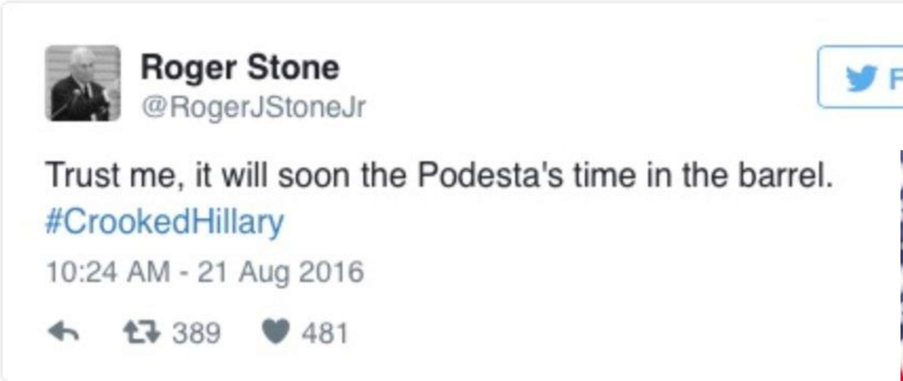
CS 5435

Phishing

Vitaly Shmatikov

Back in 2016

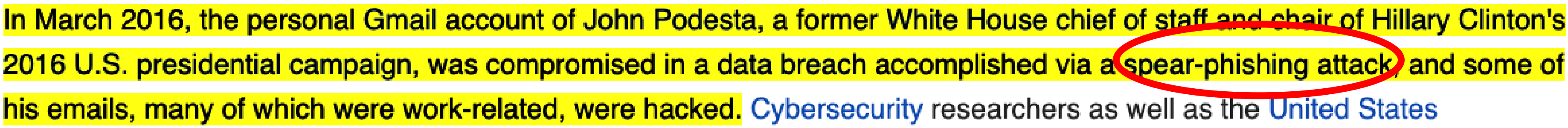


Roger Stone
@RogerJStoneJr

Trust me, it will soon the Podesta's time in the barrel. #CrookedHillary

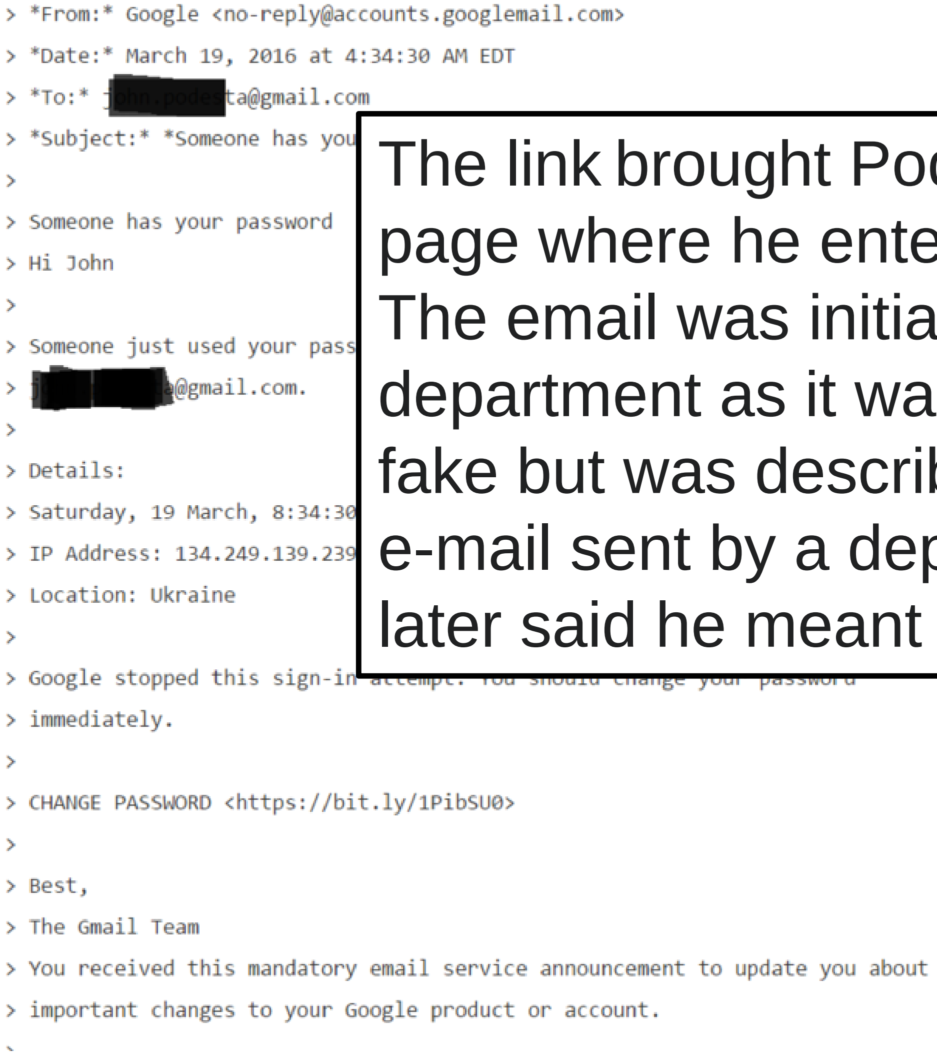
10:24 AM - 21 Aug 2016

389 481



In March 2016, the personal Gmail account of John Podesta, a former White House chief of staff and chair of Hillary Clinton's 2016 U.S. presidential campaign, was compromised in a data breach accomplished via a spear-phishing attack, and some of his emails, many of which were work-related, were hacked. Cybersecurity researchers as well as the United States

“Change Your Password Immediately”



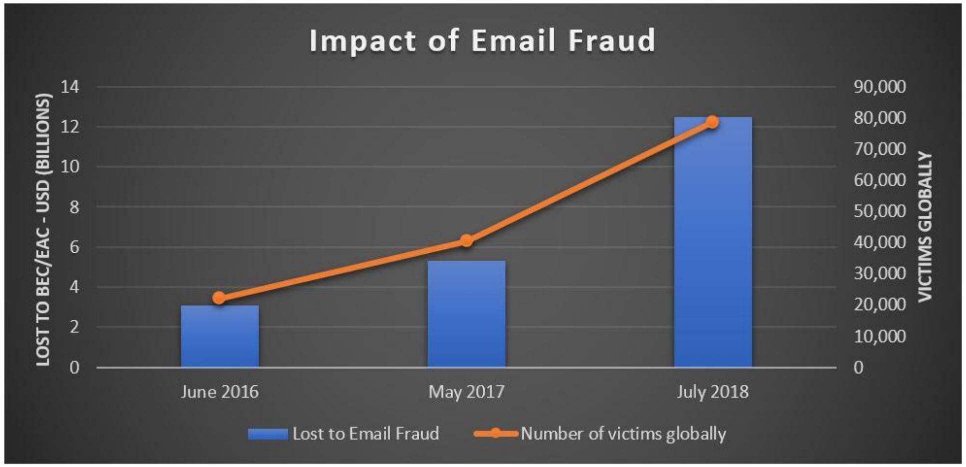
```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* [redacted]ta@gmail.com
> *Subject:* *Someone has you
>
> Someone has your password
> Hi John
>
> Someone just used your pass
> [redacted]a@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
```

The link brought Podesta to a fake log-in page where he entered his Gmail credentials. The email was initially sent to the IT department as it was suspected of being a fake but was described as "legitimate" in an e-mail sent by a department employee, who later said he meant to write "illegitimate".

Phishing and Email Fraud Statistics 2019

- The average financial cost of a data breach is $3.86m (IBM)
- Phishing accounts for 90% of data breaches
- 15% of people successfully phished will be targeted at least one more time within the year
- BEC scams accounted for over $12 billion in losses (FBI)

This Year, Phishing Causes Losses of $17,700 per minute And Ransomware Attacks Will Cost $22,184 Per Minute



Sources: https://retruster.com/blog/2019-phishing-and-email-fraud-statistics.html
https://www.proofpoint.com/us/corporate-blog/post/fbi-reports-125-billion-global-financial-losses-due-business-email-compromise
https://blog.knowbe4.com/this-year-phishing-causes-losses-of-17700-per-minute-and-ransomware-attacks-will-cost-22184-per-minute

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

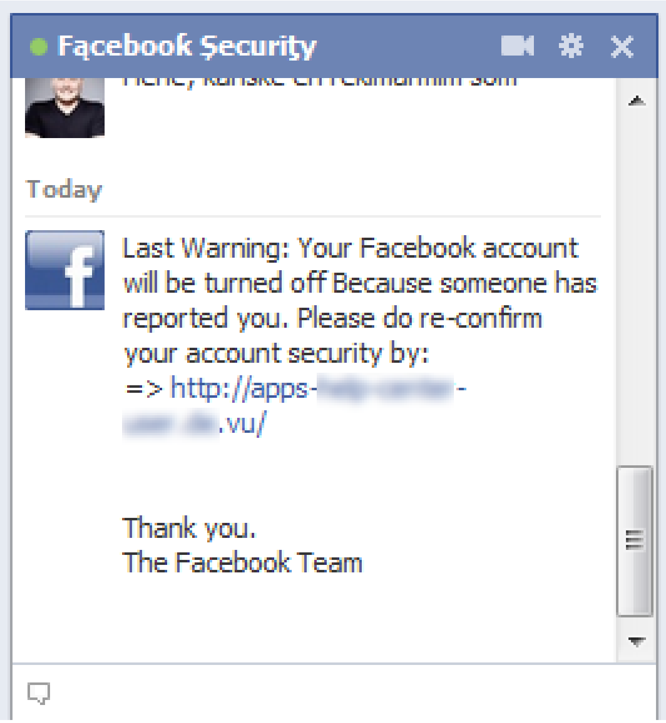
[redacted] https://securelist.com/facebook-security-phishing-attack-in-the-wild/31951/

Attack steals Facebook credentials

Changes profile picture of compromised account to f and the name to “Fąсebooƙ Şecuriţy”

- Notice anything?

Sends a message to all contacts:

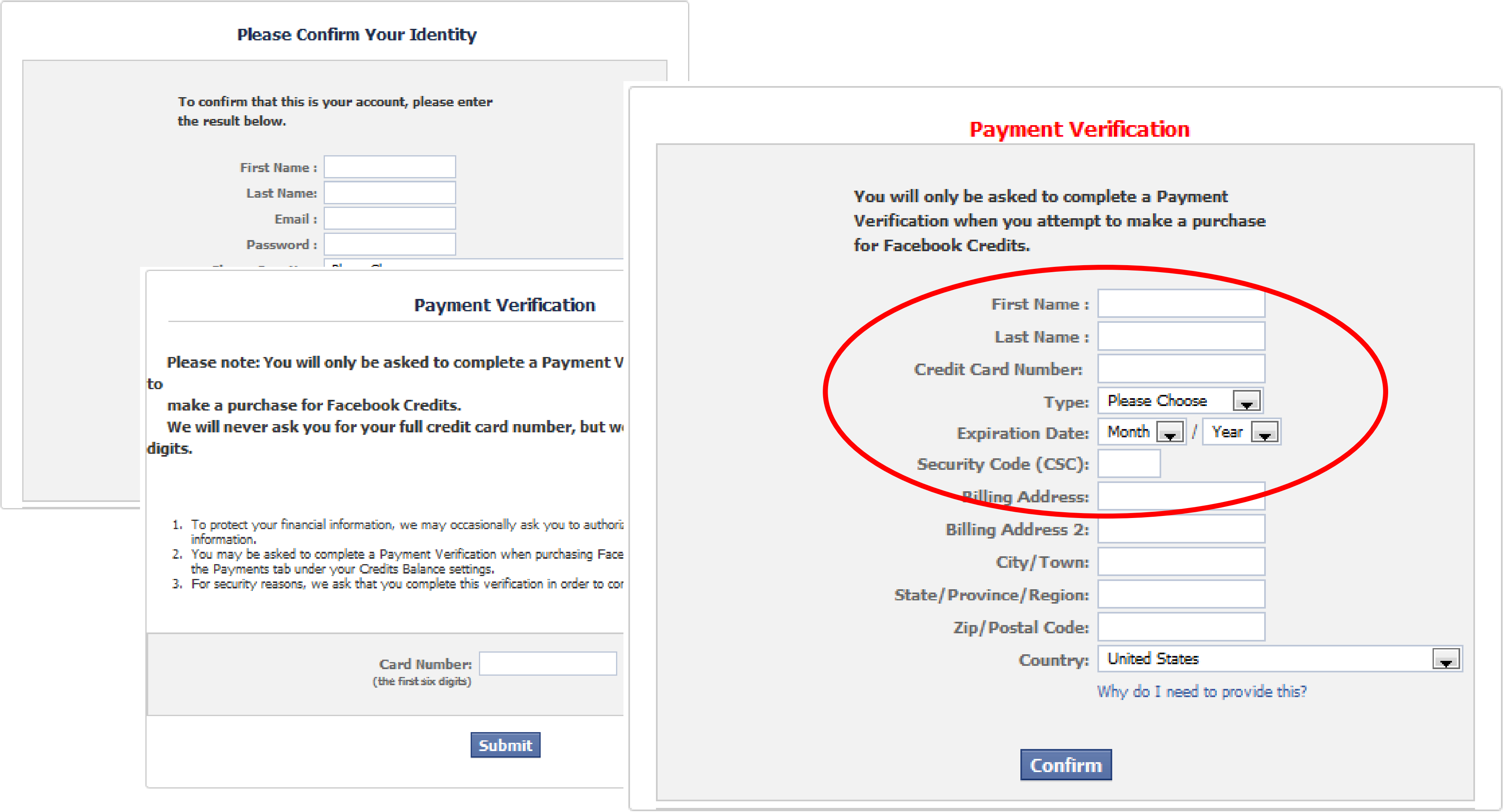


Last Warning: Your Facebook account will be turned off Because someone has reported you. Please do re-confirm your account security by:
=> http://apps-[redacted]-[redacted].vu/

Thank you.
The Facebook Team

“Payment Verification”

[redacted] https://securelist.com/facebook-security-phishing-attack-in-the-wild/31951/



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 and LinkedIn

Sent 921 Indiana University students a spoofed email that appeared to come from their friend

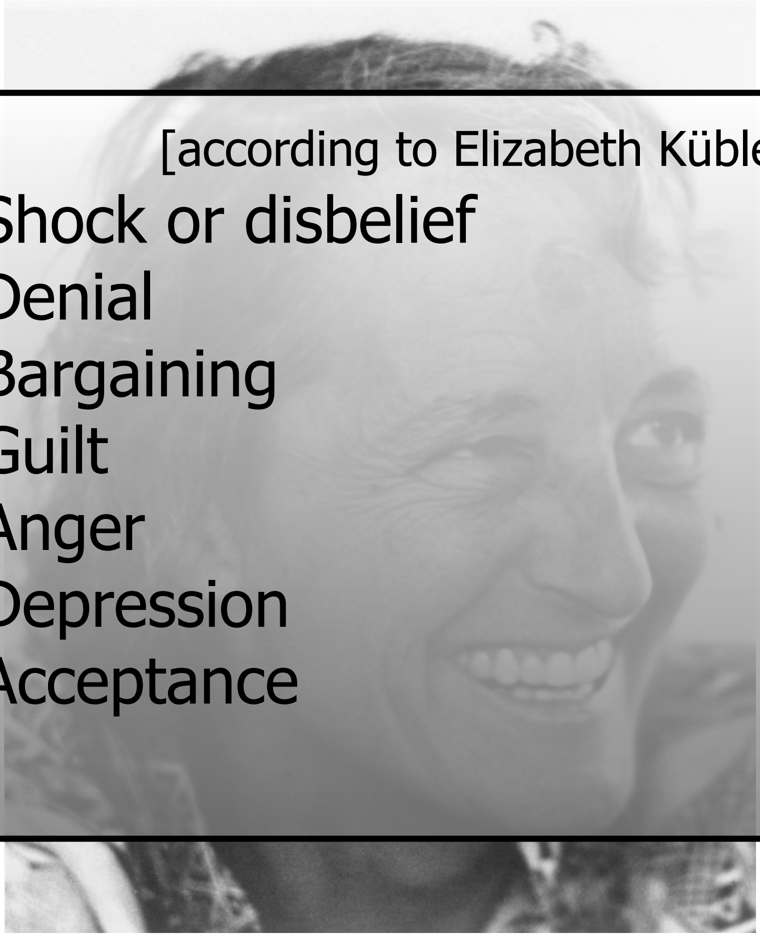
Email redirected to a spoofed site inviting the user to enter his/her secure university credentials

- 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

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.]

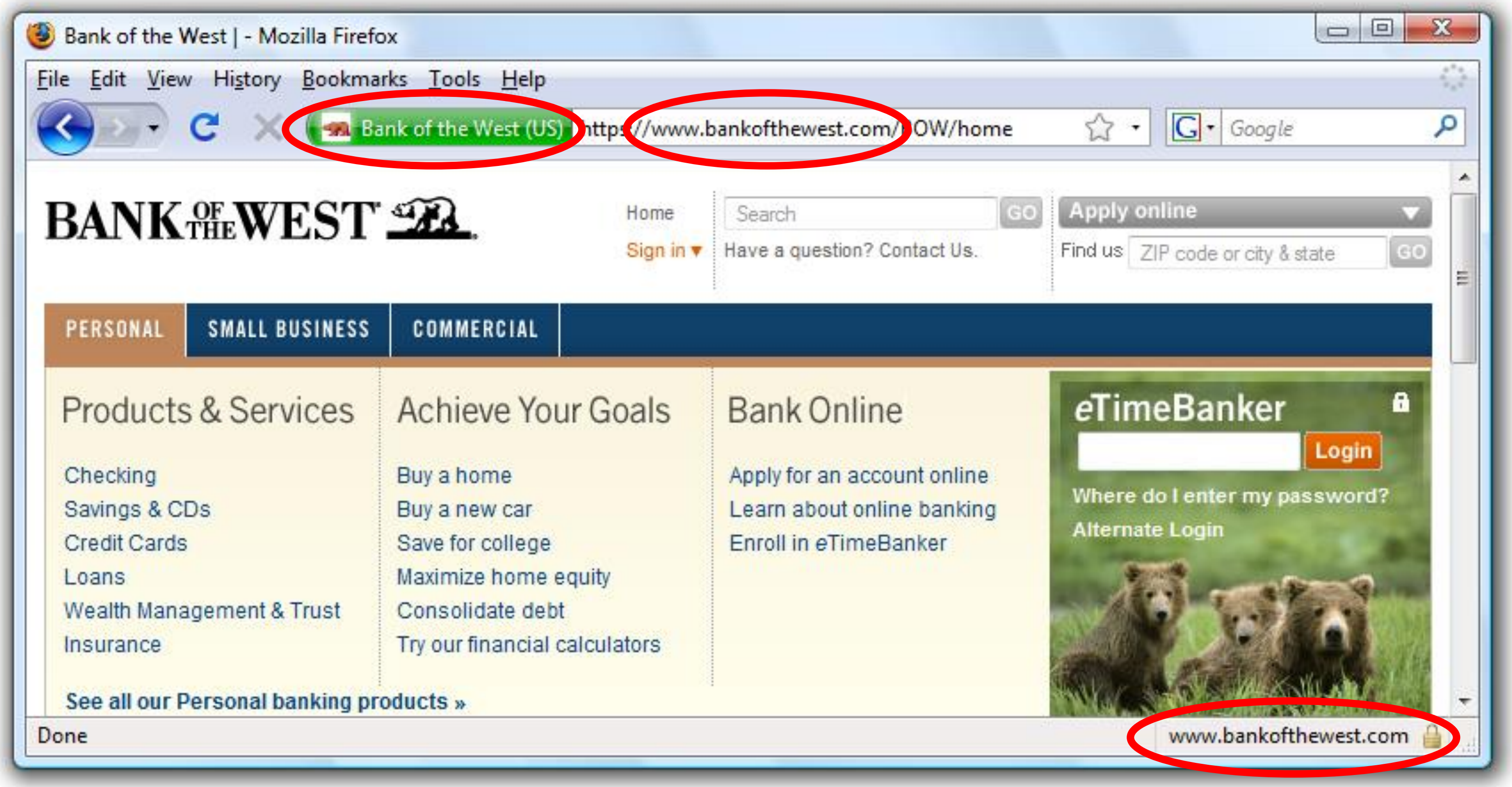
Misunderstanding

- 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?



Have a question? Contact Us.

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

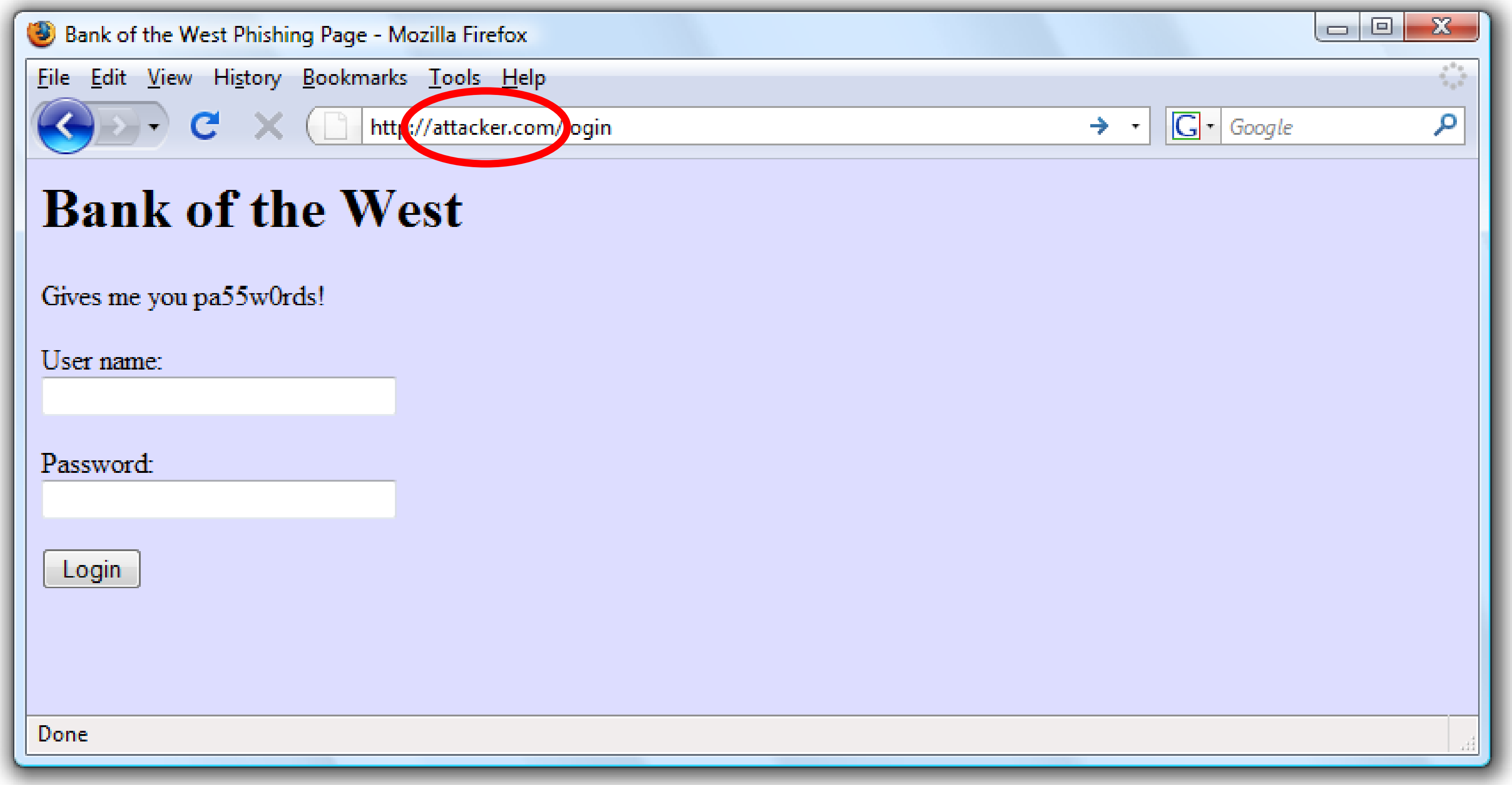
Apply for an account online
Learn about online banking
Enroll in eTimeBanker

eTimeBanker

Where do I enter my password?
Alternate Login

See all our Personal banking products »

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

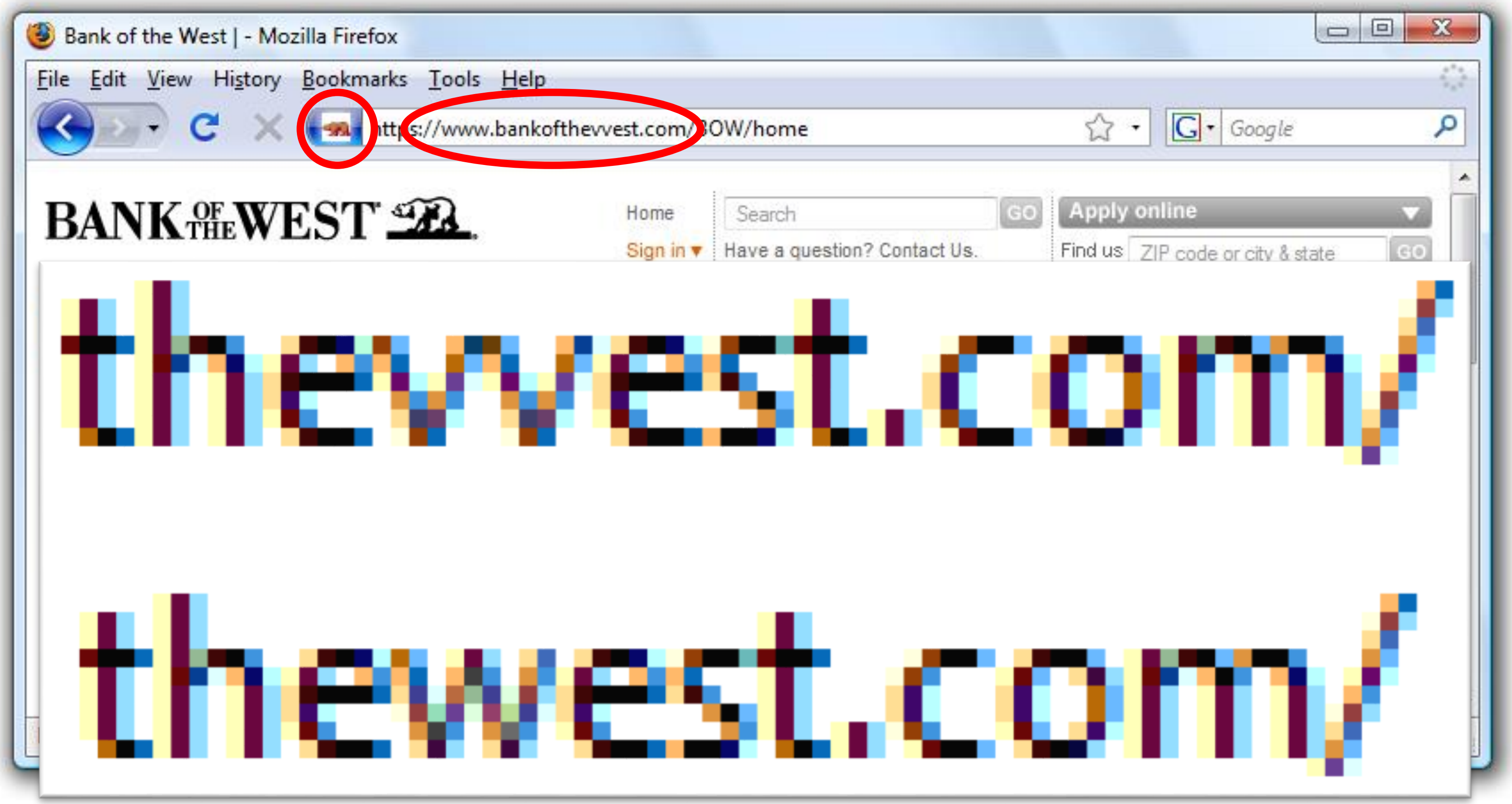
Bank of the West

Gives me you pa55w0rds!

User name:

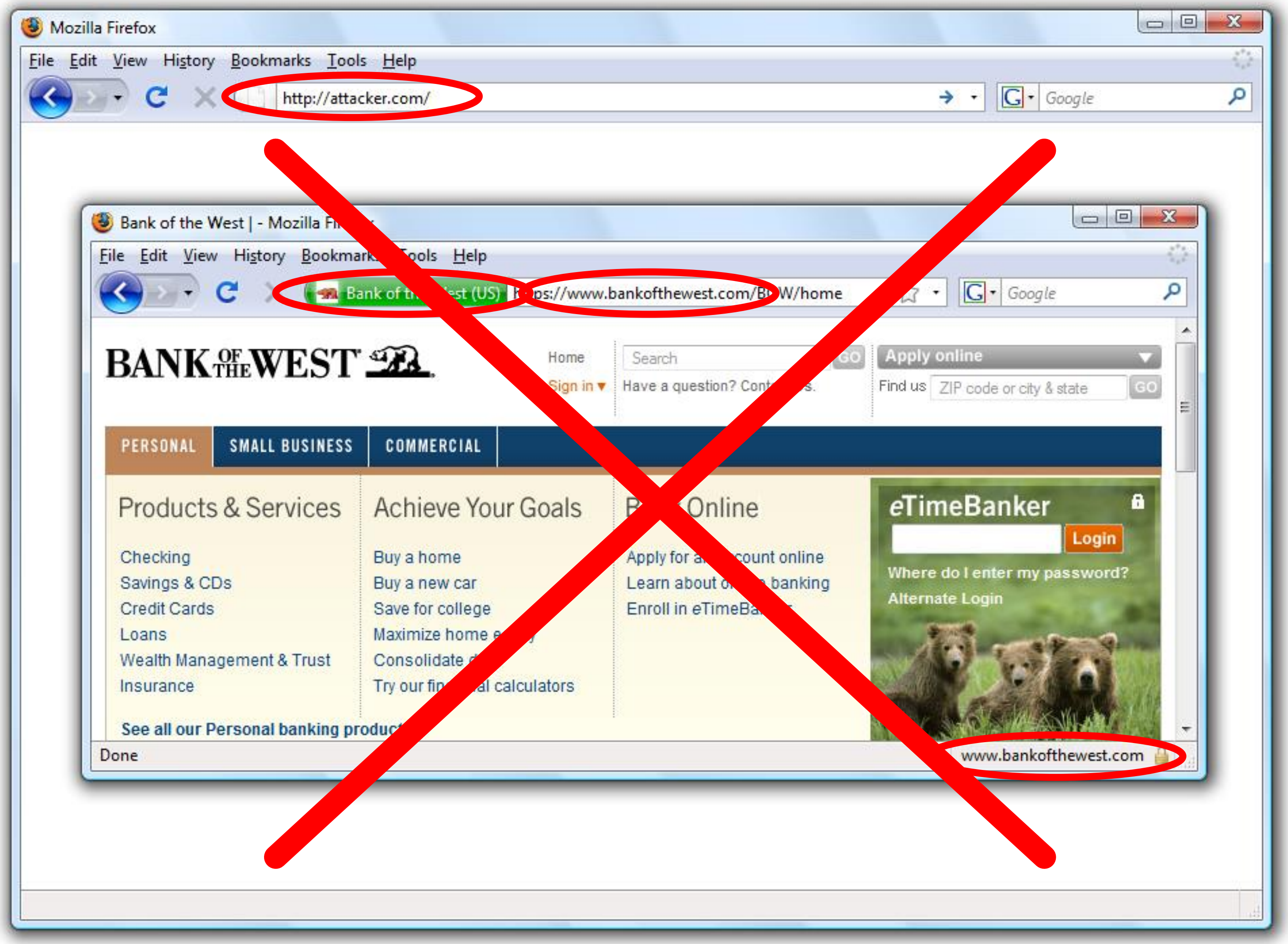
Password:

Safe to Type Your Password?

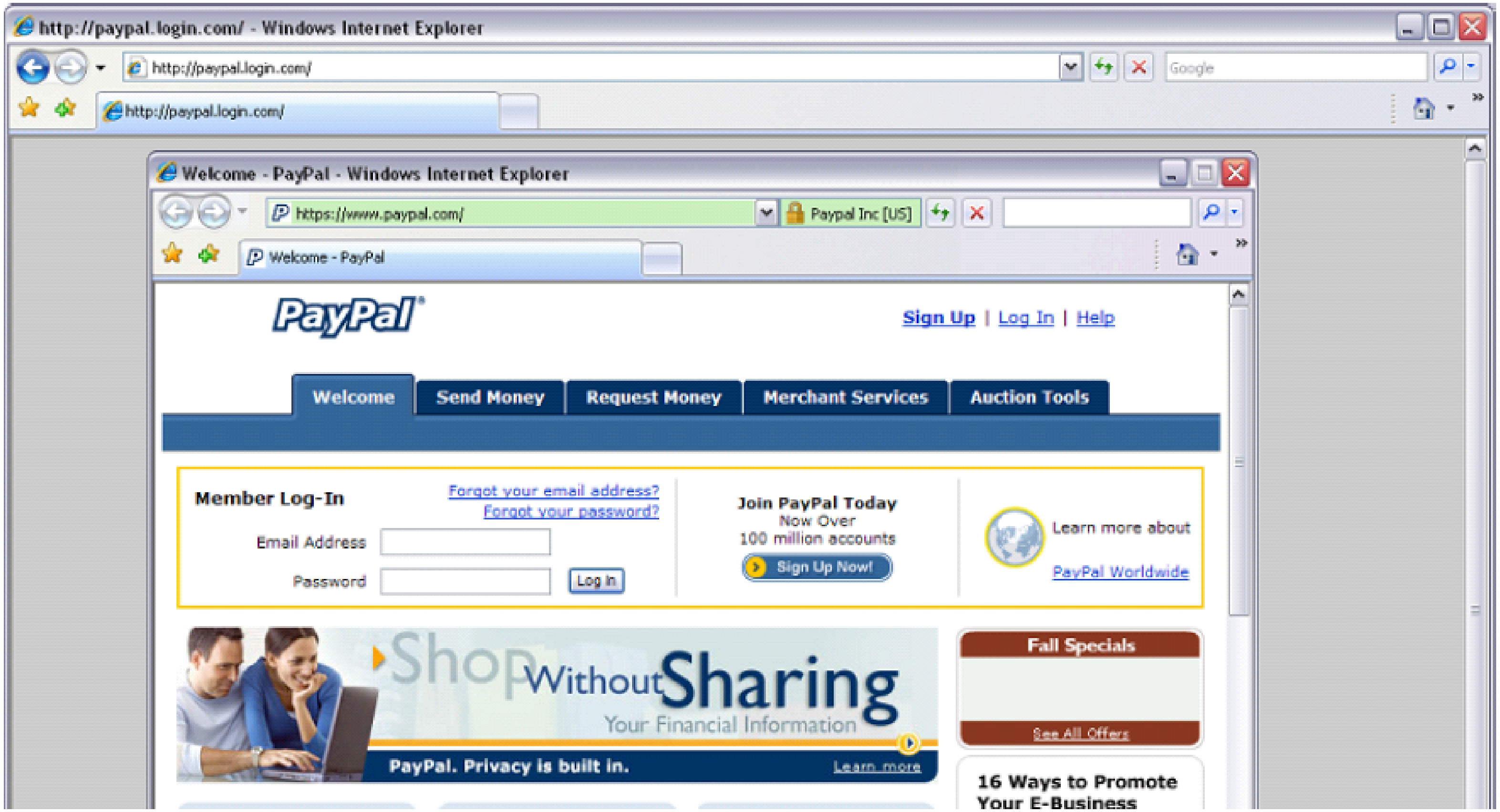


Bank of the West | - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.bankofthevvest.com/BOW/home
Google
BANK OF THE WEST
Home
Sign in
Search
GO
Have a question? Contact Us.
Apply online
Find us
ZIP code or city & state
GO
thevvest.com/
thewest.com/

Safe to Type Your Password?



Picture-in-Picture Attacks



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

Shop Without Sharing

Your Financial Information

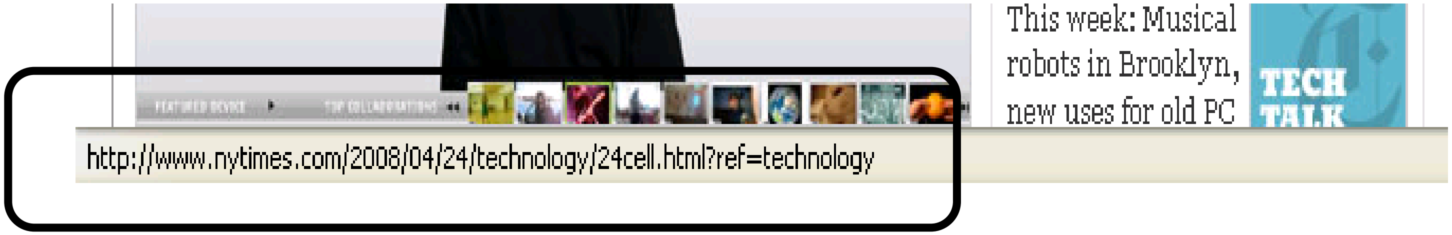
PayPal. Privacy is built in.

16 Ways to Promote

Your E-Business

Trained users are more likely to fall victim to this!

Status Bar Is Trivially Spoofable

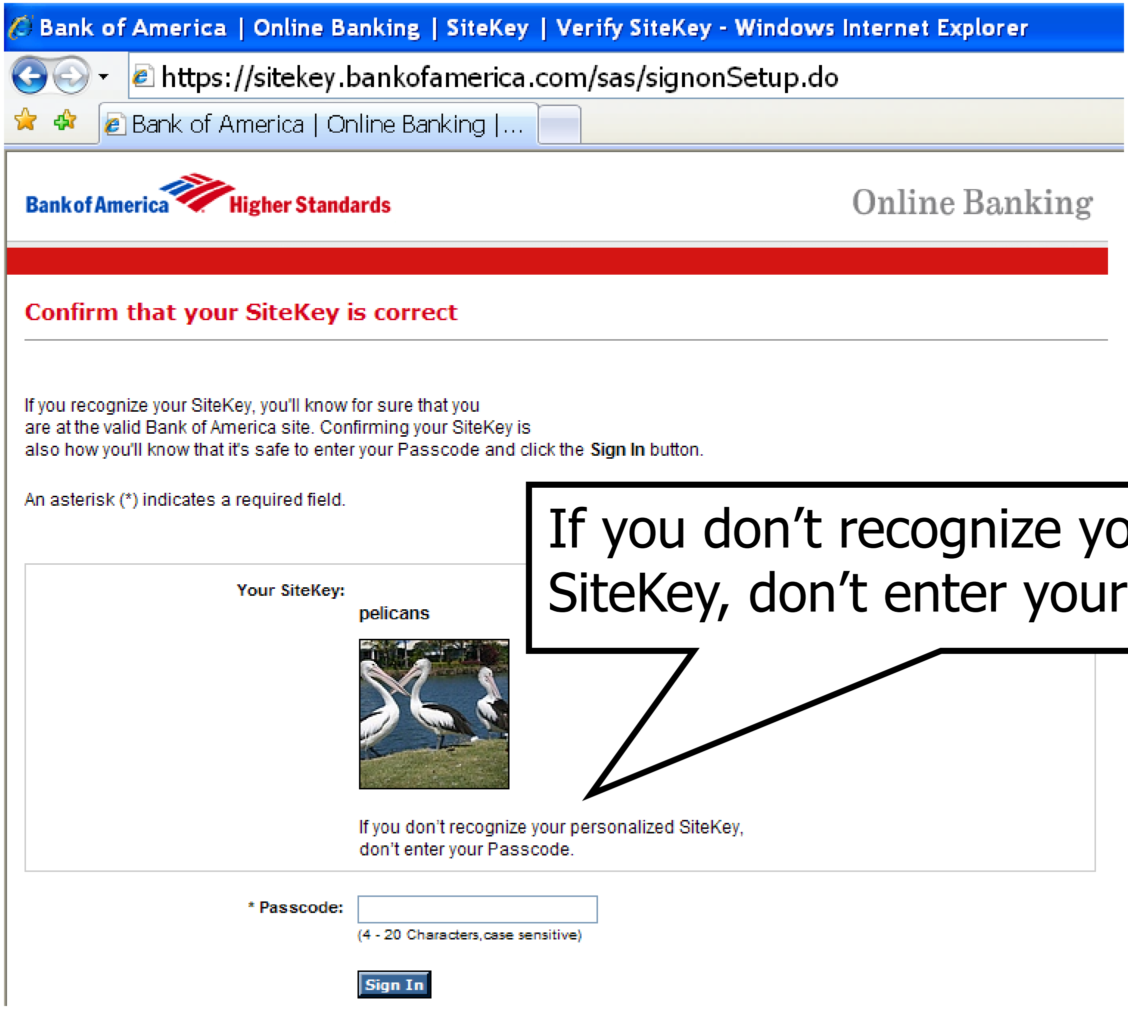


This week: Musical robots in Brooklyn, new uses for old PC

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

```
<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 | ...

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.

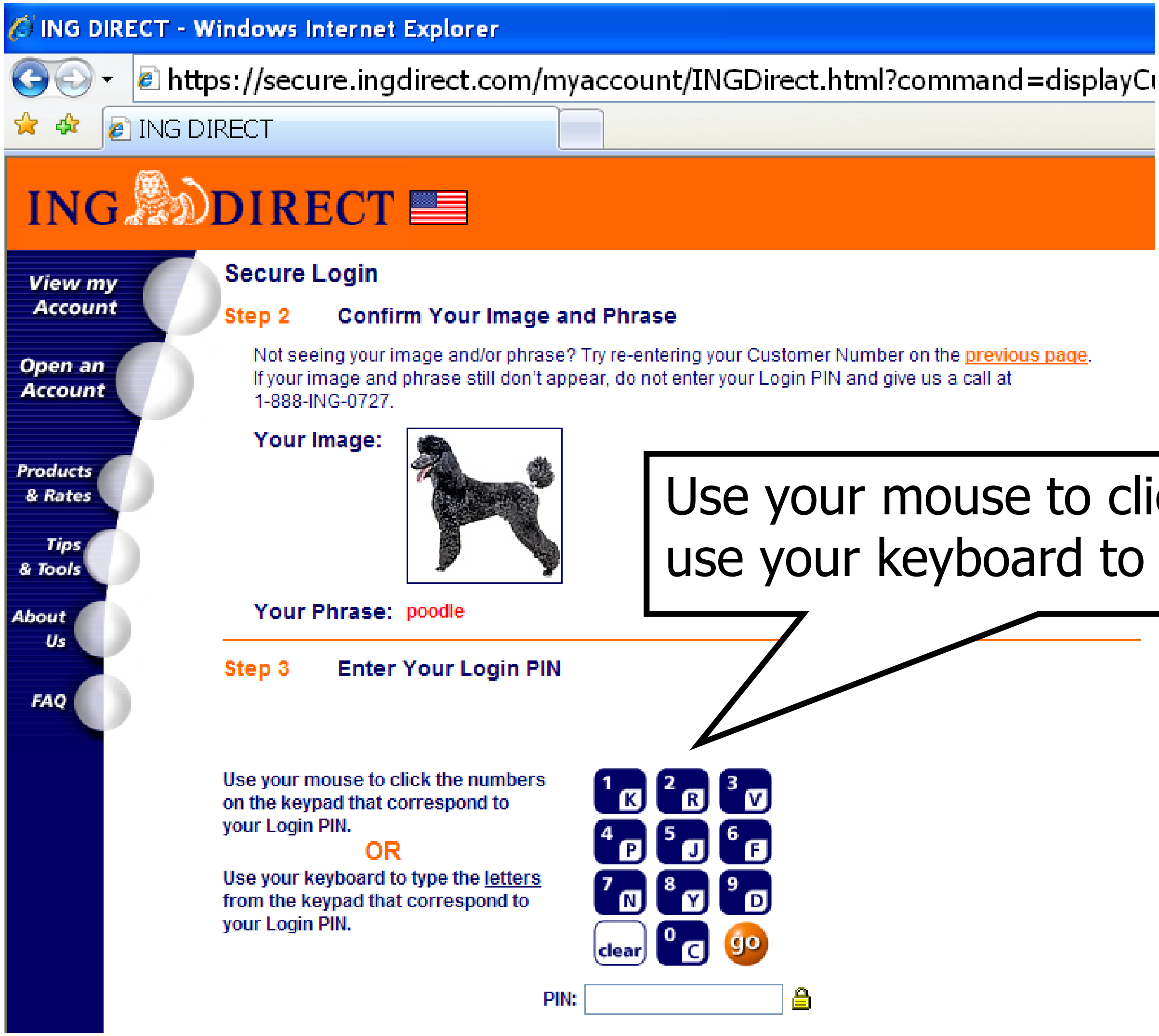
Your SiteKey: pelicans

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=displayCu

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.

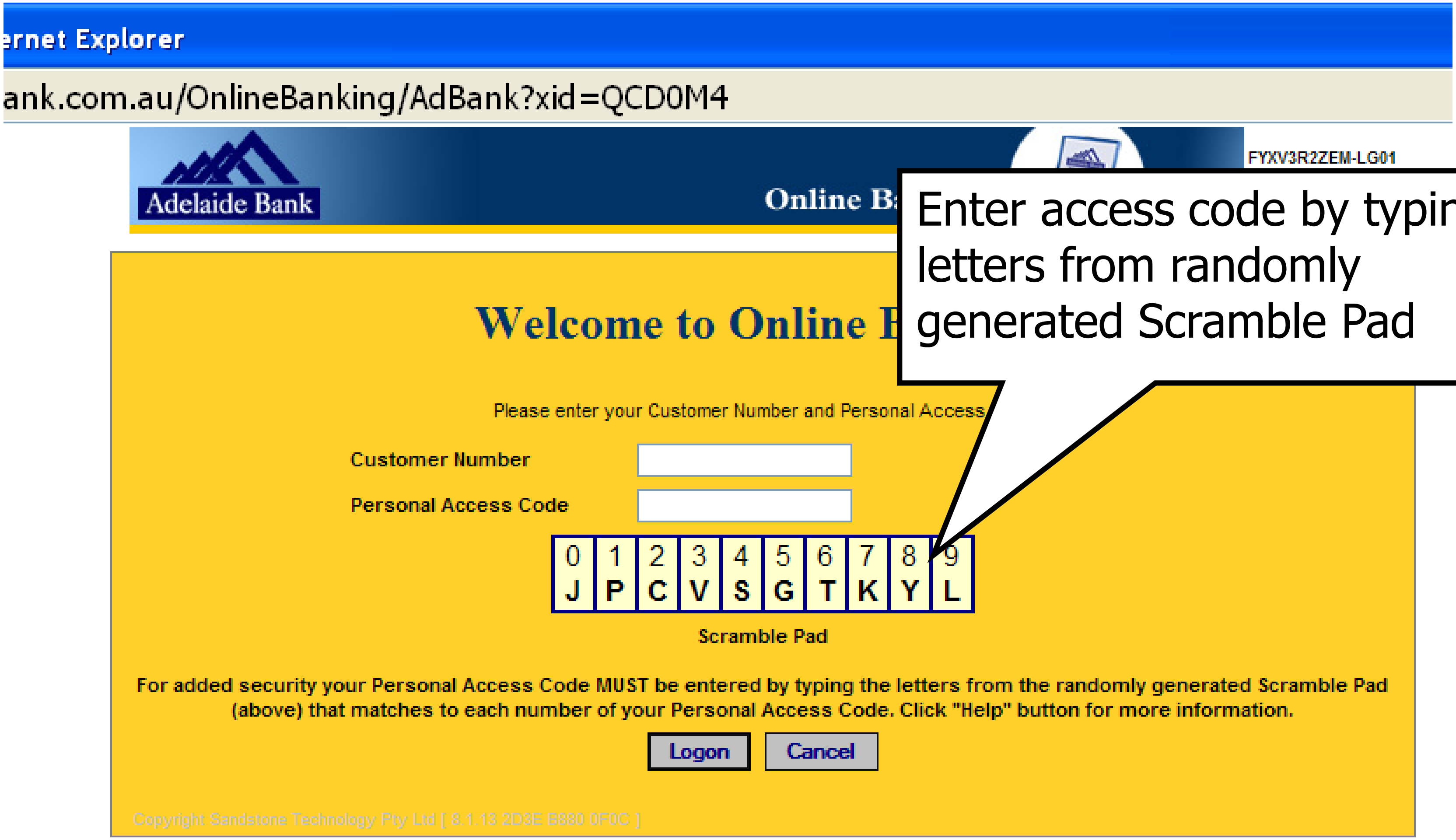
OR

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

PIN:

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

Site Defense #2A: Scramble Pad



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

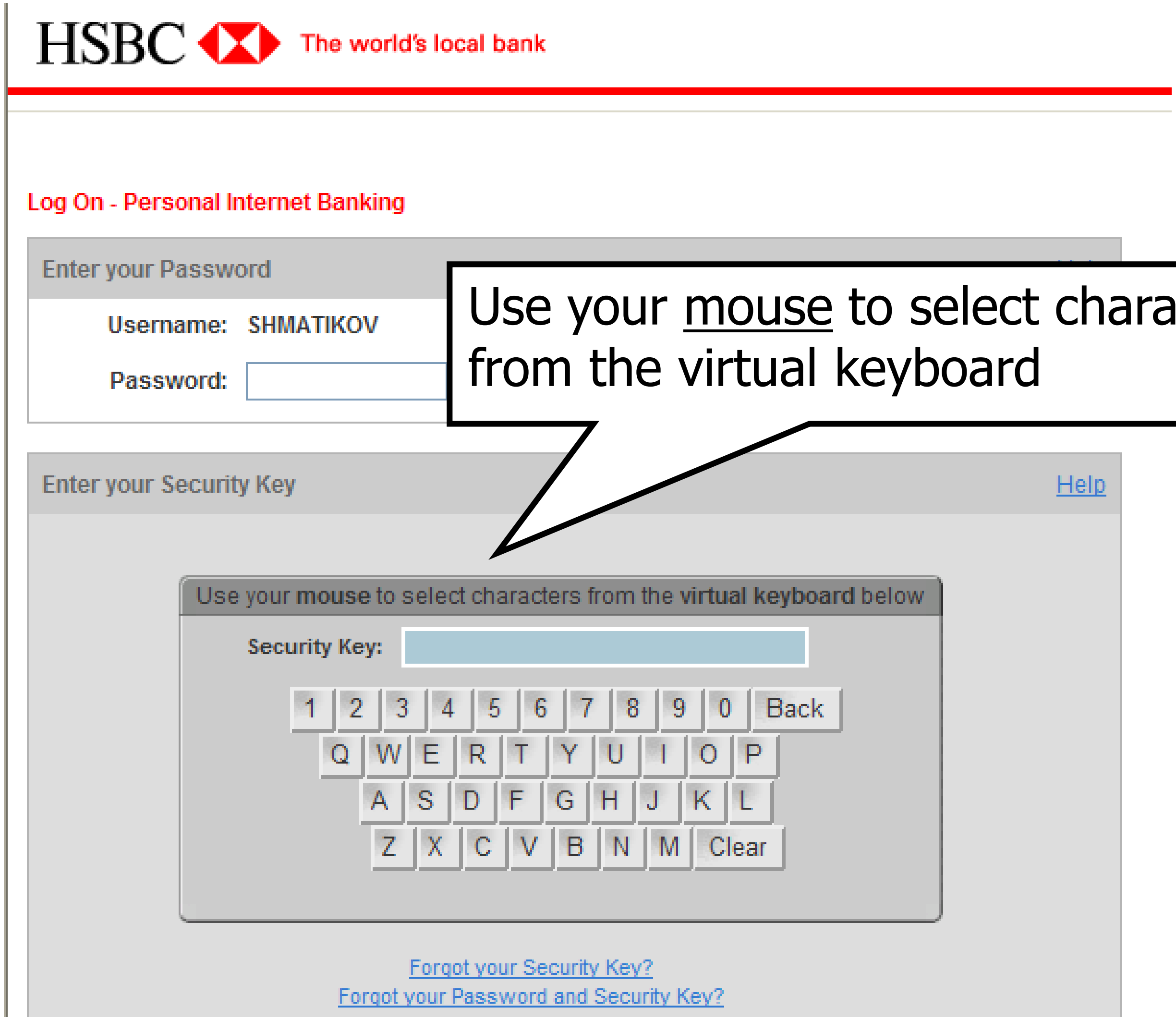
Scramble Pad

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.

Copyright Sandstone Technology Pty Ltd [8.1.13 2D3E B880 0F0C]

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

Help

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

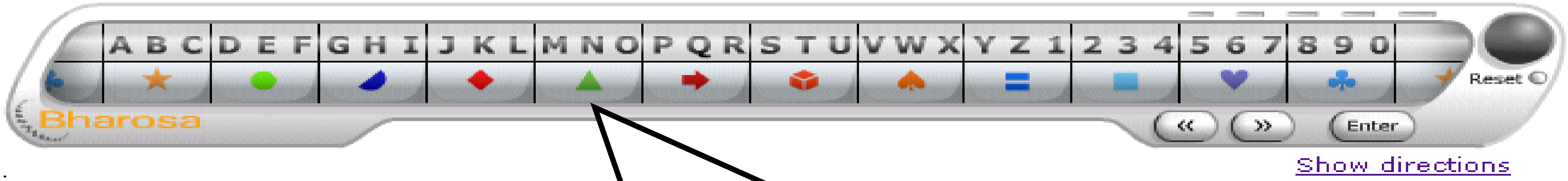
Security Key:

Forgot your Security Key?

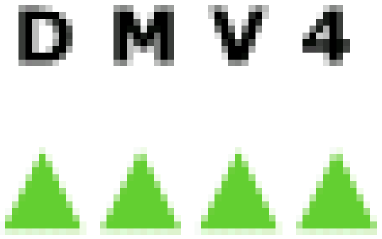
Forgot your Password and Security Key?

Use your mouse to select characters from the virtual keyboard

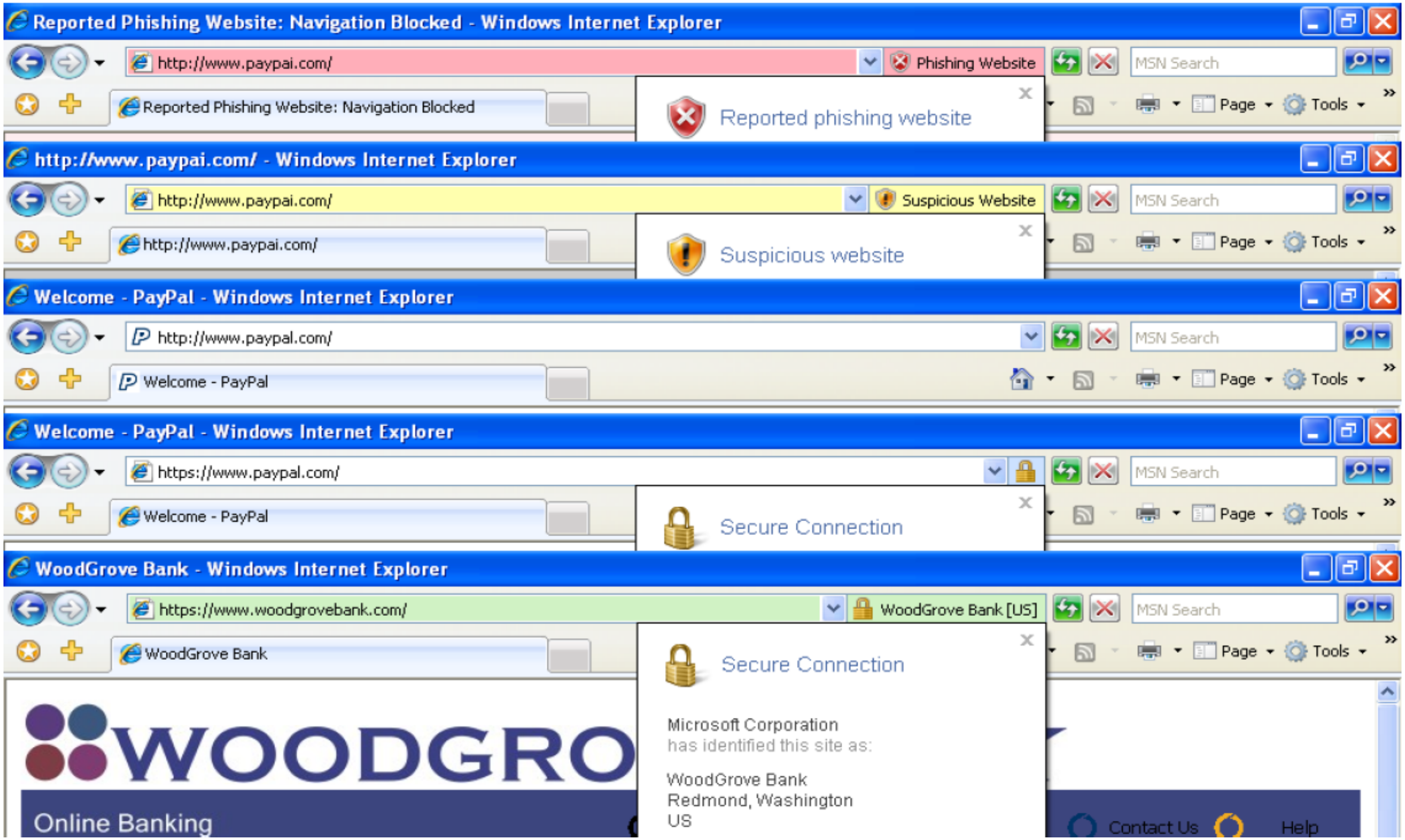
Site Defense #4: Bharosa Slider


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 active and passive warnings

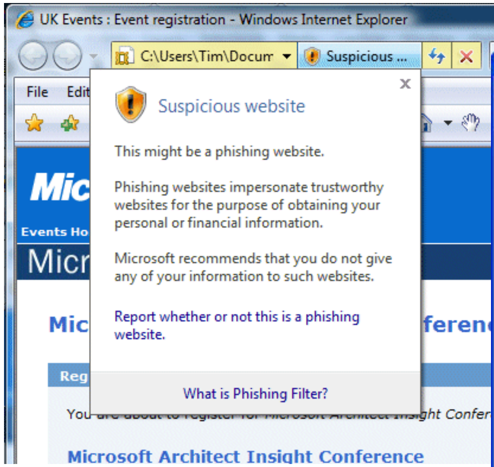
- Passive (IE): address bar changes color, pop-up box tells the user that the site is suspicious
- Active (IE): full-screen warning, must click on “Continue to this website (not recommended)” to get to site
- Active (Firefox): “Reported Web forgery” dialog, must click on “Ignore this warning” to get to site

Active vs. Passive Warnings

[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

Suspicious website

This might be a phishing website.

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

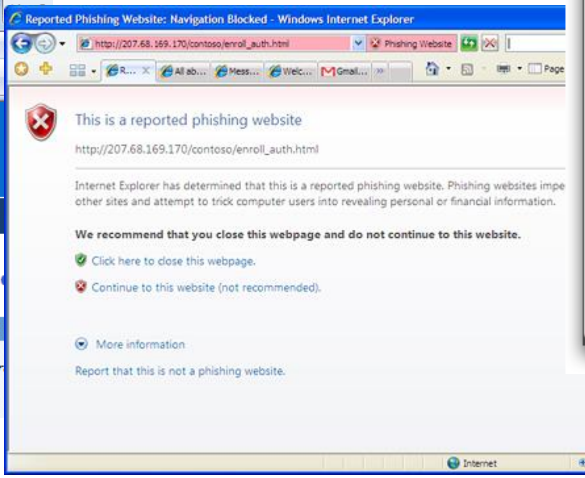
Microsoft recommends that you do not give any of your information to such websites.

Report whether or not this is a phishing website.

What is Phishing Filter?

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

Passive (IE)



Reported Phishing Website: Navigation Blocked - Windows Internet Explorer

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.

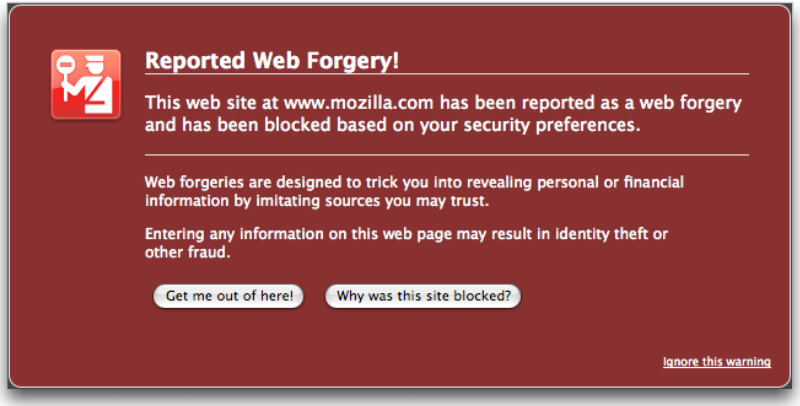
Click here to close this webpage.

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

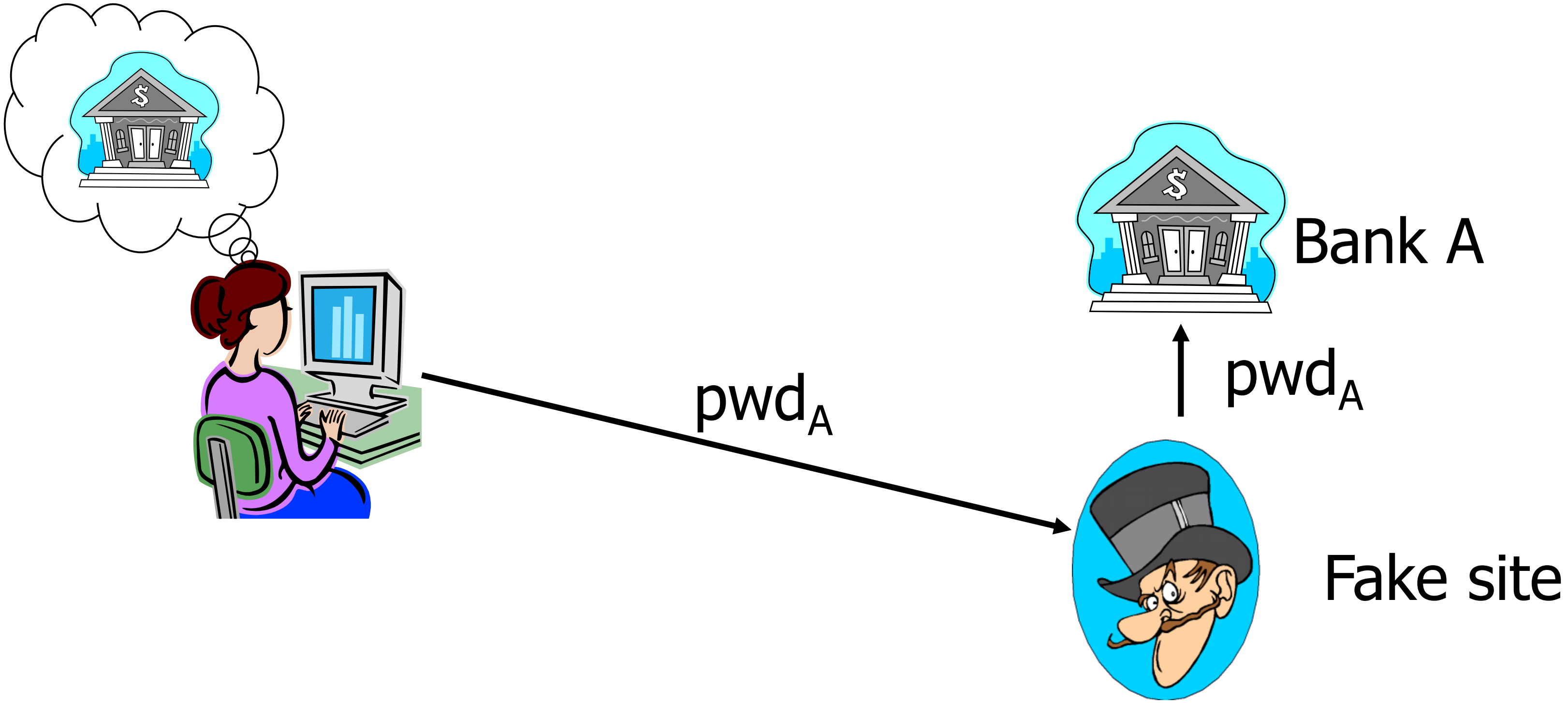
Incorrectly trust the phishing website

- 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

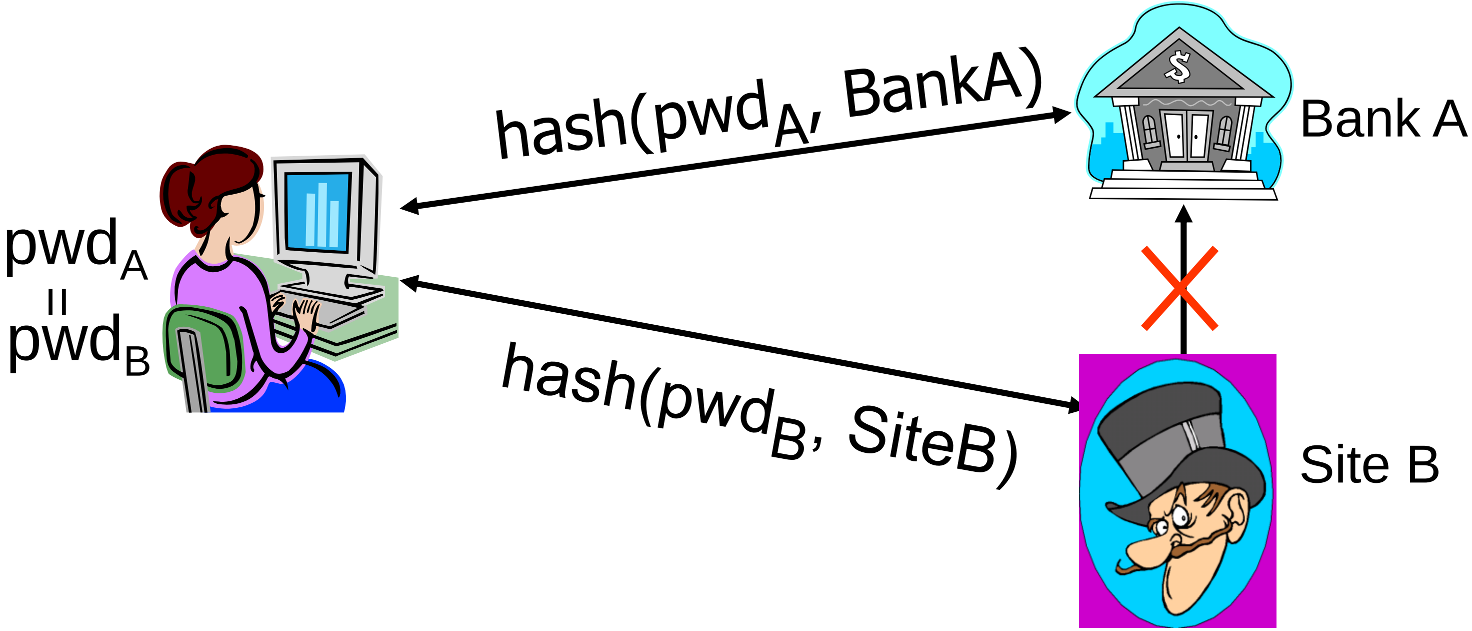


User cannot reliably identify spoofed sites

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

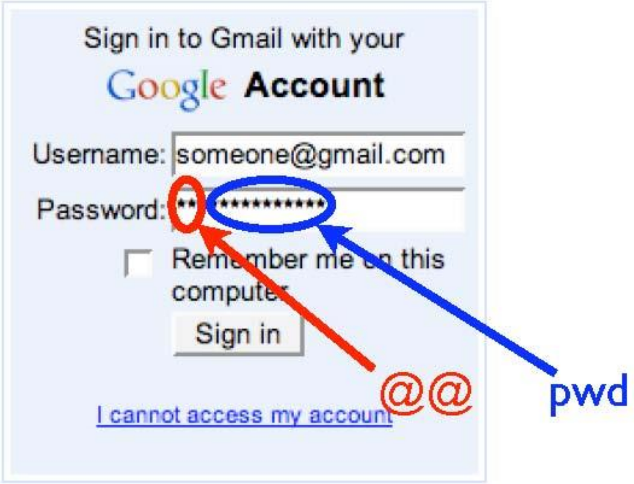
Activate it by adding @@ before the password

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"