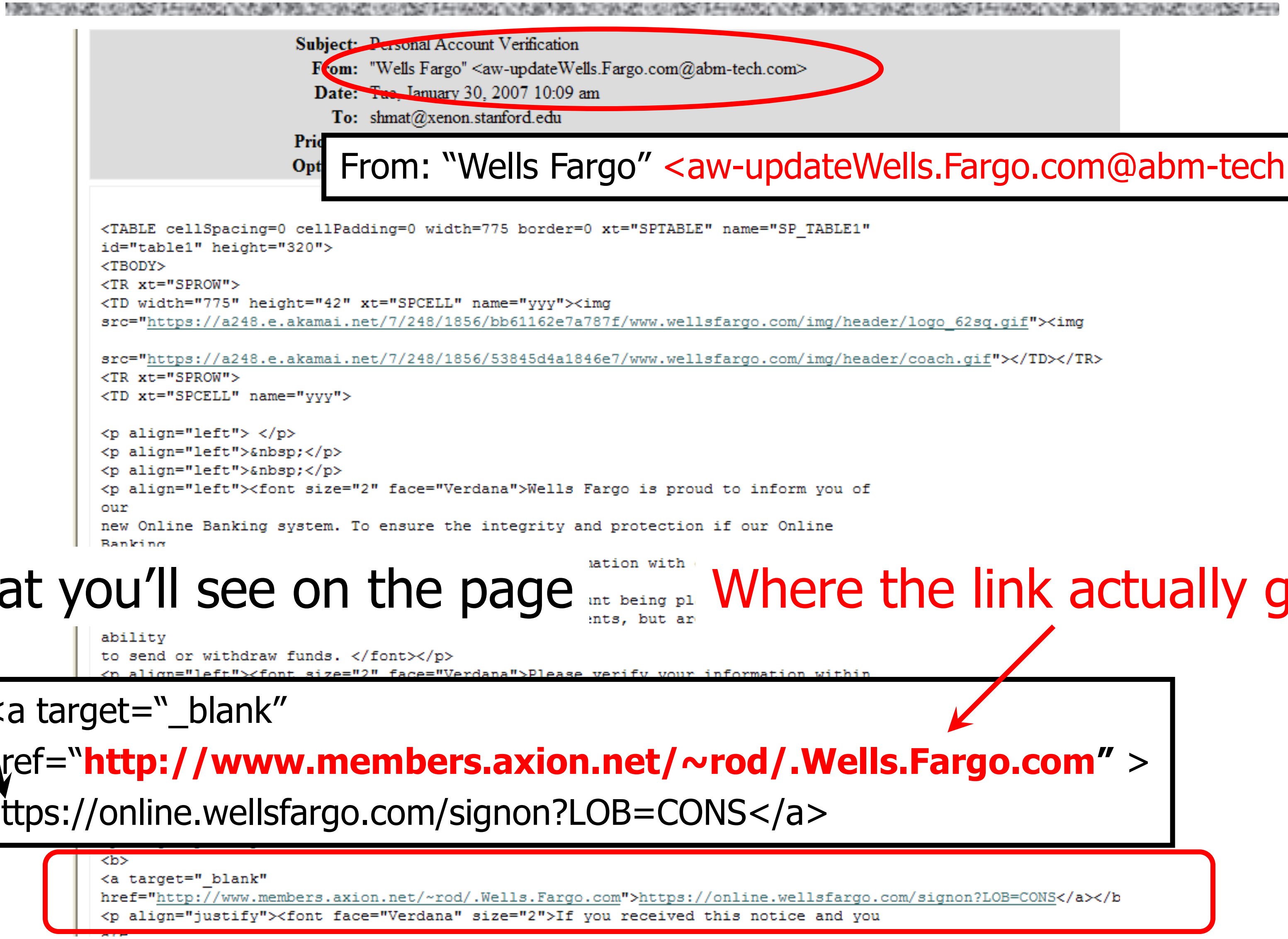
PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at https://www.paypal.com/row /securitytips

Protect Your Password

You should never give your PayPal password to anyone, including PayPal employees.

A Closer Look



Subject: Personal Account Verification
From: "Wells Fargo" <aw-updateWells.Fargo.com@abm-tech.com>
Date: Tue, January 30, 2007 10:09 am
To: shmat@xenon.stanford.edu
Pri
Opt

```
<TABLE cellSpacing=0 cellPadding=0 width=775 border=0 xt="SPTABLE" name="SP_TABLE1"
id="table1" height="320">
<TBODY>
<TR xt="SPROW">
<TD width="775" height="42" xt="SPCELL" name="yyy"><img
src="https://a248.e.akamai.net/7/248/1856/bb61162e7a787f/www.wellsfargo.com/img/header/logo_62sq.gif"><img

src="https://a248.e.akamai.net/7/248/1856/53845d4a1846e7/www.wellsfargo.com/img/header/coach.gif"></TD></TR>
<TR xt="SPROW">
<TD xt="SPCELL" name="yyy">

<p align="left"> </p>
<p align="left">&nbsp;</p>
<p align="left">&nbsp;</p>
<p align="left"><font size="2" face="Verdana">Wells Fargo is proud to inform you of
our
new Online Banking system. To ensure the integrity and protection if our Online
Banking
                                                    ation with

                                                    nt being pl
                                                    nts, but ar
ability
to send or withdraw funds. </font></p>
<p align="left"><font size="2" face="Verdana">Please verify your information within
```

```
<b>
<a target="_blank"
href="http://www.members.axion.net/~rod/.Wells.Fargo.com">https://online.wellsfargo.com/signon?LOB=CONS</a></b
<p align="justify"><font face="Verdana" size="2">If you received this notice and you
```

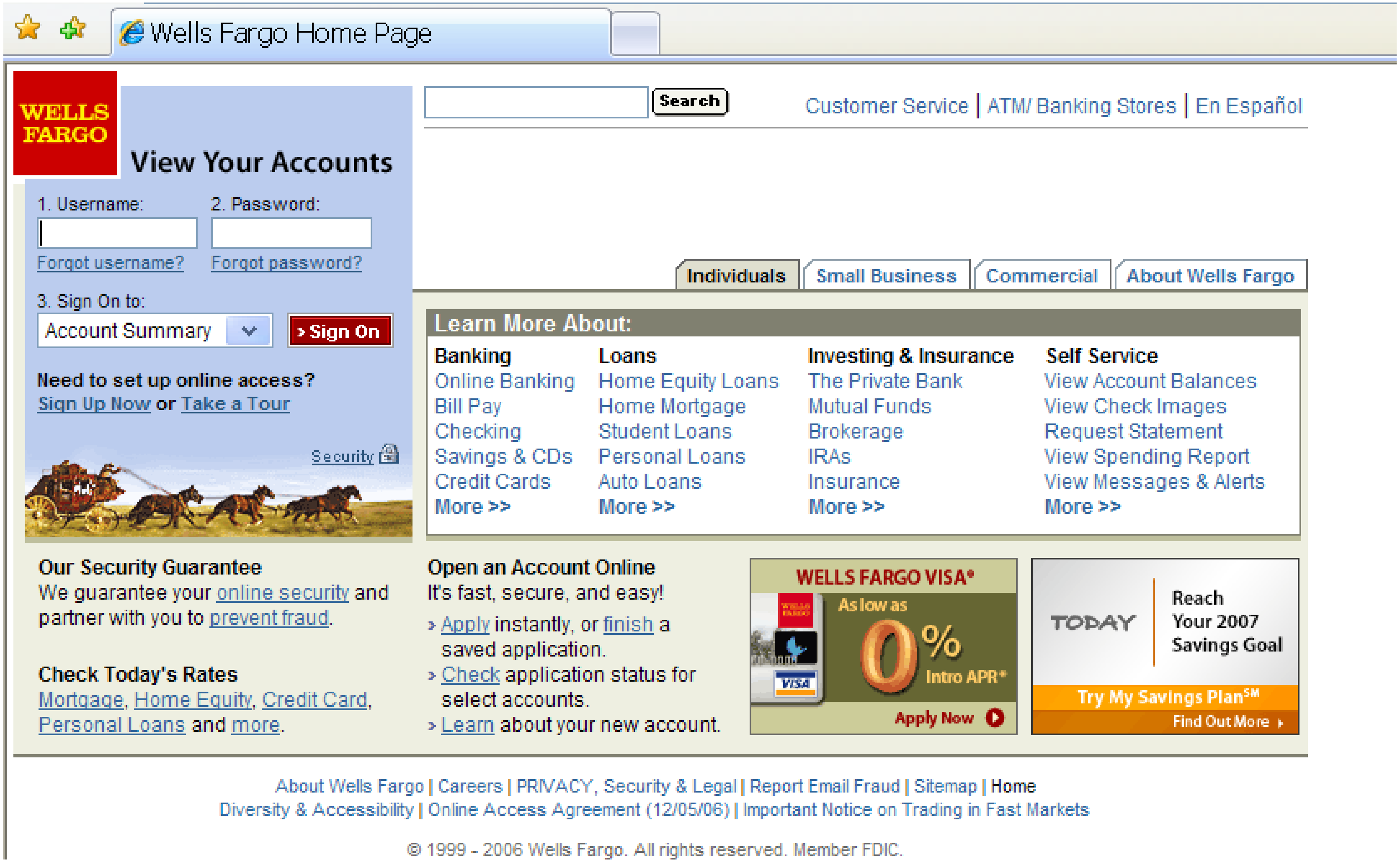
From: "Wells Fargo" <aw-updateWells.Fargo.com@abm-tech.com>

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</a>

And You End Up Here



Wells Fargo Home Page

WELLS FARGO

Search

Customer Service | ATM/ Banking Stores | En Español

View Your Accounts

1. Username:

2. Password:

Forgot username?

Forgot password?

3. Sign On to:

Account Summary

› Sign On

Need to set up online access?
Sign Up Now or Take a Tour

Security

Individuals | Small Business | Commercial | About Wells Fargo

Learn More About:

Banking	Loans	Investing & Insurance	Self Service
Online Banking	Home Equity Loans	The Private Bank	View Account Balances
Bill Pay	Home Mortgage	Mutual Funds	View Check Images
Checking	Student Loans	Brokerage	Request Statement
Savings & CDs	Personal Loans	IRAs	View Spending Report
Credit Cards	Auto Loans	Insurance	View Messages & Alerts
More >>	More >>	More >>	More >>

Our Security Guarantee
We guarantee your online security and partner with you to prevent fraud.

Check Today's Rates
Mortgage, Home Equity, Credit Card, Personal Loans and more.

Open an Account Online
It's fast, secure, and easy!

- › Apply instantly, or finish a saved application.
- › Check application status for select accounts.
- › Learn about your new account.

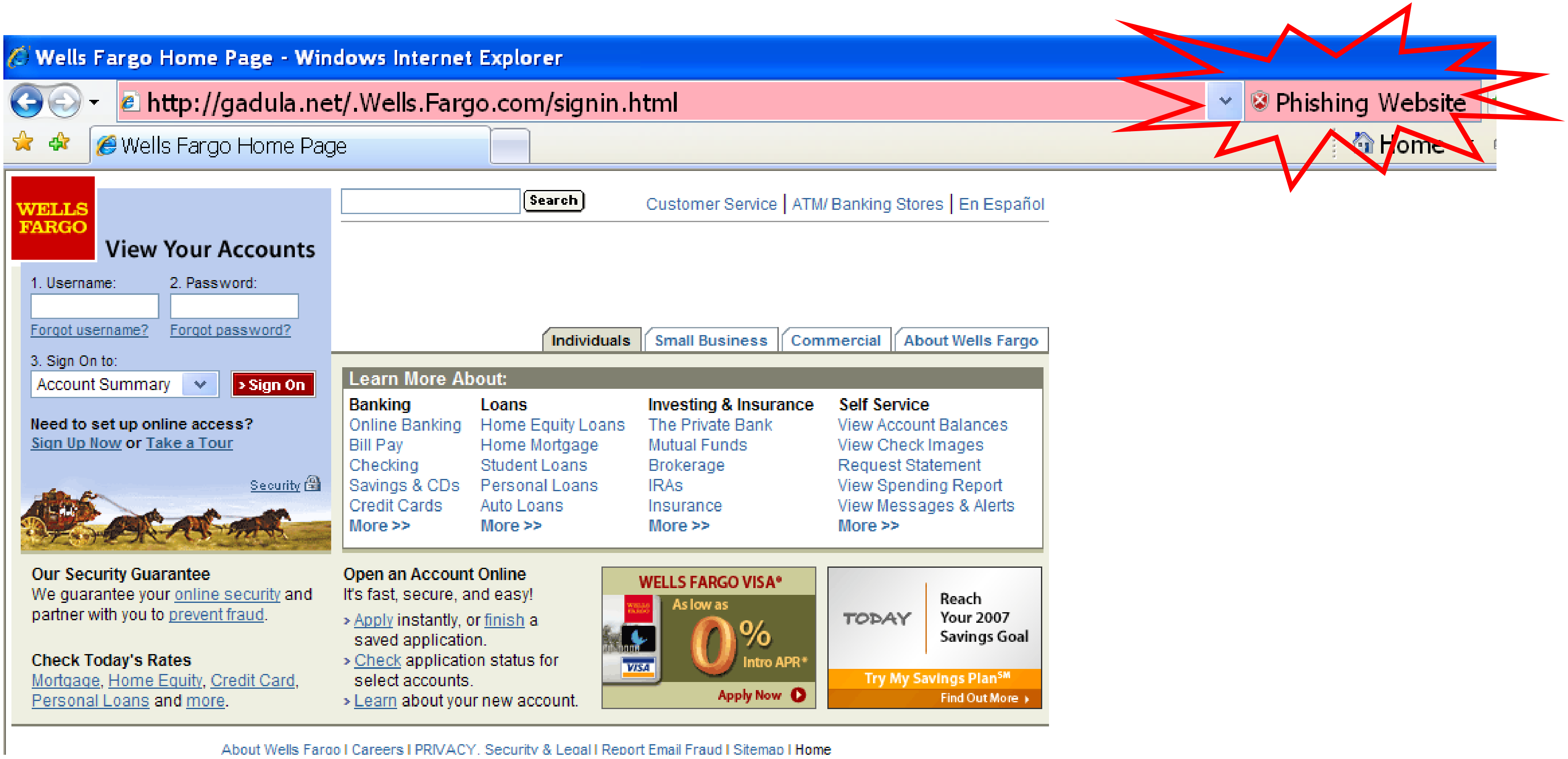
WELLS FARGO VISA®
As low as 0% Intro APR*
Apply Now

TODAY
Reach Your 2007 Savings Goal
Try My Savings Plan℠
Find Out More ›

About Wells Fargo | Careers | PRIVACY, Security & Legal | Report Email Fraud | Sitemap | Home
Diversity & Accessibility | Online Access Agreement (12/05/06) | Important Notice on Trading in Fast Markets

© 1999 - 2006 Wells Fargo. All rights reserved. Member FDIC.

Thank Goodness for IE ☺



Wells Fargo Home Page - Windows Internet Explorer

http://gadula.net/.Wells.Fargo.com/signin.html

Phishing Website

Wells Fargo Home Page

Home

WELLS FARGO

Search

Customer Service | ATM/ Banking Stores | En Español

View Your Accounts

1. Username:

2. Password:

Forgot username? Forgot password?

3. Sign On to: Account Summary

› Sign On

Need to set up online access?
Sign Up Now or Take a Tour

Security

Individuals | Small Business | Commercial | About Wells Fargo

Learn More About:

Banking
Online Banking
Bill Pay
Checking
Savings & CDs
Credit Cards
More >>

Loans
Home Equity Loans
Home Mortgage
Student Loans
Personal Loans
Auto Loans
More >>

Investing & Insurance
The Private Bank
Mutual Funds
Brokerage
IRAs
Insurance
More >>

Self Service
View Account Balances
View Check Images
Request Statement
View Spending Report
View Messages & Alerts
More >>

Our Security Guarantee
We guarantee your online security and partner with you to prevent fraud.

Check Today's Rates
Mortgage, Home Equity, Credit Card, Personal Loans and more.

Open an Account Online
It's fast, secure, and easy!

› Apply instantly, or finish a saved application.
› Check application status for select accounts.
› Learn about your new account.

WELLS FARGO VISA®
As low as 0% Intro APR*
Apply Now

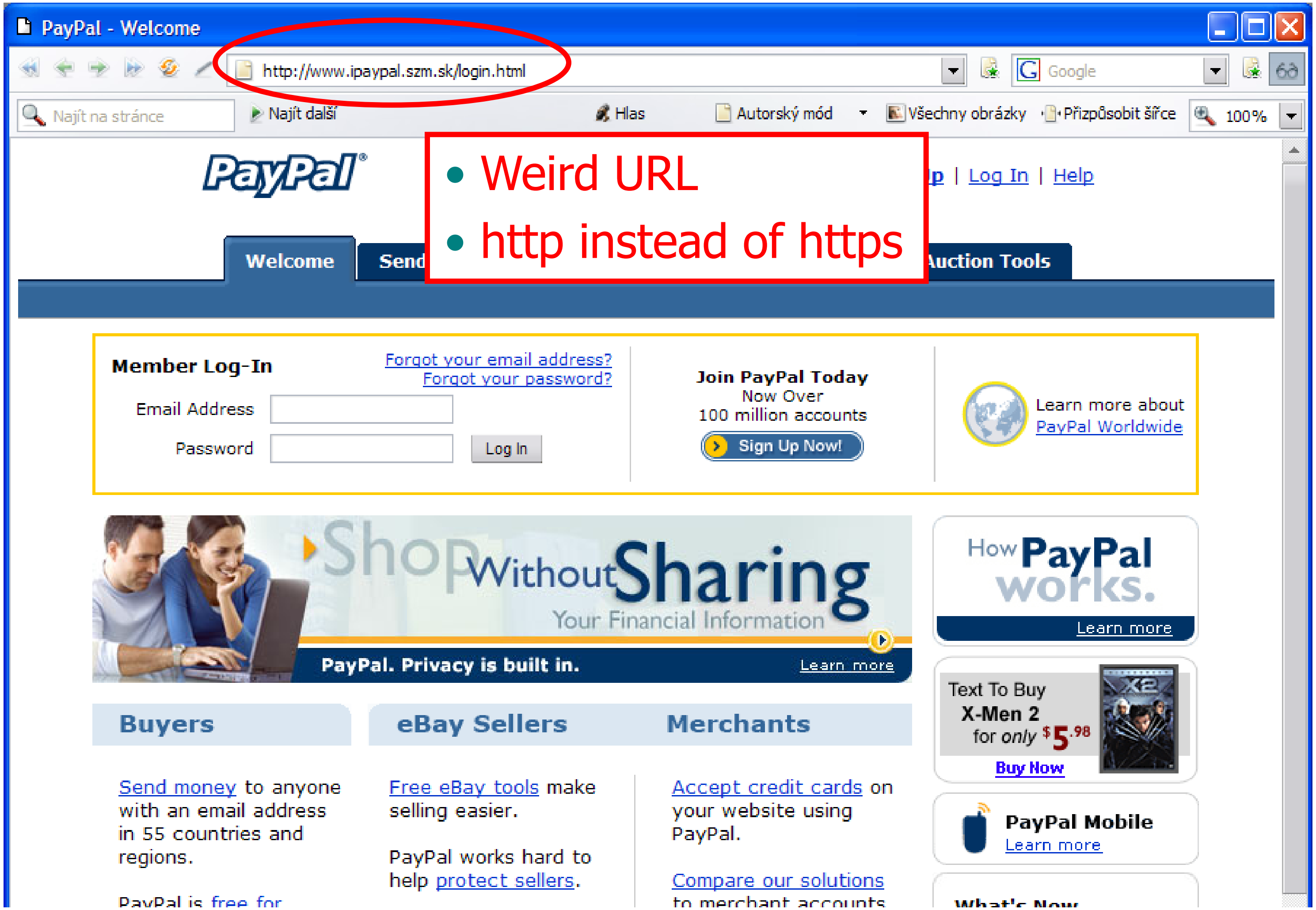
TODAY
Reach Your 2007 Savings Goal
Try My Savings Plan℠
Find Out More ›

About Wells Fargo | Careers | PRIVACY, Security & Legal | Report Email Fraud | Sitemap | Home

Typical Properties of Spoofed Sites

- Show logos found on the honest site
  - Copied image files or links to the honest site
- Have suspicious URLs
- Ask for user input
  - Debit card number, SSN, mother’s maiden name, …
- HTML copied from the honest site
  - May contain links to the honest site
  - May contain revealing mistakes
- Short-lived (cannot effectively blacklist)
  - Often hosted on compromised zombie machines

A Typical Phishing Page



- Weird URL
- http instead of https

PayPal - Welcome

http://www.ipaypal.szm.sk/login.html

Member Log-In

Forgot your email address?
Forgot your password?

Email Address

Password

Join PayPal Today
Now Over
100 million accounts

Learn more about PayPal Worldwide

Text To Buy
X-Men 2
for only $5.98
Buy Now

PayPal Mobile
Learn more

What's New

Buyers

Send money to anyone with an email address in 55 countries and regions.

PayPal is free for

eBay Sellers

Free eBay tools make selling easier.

PayPal works hard to help protect sellers.

Merchants

Accept credit cards on your website using PayPal.

Compare our solutions to merchant accounts

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 address typed by victim (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

```
 <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 *

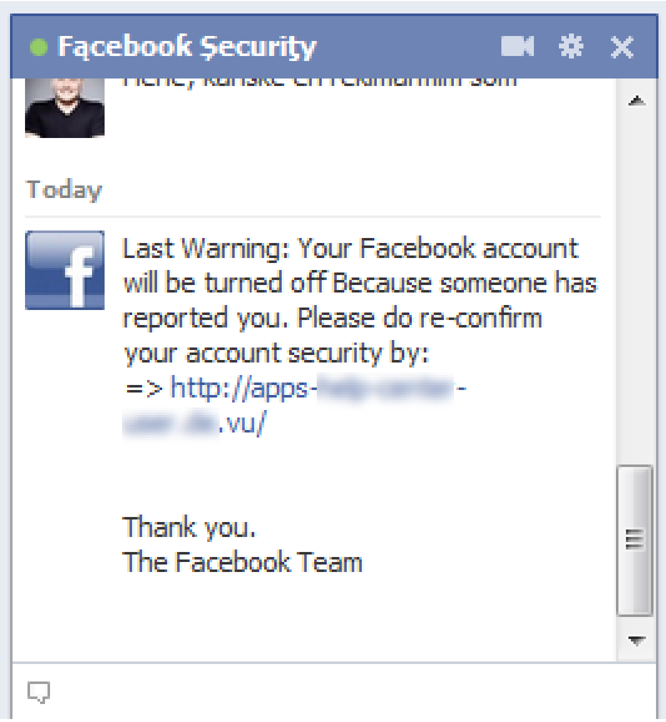
Social Engineering Tricks

- 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 relationships
  - Spoof an email from a Facebook friend
  - In a West Point experiment, 80% of cadets were deceived into following an embedded link regarding their grade report from a fictitious colonel

Facebook Phishing (January 2012)

[redacted] http://www.securelist.com/en/blog/208193325/Facebook_Security_Phishing_Attack_In_The_Wild

- Attack steals Facebook credentials
- Changes profile picture of compromised account to f and the name to “Fąceboƙ Şecuriţy”
  - Notice anything?
- Sends a message to all contacts:



Fąceboƙ Şecuriţy

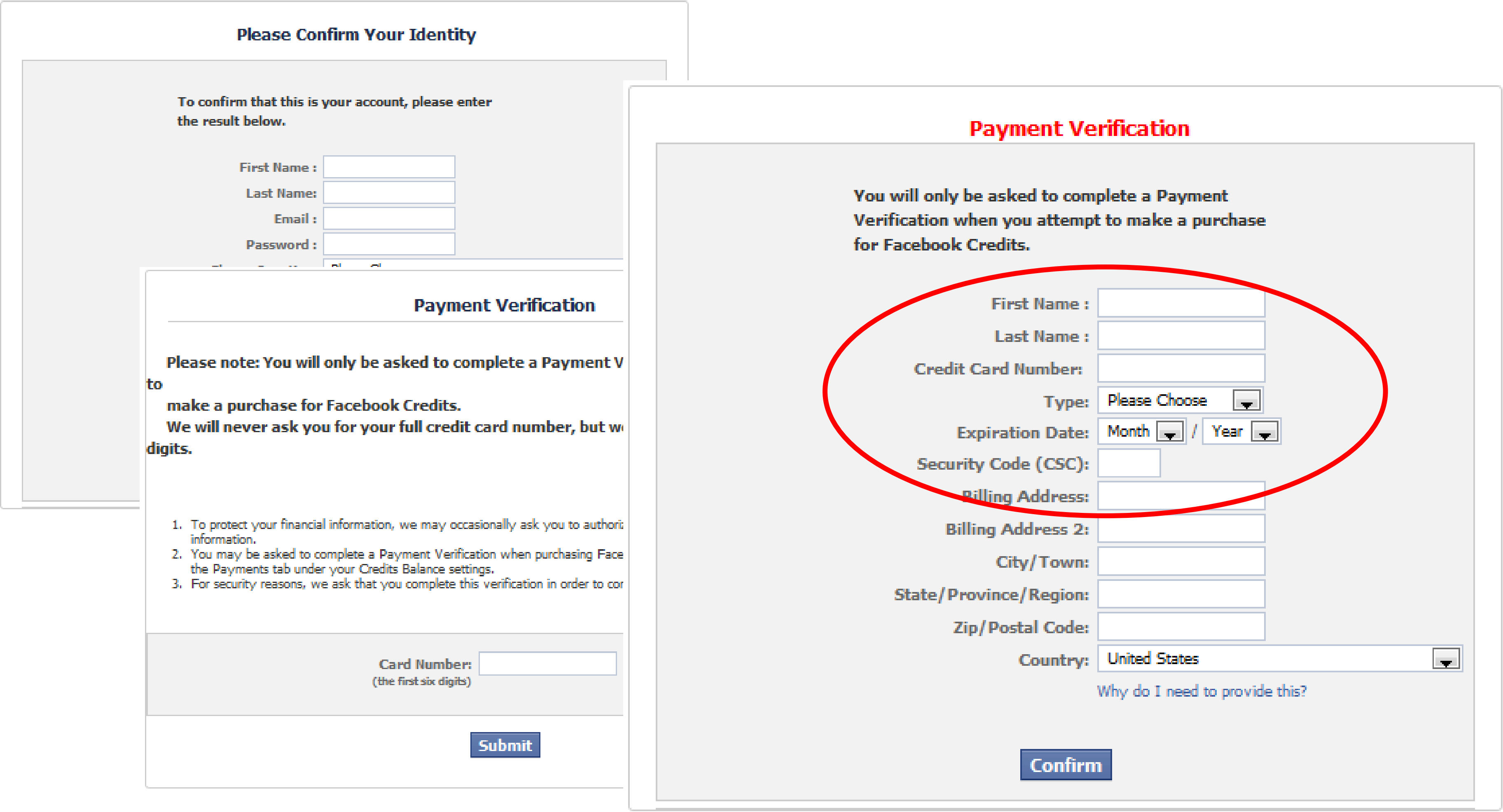
Today

Last Warning: Your Facebook account will be turned off Because someone has reported you. Please do re-confirm your account security by:
=> http://apps-[redacted]-[redacted].vu/

Thank you.
The Facebook Team

“Payment Verification”

[redacted] http://www.securelist.com/en/blog/208193325/Facebook_Security_Phishing_Attack_In_The_Wild



Please Confirm Your Identity

To confirm that this is your account, please enter the result below.

First Name :

Last Name:

Email :

Password :

Payment Verification

Please note: You will only be asked to complete a Payment V to make a purchase for Facebook Credits.

We will never ask you for your full credit card number, but w digits.

1. To protect your financial information, we may occasionally ask you to authori information.
2. You may be asked to complete a Payment Verification when purchasing Face the Payments tab under your Credits Balance settings.
3. For security reasons, we ask that you complete this verification in order to co

Card Number:
(the first six digits)

Submit

Payment Verification

You will only be asked to complete a Payment Verification when you attempt to make a purchase for Facebook Credits.

First Name :

Last Name :

Credit Card Number:

Type: Please Choose

Expiration Date: Month / Year

Security Code (CSC):

Billing Address:

Billing Address 2:

City/Town:

State/Province/Region:

Zip/Postal Code:

Country: United States

Why do I need to provide this?

Confirm

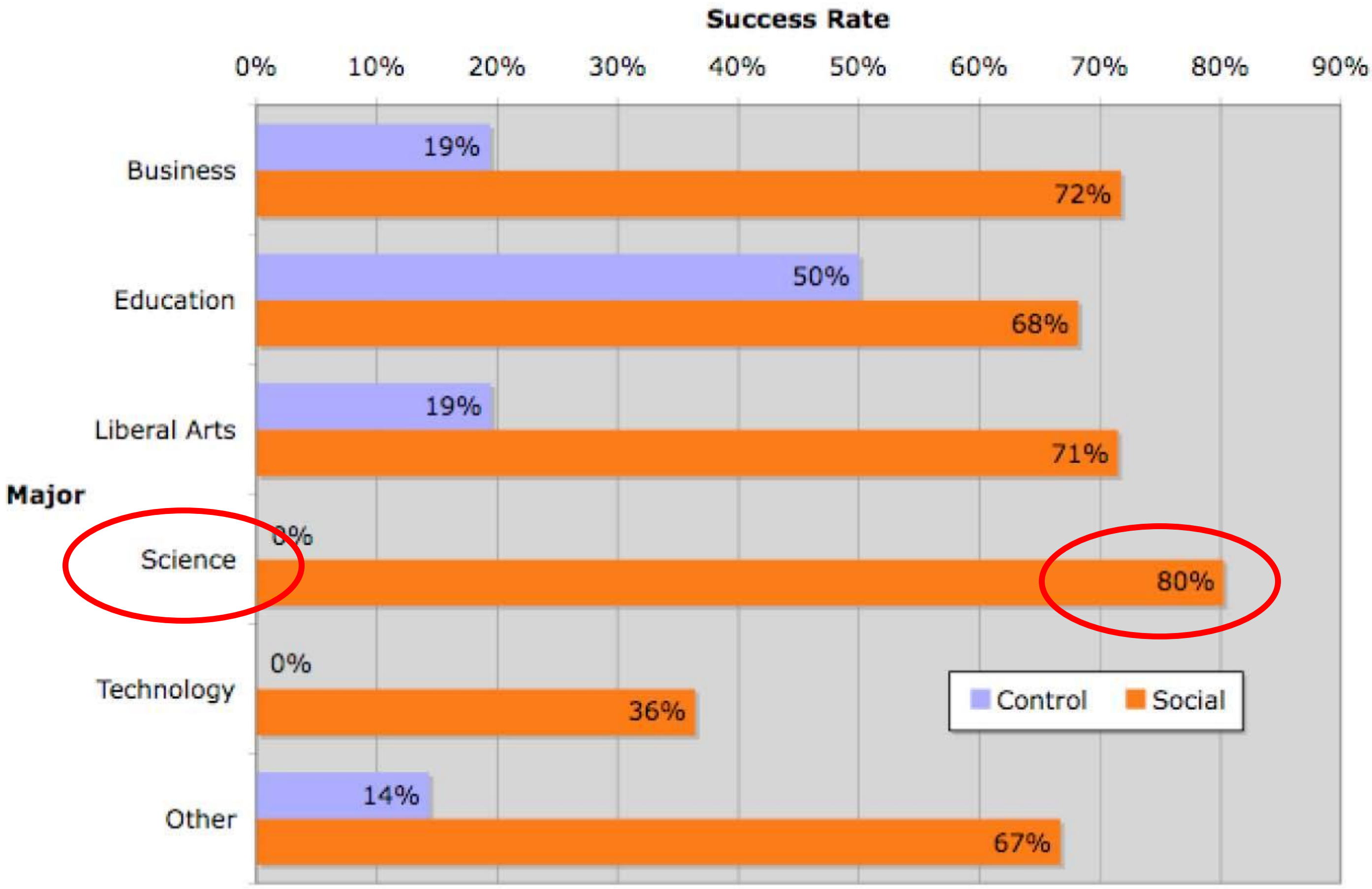
Experiments at Indiana U. (2006)

[Jagatic et al.]

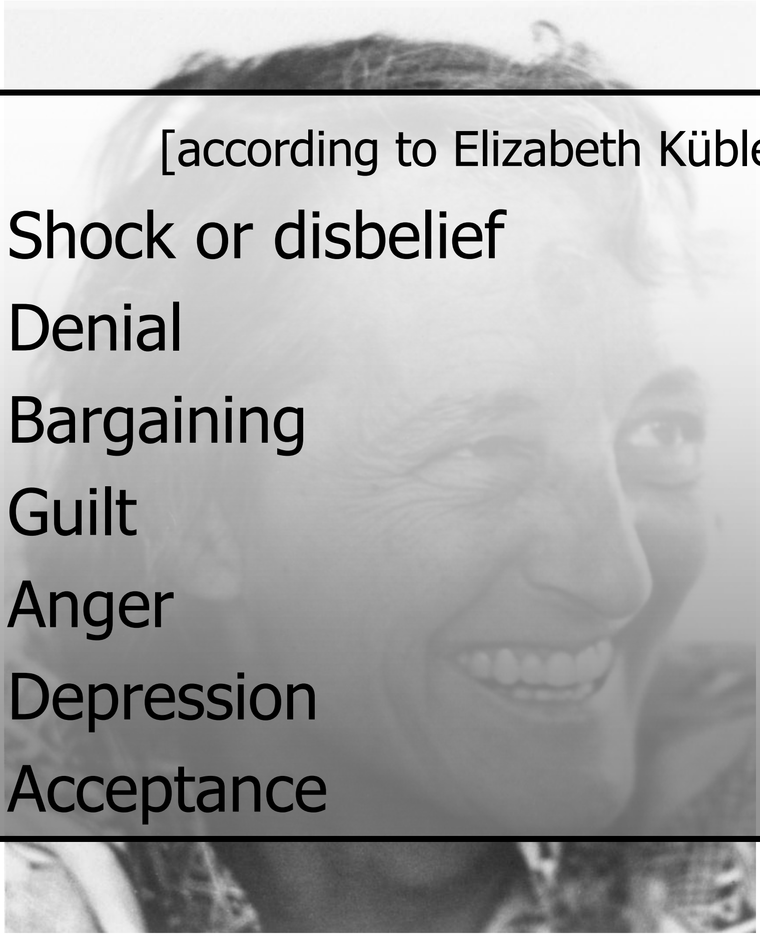
- Reconstructed the social network by crawling sites like Facebook, MySpace, LinkedIn
- Sent 921 Indiana University students a spoofed email that appeared to come from their friend
- Email redirected to a spoofed site inviting the user to enter his/her secure university credentials
  - Domain name clearly distinct from indiana.edu
- 72% of students 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?

[Jagatic et al.]



Seven Stages of Grief



[according to Elizabeth Kübler-Ross]

- Shock or disbelief
- Denial
- Bargaining
- Guilt
- Anger
- Depression
- Acceptance

Victims’ Reactions (1)

[Jagatic et al.]

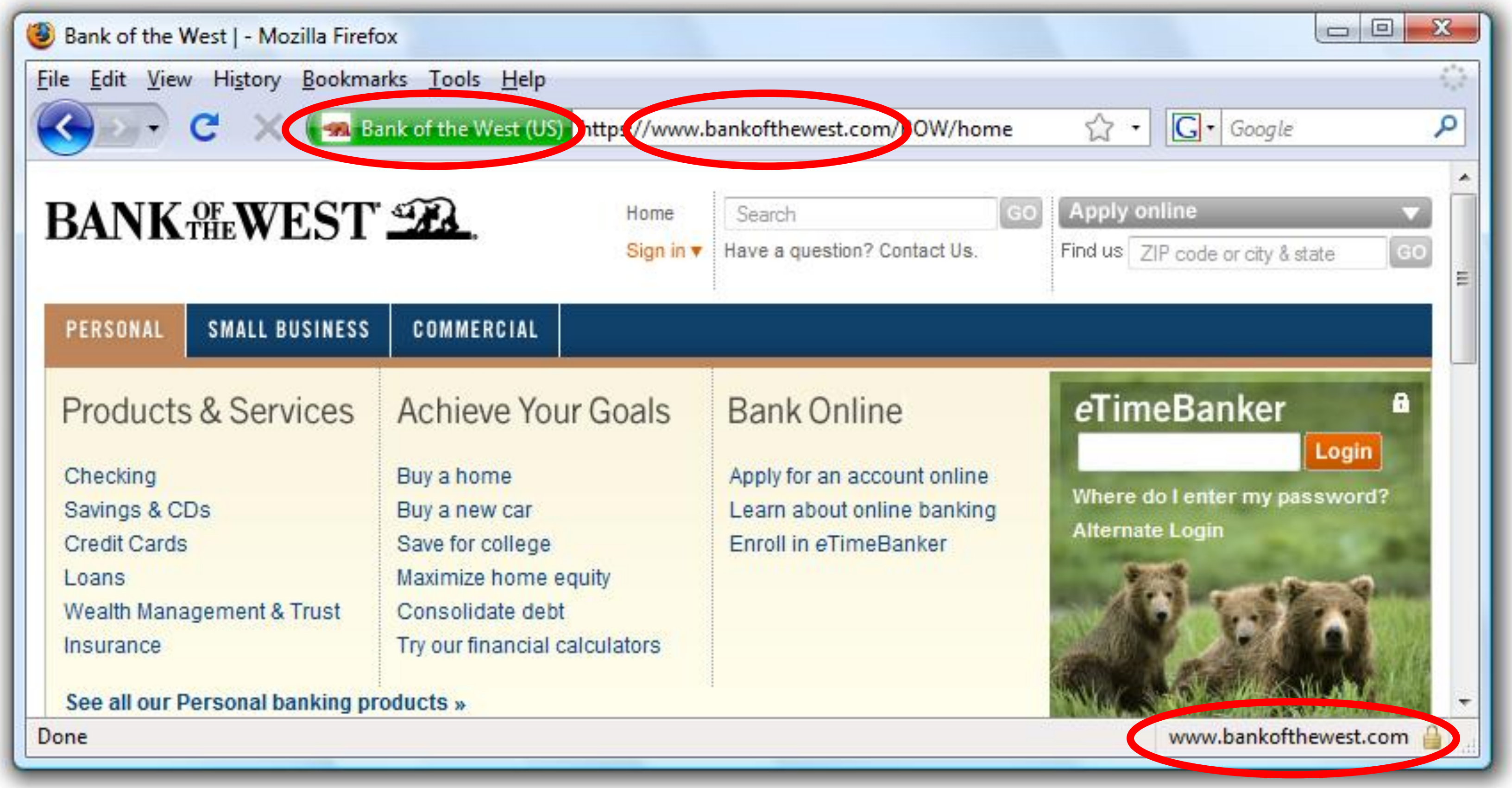
- Anger
  - Subjects called the experiment unethical, inappropriate, illegal, unprofessional, fraudulent, self-serving, useless
  - They called for the researchers conducting the study to be fired, prosecuted, expelled, or reprimanded
- Denial
  - No posted comments included an admission that the writer 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)

[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

Safe to Type Your Password?



Bank of the West | - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Bank of the West (US) https://www.bankofthewest.com/BOW/home

BANK OF THE WEST

Home

Sign in ▾

Search GO

Have a question? Contact Us.

Apply online ▾

Find us ZIP code or city & state GO

PERSONAL SMALL BUSINESS COMMERCIAL

Products & Services

- Checking
- Savings & CDs
- Credit Cards
- Loans
- Wealth Management & Trust
- Insurance

Achieve Your Goals

- Buy a home
- Buy a new car
- Save for college
- Maximize home equity
- Consolidate debt
- Try our financial calculators

Bank Online

- Apply for an account online
- Learn about online banking
- Enroll in eTimeBanker

eTimeBanker

Login

Where do I enter my password?

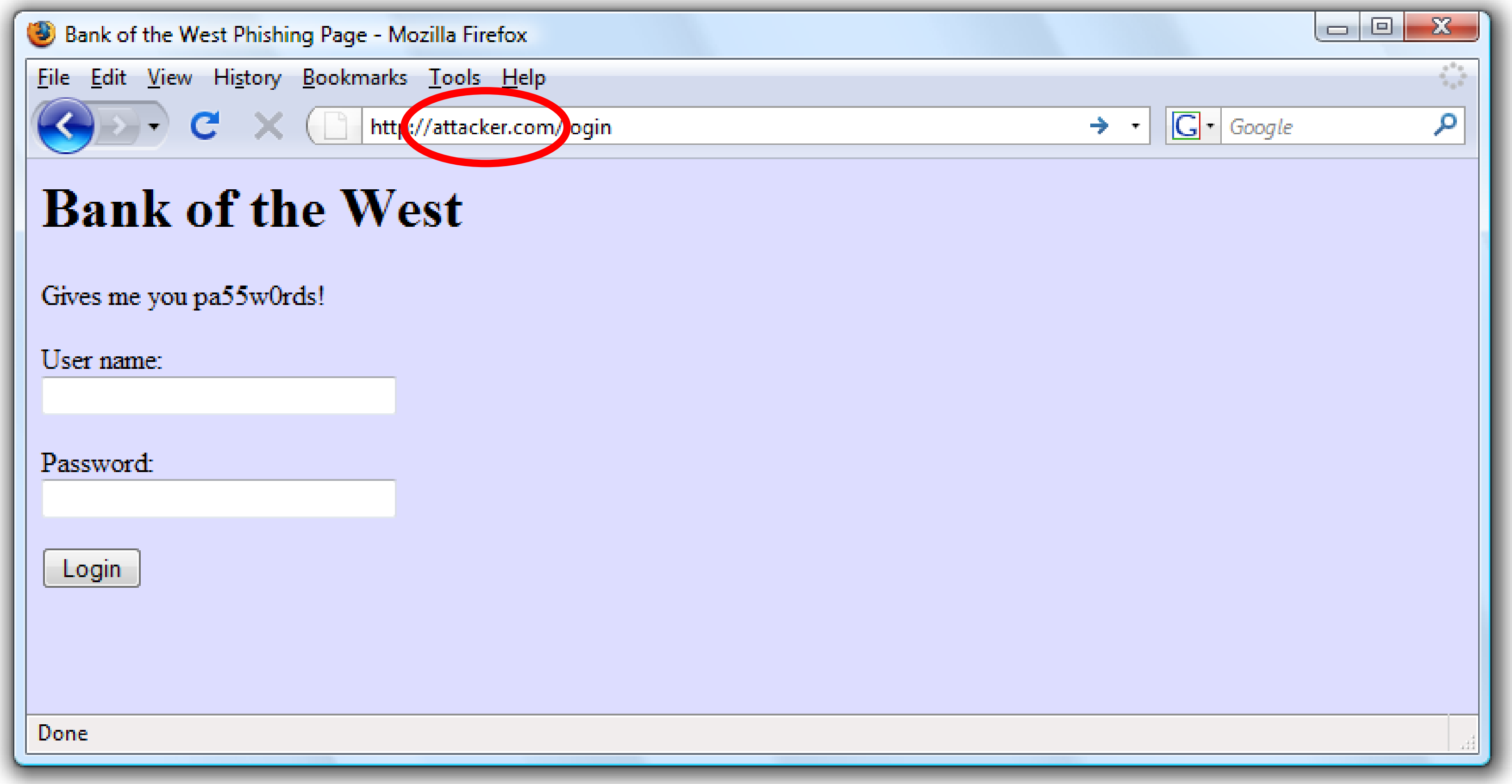
Alternate Login

See all our Personal banking products »

Done

www.bankofthewest.com

Safe to Type Your Password?



Bank of the West Phishing Page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://attacker.com/login
Google

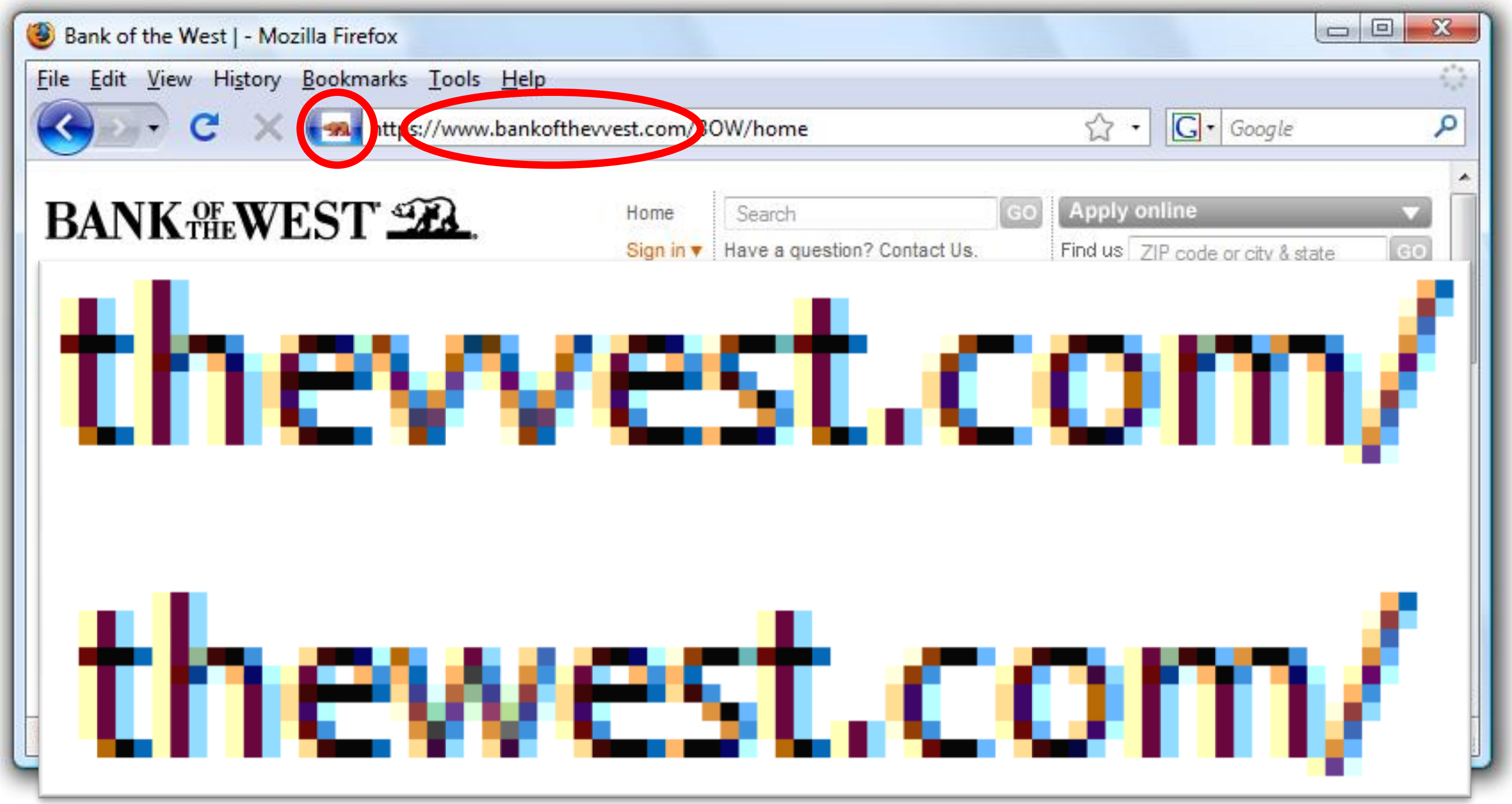
Bank of the West

Gives me you pa55w0rds!

User name:

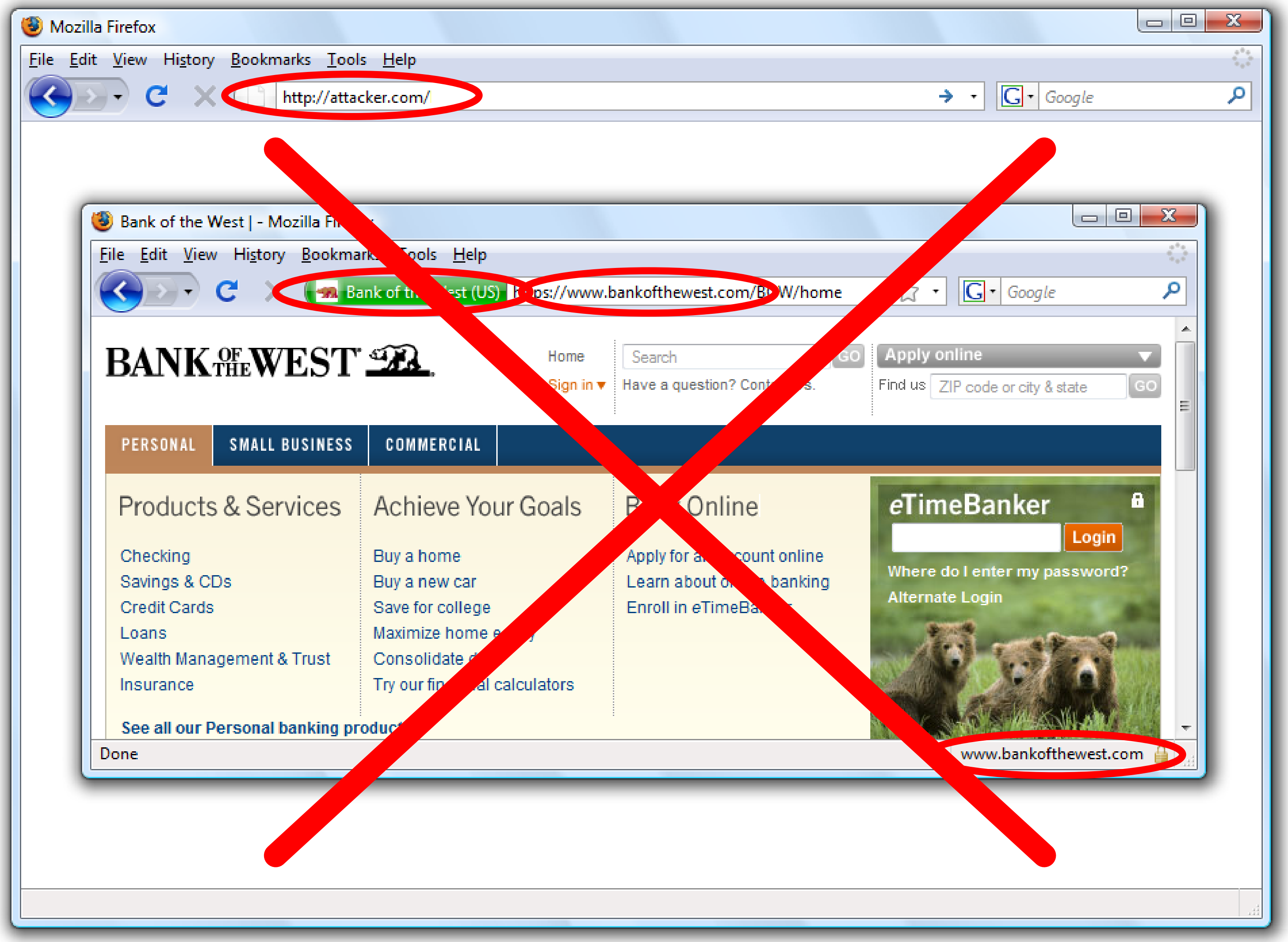
Password:

Safe to Type Your Password?

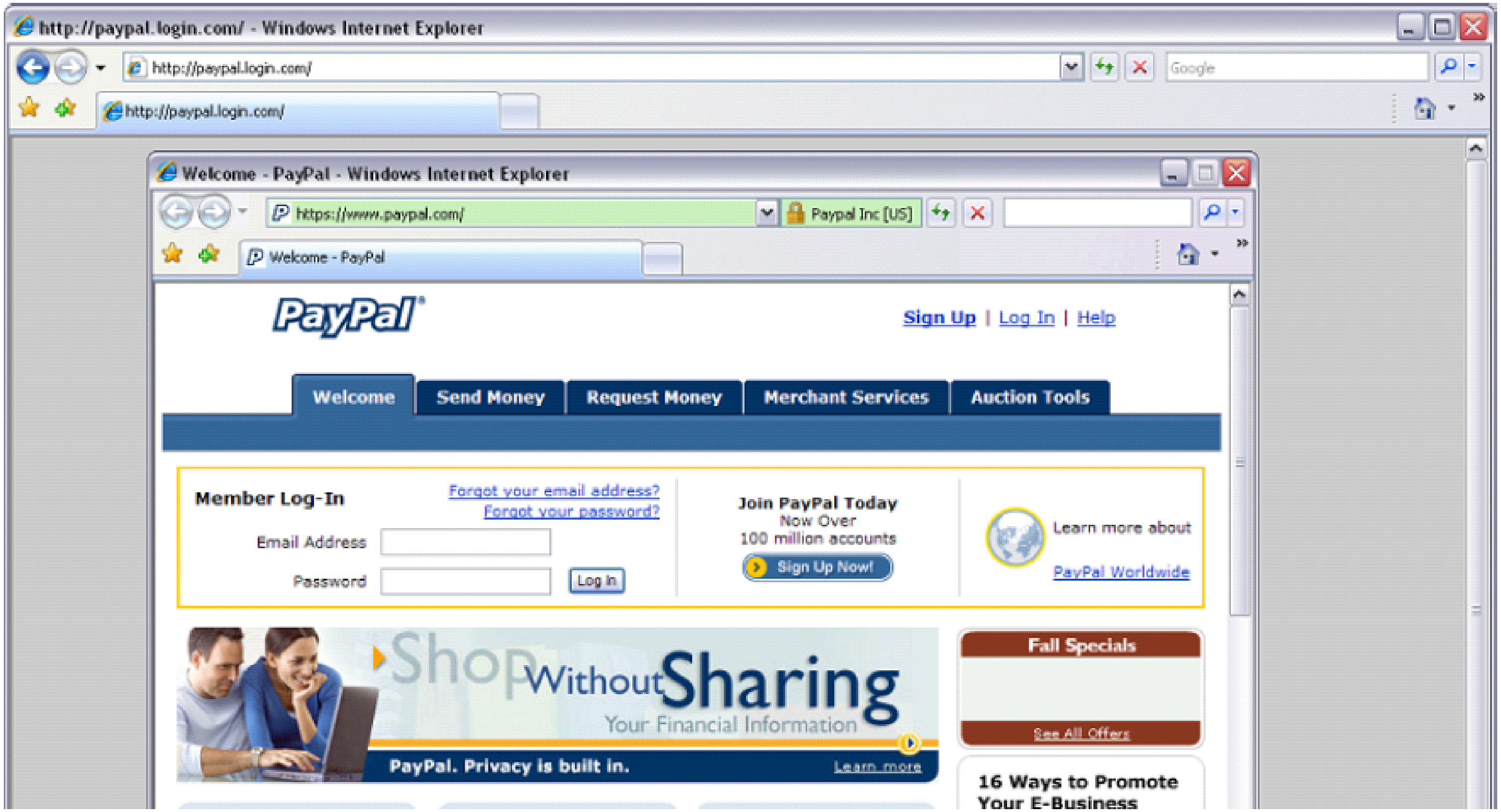


Bank of the West | - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.bankofthevvest.com/BOW/home
Google
BANK OF THE WEST
Home
Sign in ▾
Search
GO
Have a question? Contact Us.
Apply online
Find us
ZIP code or city & state
GO
thevvest.com/
thewest.com/

Safe to Type Your Password?

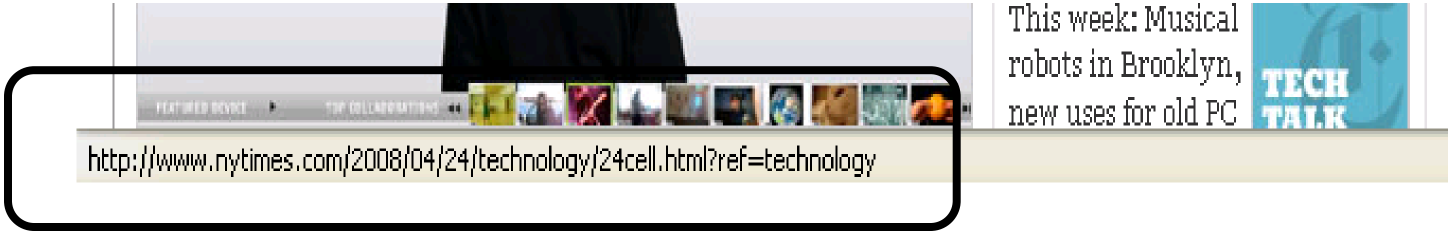


Picture-in-Picture Attacks



Trained users are more likely to fall victim to this!

Status Bar Is Trivially Spoofable

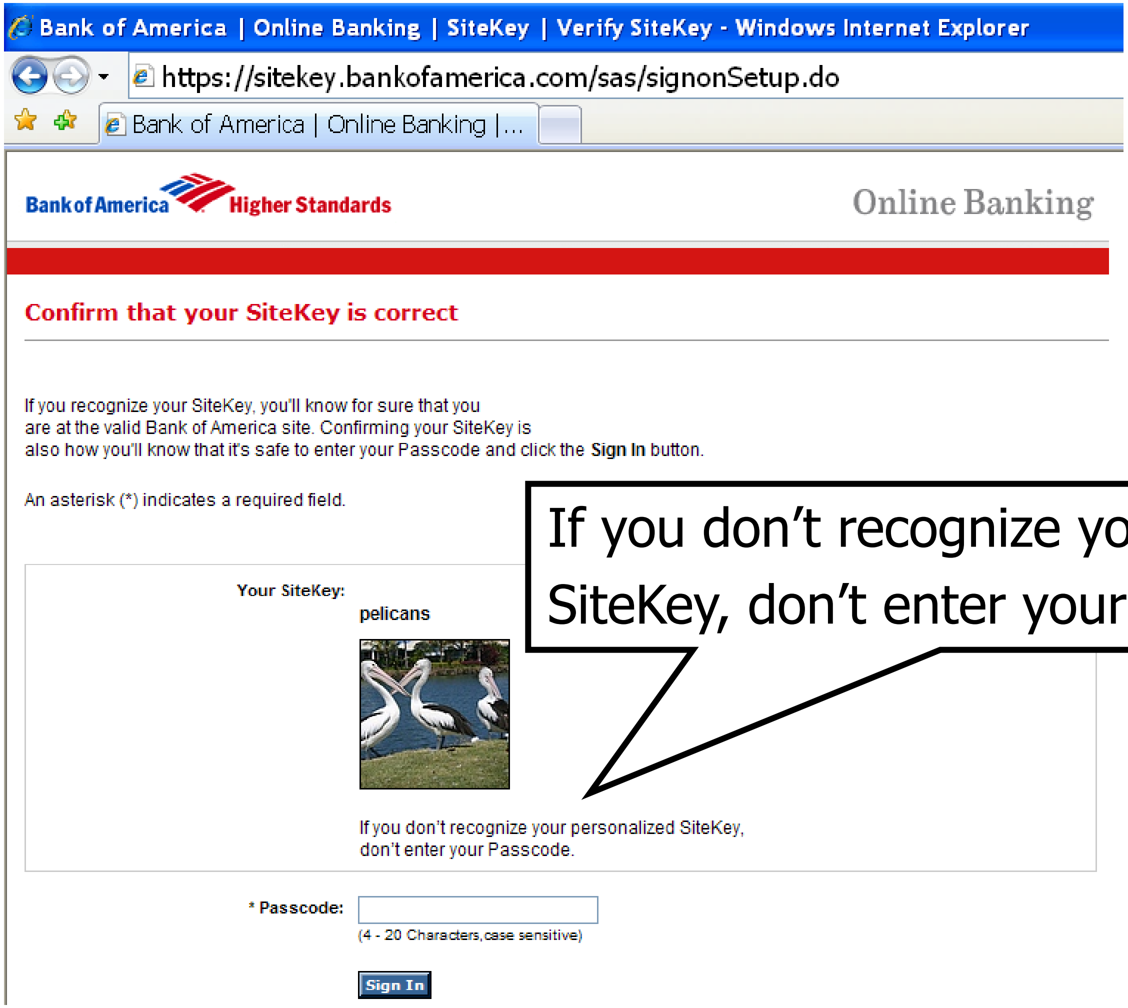


http://www.nytimes.com/2008/04/24/technology/24cell.html?ref=technology

This week: Musical robots in Brooklyn, new uses for old PC

```
<a href=“http://www.paypal.com/”
  onclick=“this.href = ‘http://www.evil.com/’;”>
  PayPal</a>
```

Site Defense #1: PassMark / SiteKey



Bank of America | Online Banking | SiteKey | Verify SiteKey - Windows Internet Explorer
https://sitekey.bankofamerica.com/sas/signonSetup.do
Bank of America | Online Banking | ...
Bank of America Higher Standards
Online Banking

Confirm that your SiteKey is correct

If you recognize your SiteKey, you'll know for sure that you are at the valid Bank of America site. Confirming your SiteKey is also how you'll know that it's safe to enter your Passcode and click the **Sign In** button.

An asterisk (*) indicates a required field.

Your SiteKey: pelicans

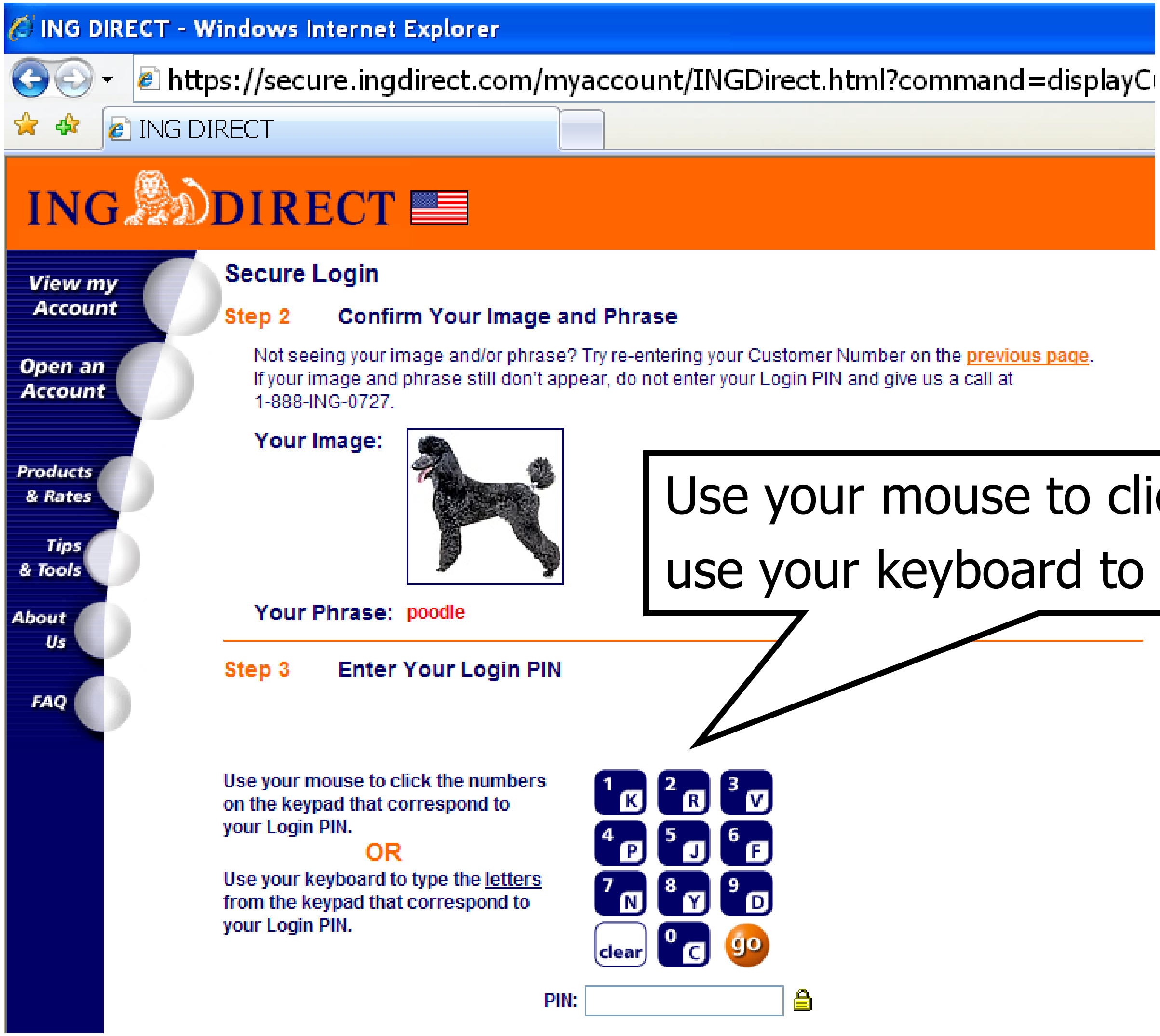
If you don't recognize your personalized SiteKey, don't enter your Passcode.

* Passcode:

(4 - 20 Characters, case sensitive)

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

Site Defense #2: PIN Guard



ING DIRECT - Windows Internet Explorer
https://secure.ingdirect.com/myaccount/INGDirect.html?command=displayC
ING DIRECT
ING DIRECT
View my Account
Open an Account
Products & Rates
Tips & Tools
About Us
FAQ

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.

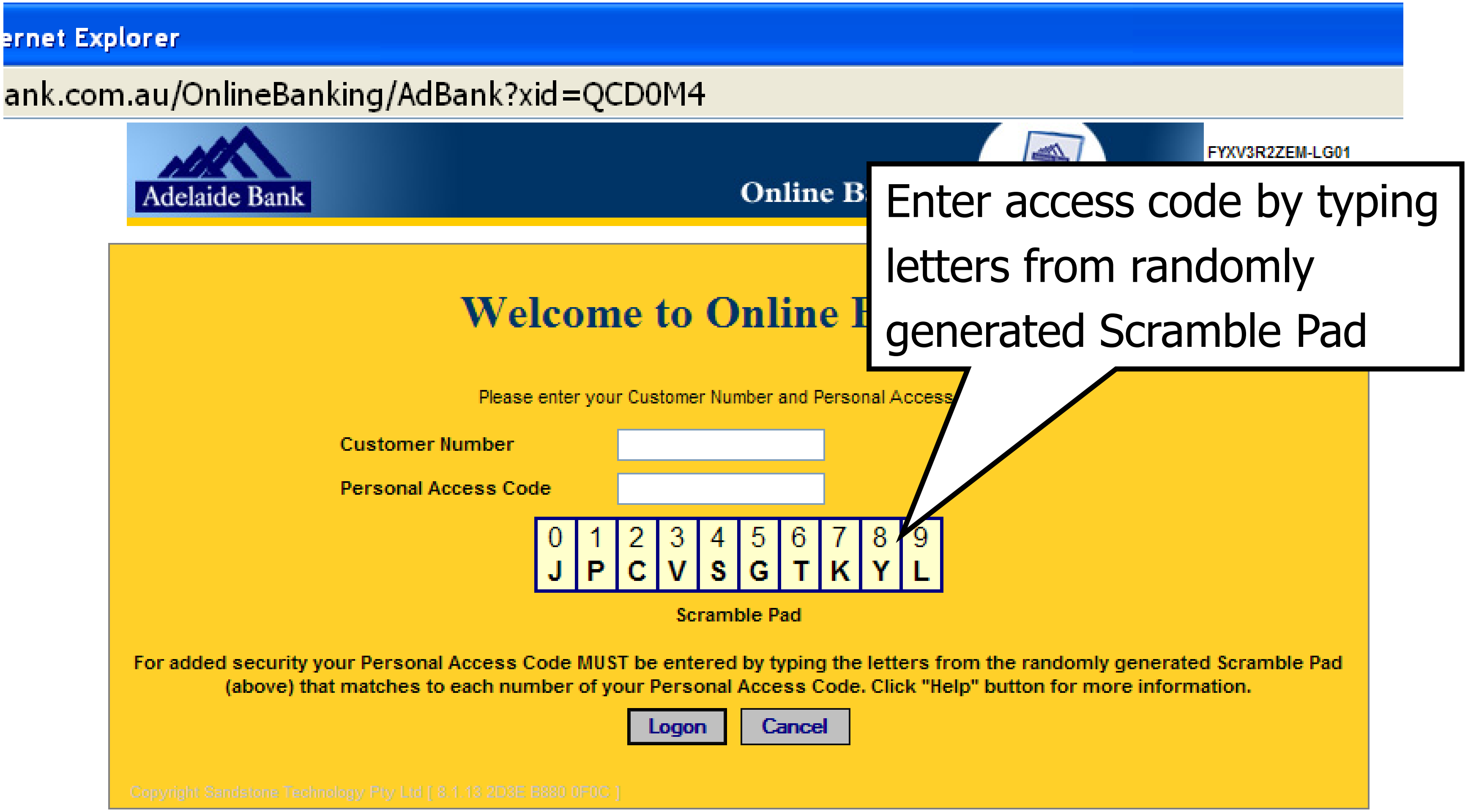
OR

Use your keyboard to type the letters from the keypad that correspond to your Login PIN.

PIN:

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

Site Defense #2A: Scramble Pad



ernet Explorer

ank.com.au/OnlineBanking/AdBank?xid=QCD0M4

Welcome to Online B

Please enter your Customer Number and Personal Access

Customer Number

Personal Access Code

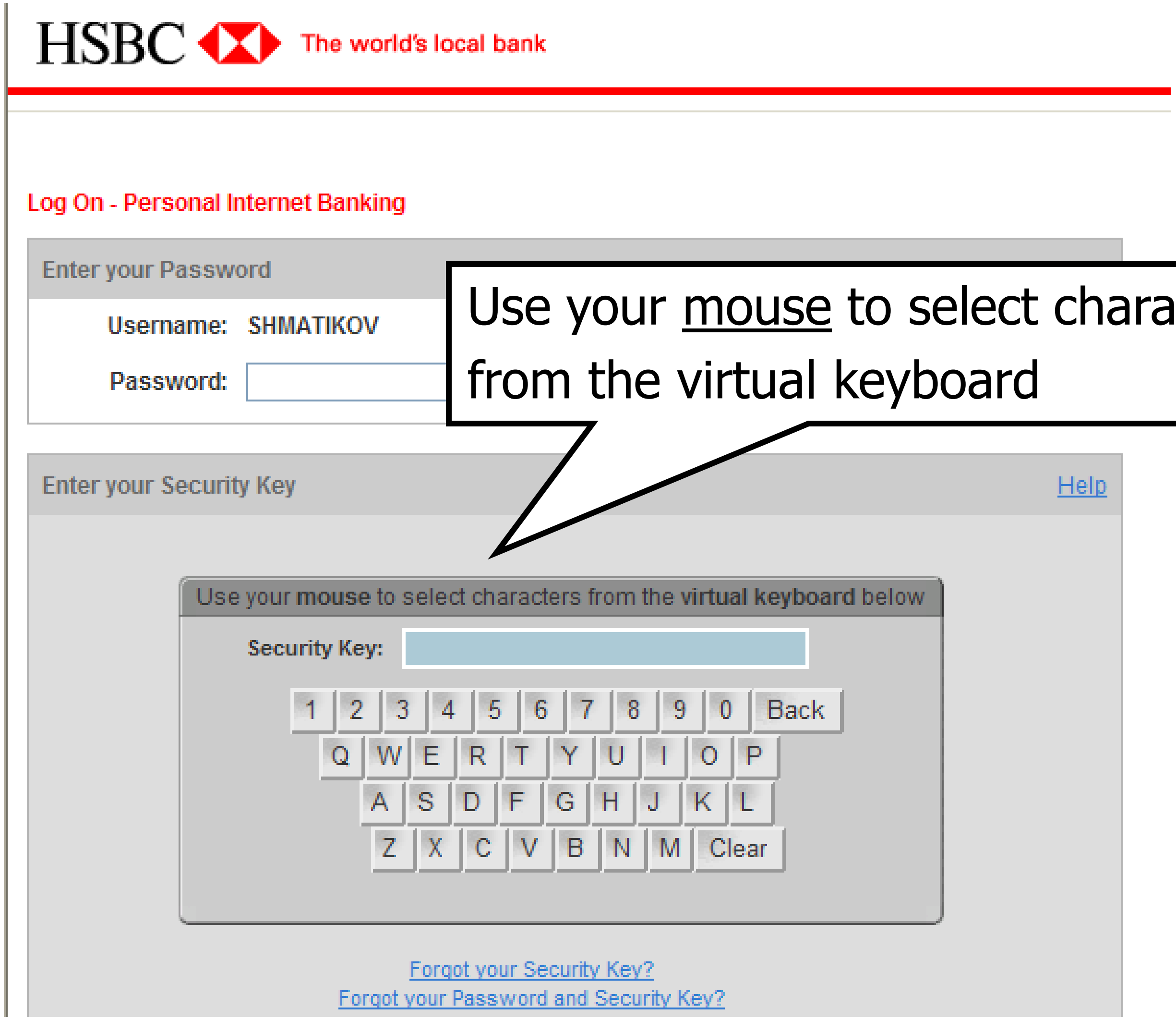
0	1	2	3	4	5	6	7	8	9
J	P	C	V	S	G	T	K	Y	L

Scramble Pad

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.

Enter access code by typing letters from randomly generated Scramble Pad

Site Defense #3: Virtual Keyboard



HSBC The world's local bank

Log On - Personal Internet Banking

Enter your Password

Username: SHMATIKOV

Password:

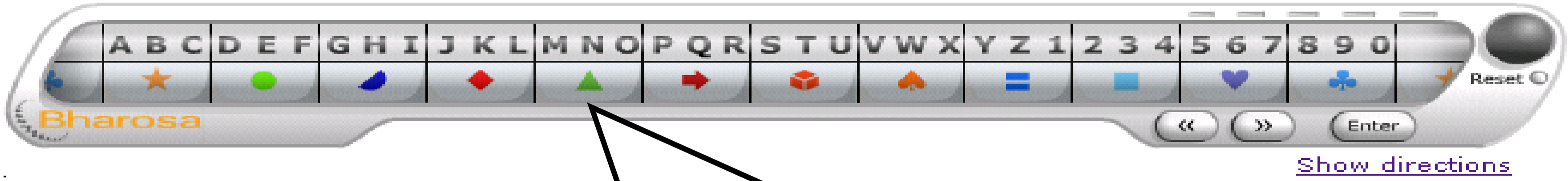
Enter your Security Key

Use your **mouse** to select characters from the **virtual keyboard** below

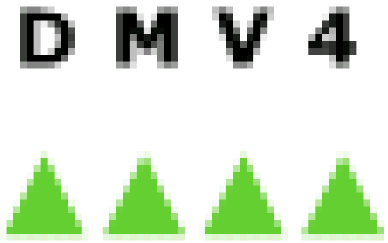
Security Key:

Use your <u>mouse</u> to select characters from the virtual keyboard

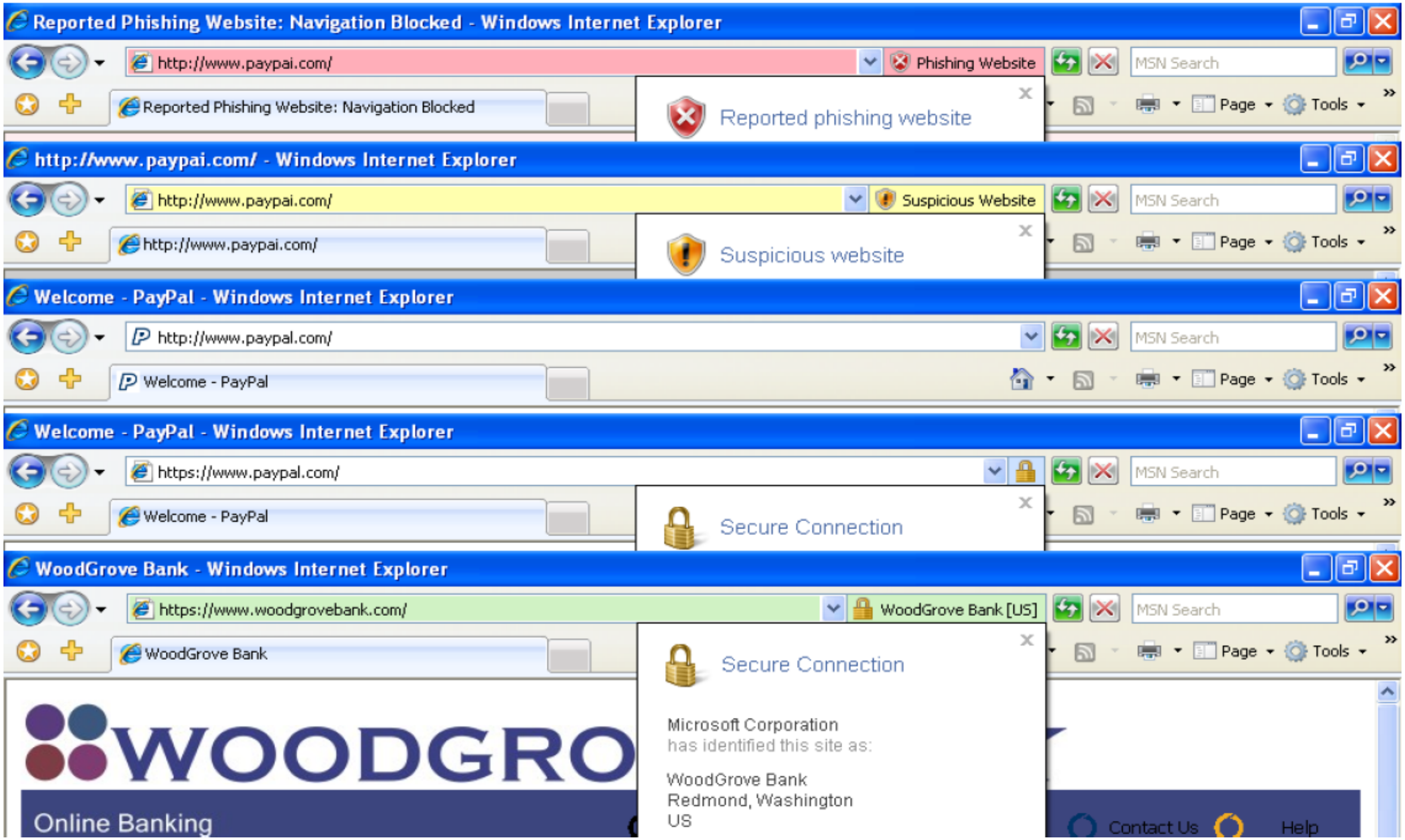
Site Defense #4: Bharosa Slider


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

On first login, user picks a symbol.
On subsequent logins all letters and numbers
in the PIN must be chosen using correct symbol.



Anti-Phishing Features in IE7



Reported Phishing Website: Navigation Blocked - Windows Internet Explorer

http://www.paypai.com/ Phishing Website

Reported Phishing Website: Navigation Blocked

Reported phishing website

http://www.paypai.com/ - Windows Internet Explorer

http://www.paypai.com/ Suspicious Website

http://www.paypai.com/

Suspicious website

Welcome - PayPal - Windows Internet Explorer

http://www.paypal.com/

Welcome - PayPal

Welcome - PayPal - Windows Internet Explorer

https://www.paypal.com/

Welcome - PayPal

Secure Connection

WoodGrove Bank - Windows Internet Explorer

https://www.woodgrovebank.com/ WoodGrove Bank [US]

WoodGrove Bank

Secure Connection

Microsoft Corporation
has identified this site as:

WoodGrove Bank
Redmond, Washington
US

Are Phishing Warnings Effective?

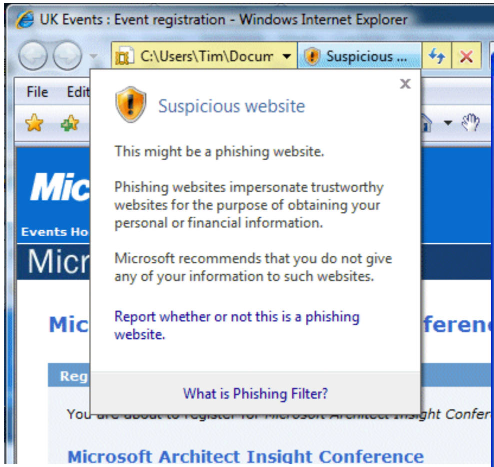
[Egelman et al.]

- 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 <u>active</u> and <u>passive</u> 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

[Egelman 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


UK Events : Event registration - Windows Internet Explorer
C:\Users\Tim\Docum
Suspicious ...
File
Edit
Mic
Events Ho
Micr
Mic
feren
Reg
You are about to register for Microsoft Architect Insight Confer
Microsoft Architect Insight Conference

Suspicious website

This might be a phishing website.

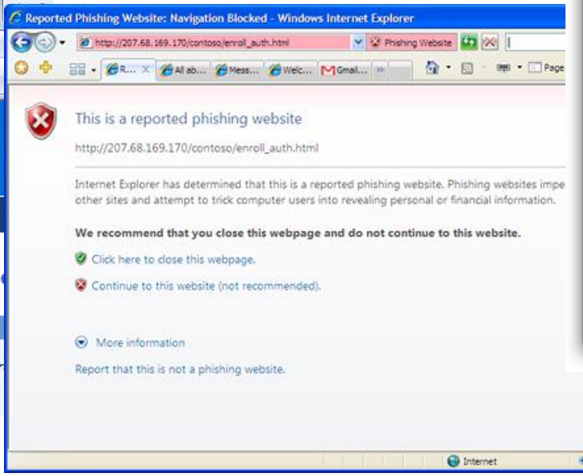
Phishing websites impersonate trustworthy websites for the purpose of obtaining your personal or financial information.

Microsoft recommends that you do not give any of your information to such websites.

Report whether or not this is a phishing website.

What is Phishing Filter?

Passive (IE)


Reported Phishing Website: Navigation Blocked - Windows Internet Explorer
http://207.68.169.170/contoso/enroll_auth.html
Phishing Website
R...
All ab...
Mess...
Welc...
Gmail...
Page
Internet
100%

This is a reported phishing website

http://207.68.169.170/contoso/enroll_auth.html

Internet Explorer has determined that this is a reported phishing website. Phishing websites impe other sites and attempt to trick computer users into revealing personal or financial information.

We recommend that you close this webpage and do not continue to this website.

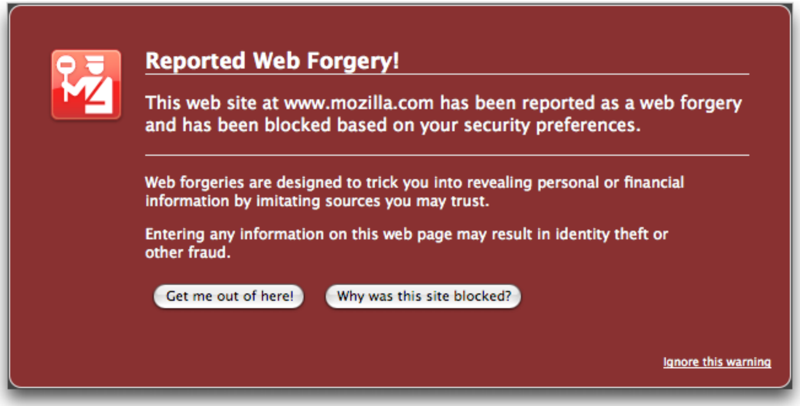
Click here to close this webpage.

Continue to this website (not recommended).

More information

Report that this is not a phishing website.

Active (IE)



Reported Web Forgery!

This web site at www.mozilla.com has been reported as a web forgery and has been blocked based on your security preferences.

Web forgeries are designed to trick you into revealing personal or financial information by imitating sources you may trust.

Entering any information on this web page may result in identity theft or other fraud.

Active (Firefox)

Users’ Mental Model

[Egelman et al.]

- 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

[Egelman et al.]

- 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.]

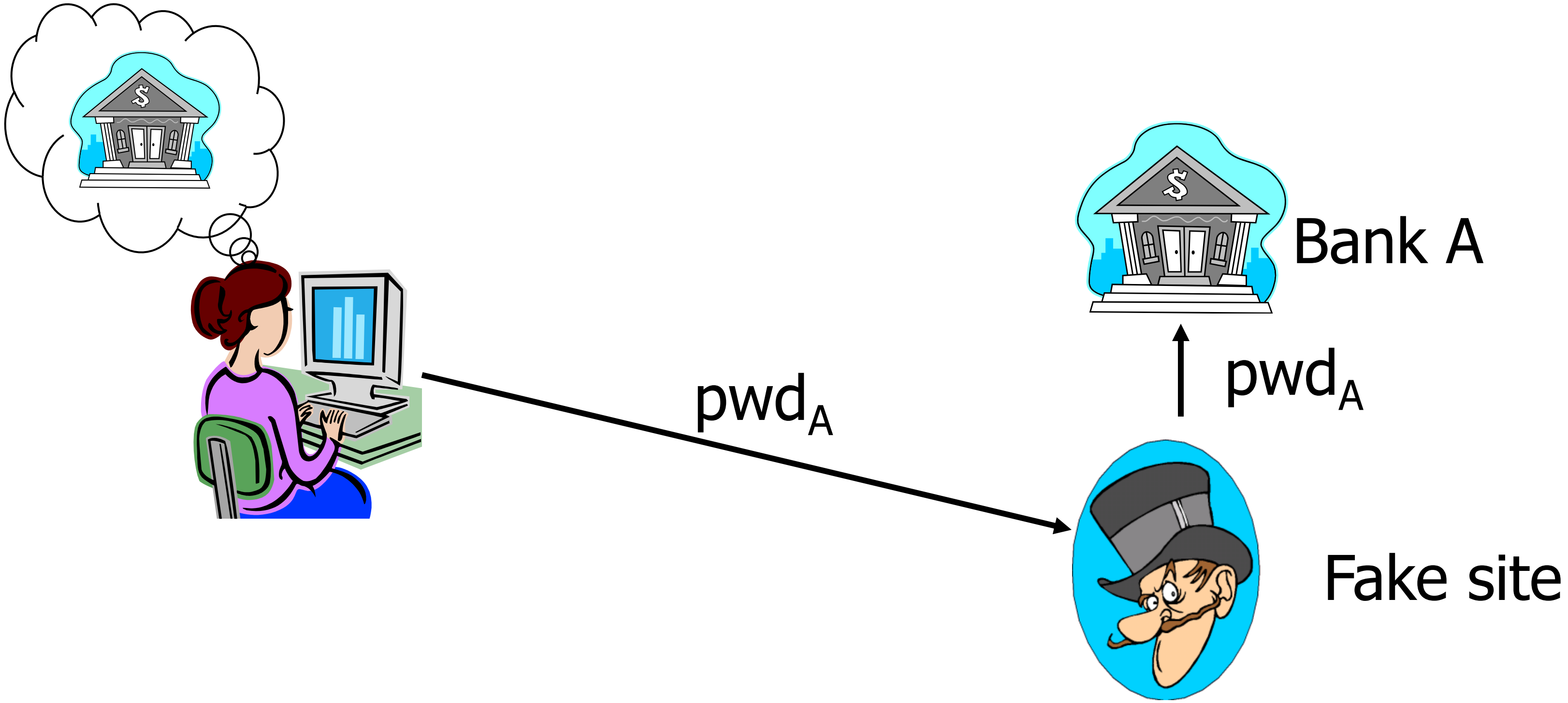
- Don’t trust the warning
  - “Since it gave me the option of still proceeding to the website, I figured it couldn’t be that bad”
- Ignore warning because it’s familiar (IE users)
  - “Oh, I always ignore those”
  - “Looked like warnings I see at work which I know to ignore”
  - “I thought that the warnings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

Misplaced Trust

[Egelman et al.]

- 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 which is a genuine address"

Password Phishing Problem



pwd_A

Bank A

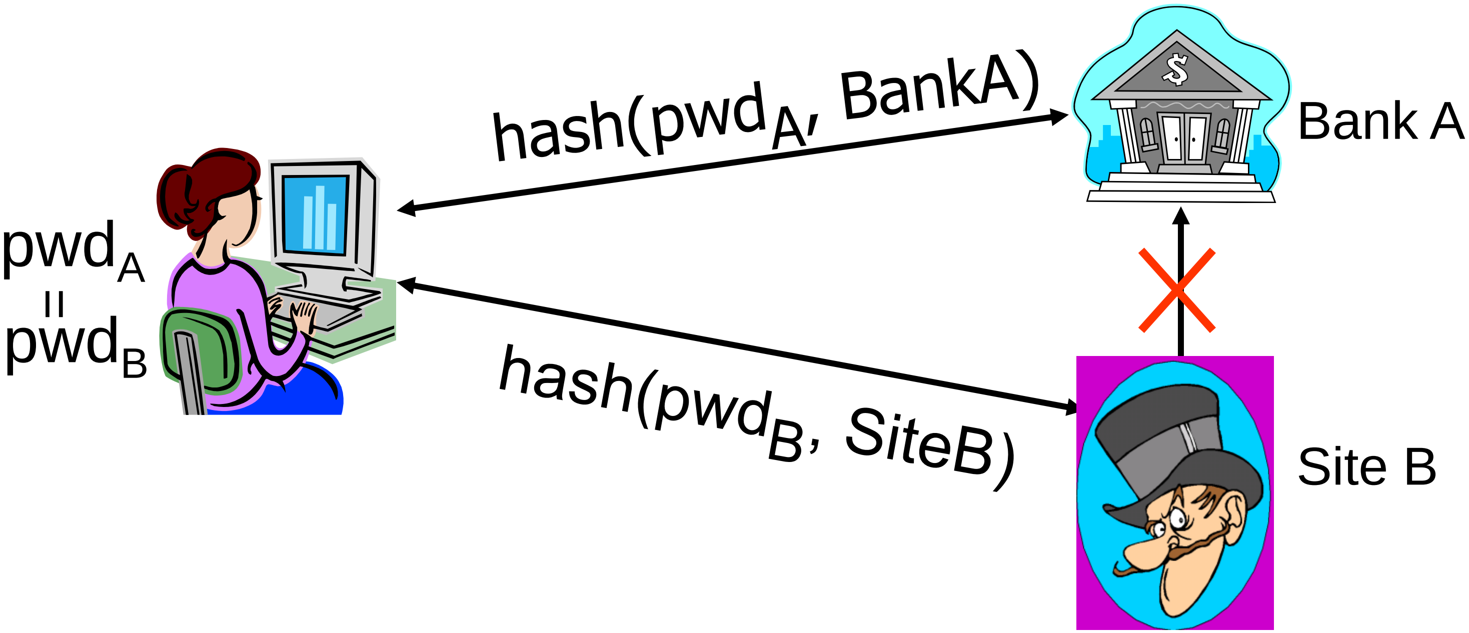
pwd_A

Fake site

- User cannot reliably identify spoofed sites
- Captured password can be used at target site

PwdHash

[Stanford project]

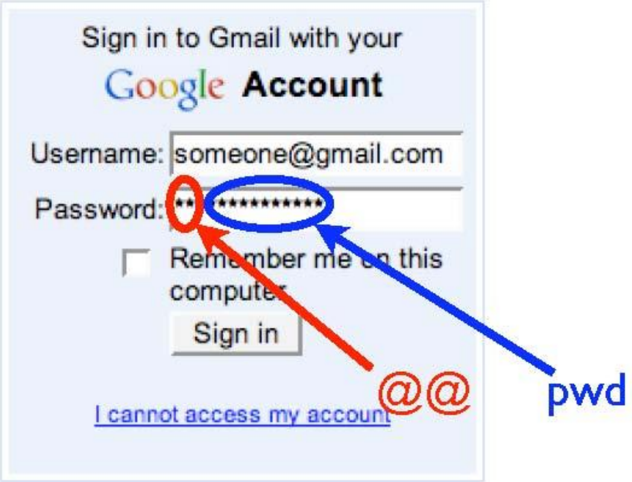


- Generate a unique password per site
  - HMAC(fido:123, banka.com) ⇒ Q7a+0ekEXb
  - HMAC(fido:123,siteb.com) ⇒ OzX2+ICiqc
- Hashed password is not usable at any other site

How PwdHash Works

- Install the free plug-in
- Activate it by adding @@ before the password
- Can also go to a remote site (www.pwdhash.com) which will generate 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

PwdHash Summary



Sign in to Gmail with your

Google Account

Username: someone@gmail.com

Password: ** ***********

□ Remember me on this computer

Sign in

I cannot access my account

@@ in front of passwords
to protect; or F2

sitePwd = func(pwd,domain)

Prevent phishing attacks

Usability Study at Carleton U.

[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

Best User Quote

"Really, I don't see how my password is safer because of two @'s in front"