

A decorative background featuring a network diagram. It consists of numerous nodes, represented by small circles, connected by thin lines. Some nodes are solid blue, while others are grey with a blue outline. The network is more densely packed on the left and right sides of the image, with the central area being mostly white space containing the text.

Social Engineering

Patch Notes

Media Archaeology Lab from Tuesday:

- ◎ <https://mediaarchaeologylab.com>
- ◎ On campus: 1320 Grandview Ave

Patch Notes

Final FCQ rate: 65% (below the 80% to drop a quiz 😞)

Regardless, thank you everyone who submitted them!

Patch Notes

Final exam on Tuesday, 7:30pm, this room! Or remote.
Whichever.

Patch Notes

Final exam on Tuesday, 7:30pm, this room! Or remote. Whichever.

Final format and review guide here (also linked in Slack):
https://docs.google.com/document/d/1xqtko1W1WGkjlWy8a_bIPAbvsHP8N9-726ildITVAPg/edit#

A decorative network diagram in the top-left corner, consisting of a complex web of interconnected nodes and lines, rendered in a light gray color. The nodes are represented by small circles, some of which are larger and have concentric circles, suggesting a hierarchical or central structure. The lines are thin and gray, connecting the nodes in a non-linear fashion.

Social Engineering:

Tricking people into doing things

A decorative network diagram in the bottom-right corner, similar to the one in the top-left, featuring a web of interconnected nodes and lines in a light gray color. The nodes are small circles, some with concentric circles, connected by thin gray lines.

A decorative graphic at the top of the slide featuring a network of interconnected nodes and lines. The nodes are represented by circles of varying sizes, some solid and some dashed, connected by thin lines. A central node is highlighted with a larger dashed circle and a blue double quote icon inside it.

“

*“The human is the weakest part of
a computer”*

“

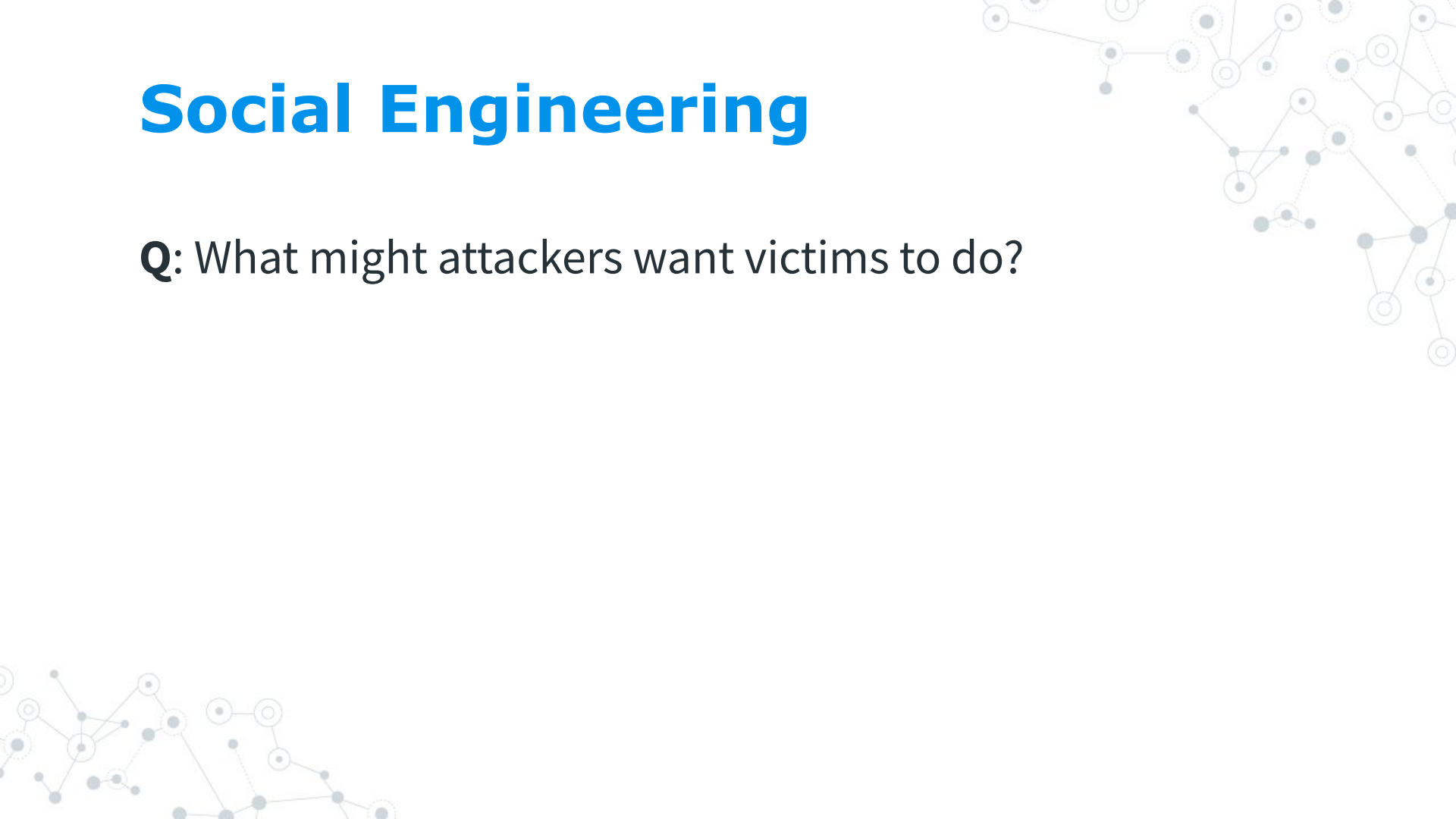
*“The human is the weakest part of
a computer”*

- The Terminator



Social Engineering

Q: What might attackers want victims to do?



Social Engineering

Q: What might attackers want victims to do?

- ⦿ Transfer money
- ⦿ Reveal passwords or 2FA codes
- ⦿ Run programs
- ⦿ Reset accounts (e.g. SIM swap)
- ⦿ ...and more!

Phishing

Phishing: Pretending to be somebody else to steal data



+3033473250

 Apr 7, 17:19 • 01:30

Right seems like the time to renew or extend. Your service contract has expired or will be expiring shortly. If you would like to keep coverage or extended, press eight to speak to a customer service agent and go over your options, press the number nine if you are declining coverage or wish not to be

Phishing



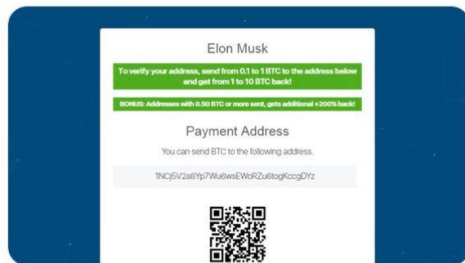
Elon Musk ✓ @patheuk

I'm giving 10 000 Bitcoin (BTC) to all community!

I left the post of director of Tesla, thank you all for your support!

I decided to make the biggest crypto-giveaway in the world, for all my readers who use Bitcoin.

Participate in giveaway - spacex.plus



💬 200

🔄 339

❤️ 1,284



📌 Promoted



Elon Musk

@alon_musk

Follow

Replying to @elonmusk

Hi guys! I'm donating 250 Ethereum to the ETH community! First 250 transactions with 0.2 ETH sent to the address below will receive 1.0 ETH in the address the 0.2 ETH came from.

0x10aF9cd8096EA75a62007b616BC999536CE
2A6fB

Phishing

Cities in Texas hit by QR-code phishing scam



GETTYIMAGES/ MARTIN-DM

<https://gcn.com/cybersecurity/2022/01/cities-texas-hit-qr-code-phishing-scam/360554/>

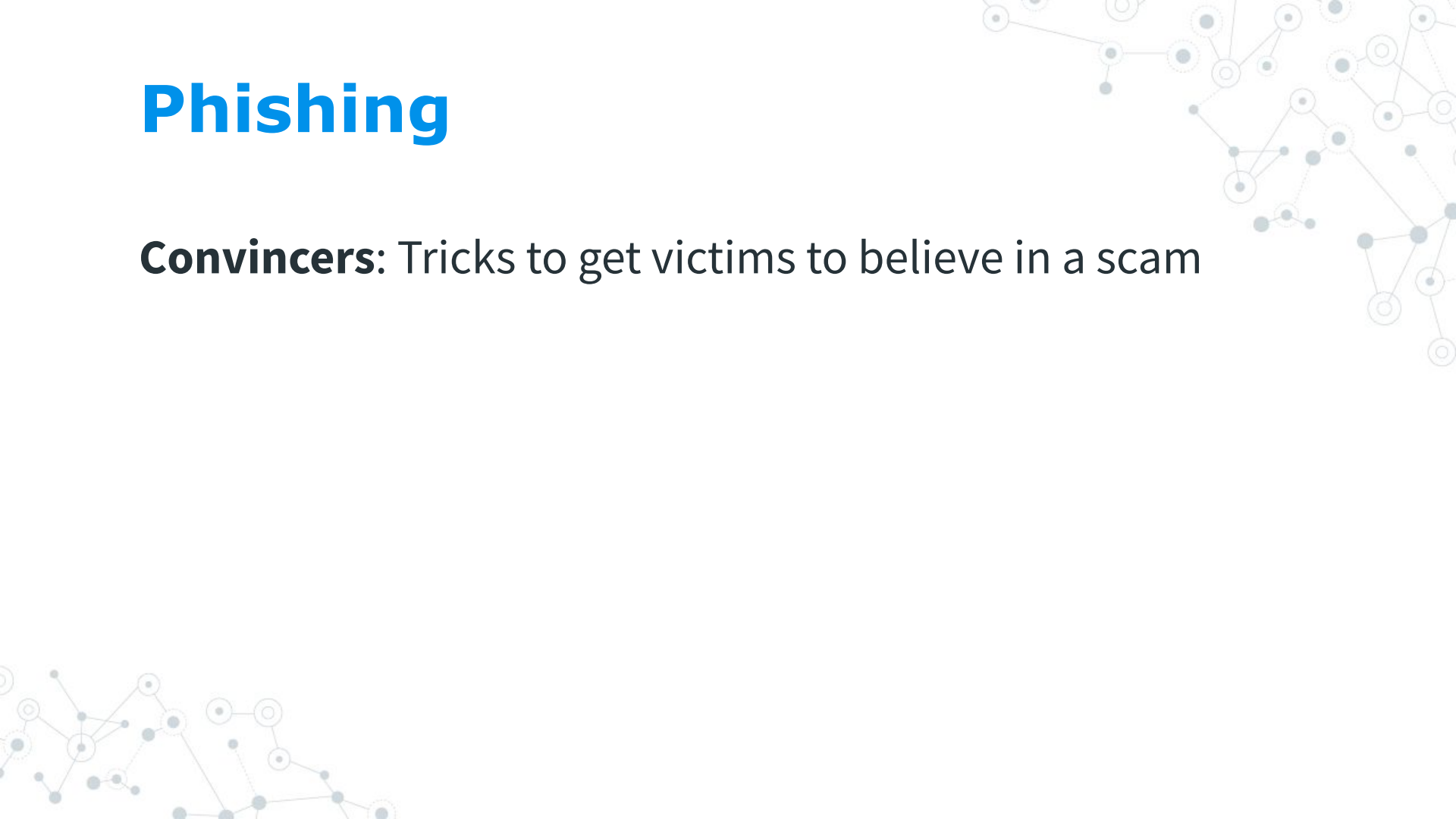
Phishing



<https://blog.malwarebytes.com/cybercrime/2012/10/pick-a-download-any-download/>

Phishing

Convincers: Tricks to get victims to believe in a scam



Phishing

Convincers: Tricks to get victims to believe in a scam

- ◎ Urgency (*“Offer expires in 24 hours!”*)

Phishing

Convincers: Tricks to get victims to believe in a scam

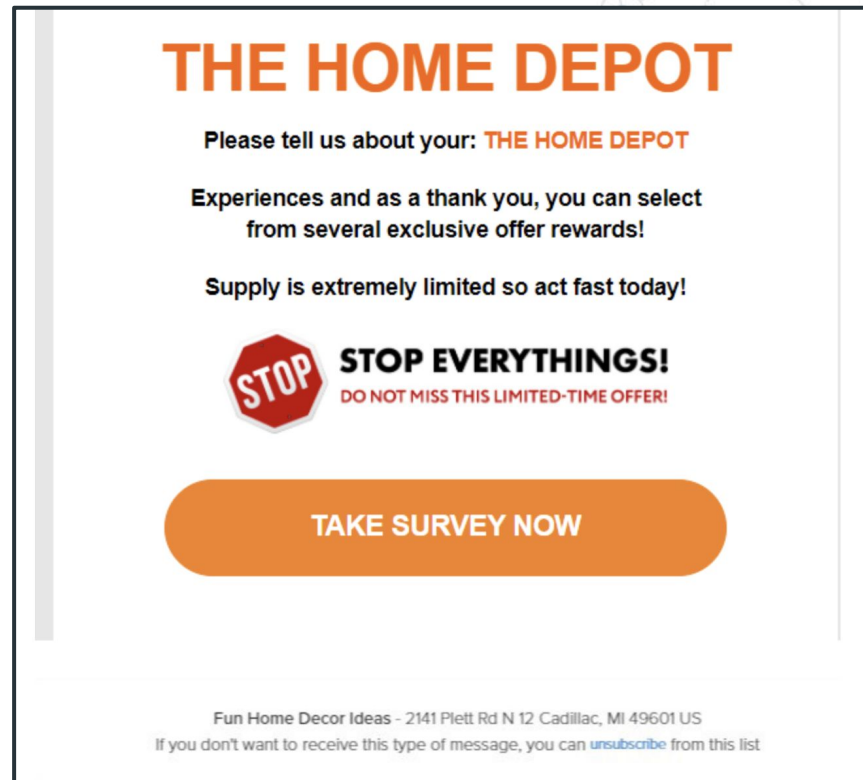
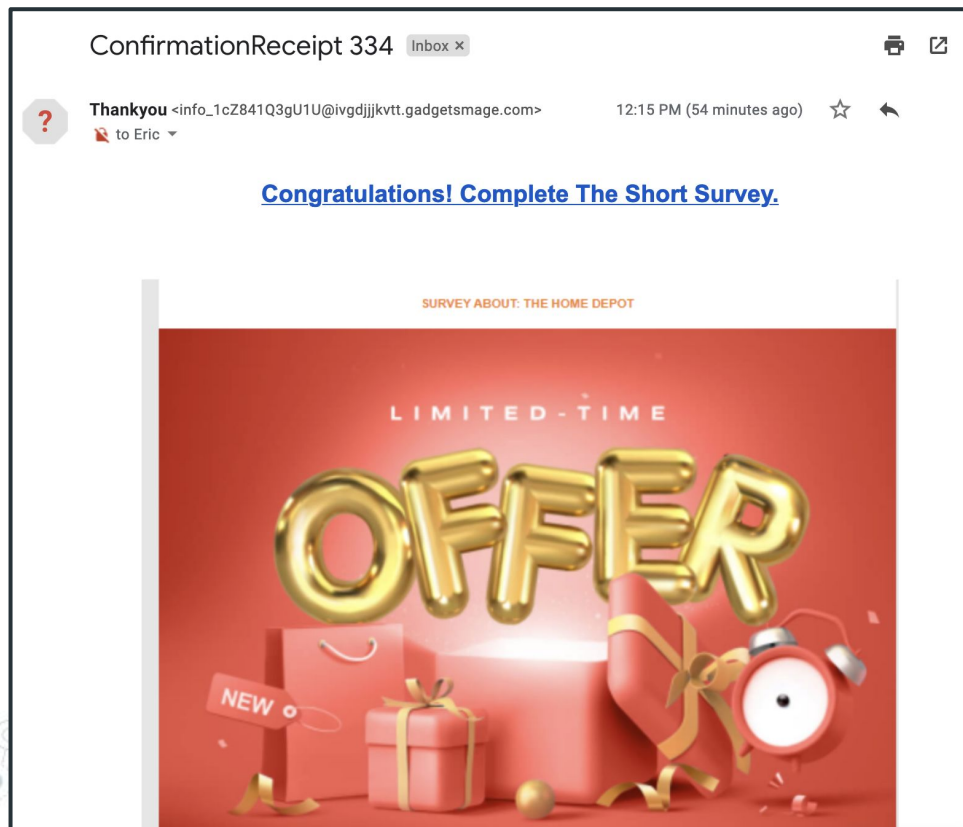
- ◎ Urgency (*“Offer expires in 24 hours!”*)
- ◎ Reward (*“We will double your Bitcoin!”*)

Phishing

Convincers: Tricks to get victims to believe in a scam

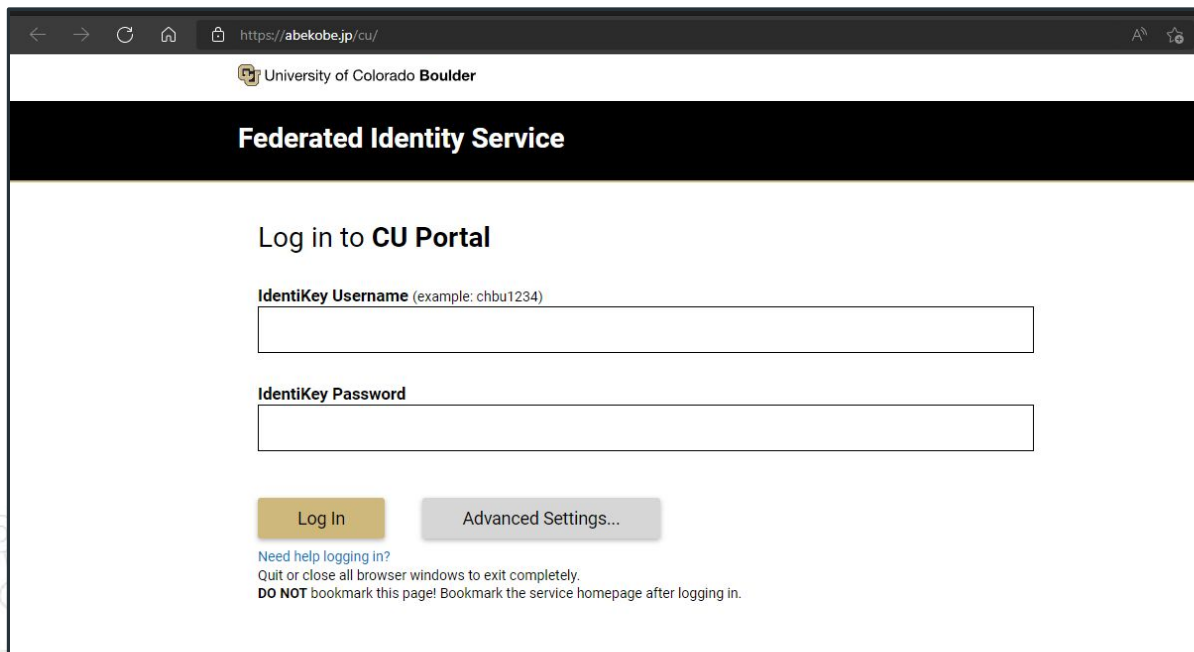
- ◎ Urgency (*“Offer expires in 24 hours!”*)
- ◎ Reward (*“We will double your Bitcoin!”*)
- ◎ Authority (*“I am the IRS / Police / Elon Musk”*)

Phishing




Spear Phishing

Spear Phishing: *A specific, targeted* phishing attack



The image shows a web browser window displaying a phishing page. The address bar shows the URL `https://abekobe.jp/cu/`. The page header includes the University of Colorado Boulder logo and name. Below this is a black banner with the text "Federated Identity Service". The main content area has the heading "Log in to CU Portal". It contains two input fields: "IdentiKey Username (example: chbu1234)" and "IdentiKey Password". Below the password field are two buttons: "Log In" and "Advanced Settings...". At the bottom, there is a link "Need help logging in?" and a warning: "Quit or close all browser windows to exit completely. DO NOT bookmark this page! Bookmark the service homepage after logging in."

← → ↻ 🏠 🔒 `https://abekobe.jp/cu/` A 🌟

 University of Colorado Boulder

Federated Identity Service

Log in to **CU Portal**

IdentiKey Username (example: chbu1234)

IdentiKey Password

Log In Advanced Settings...

[Need help logging in?](#)
Quit or close all browser windows to exit completely.
DO NOT bookmark this page! Bookmark the service homepage after logging in.

Spear Phishing

Spear Phishing convincers:

- ◎ Impersonating real people

Spear Phishing

Spear Phishing convincers:

- ◎ Impersonating real people
- ◎ Correct format

Spear Phishing

Spear Phishing convincers:

- ◎ Impersonating real people
- ◎ Correct format
- ◎ References real events

Spear Phishing

Spear Phishing convincers:

- ◎ Impersonating real people
- ◎ Correct format
- ◎ References real events
- ◎ Proper images and logos
- ◎ ...etc

Spear Phishing

Would you click this?



Alex (Instructor) 11:04 PM

Hi all! Here is a link to the final study guide:

<https://docs.google.com/document/d/1Mn50SeeyPB0c3W8lvkbBaDEcIf0SrDR7vfuLHZeW9NQ/edit>

Spear Phishing

Would you click this?

Anyone can set this



Alex (Instructor) 11:04 PM

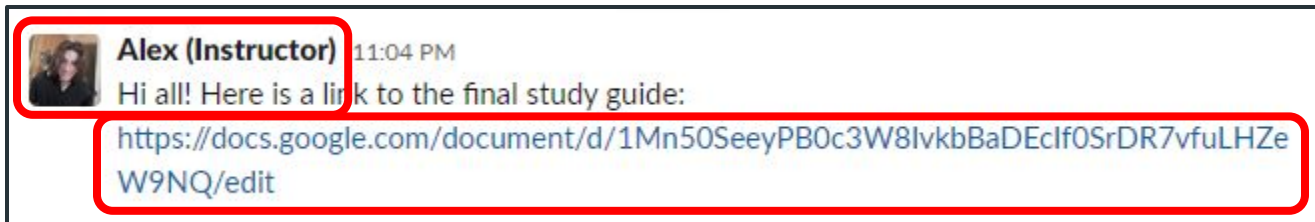
Hi all! Here is a link to the final study guide:

<https://docs.google.com/document/d/1Mn50SeeyPB0c3W8lvkbBaDEclF0SrDR7vfuLHZeW9NQ/edit>

Spear Phishing

Would you click this?

Anyone can set this



The link *text* is not the link *location*!

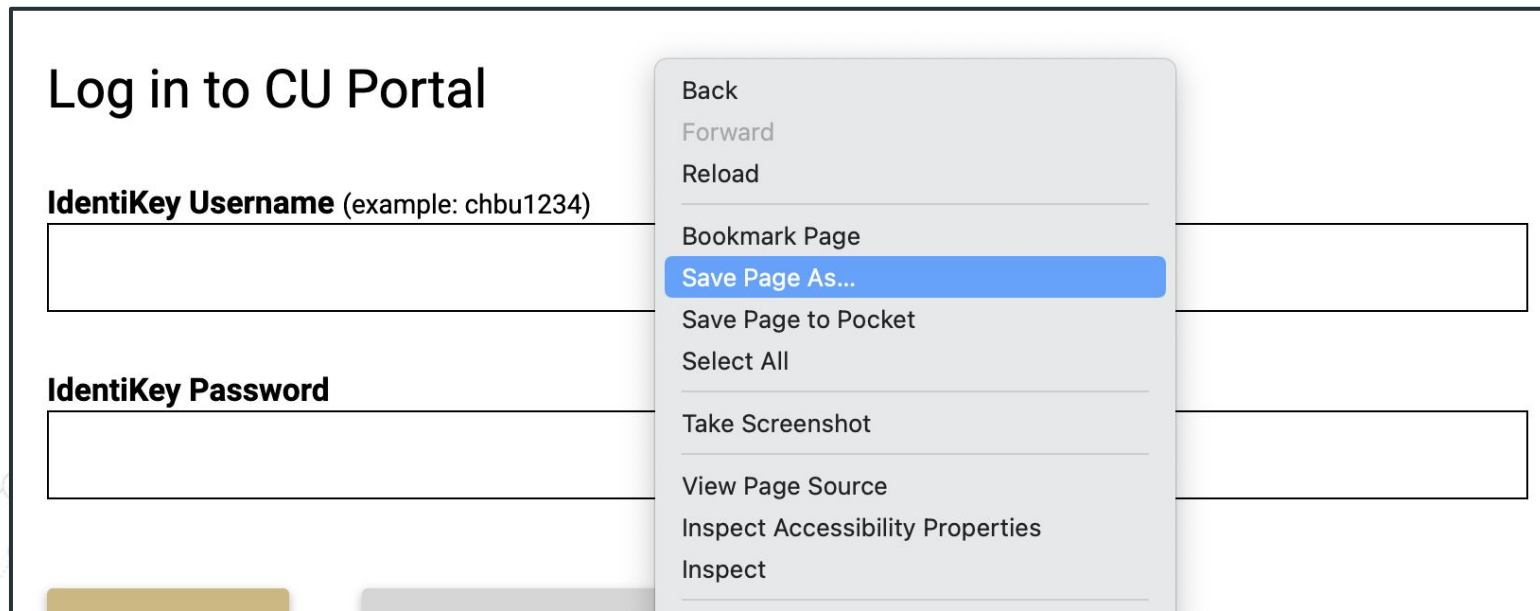
Spear Phishing

You can only see the actual link by hovering...



Spear Phishing

Coping a website is really easy



The image shows a web browser window with a login page titled "Log in to CU Portal". The page has two input fields: "IdentiKey Username (example: chbu1234)" and "IdentiKey Password". A context menu is open over the username field, displaying various browser actions. The "Save Page As..." option is highlighted in blue. The background of the slide features a decorative network diagram with nodes and connecting lines.

Log in to CU Portal

IdentiKey Username (example: chbu1234)

IdentiKey Password

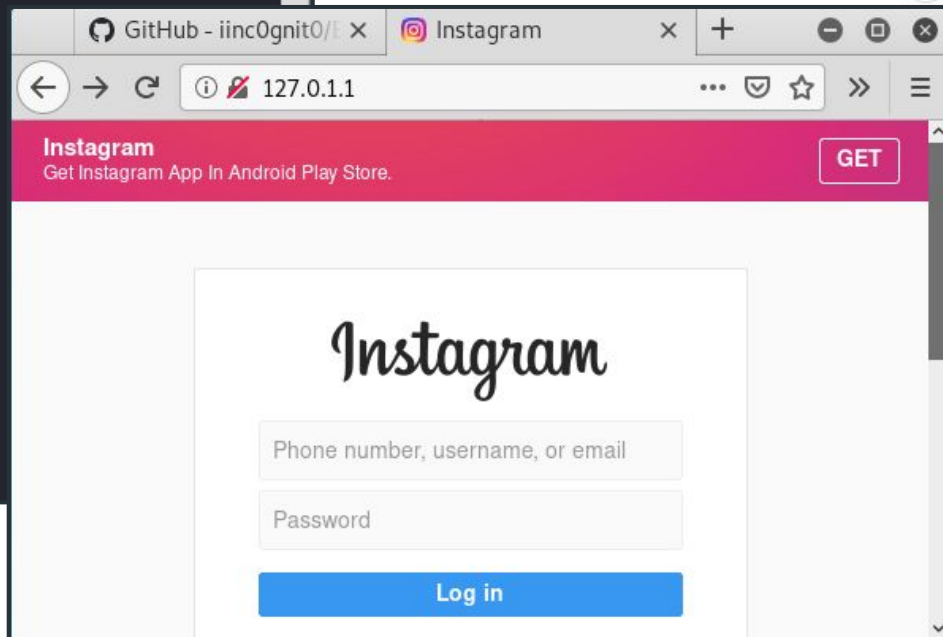
- Back
- Forward
- Reload
- Bookmark Page
- Save Page As...**
- Save Page to Pocket
- Select All
- Take Screenshot
- View Page Source
- Inspect Accessibility Properties
- Inspect

Spear Phishing

```
root@kali: ~/Desktop/BlackPhish
File Actions Edit View Help
Big Thanks to: [ DarkSecDevelopers ]

[1] Instagram
[2] Google
[3] Facebook
[4] Netflix
[5] Twitter
[6] Snapchat
[0] Clean
[x] Exit

[BlackPhish] →
```



Spear Phishing

LEGAL

Intuit Faces Class-Action Lawsuit Over Trezor Phishing Hack

By PYMNTS  

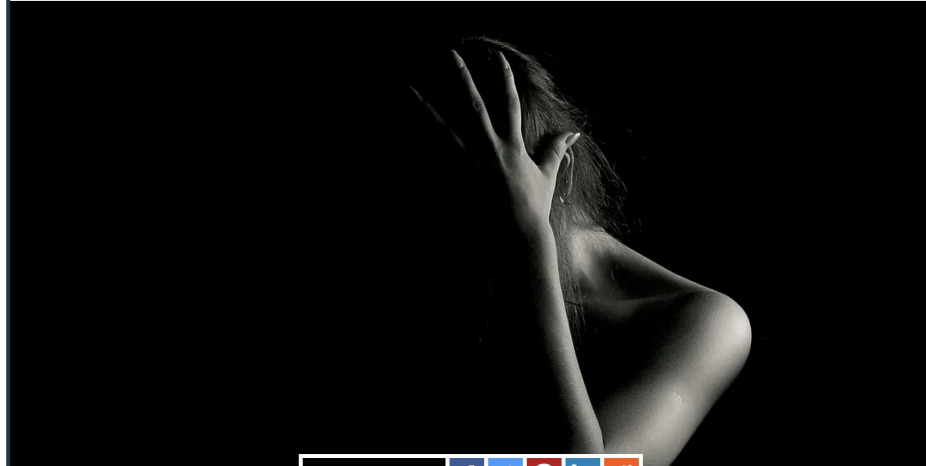
Listen to Article ▶ 

Posted on April 24, 2022



Apple tricked into releasing personal data used to sexually extort minors

Ben Lovejoy - Apr. 27th 2022 5:14 am PT  [@benlovejoy](#)



13 Comments     

<https://9to5mac.com/2022/04/27/apple-tricked-personal-data-minors/>

<https://www.pymnts.com/legal/2022/intuit-faces-class-action-lawsuit-over-trezor-phishing-hack/>

Social Engineering

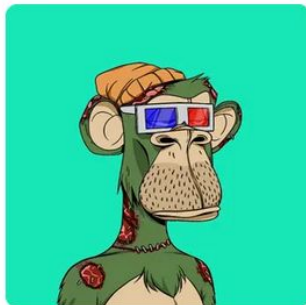
April 25, 2022

133 NFTs valued at \$2.4 million stolen when hacked Bored Apes Instagram advertises fake land airdrop

The Bored Ape Yacht Club's Instagram account was compromised and used to advertise a fake airdrop for metaverse land. This was particularly believable, as the much-anticipated project announced it would be launching this week.

The post invited people to visit a website that prompted users to connect their wallets in order to receive the airdrop. Users who did so found their NFTs transferred out of their wallet to the scammer. So far, 44 people have fallen for the scam site, transferring a total of 133 NFTs with an estimated value of around \$2.4 million. The stolen NFTs included items from pricey collections including Bored Apes, Mutant Apes, Bored Ape Kennel Club, and CloneX. Several of the NFTs had previously been sold for over \$100,000 each.

- [Tweet by Bored Ape Yacht Club](#)
- [Scammer wallet](#) on Etherscan



BAYC #7203

[\(attribution\)](#)

Other entries related to BAYC phishing attacks or Bored Ape Yacht Club

Hack or scam

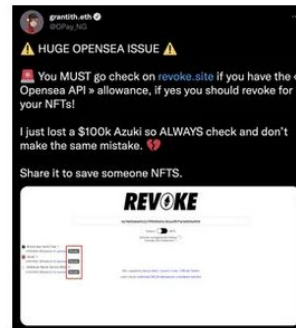
Blockchain: Ethereum | NFT

April 6, 2022

Scammer creates a fake site to revoke wallet permissions, then pretends there is an OpenSea vulnerability to trick people into using it

It's not exactly straightforward to revoke wallet permissions once they've been granted, and so many users use a site called [revoke.cash](#) to remove permissions in the case of malicious contracts or as a precautionary measure. A clever scammer created a fake website that mimics [revoke.cash](#), called [revoke.site](#), and then used a verified Twitter account to tweet about a "huge OpenSea issue" that they claimed resulted in the loss of a pricey NFT. Hoping that people would panic and try to use the site to revoke permissions, in reality the website runs a script to determine the highest value assets, and then prompts the user to "revoke" permissions for those assets—when in reality, it sets approval for those assets to be transferred to the scammer's wallet. As of the evening of April 7, the wallet had received 13 NFTs, and flipped eight of them for a total profit of 4.9 ETH (~\$16,000).

- [Scam wallet](#) on Etherscan
- [Tweet thread by 0xQuit](#)



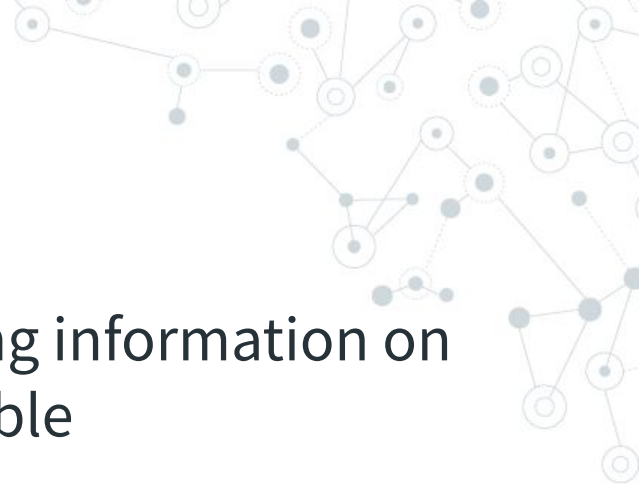
A tweet falsely claiming an OpenSea vulnerability, linking to a scam permission revocation website [\(attribution\)](#).

Hack or scam

Blockchain: Ethereum | NFT

Social Engineering

Open source intelligence (OSInt): Finding information on a person / company which is freely available



Social Engineering

Open source intelligence (OSInt): Finding information on a person / company which is freely available

- © Names / emails of friends or coworkers

Social Engineering

Open source intelligence (OSInt): Finding information on a person / company which is freely available

- ◎ Names / emails of friends or coworkers
- ◎ Projects, tools, vendors

Social Engineering

Open source intelligence (OSInt): Finding information on a person / company which is freely available

- ◎ Names / emails of friends or coworkers
- ◎ Projects, tools, vendors
- ◎ Recent events

Social Engineering

Open source intelligence (OSInt): Finding information on a person / company which is freely available

- ◎ Names / emails of friends or coworkers
- ◎ Projects, tools, vendors
- ◎ Recent events
- ◎ Logos and formatting

Social Engineering

Example: recon-ng

Looking Up Data For: Occupytheweb

```
[*] Checking: 7cup
[*] Checking: ACloudGuru
[*] Checking: asciinema
[*] Checking: AudioJungle
[*] Checking: BiggerPockets
[*] Checking: Bookcrossing
[*] Checking: buymeacoffee
[*] Checking: championat
[*] Checking: Cloudflare
[*] Checking: cnet
[*] Checking: coroflot
[*] Checking: Codewars
[*] Checking: Coderwall
[*] Checking: crevado
[*] Checking: Dating.ru
[*] Checking: Designspration
[*] Checking: dev.to
[*] Checking: Ello.co
[*] Checking: Eyeem
[*] Checking: fancy.com
[*] Checking: Gamepedia
[*] Checking: gumroad
```

SUMMARY

```
[*] 21 total (21 new) profiles found.
[recon-ng][default][profiler] > █
```

<https://www.hackers-arise.com/post/2019/05/16/OSINT-Part-2-Using-recon-ng-to-find-the-Same-Profile-across-Multiple-Sites>

Social Engineering



```
C:\Users\Beam\dev\SkypeSearch>py skypesearch.py live:chloe [REDACTED]

[+] Found 1 users
-----

Skype ID: live:chloe [REDACTED]
Display Name: Chloe

Profile Avatar: https://avatar.skype.com/v1/avatars/[REDACTED]/public
[-] Default Avatar

[+] Location found!
- Country: [REDACTED]

[+] Other info found!
- Date of Birth: 2000-05-23
- Gender: Female
- Email: [REDACTED]@outlook.com

=> The account was created between 2016 - late 2019
-----
```

Social Engineering



Tinker 🌞 @TinkerSec · Oct 8, 2021
Morning #OSINT Challenge.

Where am I? What location and city?

(Bonus points if you figure out which floor I'm on).



<https://twitter.com/TinkerSec/status/1446491011836952576>

Social Engineering



Tinker 🌞 @TinkerSec · Oct 8, 2021

Morning #OSINT Challenge.

Where am I? What location and city?

(Bonus points if you figure out which floor I'm on).



PG @Pgrees3 · Oct 8, 2021

Courtyard by Marriott Knoxville Downtown. 210 W Church Ave, Knoxville, TN 37902

Facing West by Southwest along W Church St.



3



3



Tinker 🌞
@TinkerSec

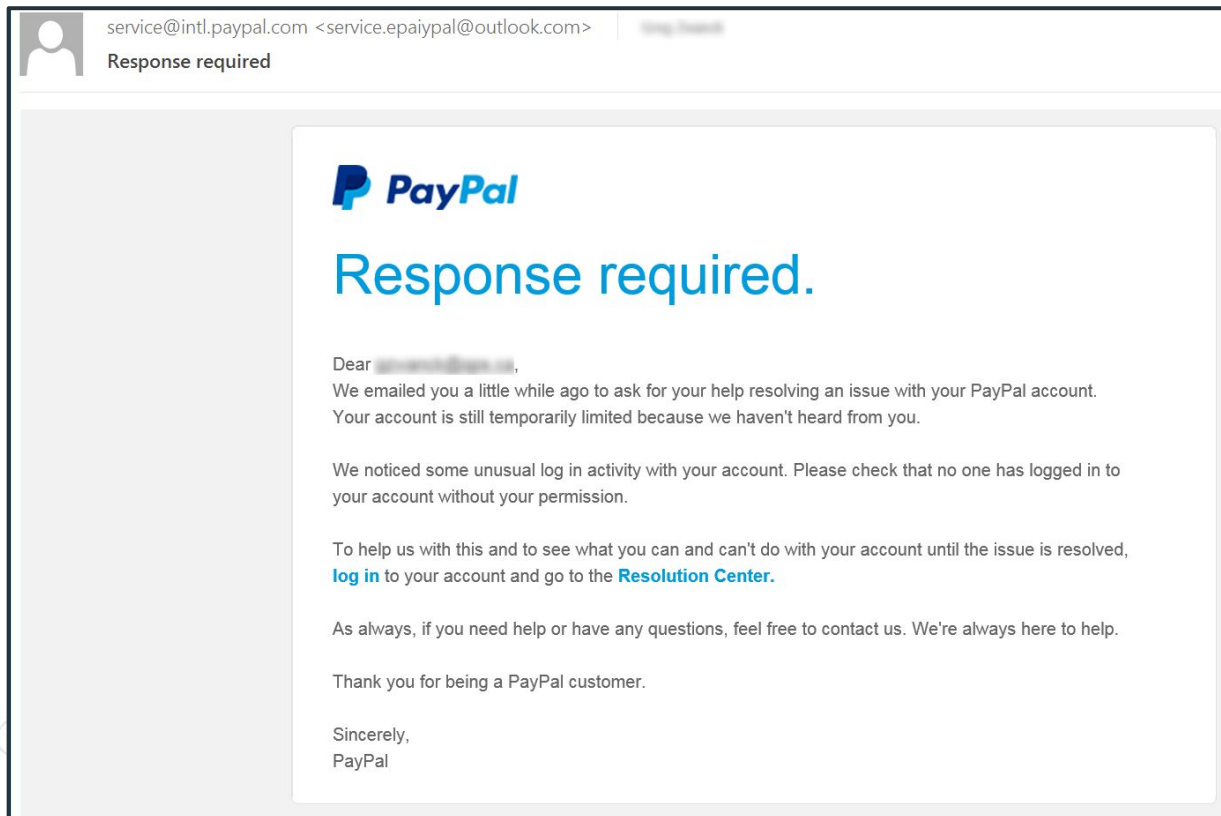
Replying to @Pgrees3

Got it! Thorough answer!

5:36 AM · Oct 9, 2021 · Twitter for iPhone

<https://twitter.com/TinkerSec/status/1446491011836952576>

Social Engineering



Social Engineering

Mitigations:

- © Just be careful

Social Engineering

Mitigations:

© ~~Just be careful~~

Social Engineering

Mitigations:

- ⦿ ~~Just be careful~~
- ⦿ Verify link domains and HTTPS



Secure

<https://www.cloudflare.com>



Not secure

<http://www.cloudflare.com>



Not secure

<http://xyz.cloudflare-com.io>

<https://www.cloudflare.com/learning/ssl/what-is-domain-spoofing/>

Social Engineering

This is hard, as many **legit** messages do this!



Secure

<https://www.cloudflare.com>



Not secure

<http://www.cloudflare.com>



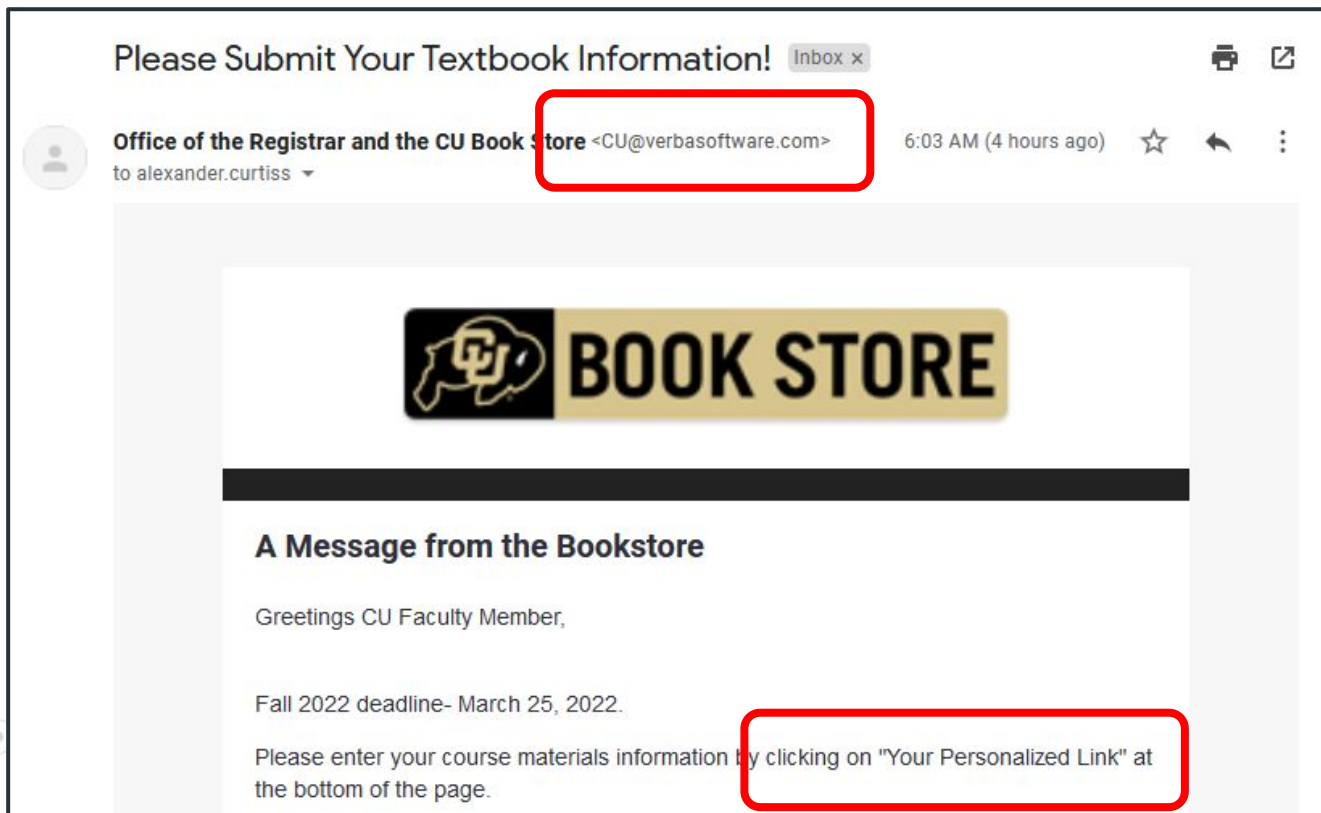
Not secure

<http://xyz.cloudflare-com.io>

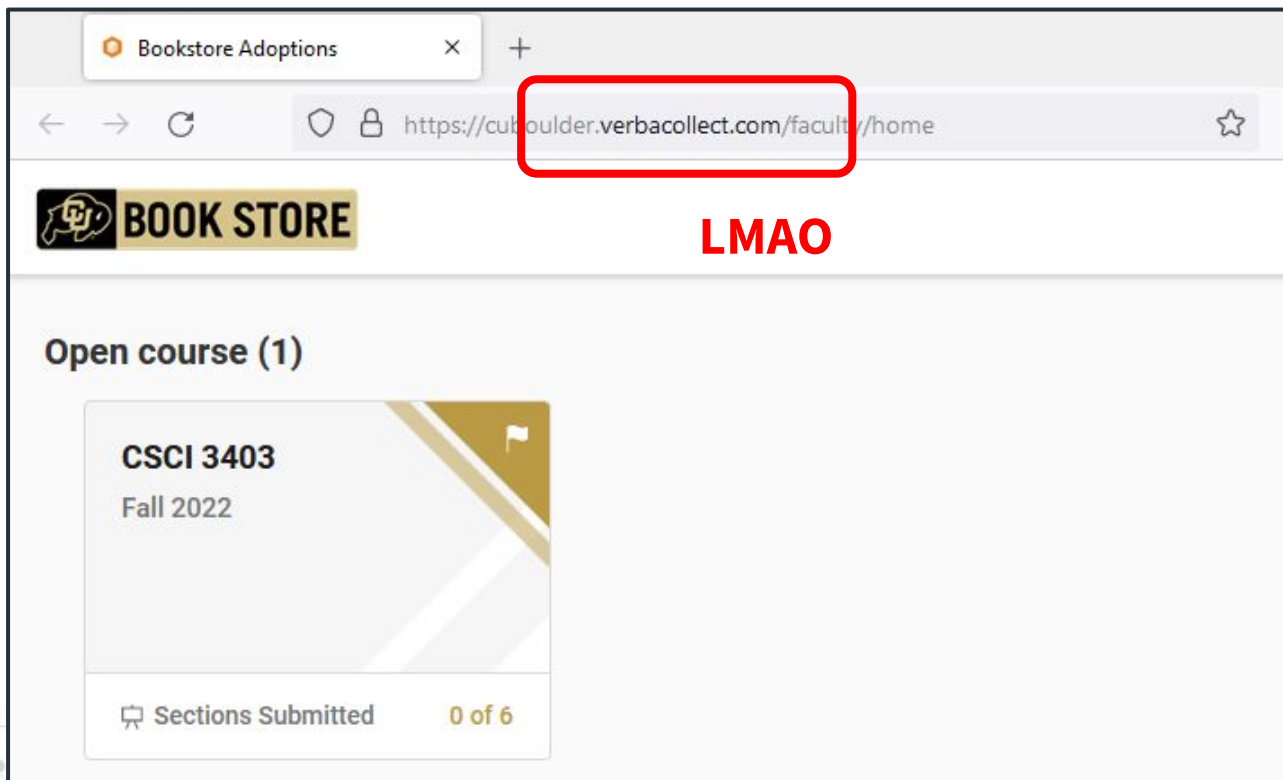
<https://www.cloudflare.com/learning/ssl/what-is-domain-spoofing/>

Social Engineering

LOL



Social Engineering



Social Engineering

Mitigations:

- ⦿ ~~Just be careful~~
- ⦿ Verify link domains and HTTPS (if you can 🙄)



Secure

| <https://www.cloudflare.com>



Not secure

| <http://www.cloudfiare.com>



Not secure

| <http://xyz.cloudflare-com.io>

<https://www.cloudflare.com/learning/ssl/what-is-domain-spoofing/>

Social Engineering

Mitigations:

- ⦿ ~~Just be careful~~
- ⦿ Verify link domains and HTTPS (*if you can* 🙄)
- ⦿ Strong 2 FA



Secure

<https://www.cloudflare.com>



Not secure

<http://www.cloudflare.com>



Not secure

<http://xyz.cloudflare-com.io>

<https://www.cloudflare.com/learning/ssl/what-is-domain-spoofing/>

Social Engineering

Mitigations:

- ⦿ ~~Just be careful~~
- ⦿ Verify link domains and HTTPS (*if you can* 🙄)
- ⦿ Strong 2 FA
- ⦿ Password managers



Secure

<https://www.cloudflare.com>



Not secure

<http://www.cloudflare.com>



Not secure

<http://xyz.cloudflare-com.io>

<https://www.cloudflare.com/learning/ssl/what-is-domain-spoofing/>

Social Engineering

Federated Identity Service | University of Colorado Boulder

https://fedauth.colorado.edu/idp/profile/SAML2/POST/SSO?execution=e1s1

University of Colorado Boulder

Federated Identity

Log in to CU Portal

IdentiKey Username (example: alcu5535)

IdentiKey Password

Log In

Advanced Settings...

Search 1Password

+ New Item

Suggestions

Colorado alcu5535

Alex Alex

Alex's ... Private Autofill

Colorado Boulder

username alcu5535

password Fantastic

website https://identikey.colorado.edu

LINKED APPS

Social Engineering

More social engineering vectors:

- ◎ Vishing (“voice Phishing” over the phone)

<https://youtu.be/F78UdORll-Q?t=84>



Social Engineering

More social engineering vectors:

- © Physical entry

<https://youtu.be/pL9q2lOZ1Fw>



I talked to [redacted]. We're here from [redacted] to check on some speed issues and some other stuff with the internet.

Social Engineering

The "You have no idea who I am but you'll let me into your building anyway" starter pack



Social Engineering

Takeaways:

- ◎ Phishing is very difficult to avoid!

Social Engineering

Takeaways:

- ◎ Phishing is very difficult to avoid!
- ◎ In fact, assume that you, a friend, or a coworker, **will** be phished!

Social Engineering

Takeaways:

- ◎ Phishing is very difficult to avoid!
- ◎ In fact, assume that you, a friend, or a coworker, **will** be phished!
 - 2FA / password managers
 - Extra care when entering sensitive data
 - Separation of privilege



Any final questions?



That's all Folks!