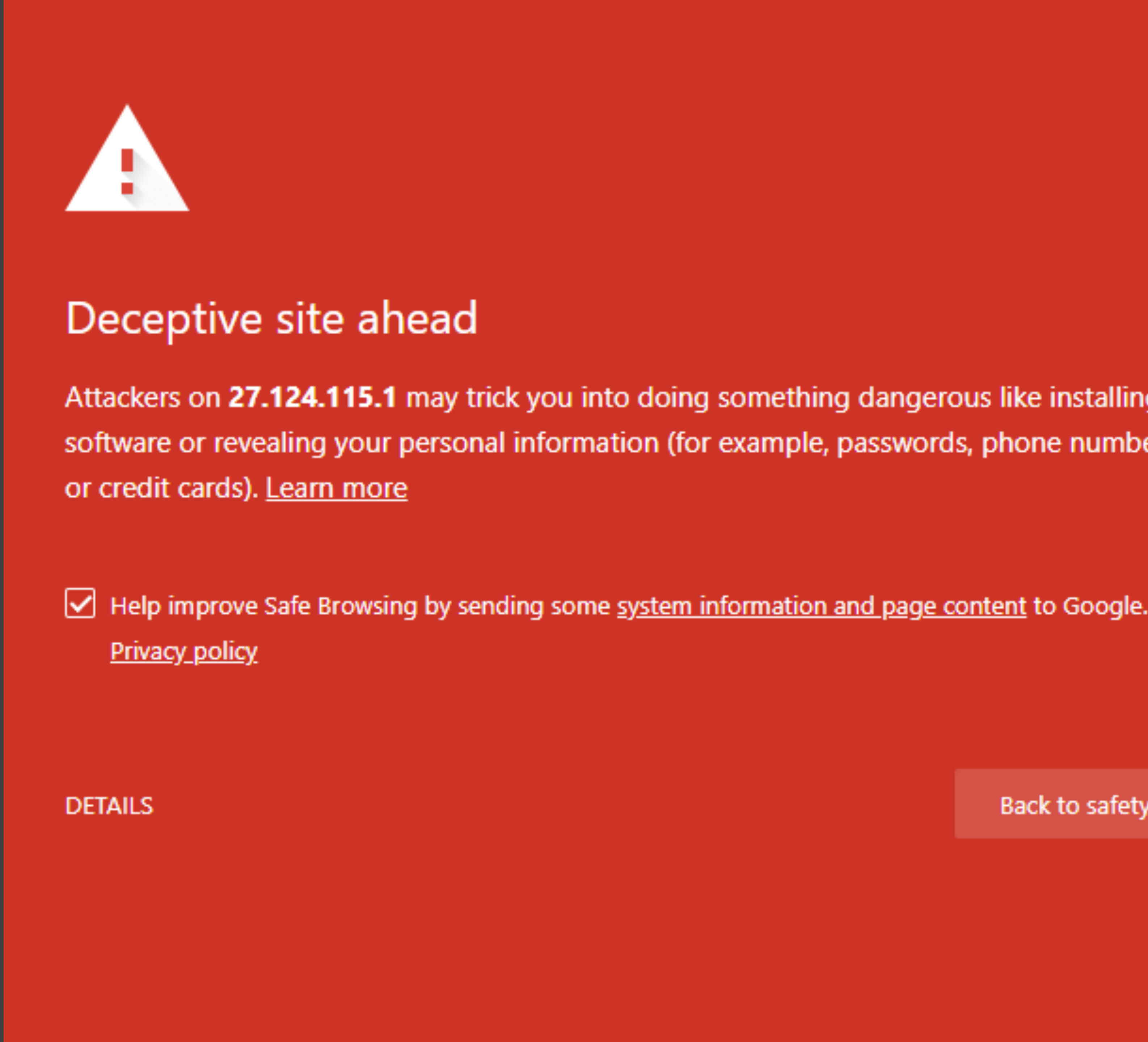
PHISHING

SECURITY WARNINGS

VITALY SHMATIKOV

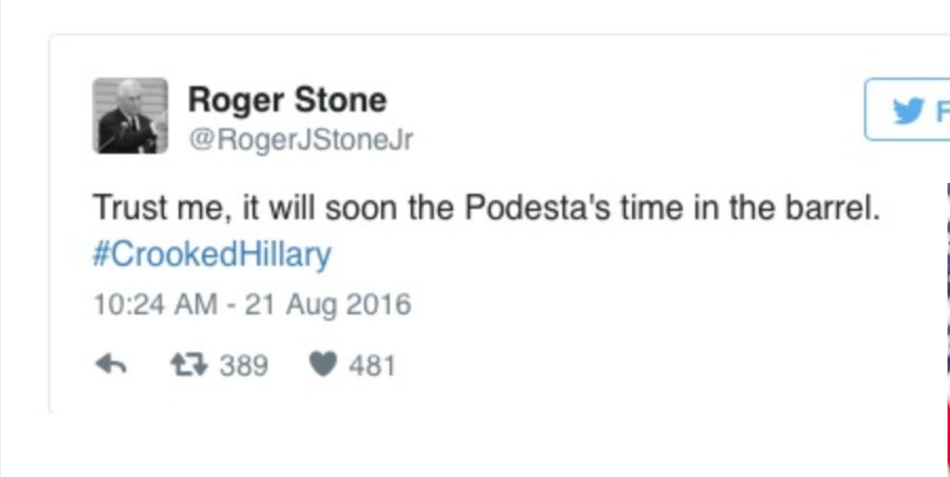


Deceptive site ahead

Attackers on **27.124.115.1** may trick you into doing something dangerous like installin software or revealing your personal information (for example, passwords, phone numbe or credit cards). Learn more

☑ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

Back in 2016

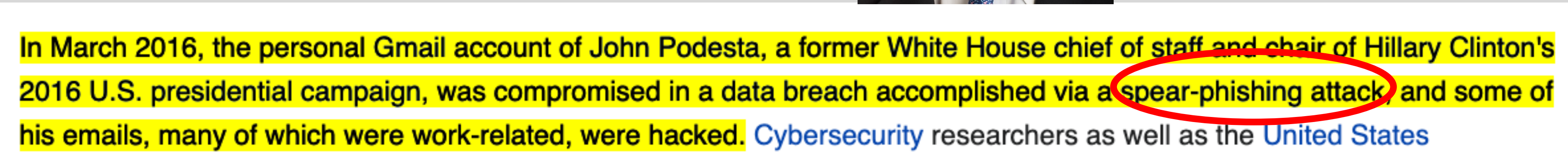


Roger Stone
@RogerJStoneJr

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

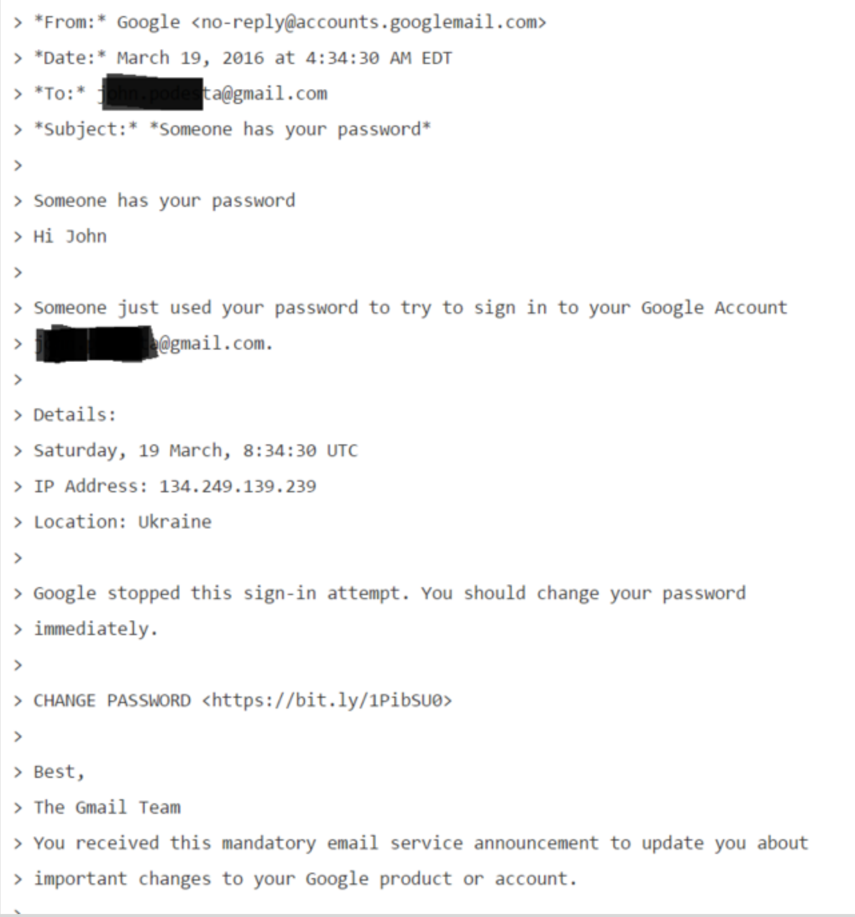
10:24 AM - 21 Aug 2016

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

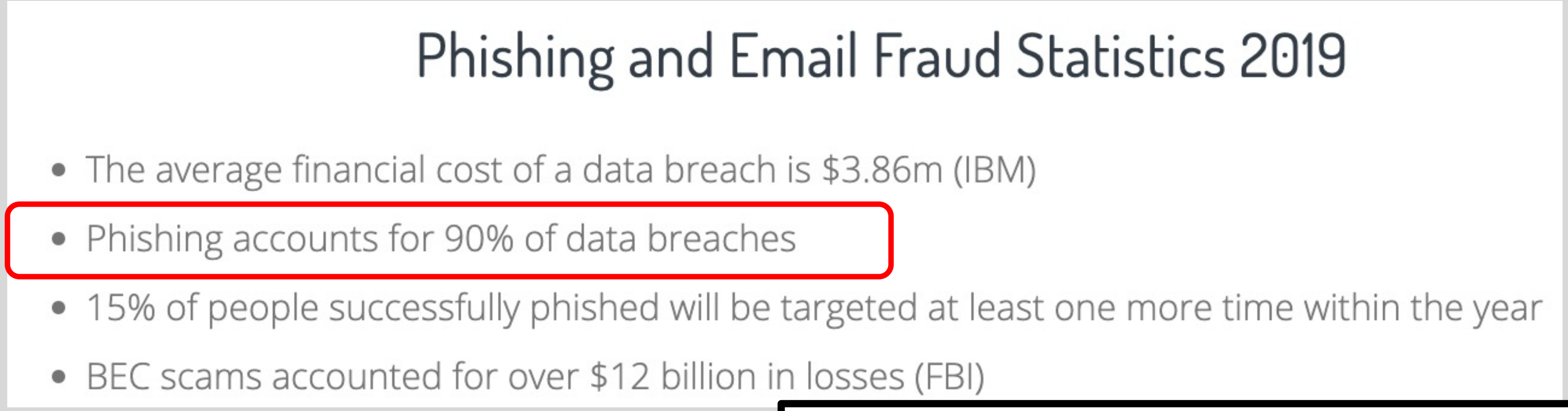
“Change Your Password Immediately”



```
> *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 your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [redacted]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> 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.

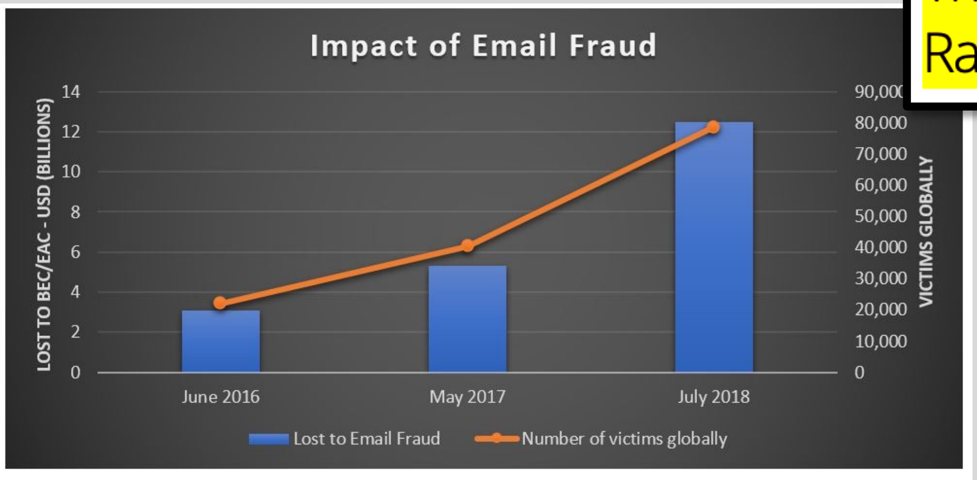
The email was initially sent to the IT department as it was suspected of being a fake but was described as "legitimate" in an e-mail sent by a department employee, who later said he meant to write "illegitimate".



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

Zirconium (APT31) Attacks

Zirconium, operating from China, has attempted to gain intelligence on organizations associated with the upcoming U.S. presidential election

…

Zirconium is using what are referred to as web bugs, or web beacons, tied to a domain they purchased and populated with content. The actor then sends the associated URL in either email text or an attachment to a targeted account. Although the domain itself may not have malicious content, the web bug allows Zirconium to check if a user attempted to access the site. For nation-state actors, this is a simple way to perform reconnaissance on targeted accounts to determine if the account is valid or the user is active.

https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/

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

Experiments at Indiana U. (2006)

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 (domain name clearly distinct from indiana.edu) inviting the user to enter his/her secure university credentials

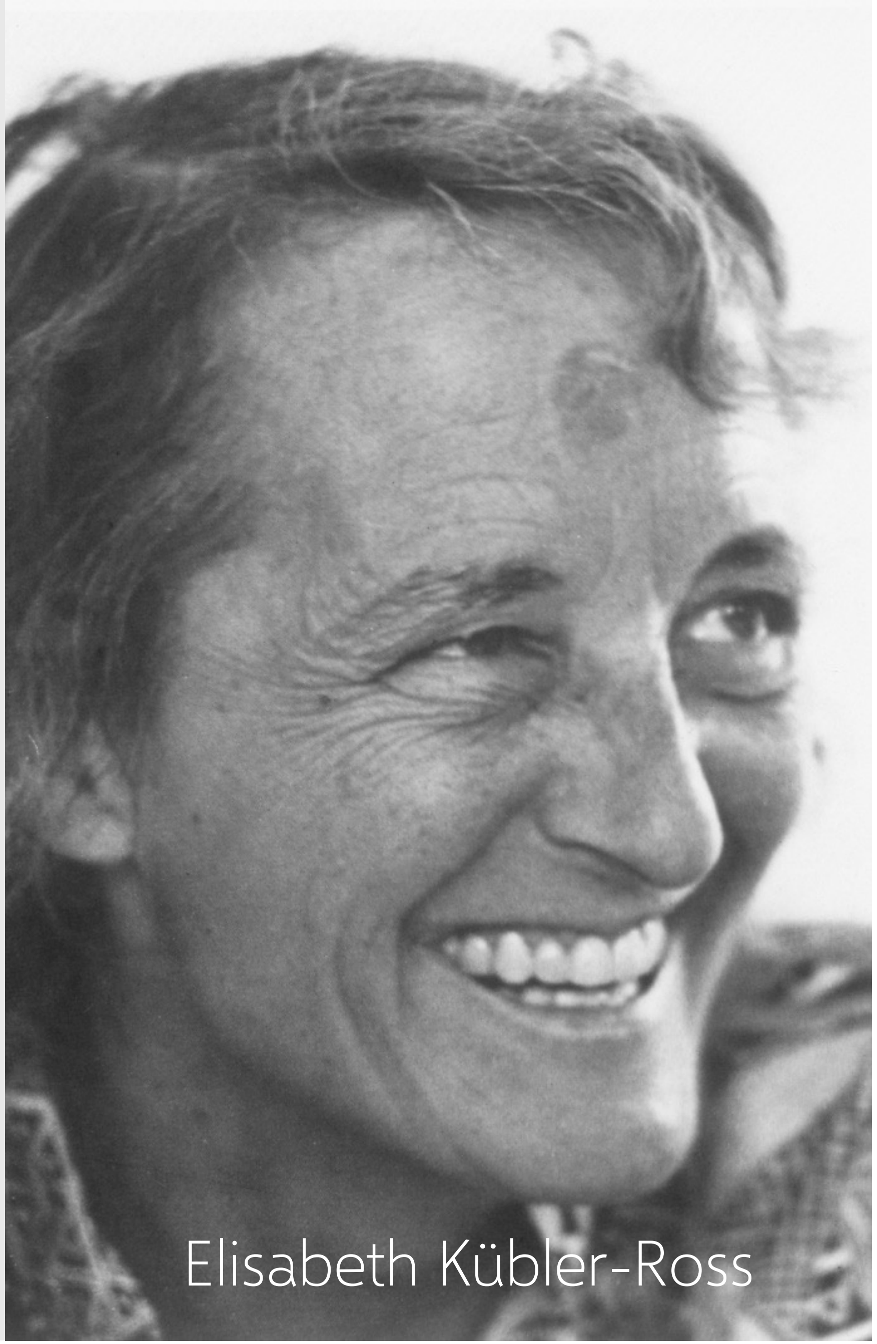
72% of students entered their real credentials into the spoofed site (most within the first 12 hours)

- Males more likely to do this if email is from a female

Jagatic et al.

Five Stages of Grief

- Denial
- Anger
- Bargaining
- Depression
- Acceptance



Elisabeth Kübler-Ross

Victims' Reactions (1)

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

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

Jagatic et al.

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

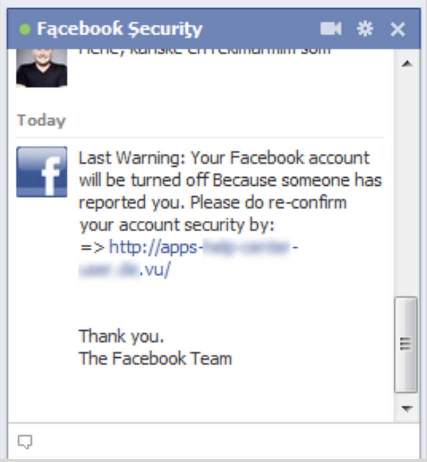
- Many subjects didn't understand how the researchers obtained information about their friends, and assumed that the researchers accessed their address books
- Others, understanding that the information was mined from social network sites, objected that their privacy had been violated by the researchers who accessed the information that they had posted online

Jagatic et al.

Facebook Phishing

- Attack steals Facebook credentials
- Changes profile picture of compromised account to f and the name to “Fąceboōk Şecurițy”
- Sends a message to all contacts:

Notice anything?



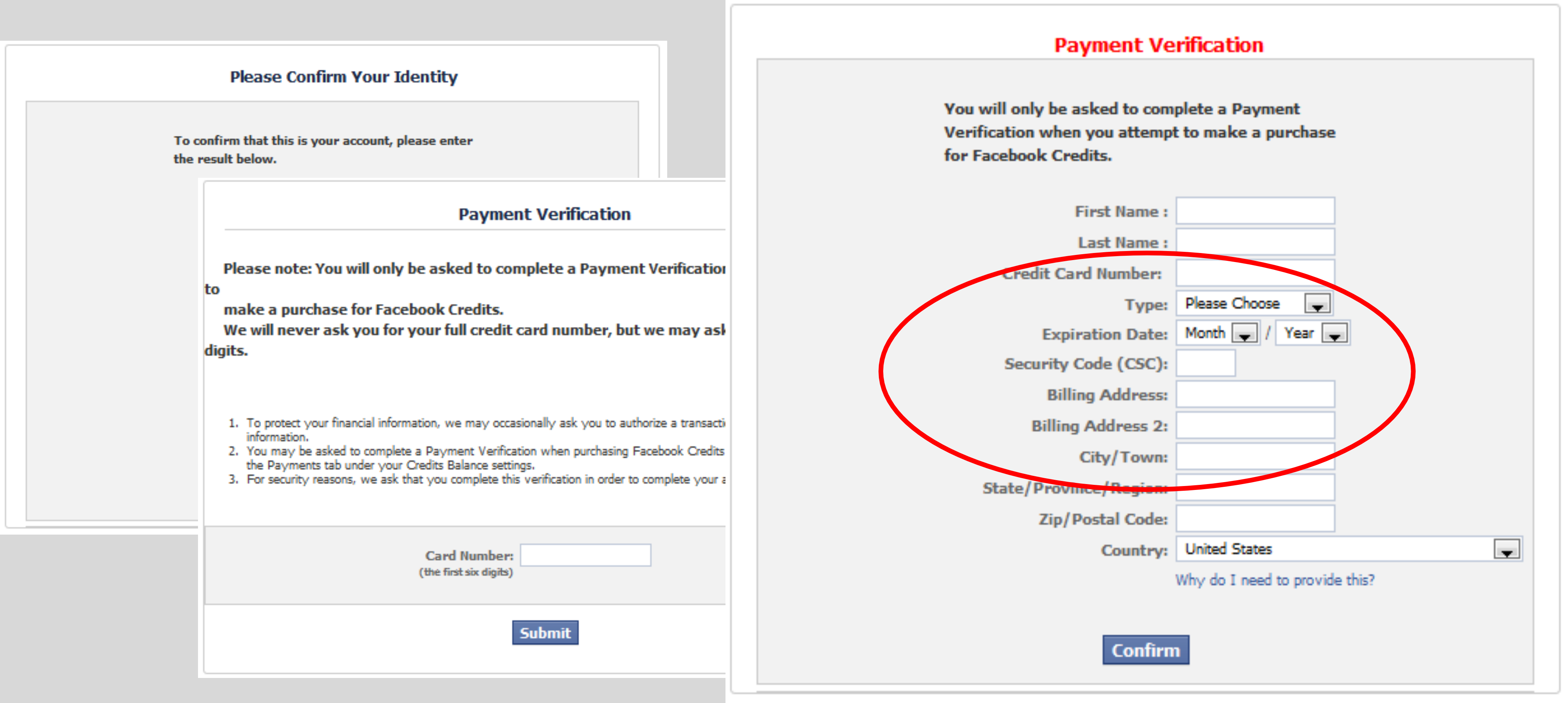
Today

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

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

“Payment Verification”



Please Confirm Your Identity

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

Payment Verification

Please note: You will only be asked to complete a Payment Verificatior to make a purchase for Facebook Credits.
We will never ask you for your full credit card number, but we may ask digits.

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

Card Number: (the first six digits)

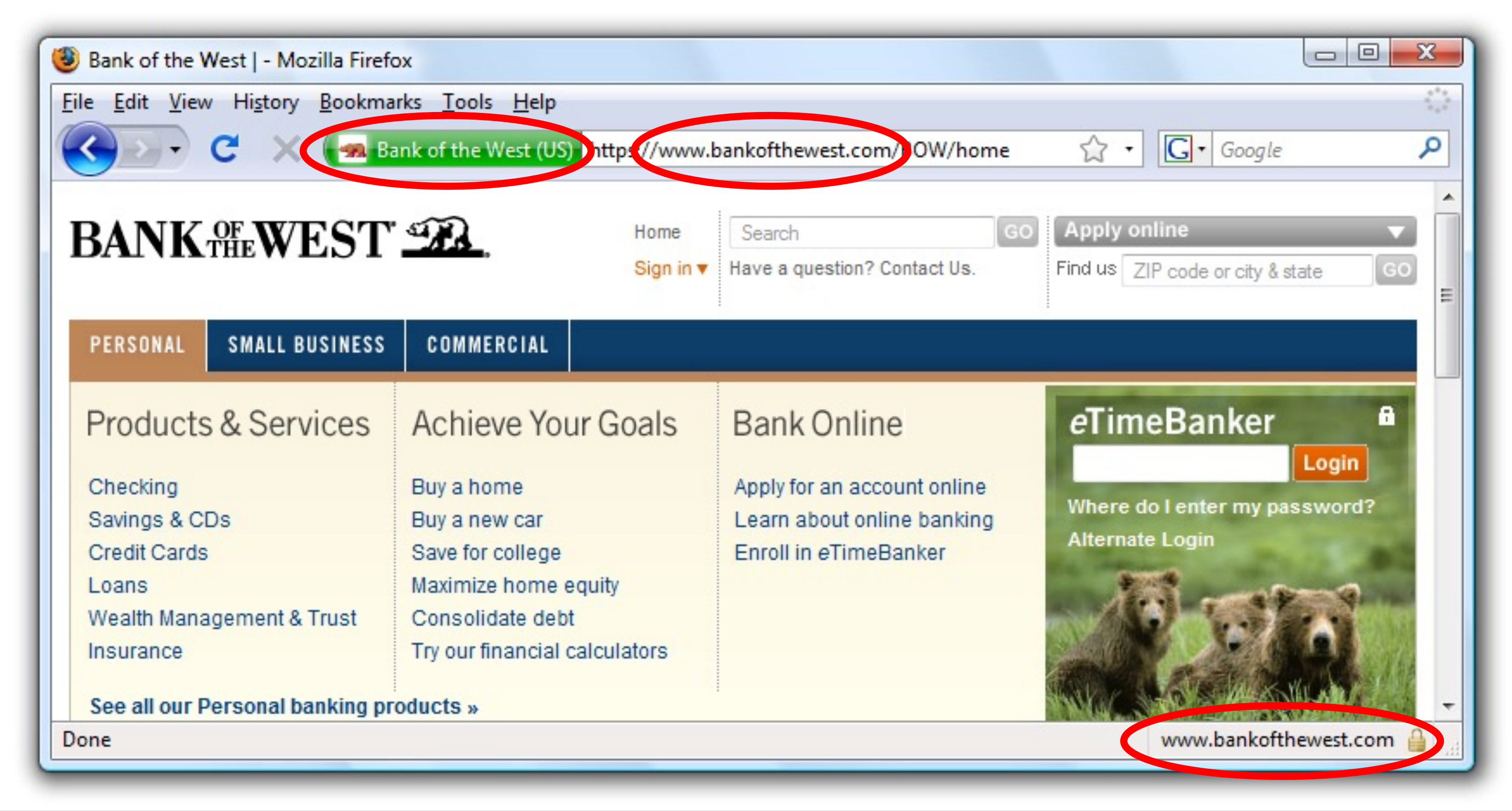
Payment Verification

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

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

Safe to Type Your Password?



Bank of the West | - Mozilla Firefox

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

BANK OF THE WEST

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

See all our Personal banking products »

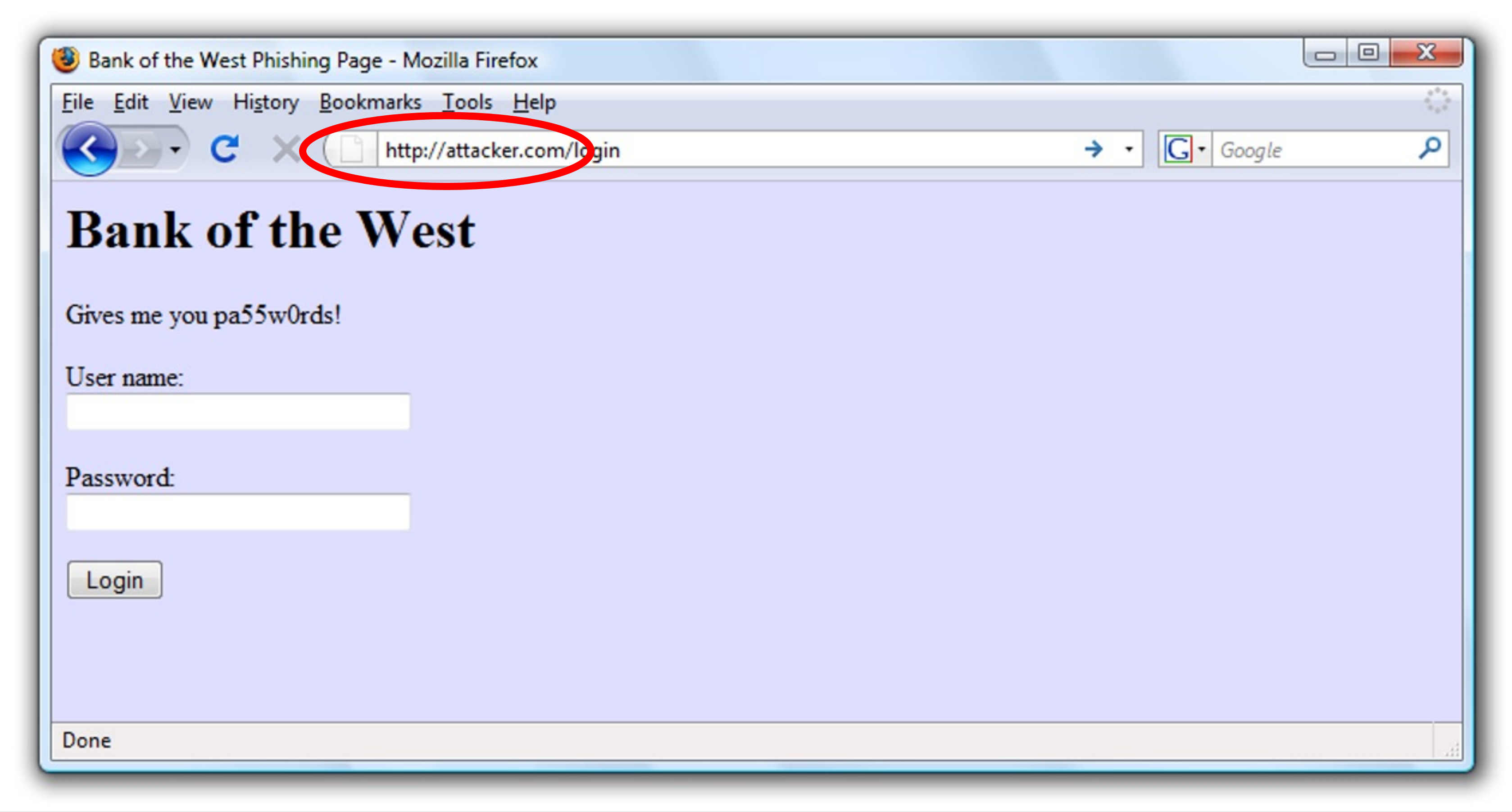
eTimeBanker

Where do I enter my password?
Alternate Login

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
Done

Bank of the West

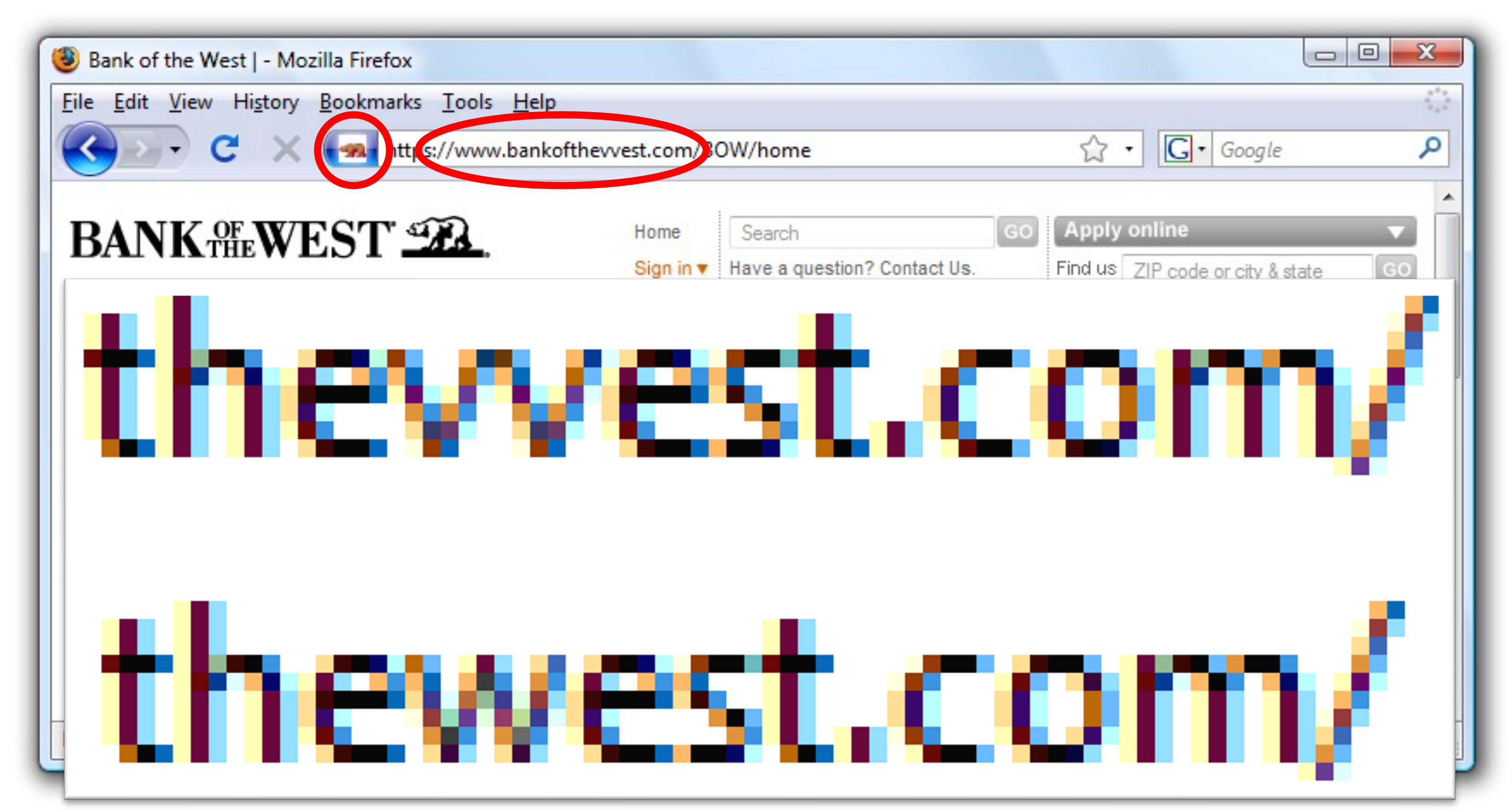
Gives me you pa55w0rds!

User name:

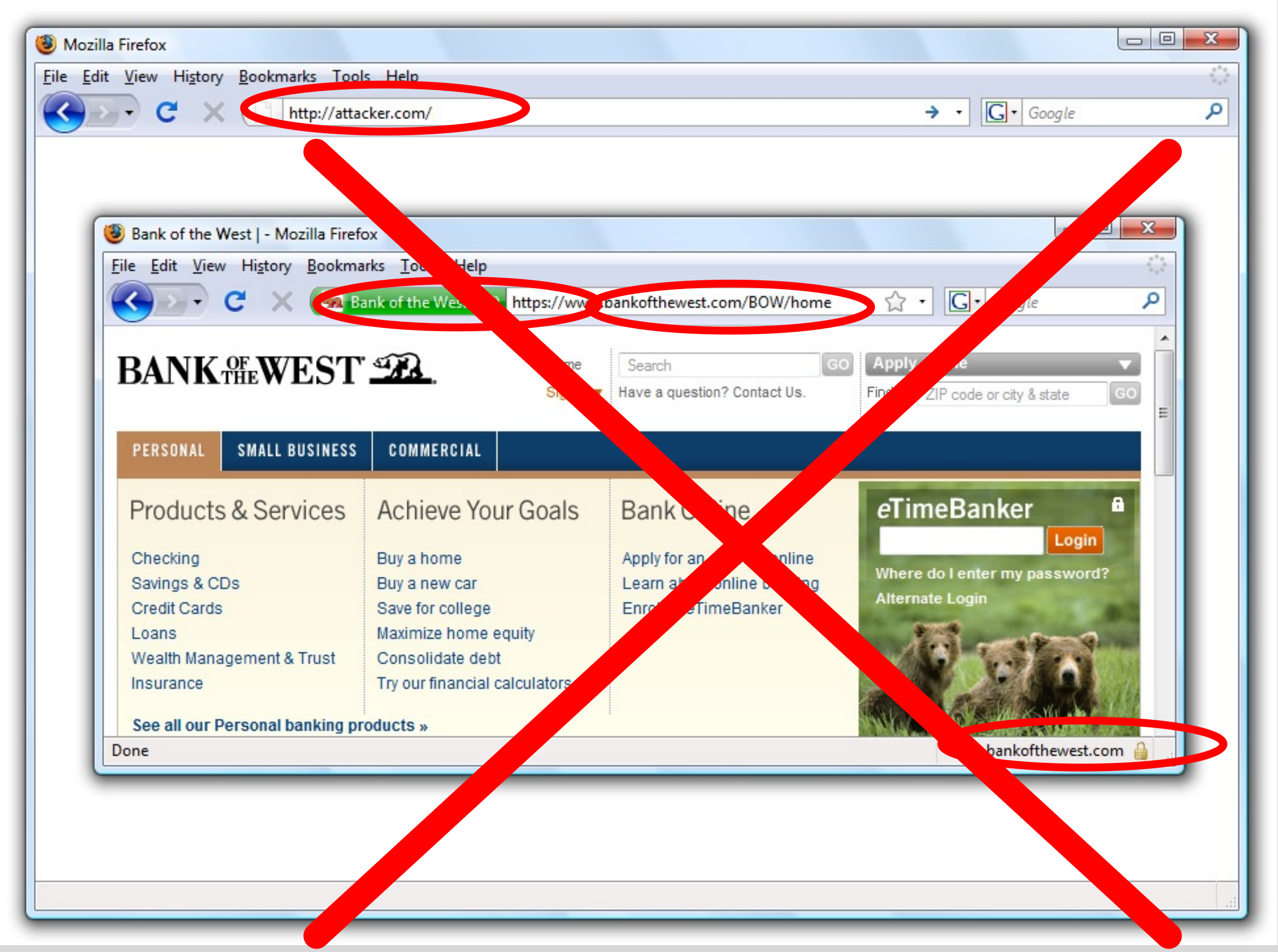
Password:

Login

Safe to Type Your Password?

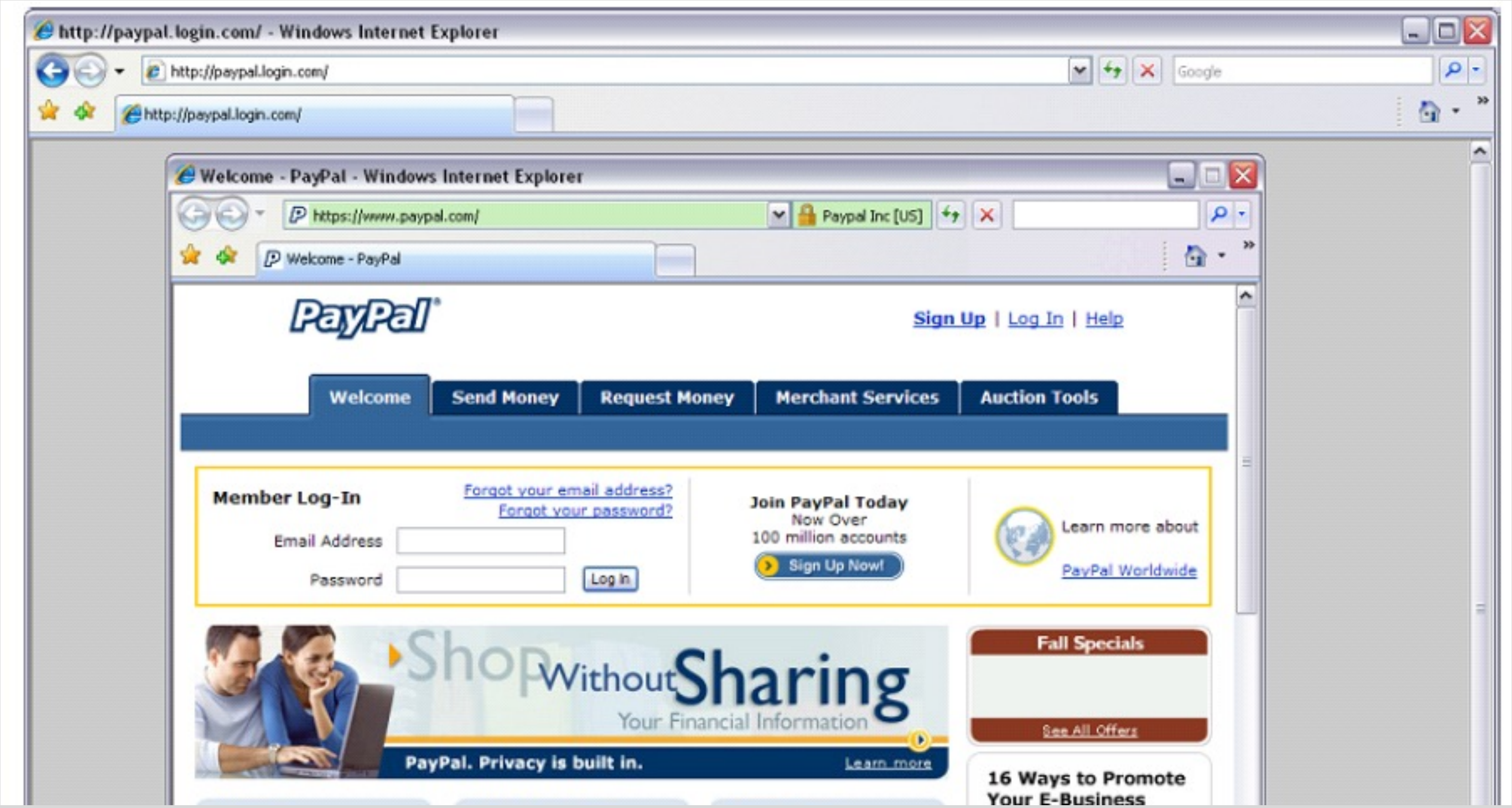


Safe to Type Your Password?



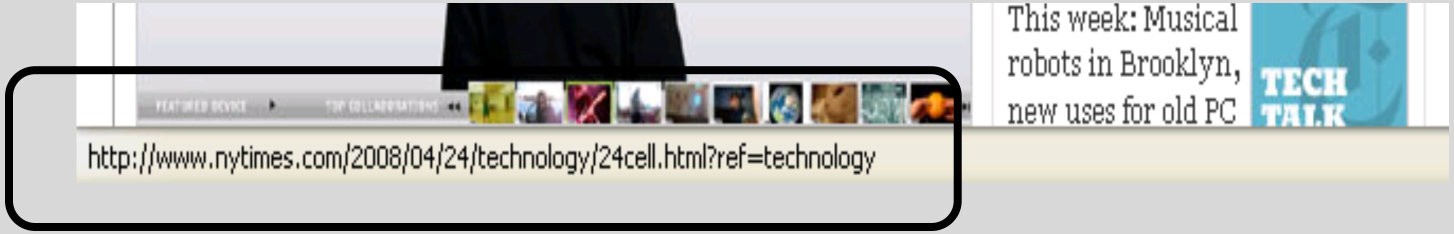
Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://attacker.com/
Google
Bank of the West | - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Bank of the West
https://www.bankofthewest.com/BOW/home
BANK OF THE WEST
Search GO
Have a question? Contact Us.
ZIP code or city & state 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
eTimeBanker
Login
Where do I enter my password?
Alternate Login
See all our Personal banking products »
Done
bankofthewest.com

Picture-in-Picture Attacks



Trained users are more likely to fall for this

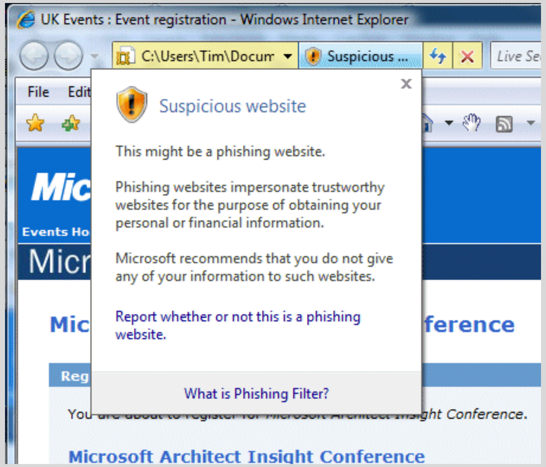
Status Bar Is Trivially Spoofable



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>
```

Browser Warnings



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.

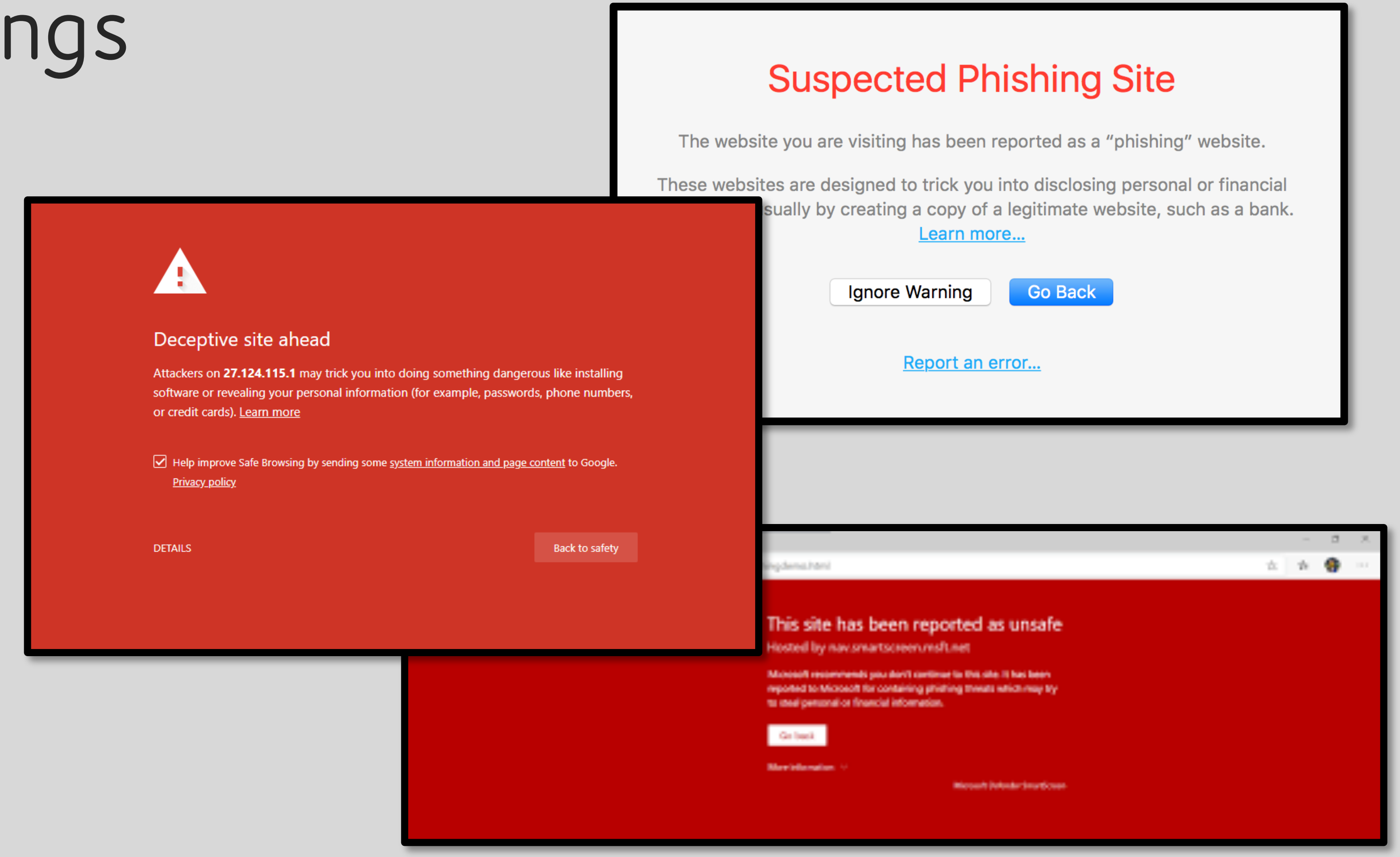
Report whether or not this is a phishing website.

What is Phishing Filter?

You are about to register for Microsoft Architect Insight Conference.

Microsoft Architect Insight Conference

Passive
(not very effective)



Suspected Phishing Site

The website you are visiting has been reported as a “phishing” website.

These websites are designed to trick you into disclosing personal or financial sually by creating a copy of a legitimate website, such as a bank. Learn more...

Report an error...

Deceptive site ahead

Attackers on **27.124.115.1** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more

☑ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

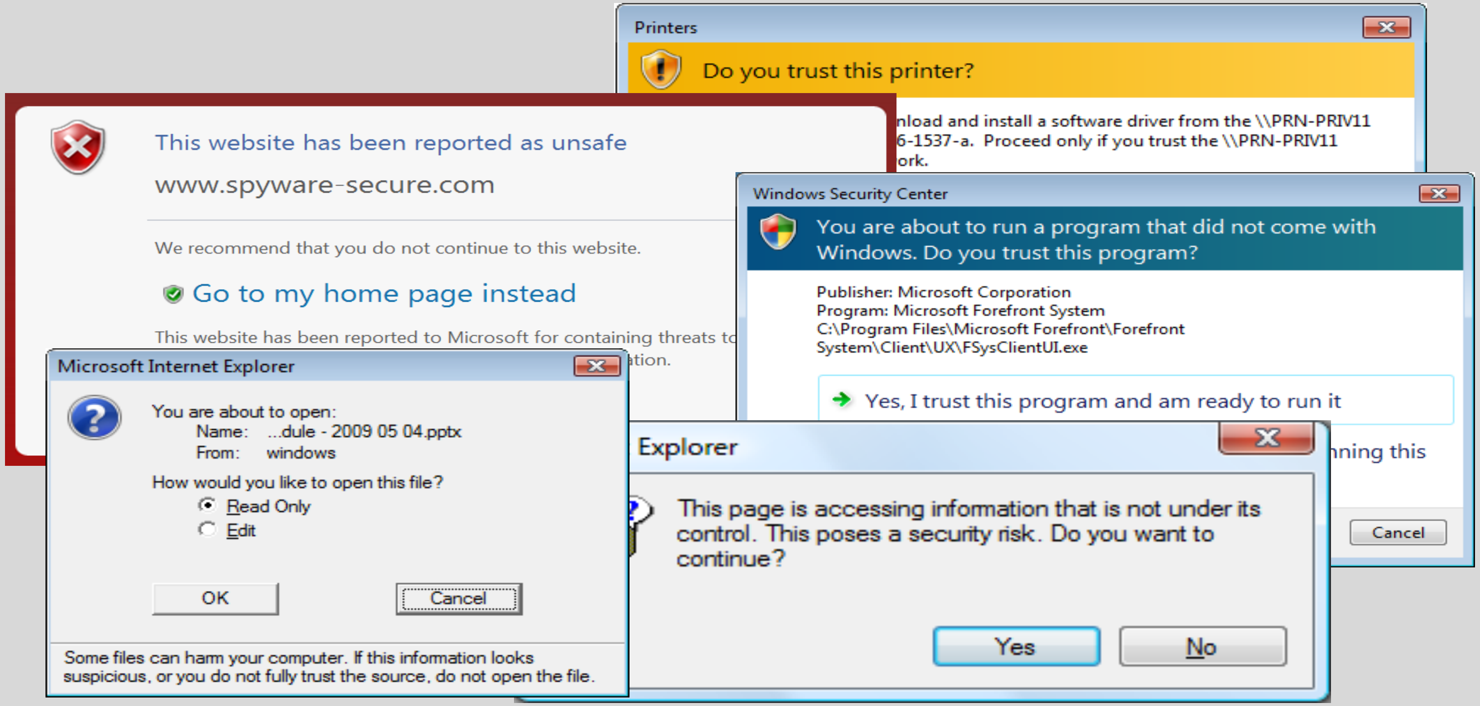
This site has been reported as unsafe

Hosted by nav.smartscreen.msft.net

Microsoft recommends you don't continue to this site. It has been reported to Microsoft for containing phishing threats which may try to steal personal or financial information.

Active

More About Security Warnings



Printers

Do you trust this printer?

nload and install a software driver from the \\PRN-PRIV11
6-1537-a. Proceed only if you trust the \\PRN-PRIV11
ork.

This website has been reported as unsafe

www.spyware-secure.com

We recommend that you do not continue to this website.

Go to my home page instead

This website has been reported to Microsoft for containing threats to
tion.

Windows Security Center

You are about to run a program that did not come with Windows. Do you trust this program?

Publisher: Microsoft Corporation
Program: Microsoft Forefront System
C:\Program Files\Microsoft Forefront\Forefront System\Client\UX\FSysClientUI.exe

Yes, I trust this program and am ready to run it

nning this

Microsoft Internet Explorer

You are about to open:
Name: ...dule - 2009 05 04.pptx
From: windows

How would you like to open this file?

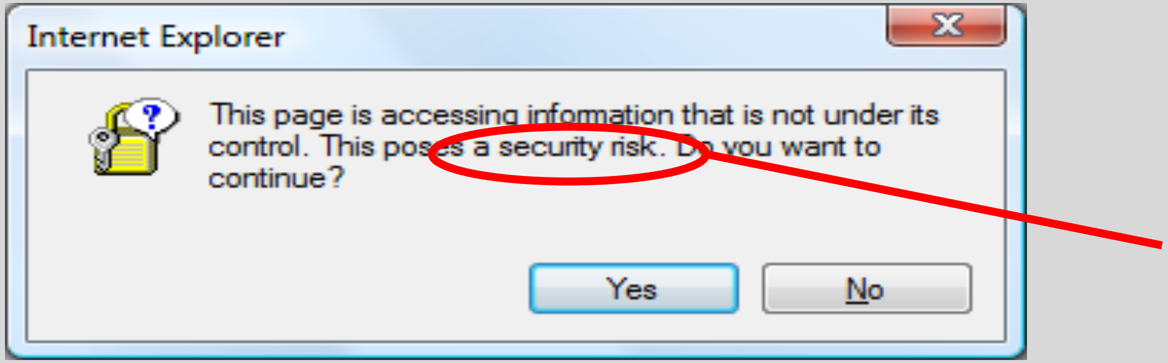
● Read Only
○ Edit

Some files can harm your computer. If this information looks suspicious, or you do not fully trust the source, do not open the file.

Explorer

This page is accessing information that is not under its control. This poses a security risk. Do you want to continue?

Bad Example: Mixed Content in IE6 (circa 2004)


Internet Explorer

This page is accessing information that is not under its control. This poses a security risk. Do you want to continue?

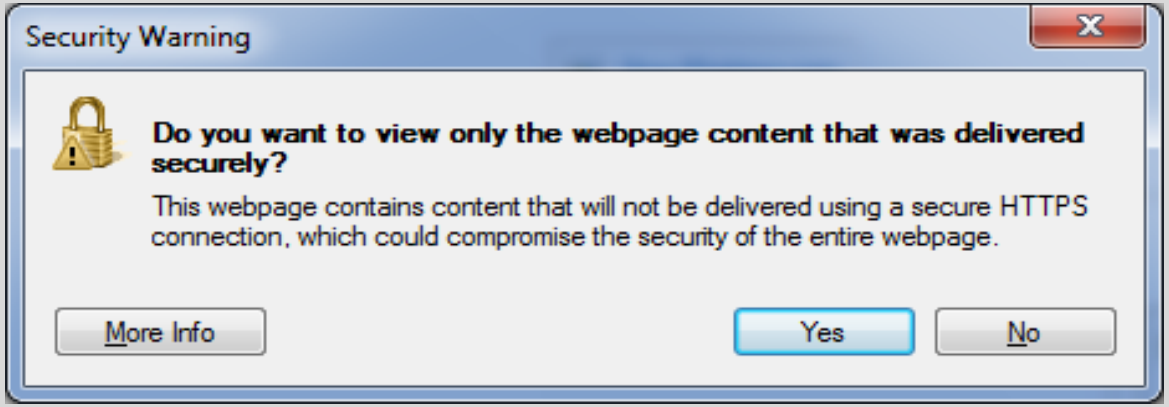
Vague threat.
What’s the risk?
What could happen?

“Yes”, the possibly less safe option, is the default

How should the user make this decision?
No clear steps for user to follow.

Better (IE8)

"Yes" does the safe thing by default!



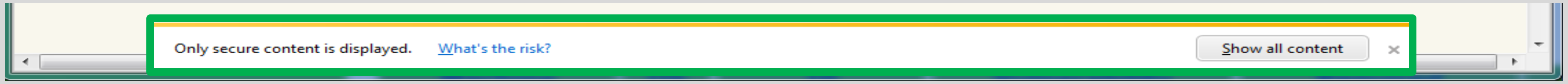
Security Warning

Do you want to view only the webpage content that was delivered securely?

This webpage contains content that will not be delivered using a secure HTTPS connection, which could compromise the security of the entire webpage.

Even better (IE9)

Load the safe content, and use the address bar to enable the rest



Only secure content is displayed. What's the risk?

Guidelines for Security Warnings

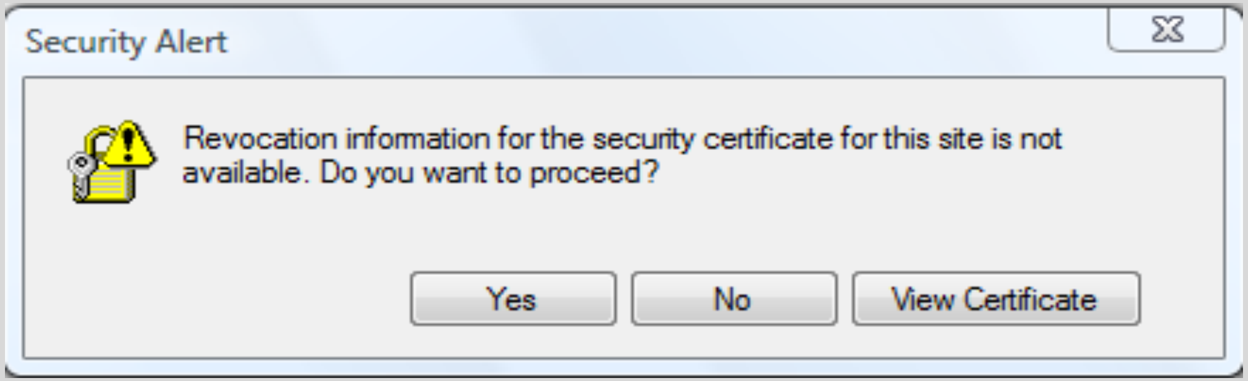
Philosophy

- Does the user have unique knowledge the system doesn't?
- Don't involve user if you don't have to
- If you involve the user, enable them to make the right decision

Make sure your security dialogs are NEAT

- **Necessary**: Can the system take action without the user? If the user has no unique knowledge, redesign system.
- **Explained**
- **Actionable**: Can users make good decisions with your UI in both malicious and benign situations?
- **Tested**: Test your dialog on a few people who haven't used the system before -- both malicious and benign situations.

Bad Example (IE6): Revoked SSL Certificate

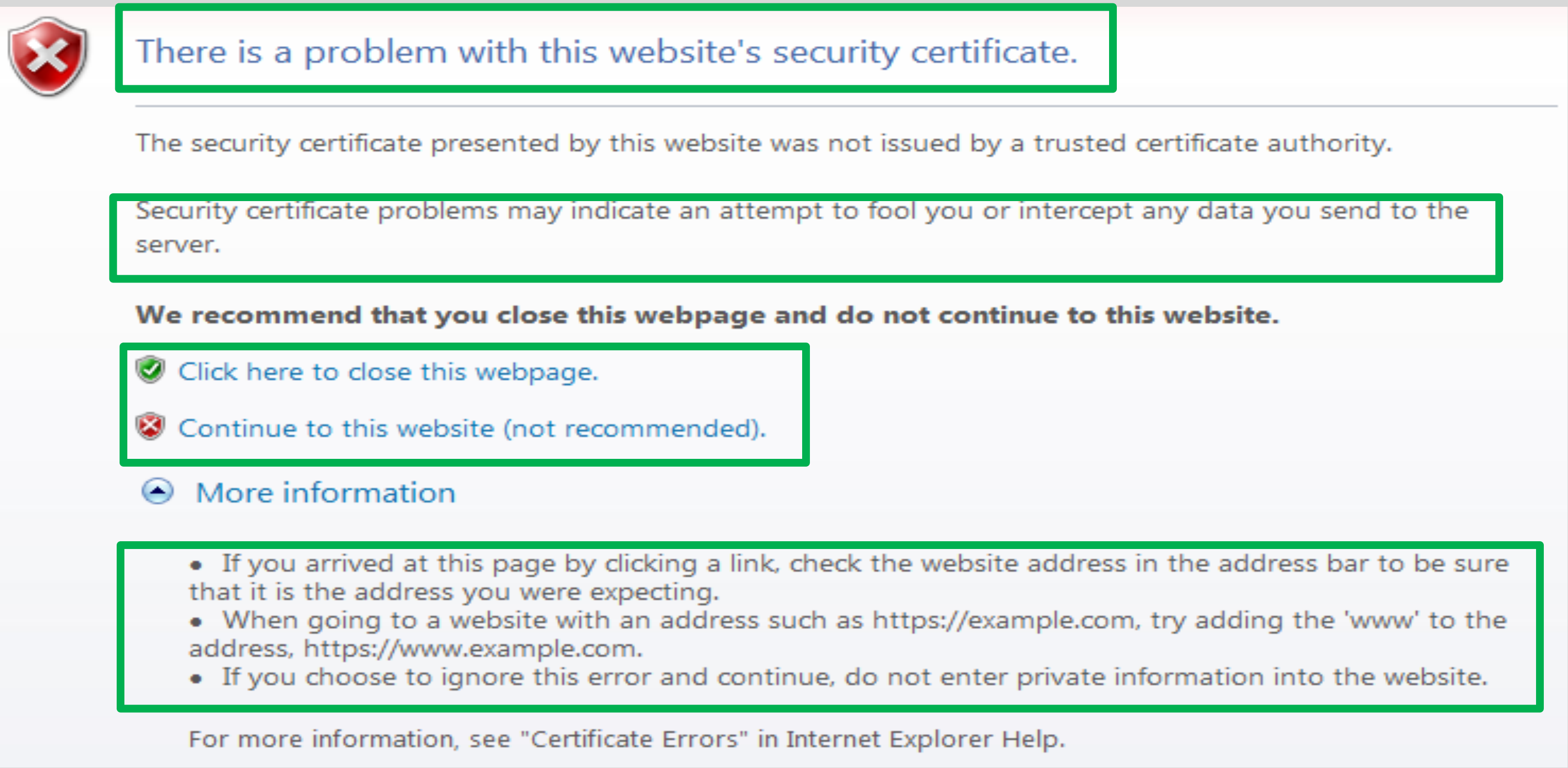


Revocation information for the security certificate for this site is not available. Do you want to proceed?

Most users will not understand “revocation information”

Choices are unclear, consequence is unclear

Better Explanation



Source

Risk

Choices

Process

There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

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

- If you arrived at this page by clicking a link, check the website address in the address bar to be sure that it is the address you were expecting.
- When going to a website with an address such as https://example.com, try adding the 'www' to the address, https://www.example.com.
- If you choose to ignore this error and continue, do not enter private information into the website.

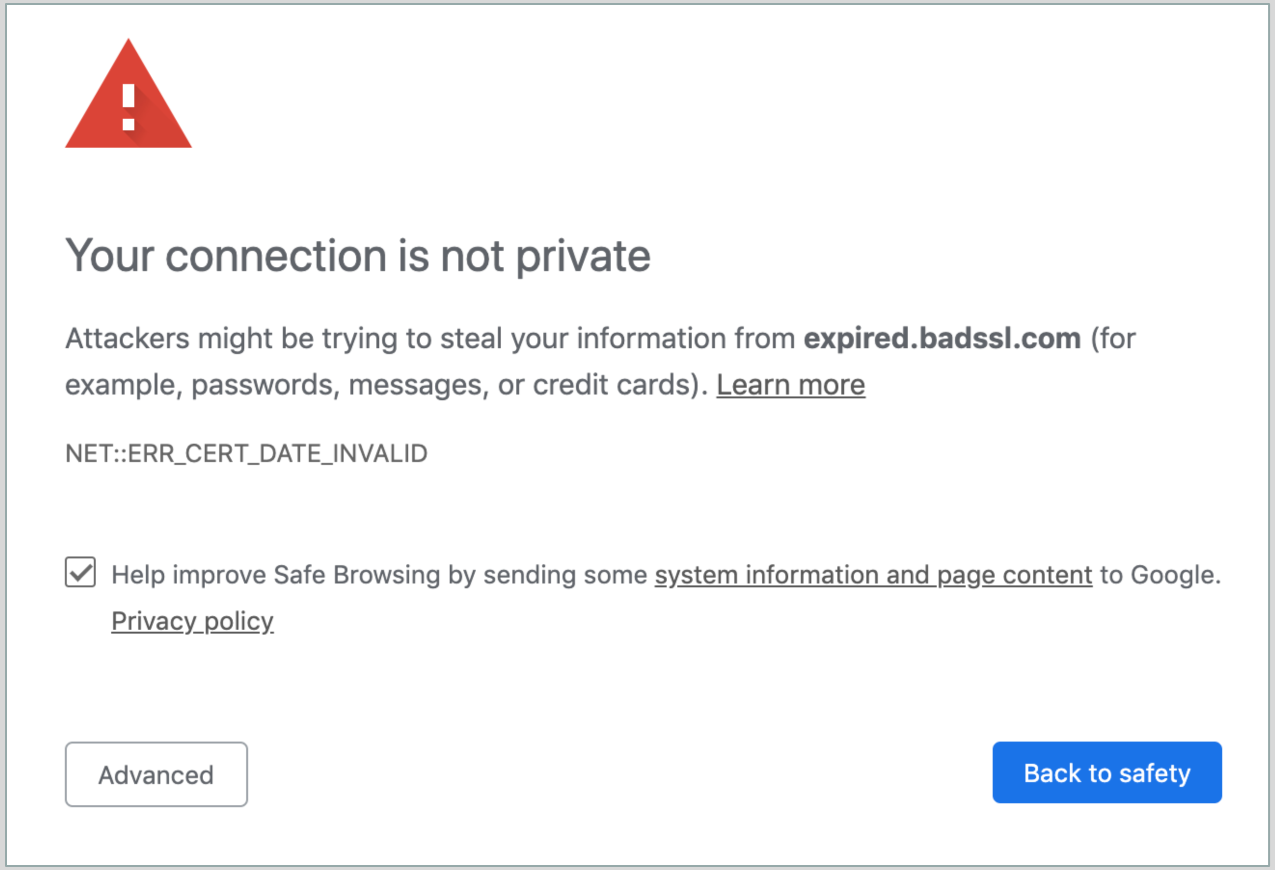
For more information, see "Certificate Errors" in Internet Explorer Help.

Chrome (2019)

Risk

Explanations

Choices



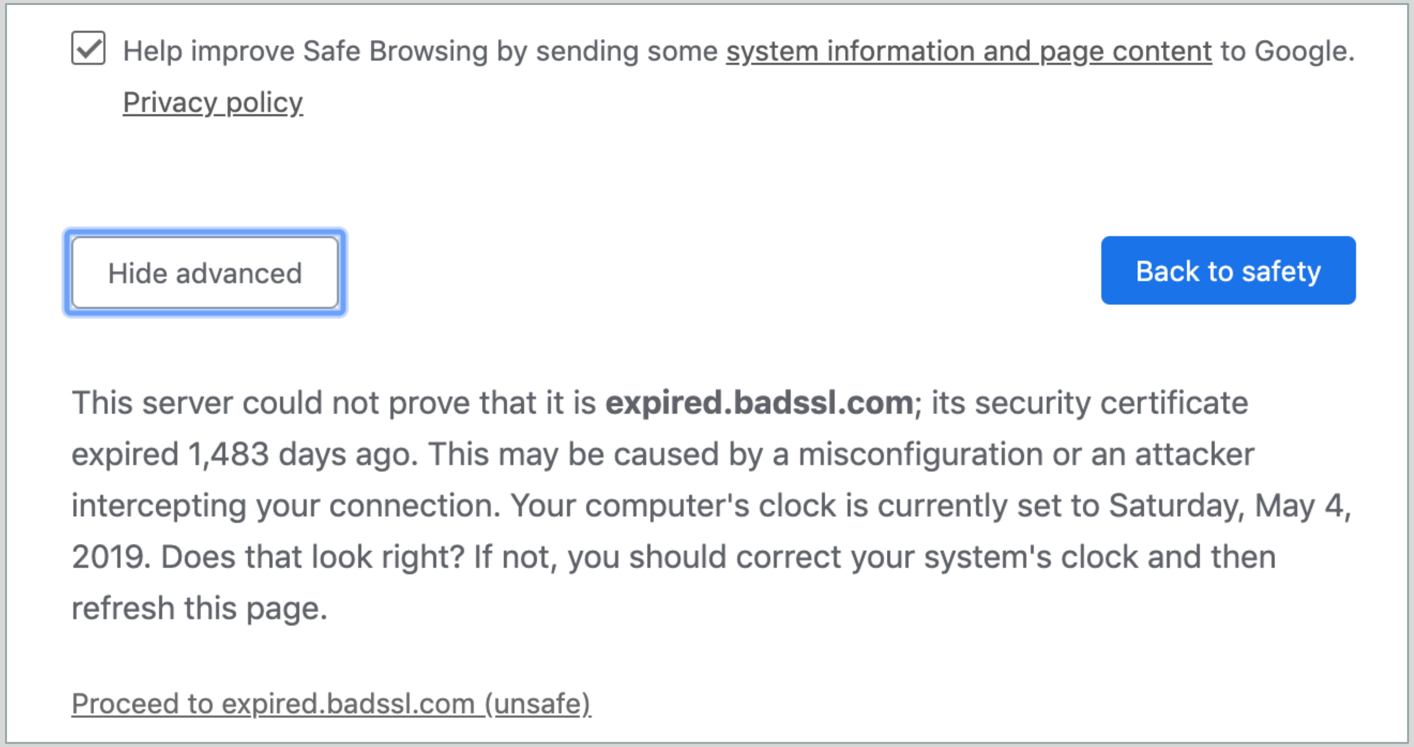
Your connection is not private

Attackers might be trying to steal your information from **expired.badssl.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_DATE_INVALID

☑ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

Chrome (2019)



☑ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

This server could not prove that it is **expired.badssl.com**; its security certificate expired 1,483 days ago. This may be caused by a misconfiguration or an attacker intercepting your connection. Your computer's clock is currently set to Saturday, May 4, 2019. Does that look right? If not, you should correct your system's clock and then refresh this page.

Proceed to expired.badssl.com (unsafe)

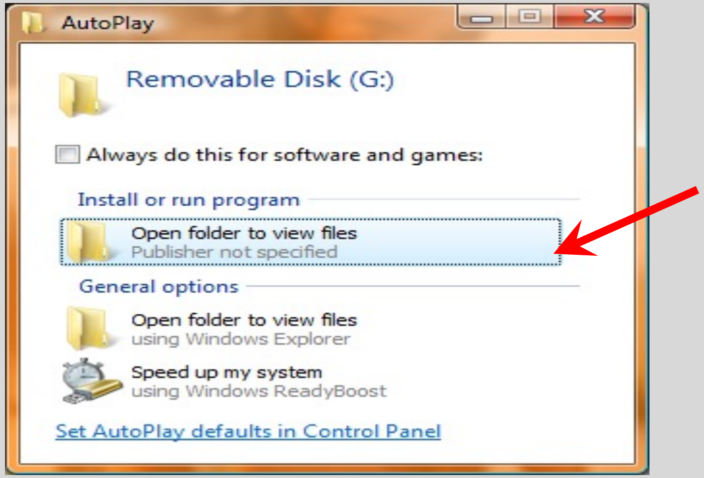
Process

Choice

(expired certificate)

Bad Explanation (Windows Vista)

AutoPlay dialog in Vista



Removable Disk (G:)

□ Always do this for software and games:

Install or run program

Open folder to view files
Publisher not specified

General options

Open folder to view files
using Windows Explorer

Speed up my system
using Windows ReadyBoost

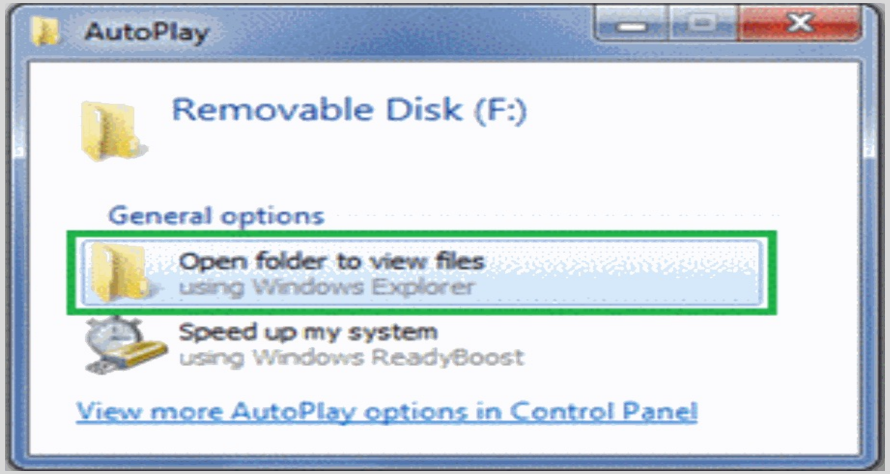
Set AutoPlay defaults in Control Panel

This is the name of a file on USB

Attacker can abuse the explanation, causing bad user decisions

Used by Conficker virus to spread through USB drives

Better Design



AutoPlay

Removable Disk (F:)

General options

Open folder to view files
using Windows Explorer

Speed up my system
using Windows ReadyBoost

View more AutoPlay options in Control Panel

Windows 7 AutoPlay removed the auto-run option