CS 370: Introduction to Security
05.18: Advanced web security III

Tu/Th 4:00 – 5:50 PM

Sanghyun Hong

sanghyun.hong@oregonstate.edu

Oregon State University

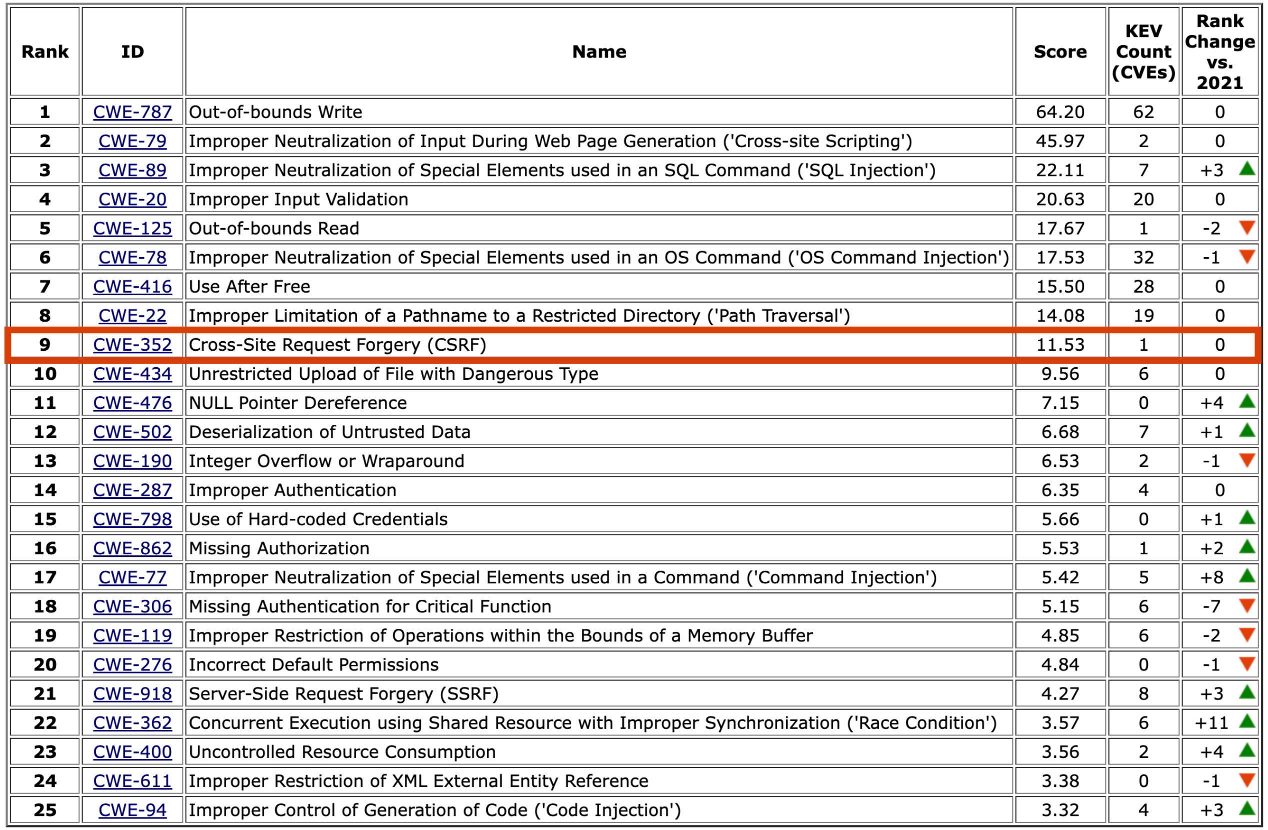
SAIL
Secure AI Systems Lab

Topics for today

- Advanced web security
  - CSRF (Cross-Site Request Forgery)
    - Cookies
    - Session
    - CSRF attacks
    - Defenses (and their potential weaknesses)
  - UI attacks
    - Clickjacking
    - Phishing
    - 2FA (and their potential weaknesses)

Security risks on the internet

- Risk III



Rank	ID	Name	Score	KEV Count (CVEs)	Rank Change vs. 2021
1	CWE-787	Out-of-bounds Write	64.20	62	0
2	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	45.97	2	0
3	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	22.11	7	+3 ▲
4	CWE-20	Improper Input Validation	20.63	20	0
5	CWE-125	Out-of-bounds Read	17.67	1	-2 ▼
6	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17.53	32	-1 ▼
7	CWE-416	Use After Free	15.50	28	0
8	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	14.08	19	0
9	CWE-352	Cross-Site Request Forgery (CSRF)	11.53	1	0
10	CWE-434	Unrestricted Upload of File with Dangerous Type	9.56	6	0
11	CWE-476	NULL Pointer Dereference	7.15	0	+4 ▲
12	CWE-502	Deserialization of Untrusted Data	6.68	7	+1 ▲
13	CWE-190	Integer Overflow or Wraparound	6.53	2	-1 ▼
14	CWE-287	Improper Authentication	6.35	4	0
15	CWE-798	Use of Hard-coded Credentials	5.66	0	+1 ▲
16	CWE-862	Missing Authorization	5.53	1	+2 ▲
17	CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')	5.42	5	+8 ▲
18	CWE-306	Missing Authentication for Critical Function	5.15	6	-7 ▼
19	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	4.85	6	-2 ▼
20	CWE-276	Incorrect Default Permissions	4.84	0	-1 ▼
21	CWE-918	Server-Side Request Forgery (SSRF)	4.27	8	+3 ▲
22	CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	3.57	6	+11 ▲
23	CWE-400	Uncontrolled Resource Consumption	3.56	2	+4 ▲
24	CWE-611	Improper Restriction of XML External Entity Reference	3.38	0	-1 ▼
25	CWE-94	Improper Control of Generation of Code ('Code Injection')	3.32	4	+3 ▲

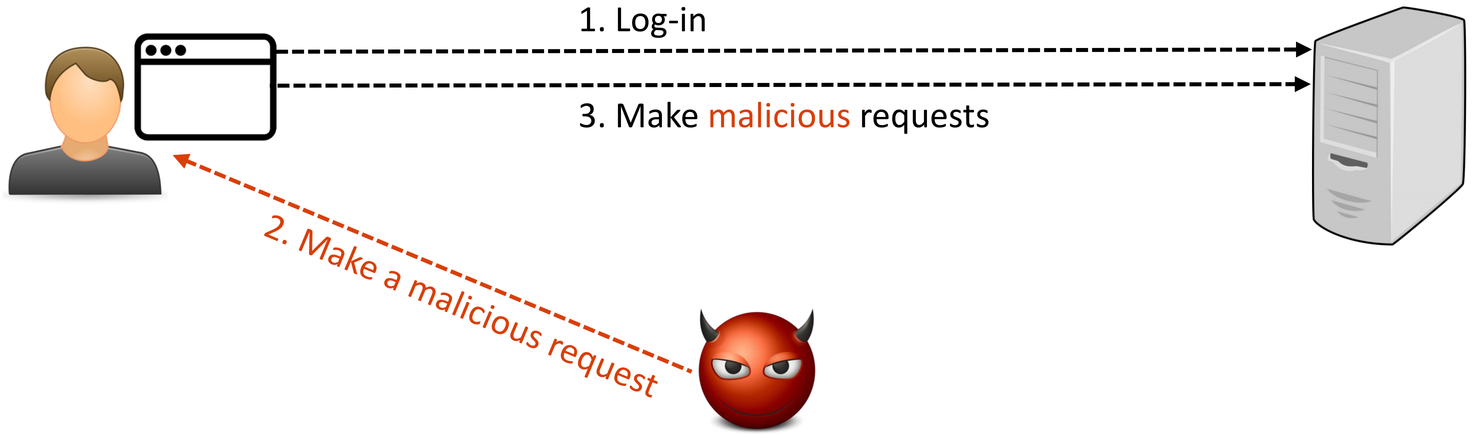
[1]https://cwe.mitre.org/top25/archive/2022/2022_cwe_top25.html

CSRF: Cross-site request forgery

- CSRF (one-click attack or session riding)
  - Make legitimate users to send malicious requests to the server
    - The attacker impersonates a legitimate user
    - The user's browser will automatically attach (malicious) cookies (It exploits the cookie-based authentication mechanism)

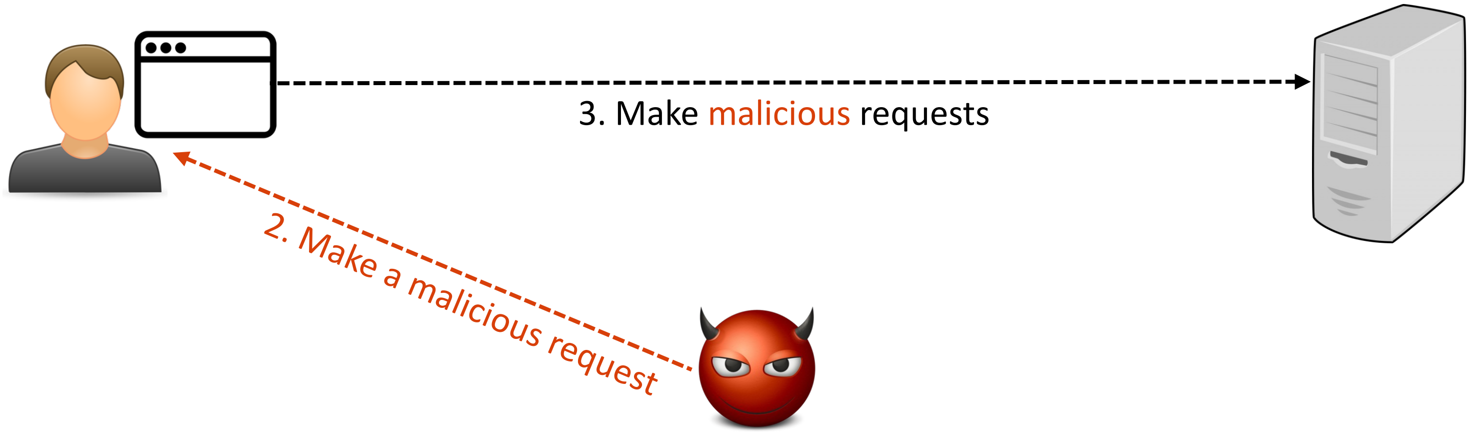
CSRF: Cross-site request forgery

- CSRF (one-click attack or session riding)
  - Attack Illustration
    - A user authenticates to the server
    - The attacker tricks the user into making a malicious request
    - The server accepts the malicious request from the legitimate user
    - The server is the target!



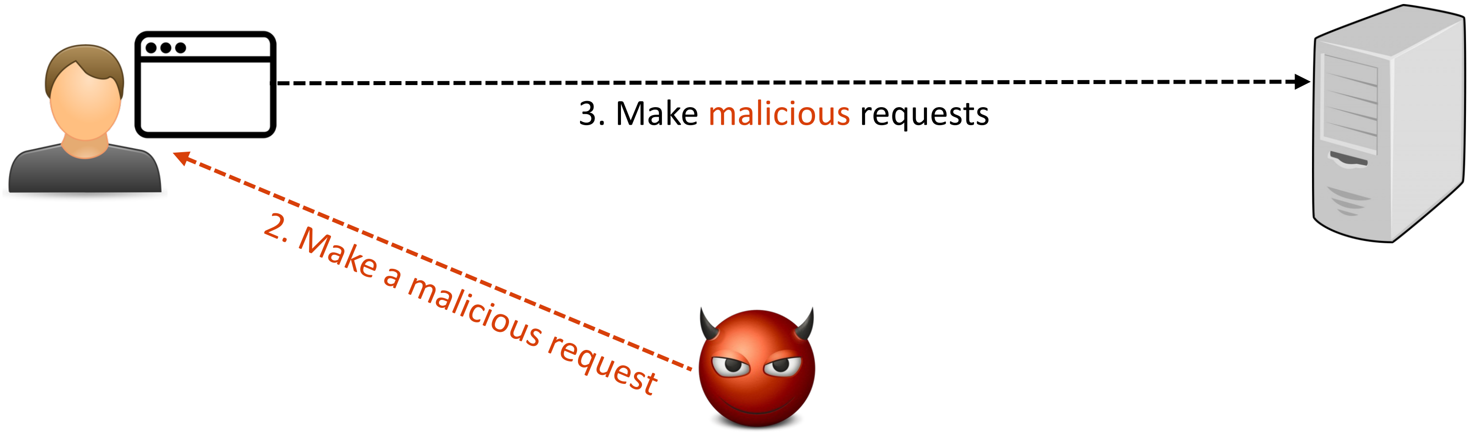
CSRF: Cross-site request forgery

- CSRF (one-click attack or session riding)
  - How can an adversary trick the user?
    - GET request:
      - Make the user into clicking a link (SMS, Spam, …)
      - `https://bank.com/transfer?amount=10000&to=Mallony`
      - Put some html on a website the victim will visit (1x1 pixel image with a request)
      - `<img src="https://bank.com/transfer?amount=10000&to=Mallony">`



CSRF: Cross-site request forgery

- CSRF (one-click attack or session riding)
  - How can an adversary trick the user?
    - Post request:
      - Make the user into clicking a link (run JavaScript on the website a user opens)
      - ex. The link opens an attacker's website, and it runs some JavaScript code
      - Put some JavaScript on a website the user will visit
      - ex. The attacker pays for an ad. and put JavaScript code there

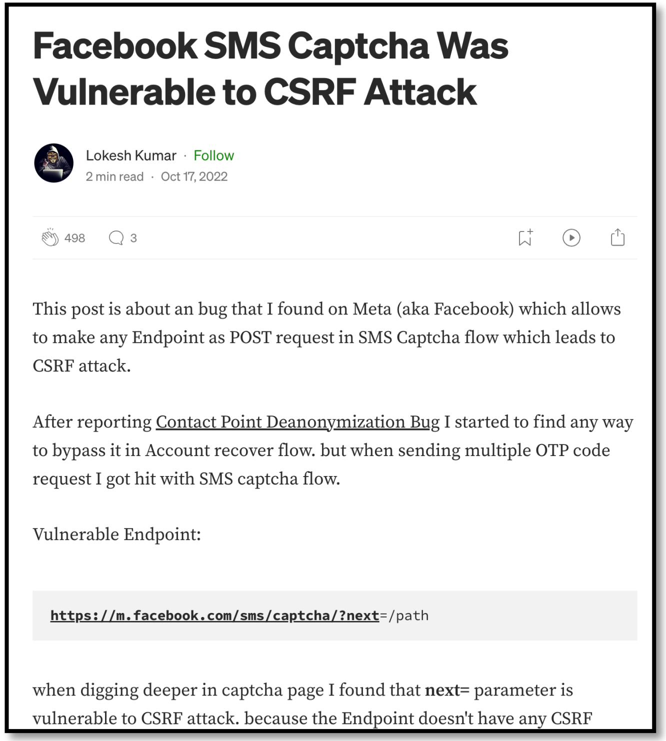


CSRF: Cross-site request forgery

- CSRF != Reflected XSS
  - Reflected XSS: Make the user (victim) run malicious scripts
  - CSRF : Make the server run malicious scripts

CSRF: Cross-site request forgery

- Real-world examples (Facebook, YouTube)



Facebook SMS Captcha Was Vulnerable to CSRF Attack

Lokesh Kumar · Follow
2 min read · Oct 17, 2022

498 3

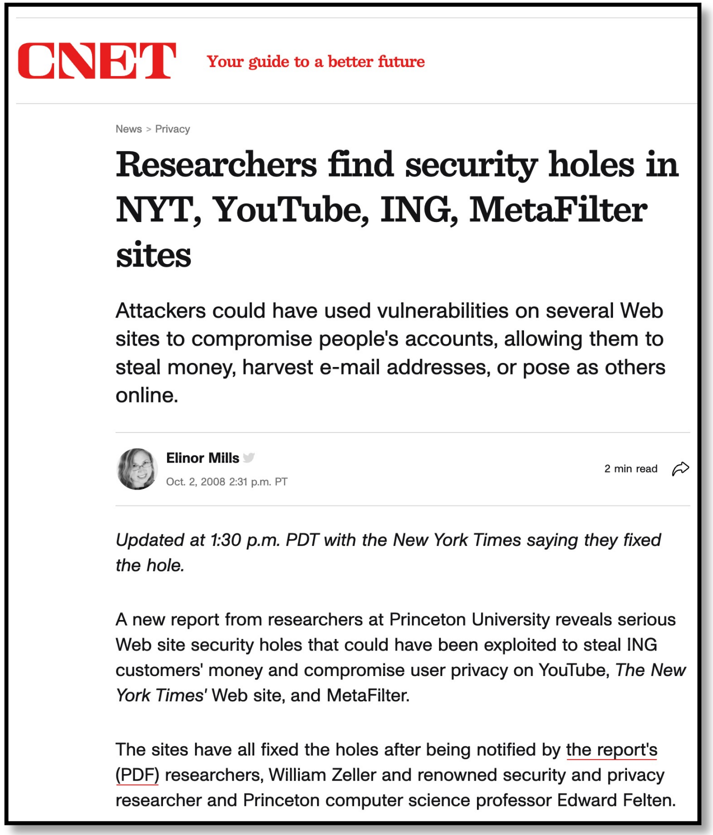
This post is about an bug that I found on Meta (aka Facebook) which allows to make any Endpoint as POST request in SMS Captcha flow which leads to CSRF attack.

After reporting Contact Point Deanonymization Bug I started to find any way to bypass it in Account recover flow. but when sending multiple OTP code request I got hit with SMS captcha flow.

Vulnerable Endpoint:

```
https://m.facebook.com/sms/captcha/?next=/path
```

when digging deeper in captcha page I found that **next=** parameter is vulnerable to CSRF attack. because the Endpoint doesn't have any CSRF



CNET Your guide to a better future

News > Privacy

Researchers find security holes in NYT, YouTube, ING, MetaFilter sites

Attackers could have used vulnerabilities on several Web sites to compromise people's accounts, allowing them to steal money, harvest e-mail addresses, or pose as others online.

Elinor Mills
Oct. 2, 2008 2:31 p.m. PT
2 min read

Updated at 1:30 p.m. PDT with the New York Times saying they fixed the hole.

A new report from researchers at Princeton University reveals serious Web site security holes that could have been exploited to steal ING customers' money and compromise user privacy on YouTube, *The New York Times'* Web site, and MetaFilter.

The sites have all fixed the holes after being notified by the report's (PDF) researchers, William Zeller and renowned security and privacy researcher and Princeton computer science professor Edward Felten.

CSRF: Cross-site request forgery

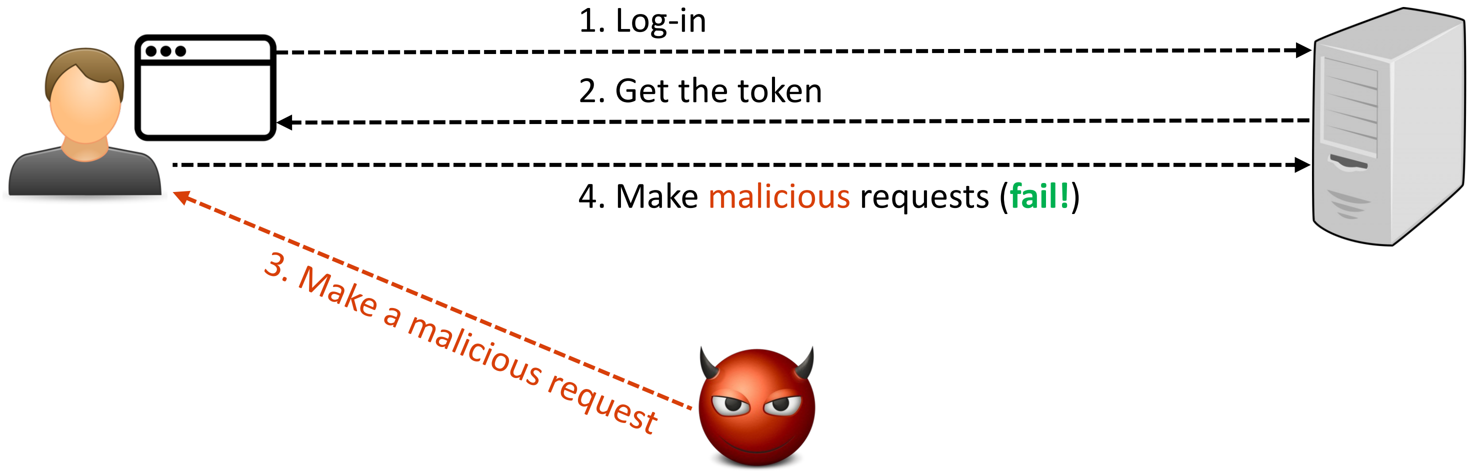
- Defenses
  - CSRF tokens
  - Referer validation
  - Same-site cookie attribute

CSRF: Cross-site request forgery

- Defenses
  - CSRF tokens
    - A secret value that the server provides to the user
    - The user must include the same value in the request for the server
  - Note
    - The token should not be sent to the server in a cookie
    - The token must be sent somewhere else and stored to a separate storage
    - The token shouldn't be like a session token (it should expire after 1-2 requests)
  - Example:
    - HTML forms: vulnerable to CSRF (the attacker can do a POST request with their forms)
    - If a user requests from a form, the server attaches a CSRF token as *a hidden form* field
    - The attacker's JavaScript won't be able to create a valid form

CSRF: Cross-site request forgery

- Defenses
  - CSRF tokens
    - A secret value that the server provides to the user
    - The user must include the same value in the request for the server


1. Log-in
2. Get the token
4. Make malicious requests (fail!)
3. Make a malicious request

CSRF: Cross-site request forgery

- Defenses
  - CSRF tokens
  - Referer header
    - A header in an HTTP request that shows which webpage made the request
    - In CSRF, the user makes malicious requests from a different website
      - “Referer” is a 30-year typo in the HTTP standard…
      - If we make a request from “facebook.com” then the header is “https://www.facebook.com”
      - If an “img” tag on a forum makes your browser to make a request then the Referer header will be “the forum’s URL”
      - If JavaScript on an attacker’s website makes your browswer to make a request then the header will be “the attacker’s website URL”
    - The server checks the Referer header
      - Reject if it’s not from the same-site
      - Accept if it’s from the the same-site

CSRF: Cross-site request forgery

- Defenses
  - CSRF tokens
  - Referer header
    - A header in an HTTP request that shows which webpage made the request
    - Potential issues:
      - The server can “observe” the user’s private info. from the header (ex. “facebook.com/<your-friend-name>/posting_1234”)
      - Oftentimes, network firewalls (or your browswers) remove this header…
      - The header is optional; some requests can come without the header (what should we do…)

CSRF: Cross-site request forgery

- Defenses
  - CSRF tokens
  - Referer header
  - Same-site cookies
    - Set a flag on a cookie unexploitable by CSRF attacks
    - The browser will send requests when the domain of the cookie = that of the origin
      - SameSite = none
      - SameSite = strict: check if the domain matches
    - Potential issue: not all browsers implements this attribute

Topics for today

- Advanced web security
  - CSRF (Cross-Site Request Forgery)
    - Cookies
    - Session
    - CSRF attacks
    - Defenses (and their potential weaknesses)
  - UI attacks
    - Clickjacking
    - Phishing
    - 2FA (and their potential weaknesses)

Overview

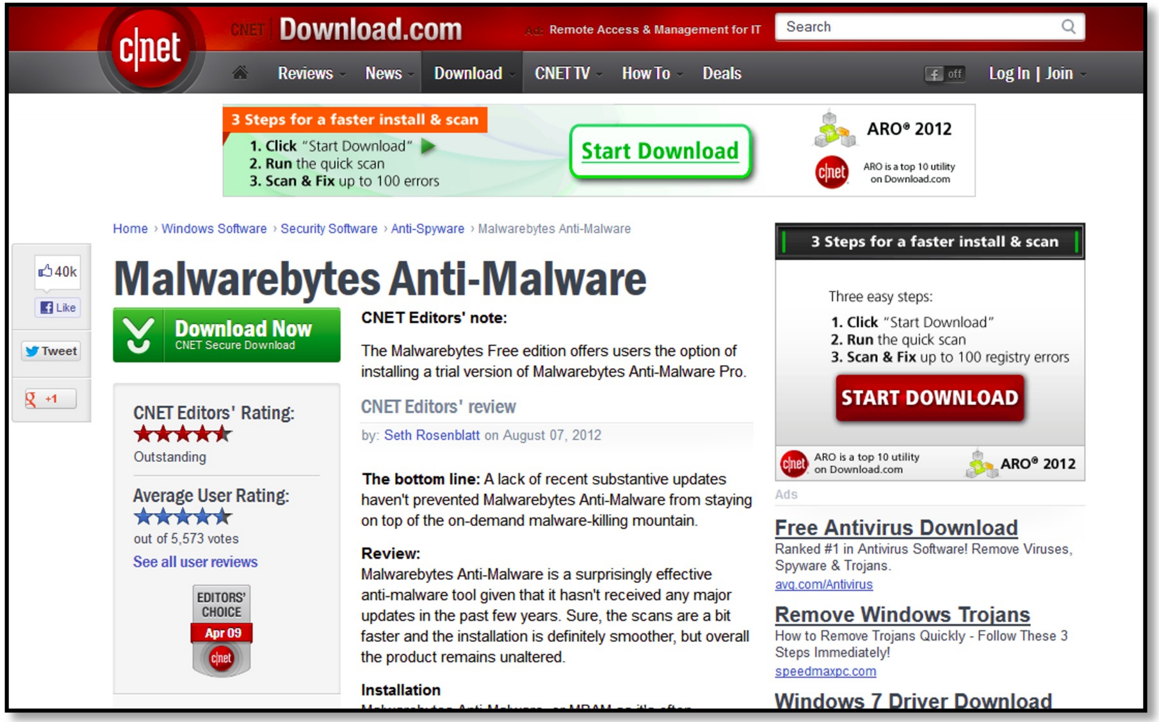
- UI attacks
  - What is it?
    - The attacker tricks the victim into thinking
    - They are taking an intended action when they are actually taking a malicious action
  - What to exploit?
    - User interfaces: the trusted path between the user and the computer
    - Your browser blocks the website to interact across different origins (SOP)
    - But trusts the user to do whatever they want
  - Two representative attacks
    - Clickjacking: Trick the victim into clicking on something from the attacker
    - Phishing: Trick the victim into sending the attacker personal information

Clickjacking

- Clickjacking
  - What is it?
    - Trick the victim into clicking on something from the attacker
  - What to exploit?
    - User interfaces: the trusted path between the user and the computer
    - Your browser trusts “your clicks”
    - If you click something, the browser believes you intend to click that
  - What can the attacker do?
    - Download a malicious program
    - Like a YouTube video(s), Instagram pages, or Amazon products
    - Steal keystrokes (once sth is downloaded)
      - Good luck to your credit card numbers, passwords, or any personal info.

Clickjacking example

- Download buttons
  - What is the *right* button?
  - What happens if I click the *wrong* button(s)?



3 Steps for a faster install & scan

1. Click "Start Download"
2. Run the quick scan
3. Scan & Fix up to 100 errors

Home › Windows Software › Security Software › Anti-Spyware › Malwarebytes Anti-Malware

Malwarebytes Anti-Malware

CNET Editors' note:

The Malwarebytes Free edition offers users the option of installing a trial version of Malwarebytes Anti-Malware Pro.

CNET Editors' review

by: Seth Rosenblatt on August 07, 2012

The bottom line: A lack of recent substantive updates haven't prevented Malwarebytes Anti-Malware from staying on top of the on-demand malware-killing mountain.

Review:
Malwarebytes Anti-Malware is a surprisingly effective anti-malware tool given that it hasn't received any major updates in the past few years. Sure, the scans are a bit faster and the installation is definitely smoother, but overall the product remains unaltered.

Installation

CNET Editors' Rating:
★★★★★
Outstanding

Average User Rating:
★★★★★
out of 5,573 votes

See all user reviews

3 Steps for a faster install & scan

Three easy steps:
1. Click "Start Download"
2. Run the quick scan
3. Scan & Fix up to 100 registry errors

Ads

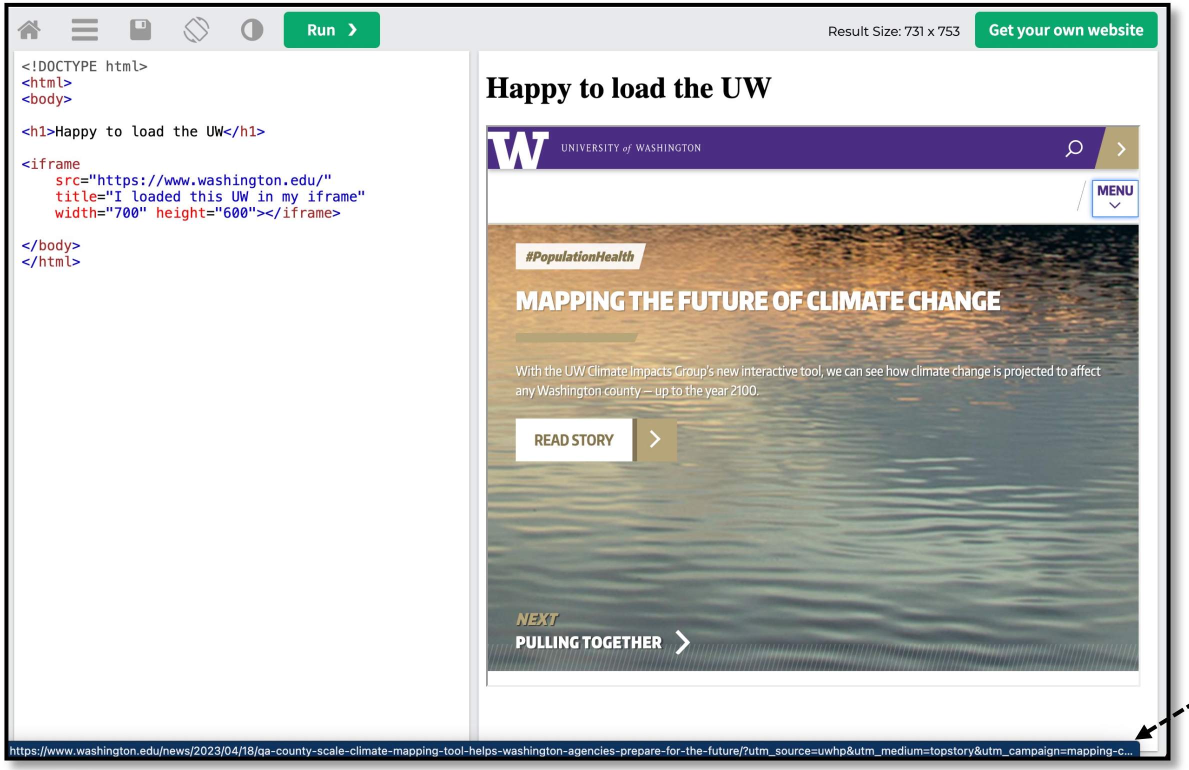
Free Antivirus Download
Ranked #1 in Antivirus Software! Remove Viruses, Spyware & Trojans.
avg.com/Antivirus

Remove Windows Trojans
How to Remove Trojans Quickly - Follow These 3 Steps Immediately!
speedmaxpc.com

Windows 7 Driver Download

Clickjacking example

- "iframe" can be vulnerable


Run
Result Size: 731 x 753
Get your own website

```
<!DOCTYPE html>
<html>
<body>

<h1>Happy to load the UW</h1>

<iframe
    src="https://www.washington.edu/"
    title="I loaded this UW in my iframe"
    width="700" height="600"></iframe>

</body>
</html>
```

Happy to load the UW

UNIVERSITY of WASHINGTON
MENU
#PopulationHealth
MAPPING THE FUTURE OF CLIMATE CHANGE
With the UW Climate Impacts Group's new interactive tool, we can see how climate change is projected to affect any Washington county — up to the year 2100.
READ STORY
NEXT
PULLING TOGETHER

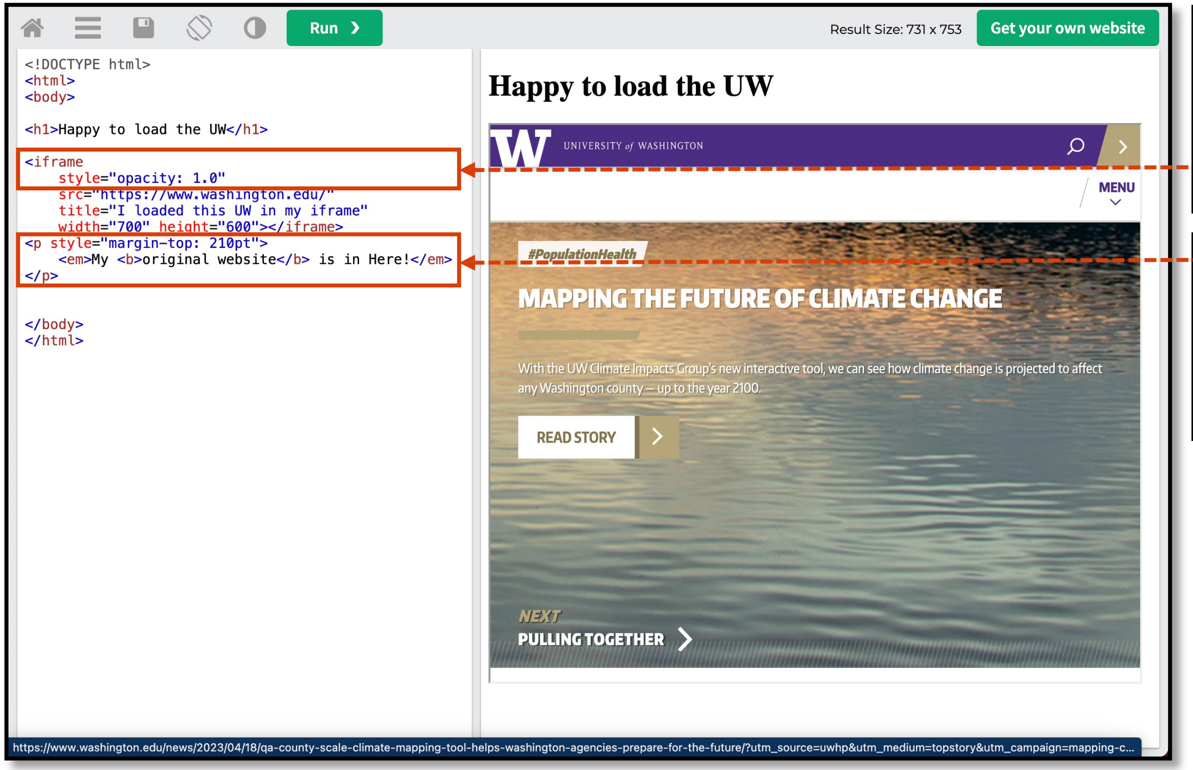
https://www.washington.edu/news/2023/04/18/qa-county-scale-climate-mapping-tool-helps-washington-agencies-prepare-for-the-future/?utm_source=uwhp&utm_medium=topstory&utm_campaign=mapping-c...

Note: any links on the website in the iframe are "washington.edu"

Users can click it, but we cannot make the website automatically click this link due to the same origin policy

Clickjacking example

- "iframe" can be vulnerable – let's change the code a bit


Run
Result Size: 731 x 753
Get your own website

```
<!DOCTYPE html>
<html>
<body>

<h1>Happy to load the UW</h1>

<iframe
    style="opacity: 1.0"
    src="https://www.washington.edu/"
    title="I loaded this UW in my iframe"
    width="700" height="600"></iframe>
<p style="margin-top: 210pt">
    <em>My <b>original website</b> is in Here!</em>
</p>


</body>
</html>
```

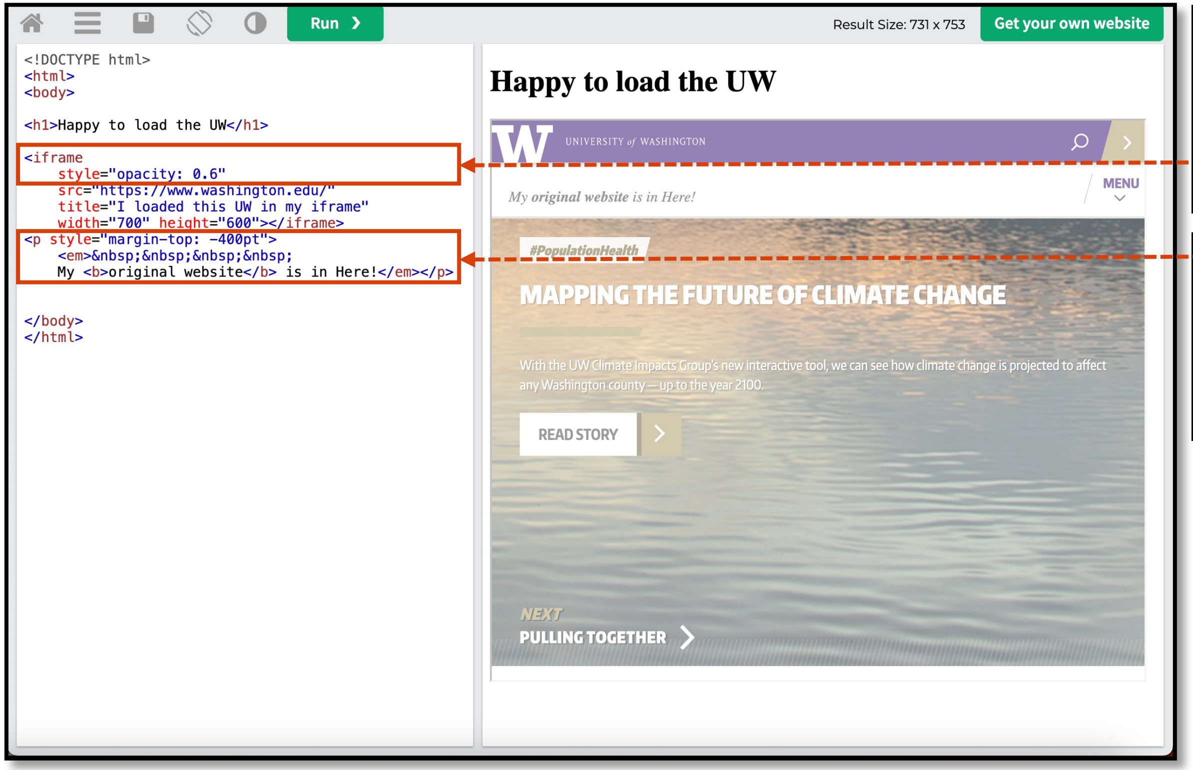
Happy to load the UW
UNIVERSITY of WASHINGTON
MENU
#PopulationHealth
MAPPING THE FUTURE OF CLIMATE CHANGE
With the UW Climate Impacts Group's new interactive tool, we can see how climate change is projected to affect any Washington county – up to the year 2100.
READ STORY
NEXT
PULLING TOGETHER
https://www.washington.edu/news/2023/04/18/qa-county-scale-climate-mapping-tool-helps-washington-agencies-prepare-for-the-future/?utm_source=uwhp&utm_medium=topstory&utm_campaign=mapping-c...

Put style: opacity to control the "opacity"

There's a text behind the iframe loaded the "washington.edu"

Clickjacking example

- “iframe” can be vulnerable – let’s add some opacity


Run
Result Size: 731 x 753
Get your own website

```
<!DOCTYPE html>
<html>
<body>

<h1>Happy to load the UW</h1>

<iframe
    style="opacity: 0.6"
    src="https://www.washington.edu/"
    title="I loaded this UW in my iframe"
    width="700" height="600"></iframe>
<p style="margin-top: -400pt">
    <em>&nbsp;&nbsp;&nbsp;&nbsp;
    My <b>original website</b> is in Here!</em></p>

</body>
</html>
```

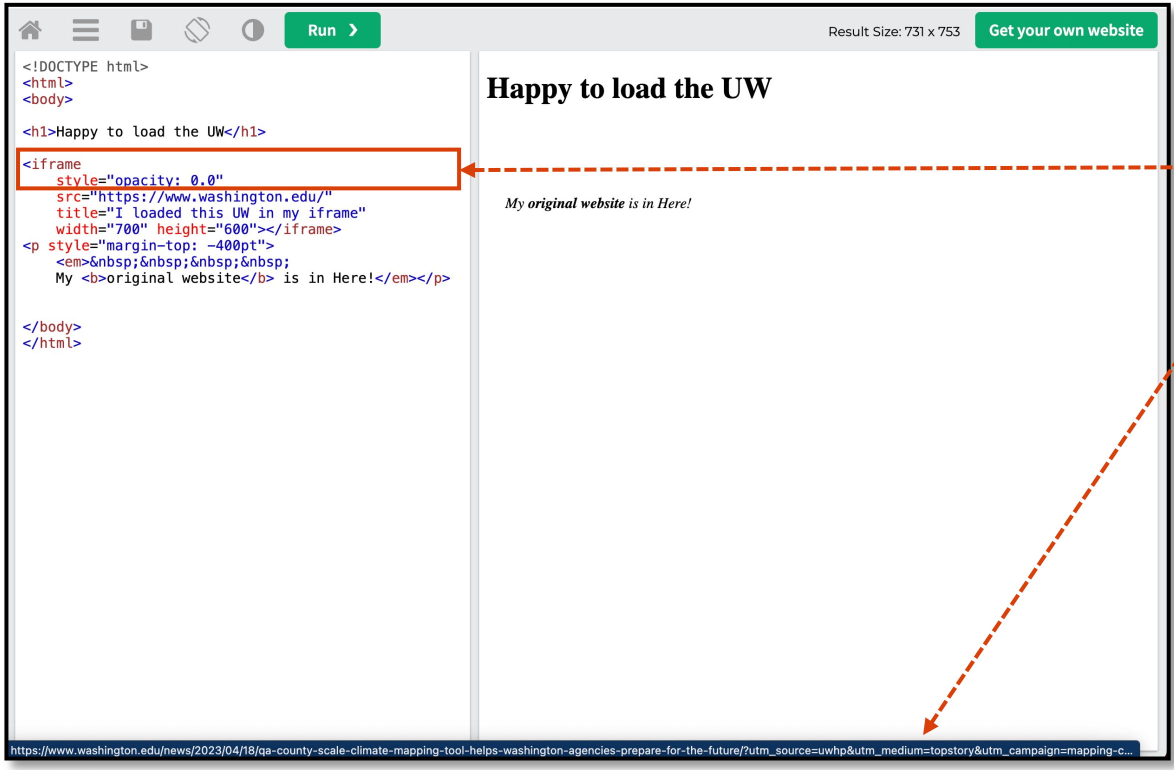
Happy to load the UW
UNIVERSITY of WASHINGTON
MENU
My original website is in Here!
#PopulationHealth
MAPPING THE FUTURE OF CLIMATE CHANGE
With the UW Climate Impacts Group's new interactive tool, we can see how climate change is projected to affect any Washington county — up to the year 2100.
READ STORY
NEXT
PULLING TOGETHER

Put style: opacity to control the “opacity”

There’s a text behind the iframe loaded the “washington.edu”

Clickjacking example

- “iframe” can be vulnerable – some more (or do extremely)



```
<!DOCTYPE html>
<html>
<body>

<h1>Happy to load the UW</h1>

<iframe
    style="opacity: 0.0"
    src="https://www.washington.edu/"
    title="I loaded this UW in my iframe"
    width="700" height="600"></iframe>
<p style="margin-top: -400pt">
    <em>&nbsp;&nbsp;&nbsp;&nbsp;
    My <b>original website</b> is in Here!</em></p>


</body>
</html>
```

Happy to load the UW

*My **original website** is in Here!*

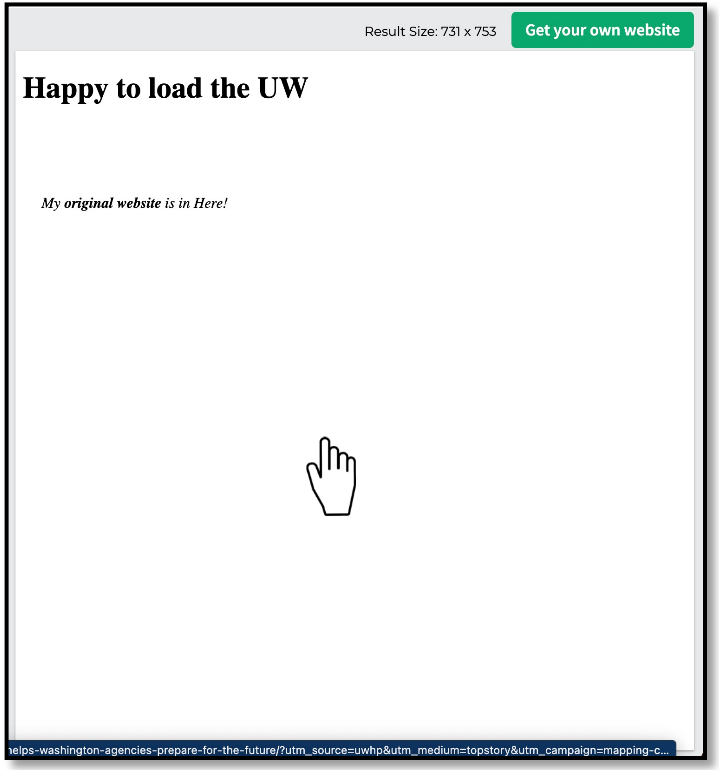
https://www.washington.edu/news/2023/04/18/qa-county-scale-climate-mapping-tool-helps-washington-agencies-prepare-for-the-future/?utm_source=uwhp&utm_medium=topstory&utm_campaign=mapping-c...

Now the website is completely opaque

But you can still click something on this website … ?!

Clickjacking example

- Invisible "iframe"s
  - The attacker puts an iframe onto the attacker's site invisibly, over visible, enticing content
  - Users (victims) think they click on the attacker's website
  - But the click is actually happened on the legitimate website
  - ex. You click sth, but it's the Facebook like btn



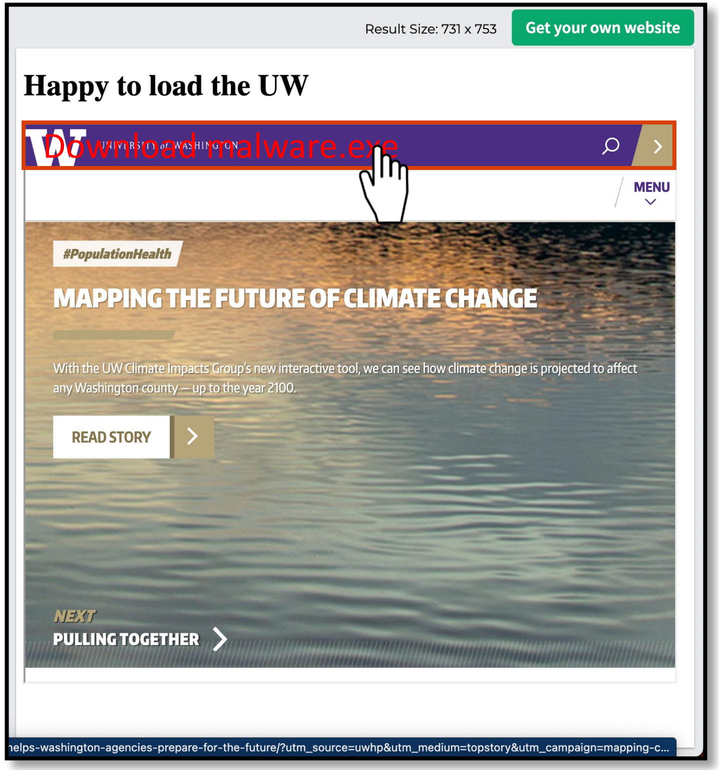
Happy to load the UW

*My **original website** is in Here!*

helps-washington-agencies-prepare-for-the-future/?utm_source=uwhp&utm_medium=topstory&utm_campaign=mapping-c...

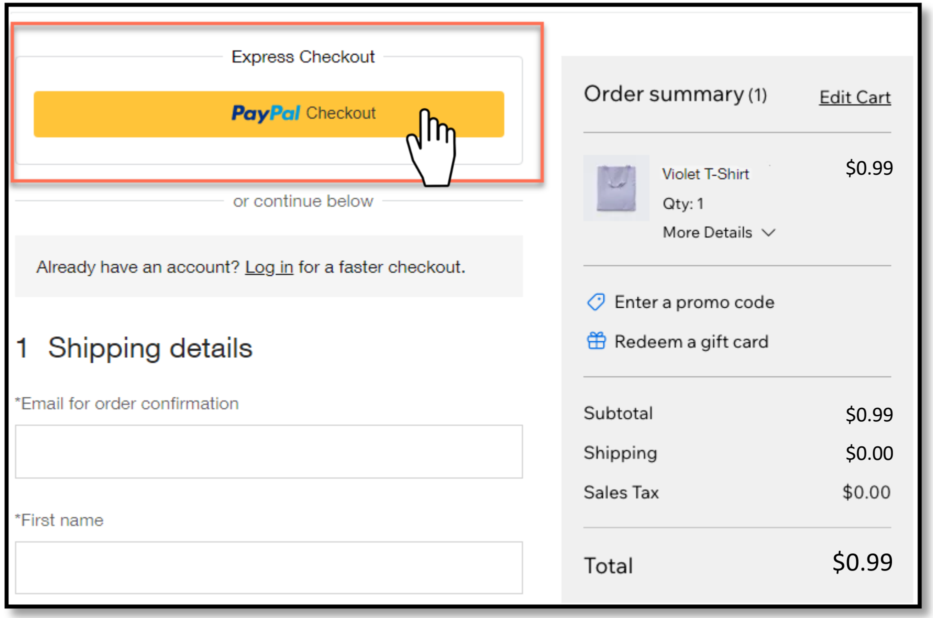
CLICKJACKING EXAMPLE

- Invisible "iframe"s – cont'd
  - The attacker puts an iframe onto the legitimate site invisibly, under invisible, malicious content
  - Users (victims) think they click on the legitimate website
  - But the click is actually happened on the attacker's website
  - ex. You click sth, and it downloads malware


Result Size: 731 x 753
Get your own website
Happy to load the UW
Download malware.exe
UNIVERSITY of WASHINGTON
MENU
#PopulationHealth
MAPPING THE FUTURE OF CLIMATE CHANGE
With the UW Climate Impacts Group's new interactive tool, we can see how climate change is projected to affect any Washington county — up to the year 2100.
READ STORY
NEXT
PULLING TOGETHER
helps-washington-agencies-prepare-for-the-future/?utm_source=uwhp&utm_medium=topstory&utm_campaign=mapping-c...

Clickjacking example

- Invisible “iframe”s – cont’d



Express Checkout

PayPal Checkout

or continue below

Already have an account? Log in for a faster checkout.

1 Shipping details

*Email for order confirmation

*First name

Order summary (1) Edit Cart

Violet T-Shirt Qty: 1 More Details	$0.99

Enter a promo code

Redeem a gift card

Subtotal	$0.99
Shipping	$0.00
Sales Tax	$0.00
Total	$0.99

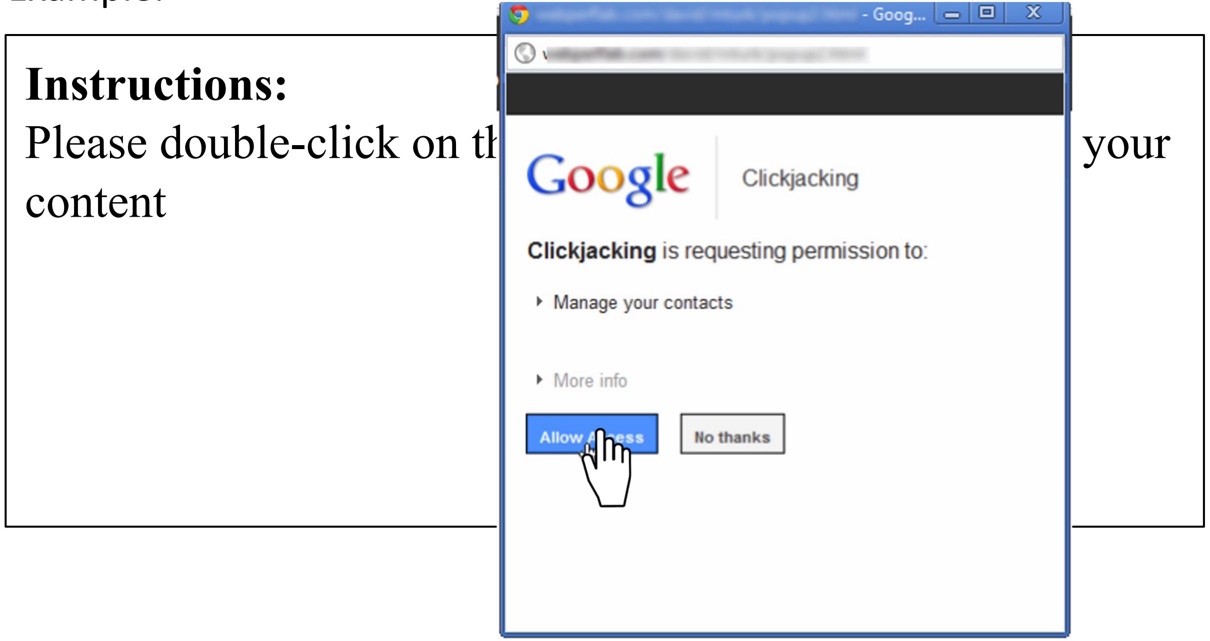
  - The attacker frames the legitimate site, with the visible malicious contents
  - ex. You click the checkout, and I wish you the best!

Clickjacking example

- Temporal attack
  - Process
    - The attacker uses JavaScript
    - that detects the position of your cursor
    - and change the website right before you click on sth.

Clickjacking example

- Temporal attack
  - Example:



Instructions:
Please double-click on th your content

- Goog...

Google Clickjacking

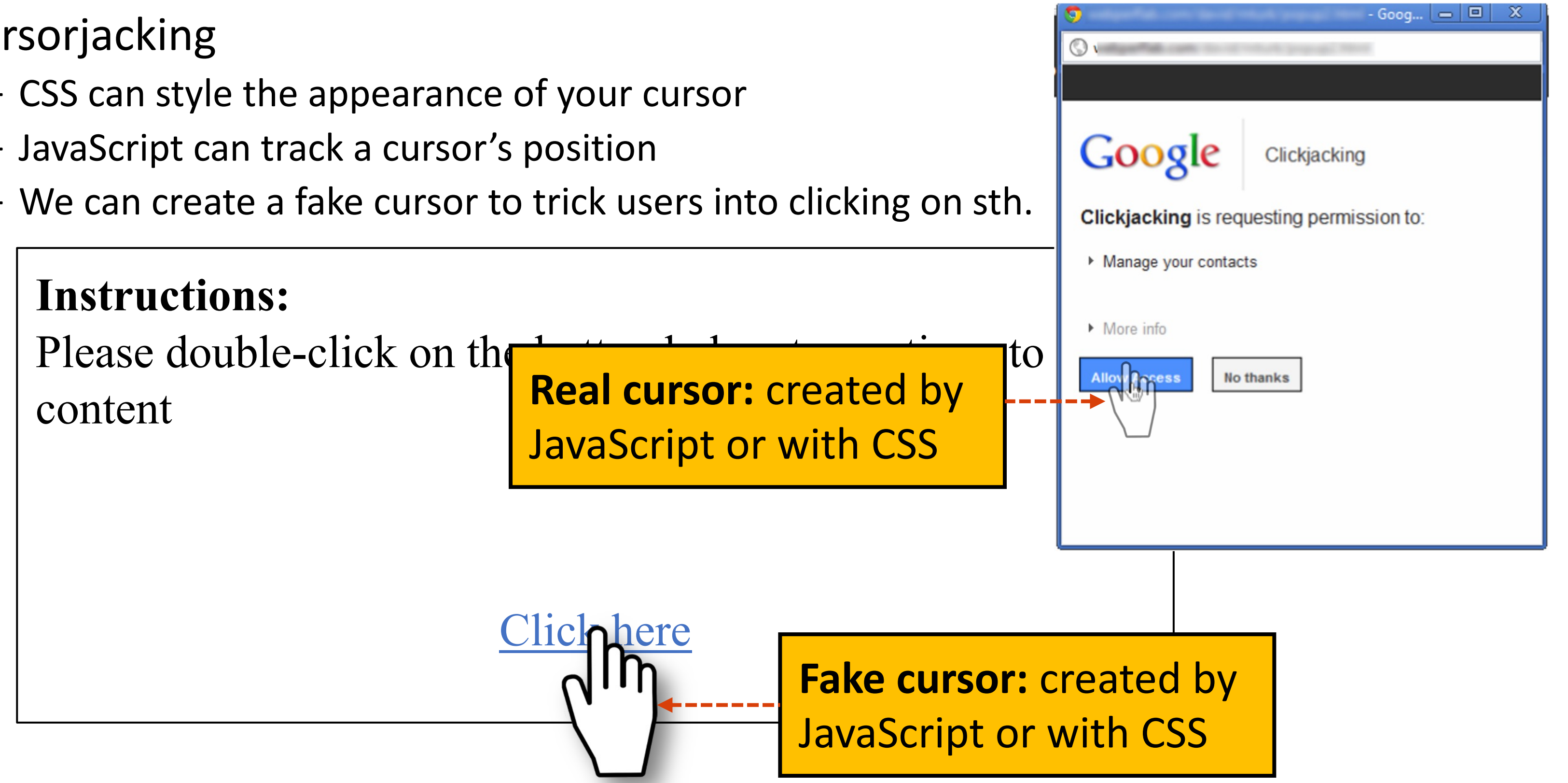
Clickjacking is requesting permission to:

Manage your contacts

More info

Clickjacking example

- Cursorjacking
  - CSS can style the appearance of your cursor
  - JavaScript can track a cursor's position
  - We can create a fake cursor to trick users into clicking on sth.



Instructions:
Please double-click on the [...] to content

Click here

Real cursor: created by JavaScript or with CSS

Fake cursor: created by JavaScript or with CSS

[redacted] - Goog...

[redacted]

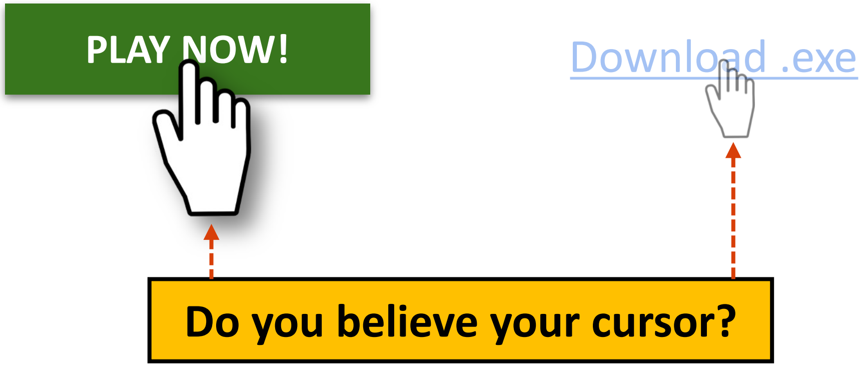
Google | Clickjacking

Clickjacking is requesting permission to:

- Manage your contacts
- More info

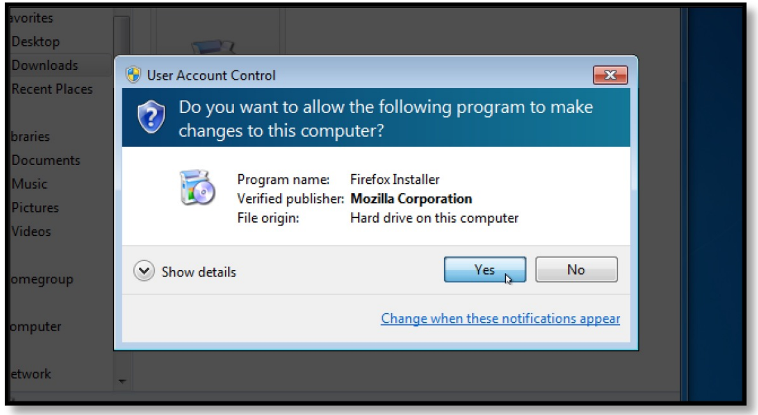
Clickjacking example

- Cursorjacking
  - CSS can style the appearance of your cursor
  - JavaScript can track a cursor's position
  - We can create a fake cursor to trick users into clicking on sth.



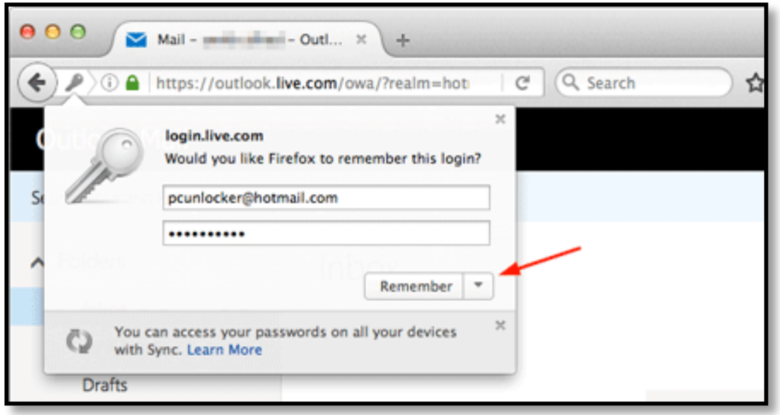
Clickjacking defenses

- Enforce visual integrity
  - Clear visual separation between important alerts and content
  - Examples:
    - Windows "User Account Control" darkens the entire screen and freezes the desktop
    - Firefox dialogs "cross the boundary" between the URL bar and content
      (Only the valid dialog can do this!)


User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Firefox Installer
Verified publisher: **Mozilla Corporation**
File origin: Hard drive on this computer


https://outlook.live.com/owa/?realm=hot

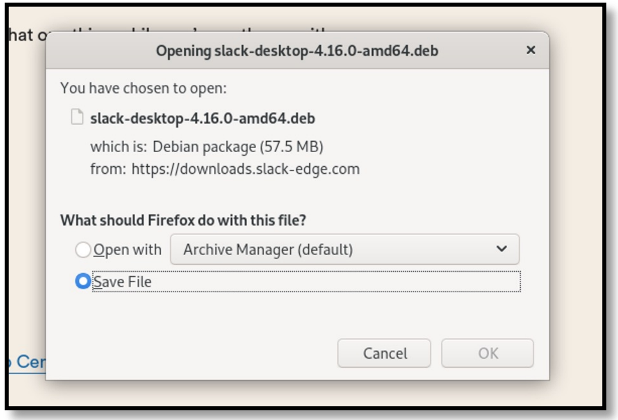
login.live.com
Would you like Firefox to remember this login?

pcunlocker@hotmail.com
••••••••••

You can access your passwords on all your devices with Sync. Learn More

Clickjacking defenses

- Enforce temporal integrity
  - Sufficient time for a user to register what they are clicking on
  - Example:
    - Firefox blocks the “OK” button until 1 second after the dialog has been focused


Opening slack-desktop-4.16.0-amd64.deb

You have chosen to open:

slack-desktop-4.16.0-amd64.deb

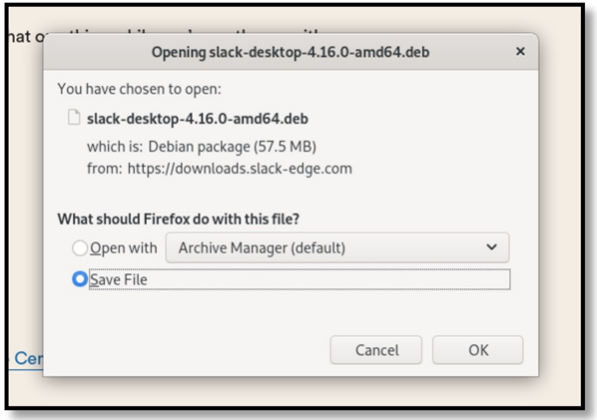
which is: Debian package (57.5 MB)

from: https://downloads.slack-edge.com

What should Firefox do with this file?

Open with Archive Manager (default)

[✓ Save File]


Opening slack-desktop-4.16.0-amd64.deb

You have chosen to open:

slack-desktop-4.16.0-amd64.deb

which is: Debian package (57.5 MB)

from: https://downloads.slack-edge.com

What should Firefox do with this file?

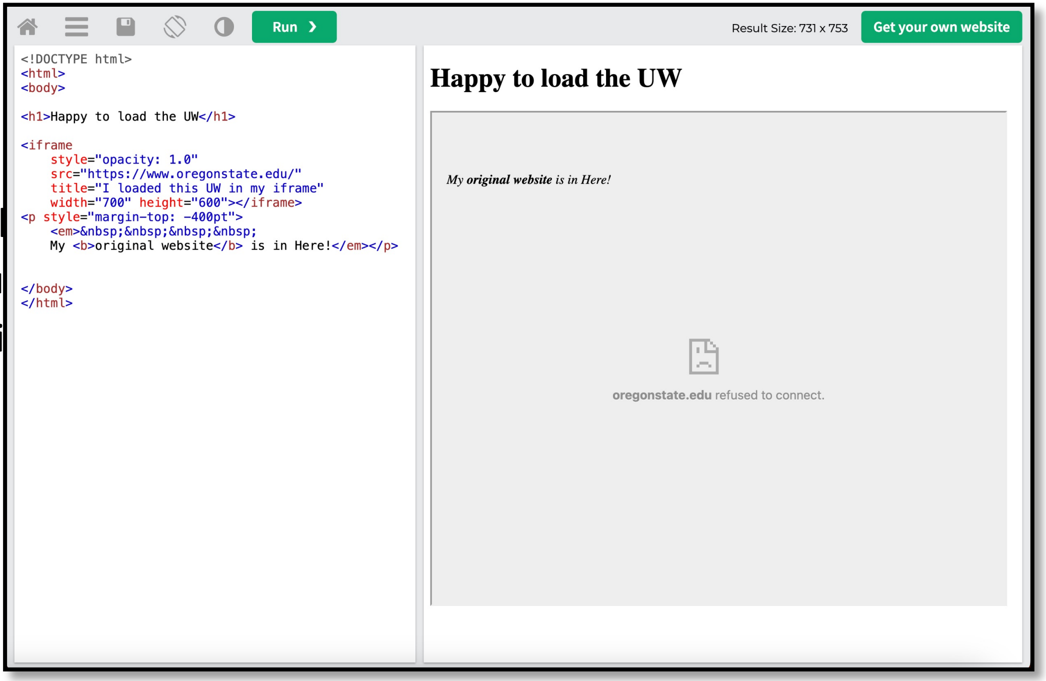
Open with Archive Manager (default)

[✓ Save File]

Clickjacking defenses

- Require confirmation from users
  - The browser needs to confirm that the user's click was intentional
  - Downside: asking for confirmation annoys users

- Frame-busting
  - The legitimate website forbids ot
  - Defeats the invisible iframe attac
  - Can be enforced by Content Secu
  - Can be enforced by X-Frame-Opti



```
<!DOCTYPE html>
<html>
<body>

<h1>Happy to load the UW</h1>

<iframe
    style="opacity: 1.0"
    src="https://www.oregonstate.edu/"
    title="I loaded this UW in my iframe"
    width="700" height="600"></iframe>
<p style="margin-top: -400pt">
    <em>&nbsp;&nbsp;&nbsp;&nbsp;
    My <b>original website</b> is in Here!</em></p>


</body>
</html>
```

Happy to load the UW

*My **original website** is in Here!*

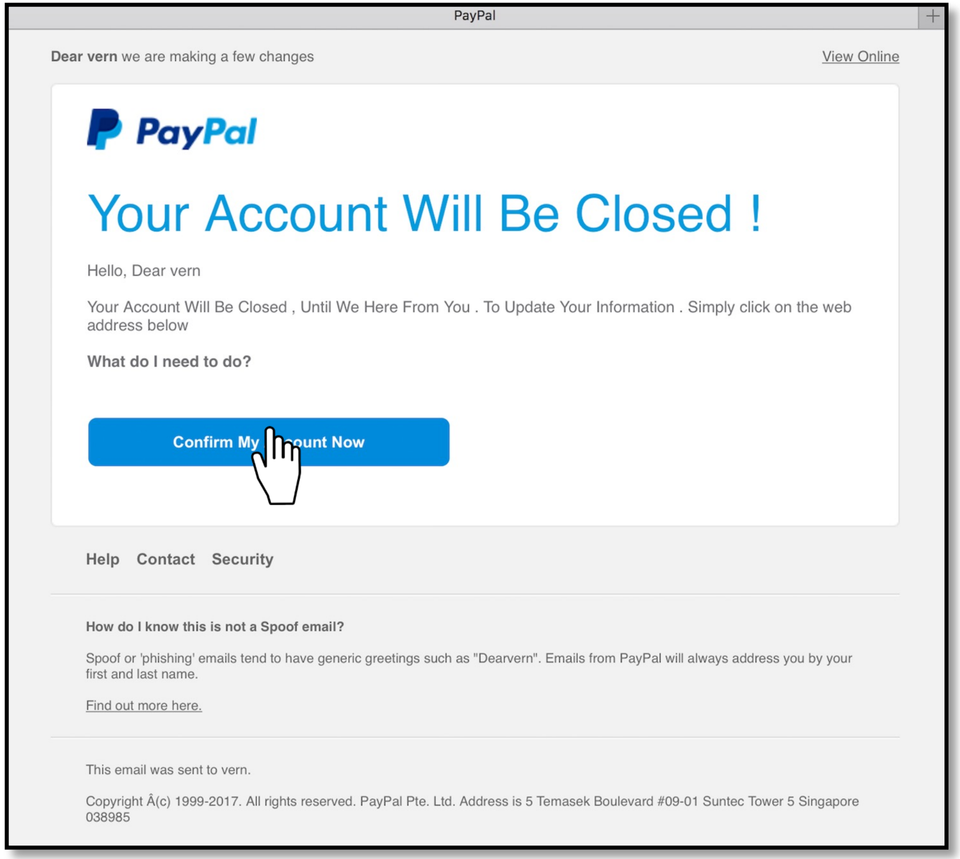
oregonstate.edu refused to connect.

Topics for today

- Advanced web security
  - CSRF (Cross-Site Request Forgery)
    - Cookies
    - Session
    - CSRF attacks
    - Defenses (and their potential weaknesses)
  - UI attacks
    - Clickjacking
    - Phishing
    - 2FA (and their potential weaknesses)

Phishing

- Your account will be closed!



PayPal

Dear vern we are making a few changes

View Online

PayPal

Your Account Will Be Closed !

Hello, Dear vern

Your Account Will Be Closed , Until We Here From You . To Update Your Information . Simply click on the web address below

What do I need to do?

Confirm My Account Now

Help **Contact** **Security**

How do I know this is not a Spoof email?

Spoof or 'phishing' emails tend to have generic greetings such as "Dearvern". Emails from PayPal will always address you by your first and last name.

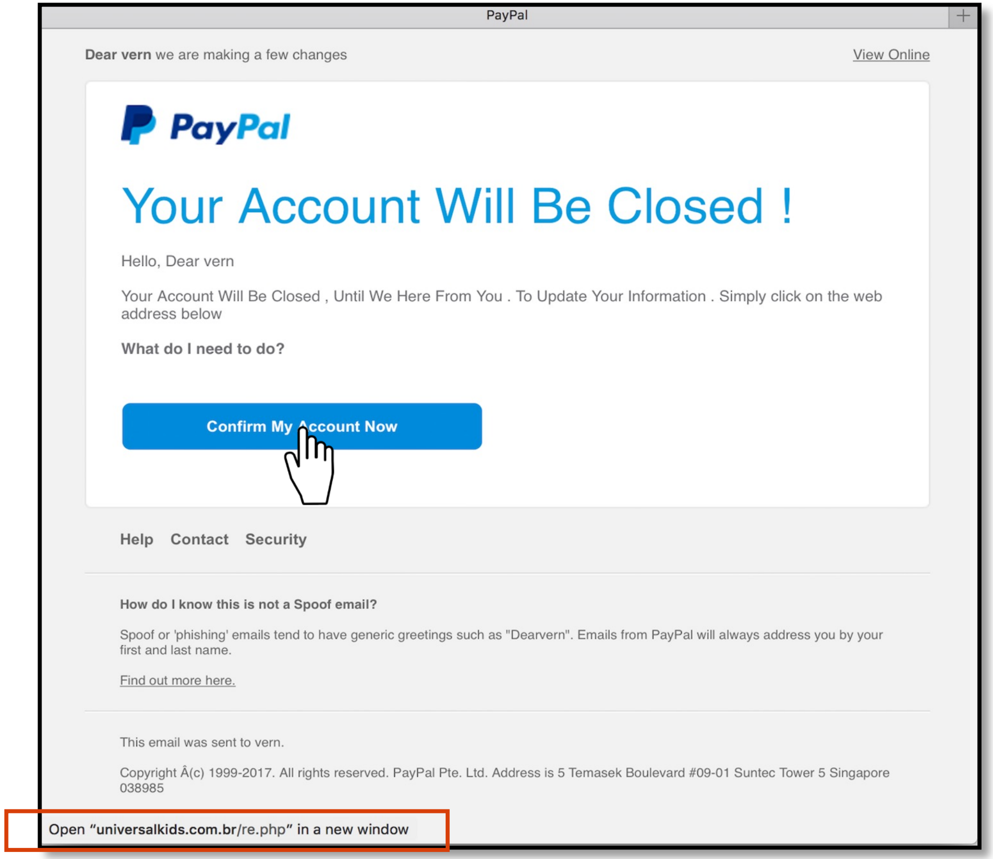
Find out more here.

This email was sent to vern.

Copyright Â(c) 1999-2017. All rights reserved. PayPal Pte. Ltd. Address is 5 Temasek Boulevard #09-01 Suntec Tower 5 Singapore 038985

Phishing

- Your account will be closed!
- … is it?



PayPal

Dear vern we are making a few changes View Online

PayPal

Your Account Will Be Closed !

Hello, Dear vern

Your Account Will Be Closed , Until We Here From You . To Update Your Information . Simply click on the web address below

What do I need to do?

Confirm My Account Now

Help Contact Security

How do I know this is not a Spoof email?

Spoof or 'phishing' emails tend to have generic greetings such as "Dearvern". Emails from PayPal will always address you by your first and last name.

Find out more here.

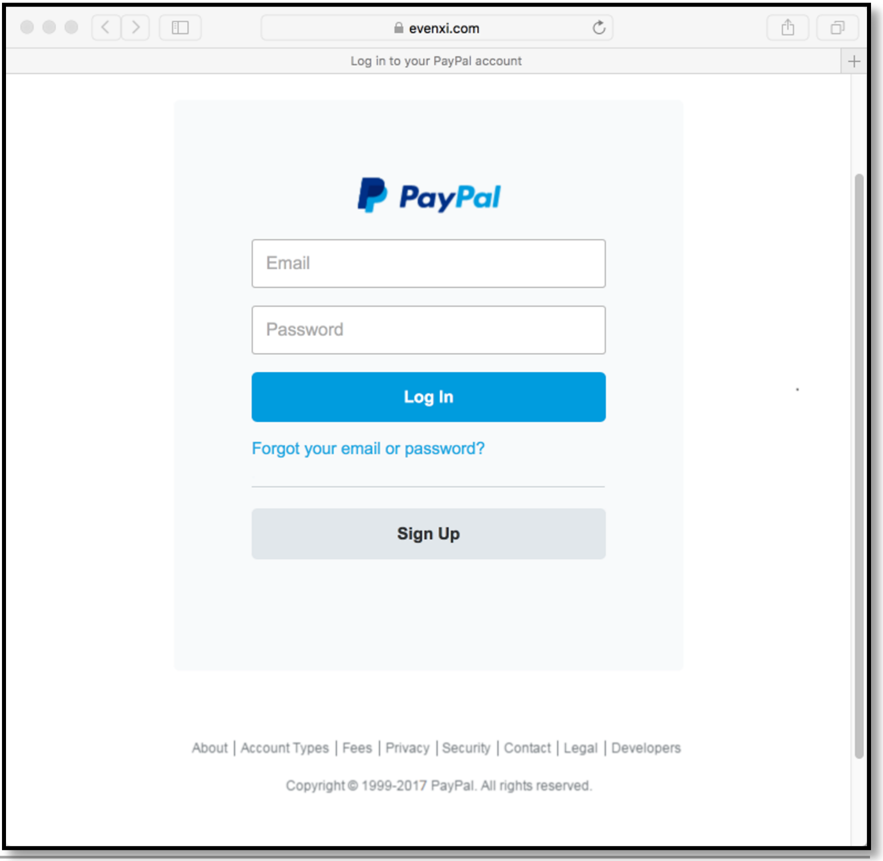
This email was sent to vern.

Copyright Â(c) 1999-2017. All rights reserved. PayPal Pte. Ltd. Address is 5 Temasek Boulevard #09-01 Suntec Tower 5 Singapore 038985

Open "universalkids.com.br/re.php" in a new window

Phishing

- You need to log-in to PayPal


evenxi.com

Log in to your PayPal account

PayPal

Email

Password

Log In

Forgot your email or password?

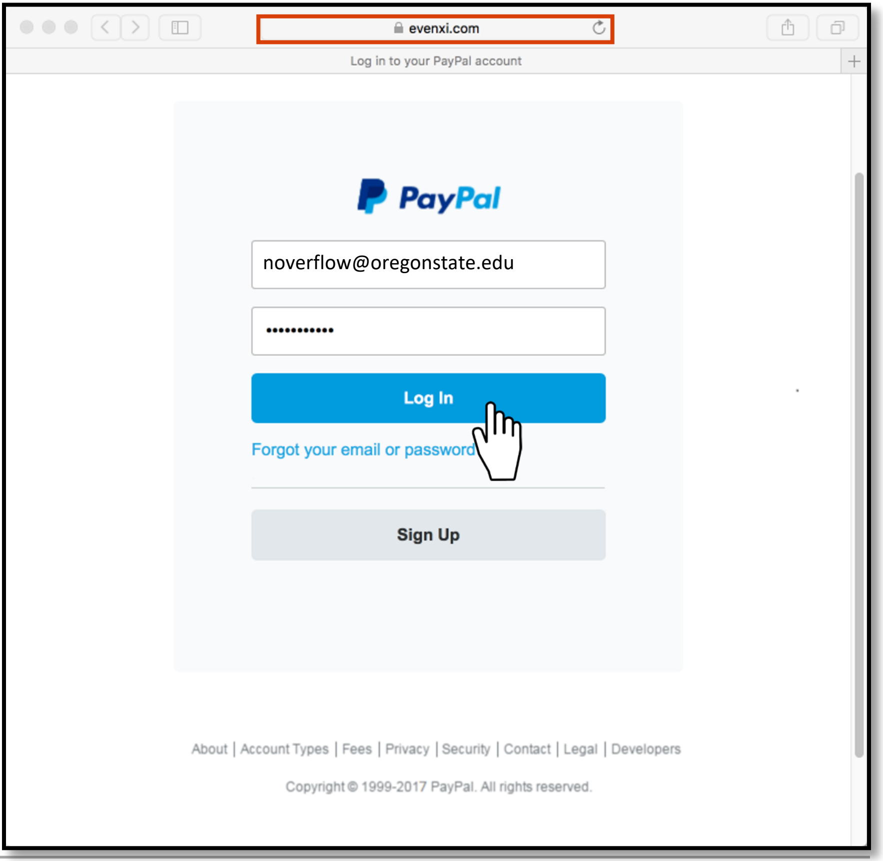
Sign Up

About | Account Types | Fees | Privacy | Security | Contact | Legal | Developers

Copyright © 1999-2017 PayPal. All rights reserved.

Phishing

- You need to log-in to PayPal
- … is it?


evenxi.com

Log in to your PayPal account

noverflow@oregonstate.edu

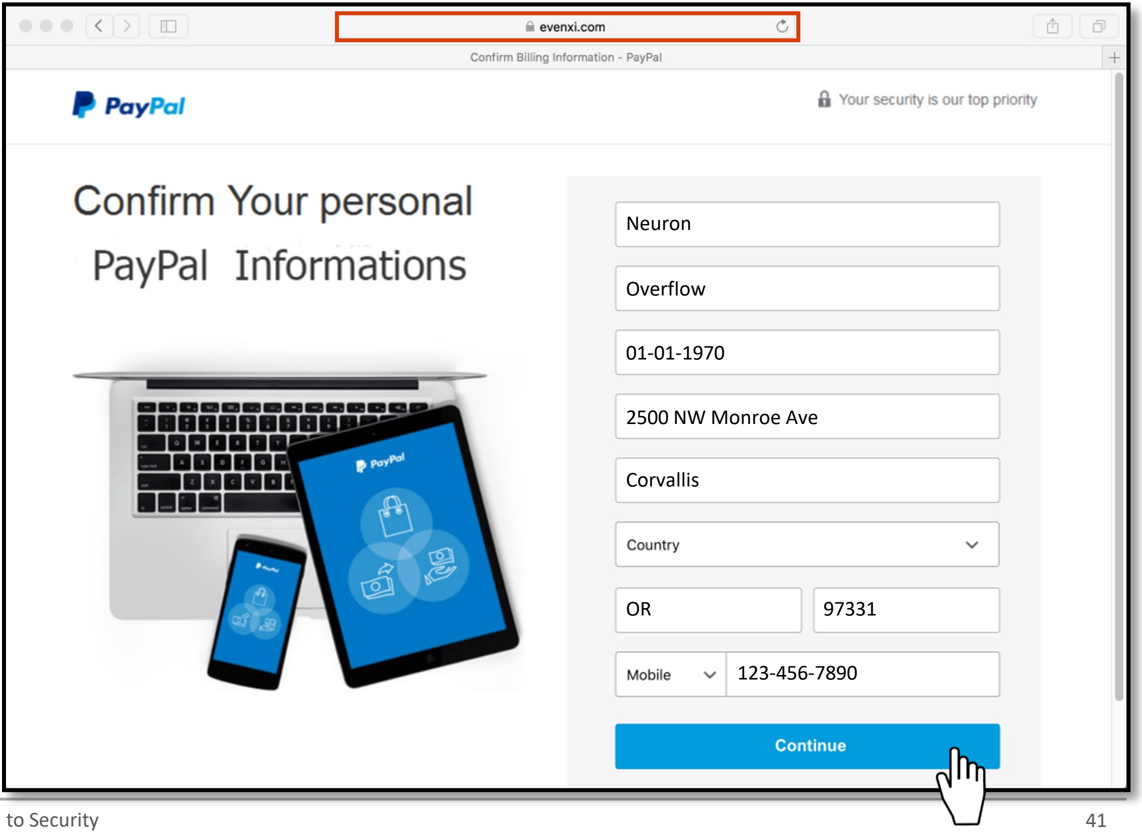
••••••••••••

Log In
Forgot your email or password?
Sign Up
About | Account Types | Fees | Privacy | Security | Contact | Legal | Developers

Copyright © 1999-2017 PayPal. All rights reserved.

Phishing

- You need to log-in to PayPal
- … is it?
- … is it?


evenxi.com

Confirm Billing Information - PayPal

PayPal

Your security is our top priority

Confirm Your personal PayPal Informations

Neuron

Overflow

01-01-1970

2500 NW Monroe Ave

Corvallis

Country

OR

97331

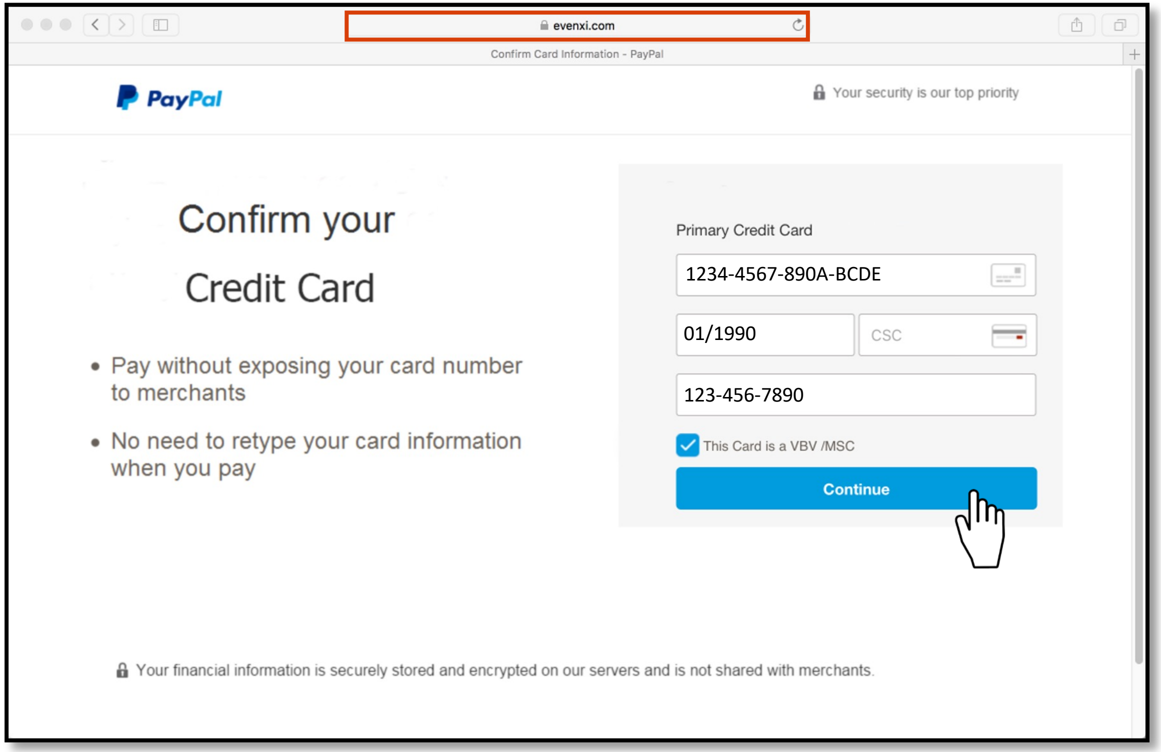
Mobile

123-456-7890

Continue

Phishing

- You need to log-in to PayPal
- … is it?
- … is it?
- … is it?



evenxi.com

Confirm Card Information - PayPal

PayPal

Your security is our top priority

Confirm your Credit Card

- Pay without exposing your card number to merchants
- No need to retype your card information when you pay

Primary Credit Card

1234-4567-890A-BCDE

01/1990

CSC

123-456-7890

✓ This Card is a VBV /MSC

Continue

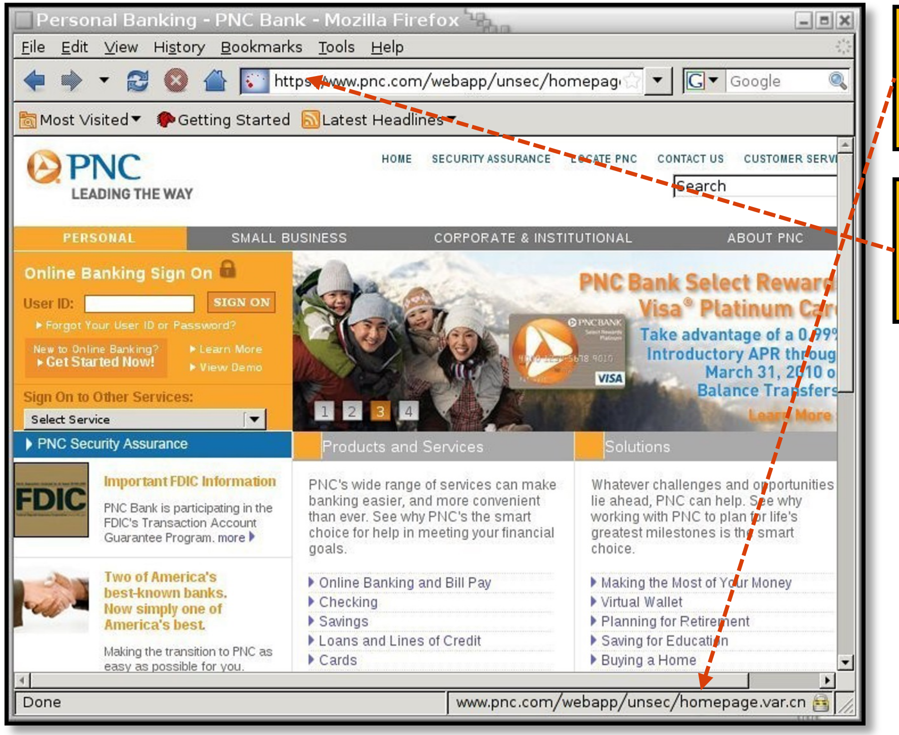
Your financial information is securely stored and encrypted on our servers and is not shared with merchants.

Phishing

- Phishing
  - Trick the victim into sending the attacker personal information
  - Exploit:
    - Users can't distinguish between a legitimate website and a website impersonating the legitimate website

Phishing: check the URL?

- Is this website real?


Personal Banking - PNC Bank - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.pnc.com/webapp/unsec/homepag
Google
Most Visited
Getting Started
Latest Headlines
PNC
LEADING THE WAY
HOME
SECURITY ASSURANCE
LOCATE PNC
CONTACT US
CUSTOMER SERVI
Search
PERSONAL
SMALL BUSINESS
CORPORATE & INSTITUTIONAL
ABOUT PNC
Online Banking Sign On
User ID:
SIGN ON
Forgot Your User ID or Password?
New to Online Banking? Get Started Now!
Learn More
View Demo
Sign On to Other Services:
Select Service
PNC Security Assurance
PNC Bank Select Reward Visa Platinum Car
Take advantage of a 0.99% Introductory APR throug March 31, 2010 o Balance Transfers
Learn More
Products and Services
Solutions
Important FDIC Information
Two of America's best-known banks. Now simply one of America's best.
Online Banking and Bill Pay
Checking
Savings
Loans and Lines of Credit
Cards
Making the Most of Your Money
Virtual Wallet
Planning for Retirement
Saving for Education
Buying a Home
Done
www.pnc.com/webapp/unsec/homepage.var.cn

PNC Bank is participating in the FDIC's Transaction Account Guarantee Program. more

PNC's wide range of services can make banking easier, and more convenient than ever. See why PNC's the smart choice for help in meeting your financial goals.

Whatever challenges and opportunities lie ahead, PNC can help. See why working with PNC to plan for life's greatest milestones is the smart choice.

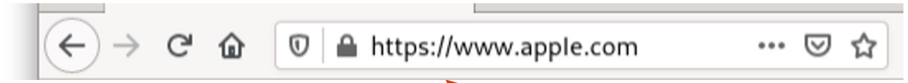
Making the transition to PNC as easy as possible for you.

"www.pnc.com/webapp/unsec/homepage.var.cn" is an entire domain!

The attacker can also register an HTTP certificate for this valid domain

Phishing: check the URL?

- Is this website real?

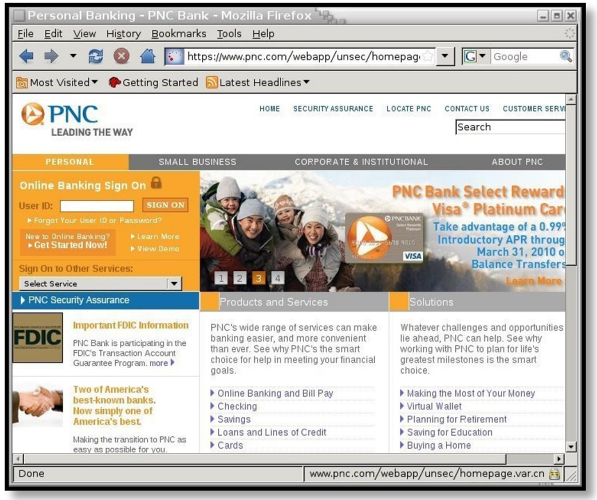


https://www.apple.com

These letters come from the Cyrllic alphabet, not the Latin alphabet! They’re rendered the same but have completely different bytes!

Phishing: homograph attack

- Homograph attack
  - Create malicious URLs that look similar (or the same) to legitimate URLs
  - Homograph: two words that look the same, but have different meanings



Personal Banking - PNC Bank - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://www.pnc.com/webapp/unsec/homepag

Google

Most Visited Getting Started Latest Headlines

PNC LEADING THE WAY

HOME SECURITY ASSURANCE LOCATE PNC CONTACT US CUSTOMER SERV

Search

PERSONAL SMALL BUSINESS CORPORATE & INSTITUTIONAL ABOUT PNC

Online Banking Sign On

User ID: SIGN ON

Forgot Your User ID or Password?

New to Online Banking? Get Started Now! Learn More View Demo

Sign On to Other Services: Select Service

PNC Security Assurance

PNC Bank Select Reward Visa® Platinum Car

Take advantage of a 0.99% Introductory APR throug March 31, 2010 o Balance Transfers

Learn More

1 2 3 4

Important FDIC Information

PNC Bank is participating in the FDIC's Transaction Account Guarantee Program. more

Two of America's best-known banks. Now simply one of America's best.

Making the transition to PNC as easy as possible for you.

Products and Services

PNC's wide range of services can make banking easier, and more convenient than ever. See why PNC's the smart choice for help in meeting your financial goals.

- Online Banking and Bill Pay
- Checking
- Savings
- Loans and Lines of Credit
- Cards

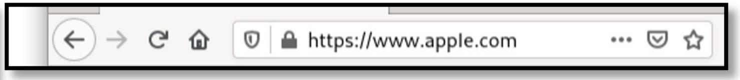
Solutions

Whatever challenges and opportunities lie ahead, PNC can help. See why working with PNC to plan for life's greatest milestones is the smart choice.

- Making the Most of Your Money
- Virtual Wallet
- Planning for Retirement
- Saving for Education
- Buying a Home

Done

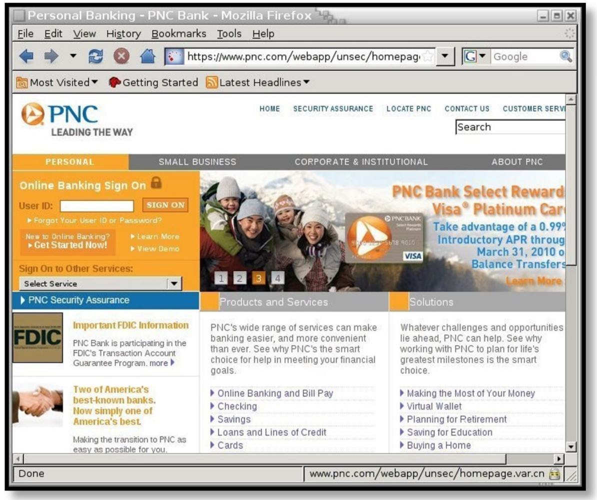
www.pnc.com/webapp/unsec/homepage.var.cn



https://www.apple.com

Phishing: homograph attack

- Homograph attack
  - Create malicious URLs that look similar (or the same) to legitimate URLs
  - Homograph: two words that look the same, but have different meanings



Personal Banking - PNC Bank - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://www.pnc.com/webapp/unsec/homepag

Most Visited Getting Started Latest Headlines

PNC LEADING THE WAY

HOME SECURITY ASSURANCE LOCATE PNC CONTACT US CUSTOMER SERV

Search

PERSONAL SMALL BUSINESS CORPORATE & INSTITUTIONAL ABOUT PNC

Online Banking Sign On

User ID: SIGN ON

Forgot Your User ID or Password?

New to Online Banking? Get Started Now! Learn More View Demo

Sign On to Other Services: Select Service

PNC Security Assurance

PNC Bank Select Reward Visa® Platinum Car

Take advantage of a 0.99 Introductory APR throug March 31, 2010 o Balance Transfers

Learn More

Products and Services

PNC's wide range of services can make banking easier, and more convenient than ever. See why PNC's the smart choice for help in meeting your financial goals.

- Online Banking and Bill Pay
- Checking
- Savings
- Loans and Lines of Credit
- Cards

Solutions

Whatever challenges and opportunities lie ahead, PNC can help. See why working with PNC to plan for life's greatest milestones is the smart choice.

- Making the Most of Your Money
- Virtual Wallet
- Planning for Retirement
- Saving for Education
- Buying a Home

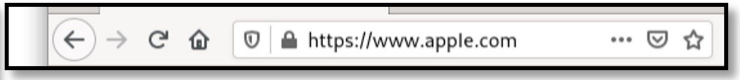
Important FDIC Information

PNC Bank is participating in the FDIC's Transaction Account Guarantee Program. more

Two of America's best-known banks. Now simply one of America's best.

Making the transition to PNC as easy as possible for you.

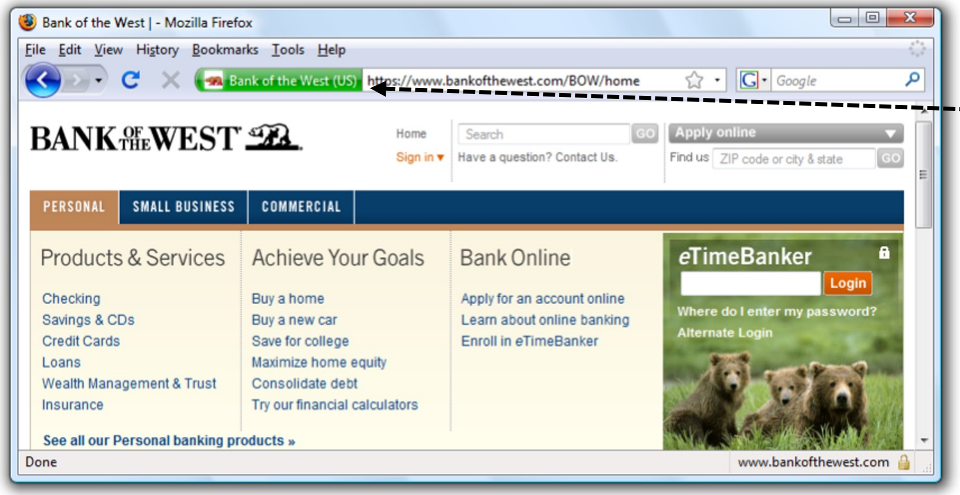
Done www.pnc.com/webapp/unsec/homepage.var.cn



https://www.apple.com

Phishing: check everything

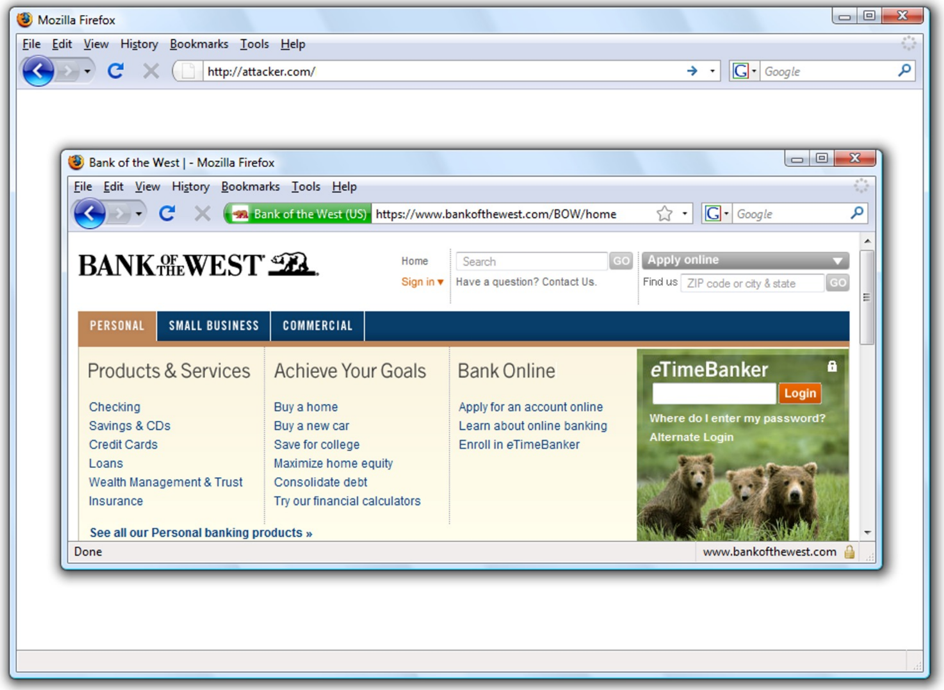
- … hmm it looks legit!



Extended Validation: CA verified the identity of the site (not just the domain)

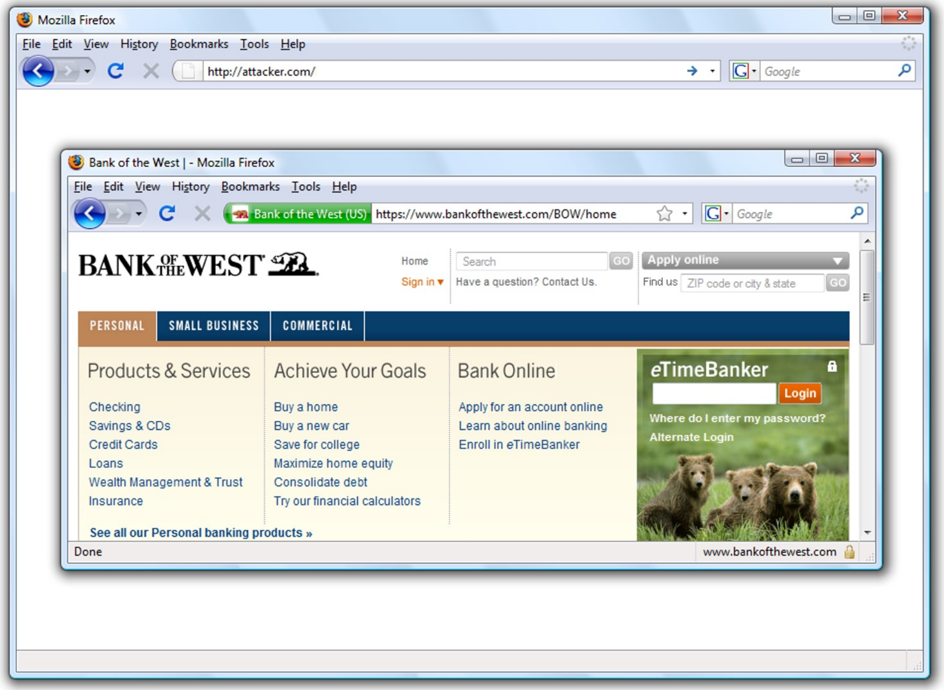
Phishing: check everything

- … hmm it looks legit!
  - Is it?


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 (US) https://www.bankofthewest.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
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

Phishing: browser-in-browser attack

- Browser-in-browser attack
  - The attacker simulates the entire web browser with JavaScript



Phishing: now who's the fault?

- Let's not blame the users
  - They are not security experts
  - Attacks are rare
    - Users do not always suspect malicious action
    - Detecting phishing is hard, even if you're on the lookout for attacks
    - Legitimate messages often look like

Title: Your Final Grades
Sender: Hóng (sanghyun@oregonstate.com)

Hey Guys,

There are some corrections on your final exam scores. I need you to confirm your scores immediately from here.

Thanks,
Sanghyun

Phishing defense: 2FA

- Two-factor authentication
  - Motivation
    - Phishing attacks may expose your passwords to the attackers
    - You want to make that the password is not sufficient for logging in
  - Two-factor authentication (2FA)
    - Prove their identity in two different ways before successfully logging-in
  - Three main ways for a user to prove their identity
    - Something the user knows: password, security questions
    - Something the user has: mobile devices, security keys
    - Something the user is: fingerprint, face ID
  - Stealing one factor (password) is not enough

Phishing defense: 2FA

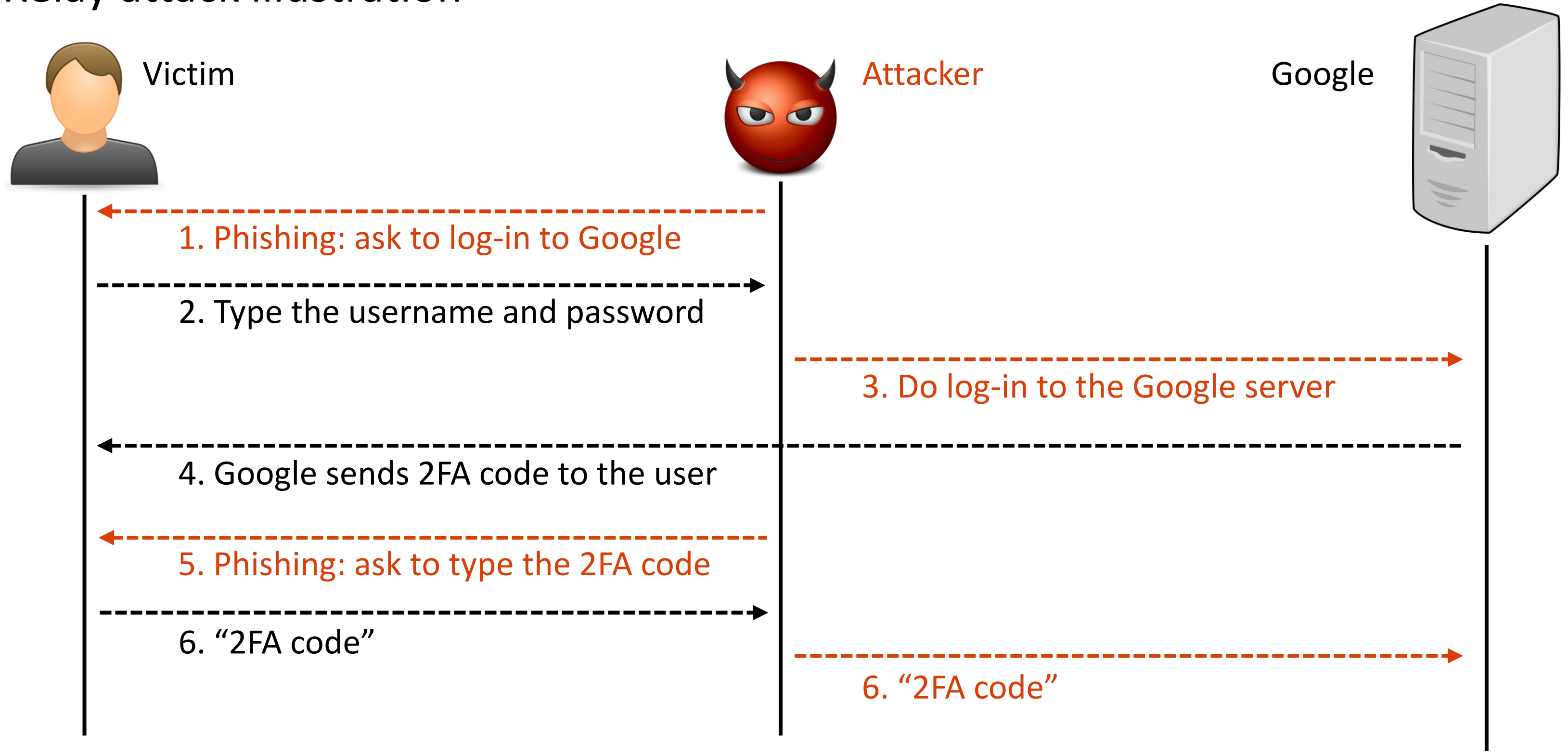
- Two-factor authentication
  - Protection scenarios
    - An attacker steals the password file and performs a dictionary attack
    - The user re-uses passwords on two different websites.
      The attacker compromises one website and tries the same password on the 2nd one

Phishing defense: 2FA weakness

- Relay attack
  - The attacker steal both factors in a single phishing (one stone for two birds)
  - Attack example
    - User uses 2FA
    - 1st : Password (something the user knows)
    - 2nd: A code sent to the user's mobile device (something the user owns)
  - Procedure
    - The phishing website asks the user to input their password (1st factor)
    - The attacker immediately tries to log-in to the actual website as the user
    - The actual website sends a code to the user
    - The phishing website asks the user to enter the code (2nd factor)
    - The attacker enters the code to log in as the user

Phishing defense: 2FA weakness

- Relay attack illustration



Victim
Attacker
Google
1. Phishing: ask to log-in to Google
2. Type the username and password
3. Do log-in to the Google server
4. Google sends 2FA code to the user
5. Phishing: ask to type the 2FA code
6. "2FA code"
6. "2FA code"

Phishing defense: 2FA weakness

- Social engineering
  - Hijacking your phone
    - Attackers can call your phone provider (e.g., T-mobile)
    - Tell them to activate the attacker’s SIM card, and will be done
    - They receive your texts
    - 2FA via SMS is not great but better than nothing
  - Bypassing customer service
    - Attackers can call customer support and ask them to deactivate 2FA!
    - Companies should validate identity if you ask to do this (but not all do)

Phishing defense: authentication token

- Auth token
  - A device that generates secure second-factor codes
  - Examples:
    - RSA SecurID and Google Authenticator
  - Usage
    - The token and the server share a common secret key k
    - When the user wants to log in, the token generates a code HMAC(k, time)
    - The time is often truncated to the nearest 30 seconds for usability
    - The code is often truncated to 6 digits for usability
    - The user submits the code to the website
    - The website uses its secret key to verify the HMAC
  - Downside(s):
    - Vulnerable to relay attacks
    - Vulnerable to online brute-force attacks
    - Possible fix: add a max number of times you can request!

Phishing defense: security key

- Security key
  - A 2nd factor designed to defeat phishing
  - User owns the security key
  - Usage scenario
    - User signs up for a website; the security key generates a new public/private key pair
    - User gives the public key to the website
    - If the user wants to log in, the server sends a nonce to the security key
    - The security key signs the nonce, website name (from the browser), and key ID
    - User gives the signature to the server
  - Security keys prevent phishing
    - In phishing, the security key generates a signature with the attacker's website name, not with the legitimate website name
    - Impervious to relay attacks!

Thank You!

Tu/Th 4:00 – 5:50 PM

Sanghyun Hong

sanghyun.hong@oregonstate.edu

Oregon State University

SAIL
Secure AI Systems Lab