Hacking Multifactor Authentication

<because nothing is unhackable>

whoami

<everyone needs an introduction>

pleasepleasework.py   aboutme.txt

whoami

- ⭐ Senior IAM Consultant
- ⭐ B.S. Cybersecurity and Information Assurance
- ⭐ In IT since 2018

```
  ／l、
（ﾟ、 。7
  l、゛~ヽ
  じし(_, )ノ
```

DISCLAIMER

<this talk is just for fun>

The problem with passwords

<they work, but…>

numberofbreachedpasswords.txt rockyou.txt

8,400,000,000

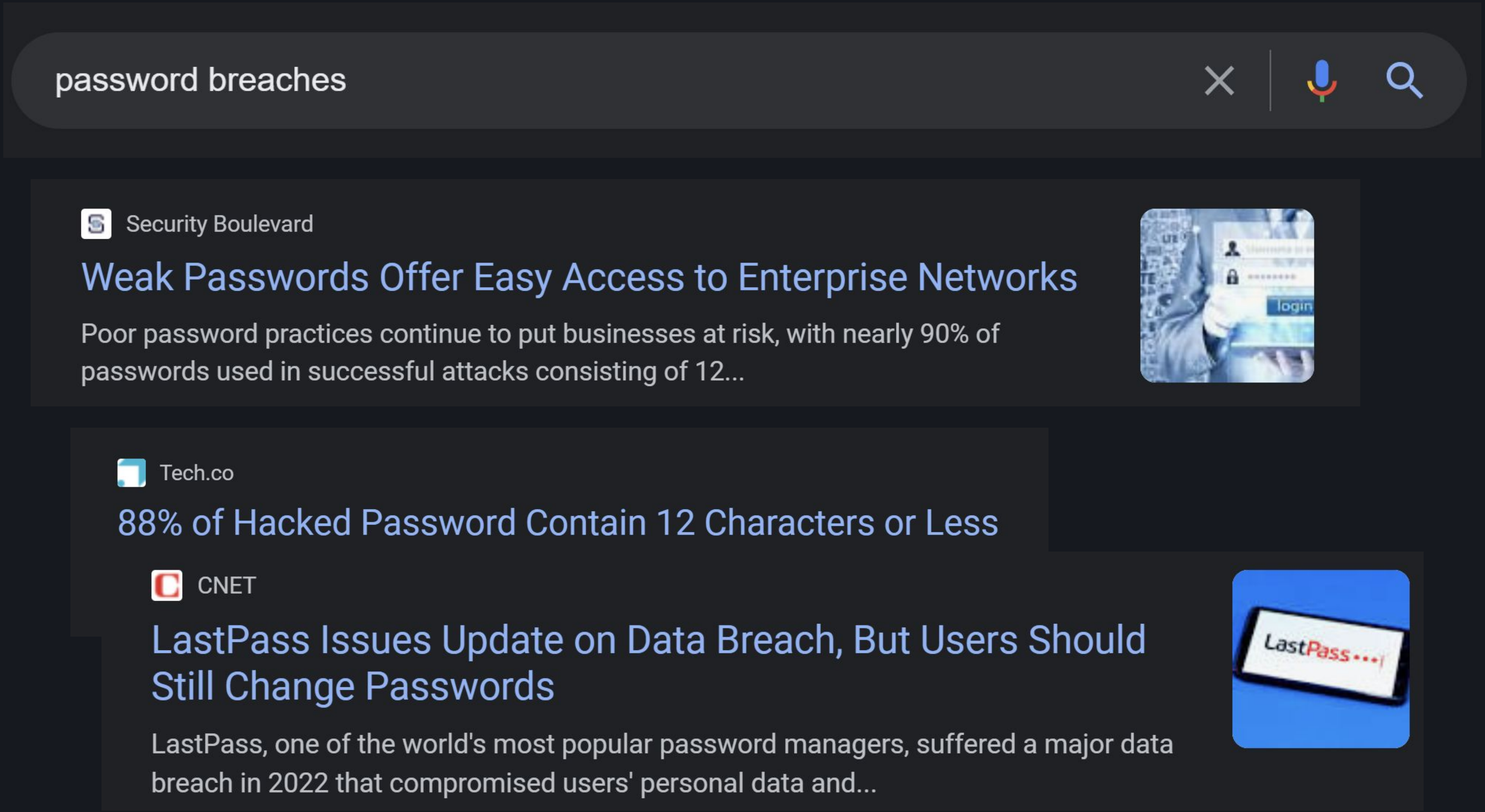
passwords have been breached (and this is a small estimate)

What makes them vulnerable?

⭐ Password reuse is common

⭐ Easily guessed depending on complexity

⭐ Insecure storage mechanisms



password breaches

Security Boulevard

Weak Passwords Offer Easy Access to Enterprise Networks

Poor password practices continue to put businesses at risk, with nearly 90% of passwords used in successful attacks consisting of 12...

Tech.co

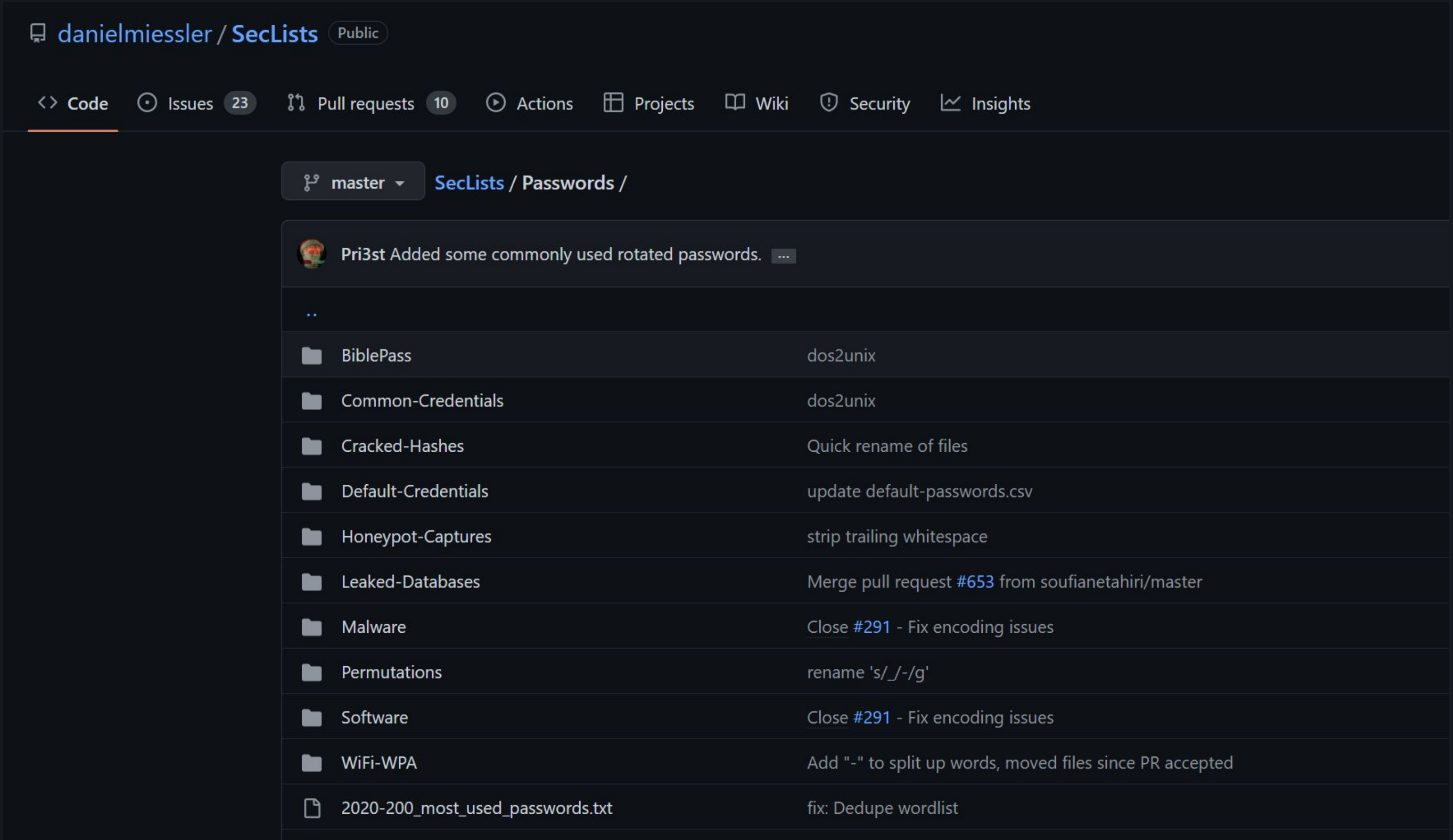
88% of Hacked Password Contain 12 Characters or Less

CNET

LastPass Issues Update on Data Breach, But Users Should Still Change Passwords

LastPass, one of the world's most popular password managers, suffered a major data breach in 2022 that compromised users' personal data and...

https://github.com/danielmiessler/SecLists



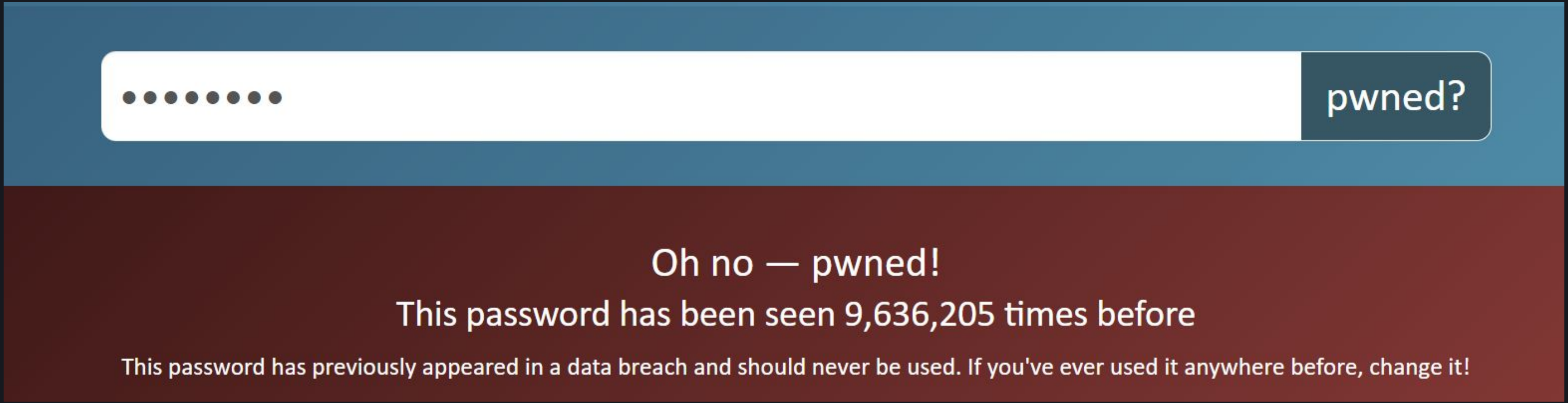
Pri3st Added some commonly used rotated passwords. ...

..

BiblePass	dos2unix
Common-Credentials	dos2unix
Cracked-Hashes	Quick rename of files
Default-Credentials	update default-passwords.csv
Honeypot-Captures	strip trailing whitespace
Leaked-Databases	Merge pull request #653 from soufianetahiri/master
Malware	Close #291 - Fix encoding issues
Permutations	rename 's/_/-/g'
Software	Close #291 - Fix encoding issues
WiFi-WPA	Add "-" to split up words, moved files since PR accepted
2020-200_most_used_passwords.txt	fix: Dedupe wordlist

https://haveibeenpwned.com

⭐ Let’s search for “password”



Oh no — pwned!

This password has been seen 9,636,205 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

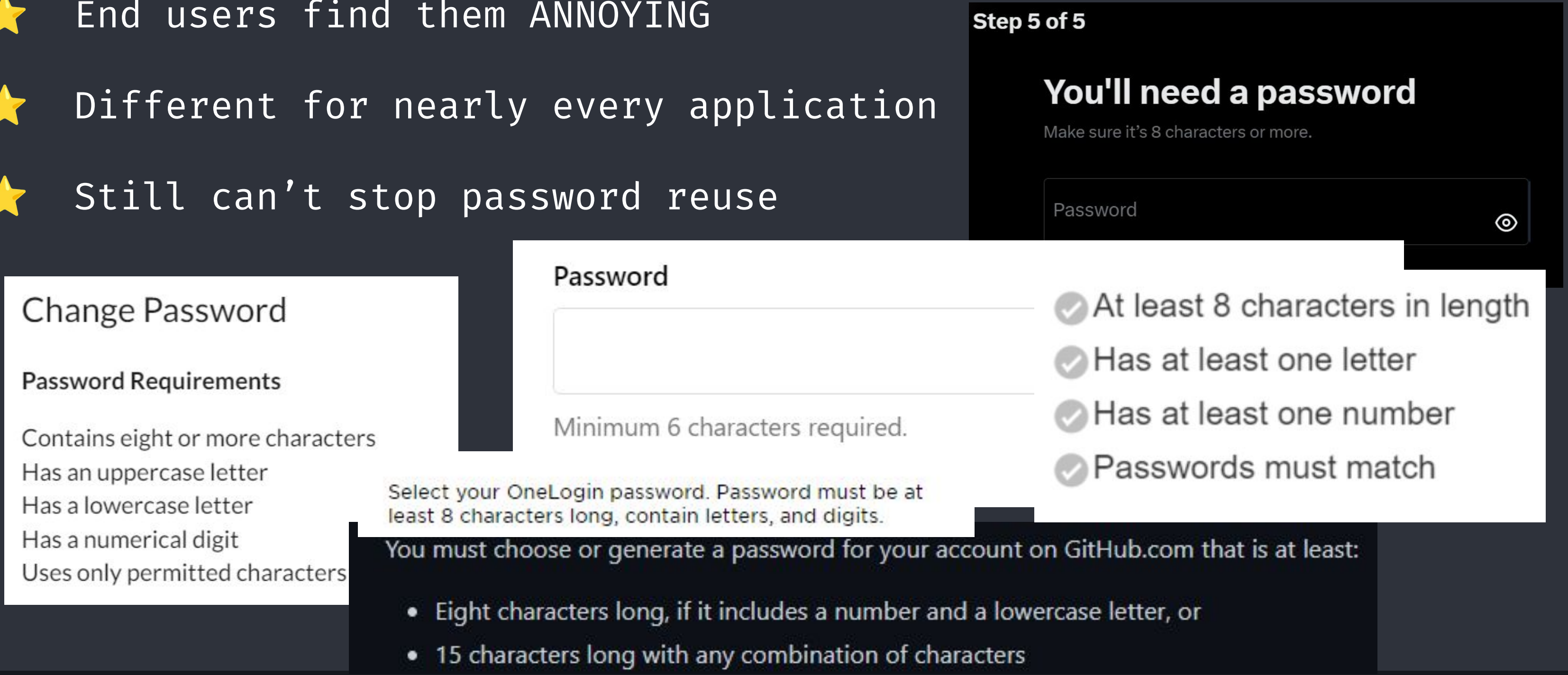
(bad guys can use this tool too)

Weak password mitigations

<it’s a start…>

Complexity requirements work, but…

- ⭐ End users find them ANNOYING
- ⭐ Different for nearly every application
- ⭐ Still can’t stop password reuse



Step 5 of 5

You'll need a password

Make sure it’s 8 characters or more.

Password

Change Password

Password Requirements

Contains eight or more characters
Has an uppercase letter
Has a lowercase letter
Has a numerical digit
Uses only permitted characters

Password

Minimum 6 characters required.

✓ At least 8 characters in length
✓ Has at least one letter
✓ Has at least one number
✓ Passwords must match

Select your OneLogin password. Password must be at least 8 characters long, contain letters, and digits.

You must choose or generate a password for your account on GitHub.com that is at least:

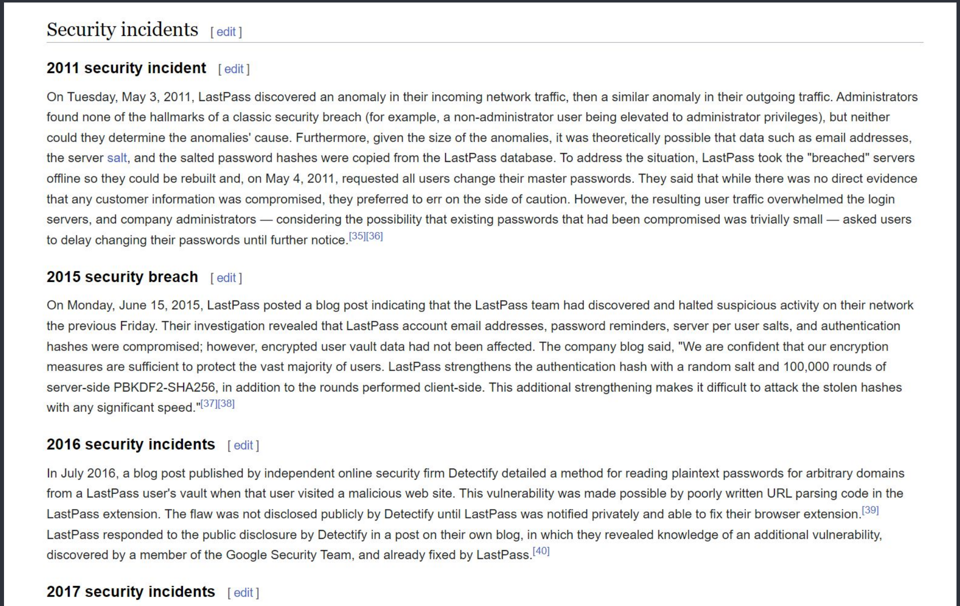
- Eight characters long, if it includes a number and a lowercase letter, or
- 15 characters long with any combination of characters

The password complexity debate

- ⭐ More characters? Less characters? Special characters?
- ⭐ Do we REALLY need to reset our passwords?
- ⭐ In any case, NEVER reuse your passwords!

Password managers are great!

⭐ (until they get hacked)



Security incidents [edit]

2011 security incident [edit]

On Tuesday, May 3, 2011, LastPass discovered an anomaly in their incoming network traffic, then a similar anomaly in their outgoing traffic. Administrators found none of the hallmarks of a classic security breach (for example, a non-administrator user being elevated to administrator privileges), but neither could they determine the anomalies' cause. Furthermore, given the size of the anomalies, it was theoretically possible that data such as email addresses, the server salt, and the salted password hashes were copied from the LastPass database. To address the situation, LastPass took the "breached" servers offline so they could be rebuilt and, on May 4, 2011, requested all users change their master passwords. They said that while there was no direct evidence that any customer information was compromised, they preferred to err on the side of caution. However, the resulting user traffic overwhelmed the login servers, and company administrators — considering the possibility that existing passwords that had been compromised was trivially small — asked users to delay changing their passwords until further notice.[35][36]

2015 security breach [edit]

On Monday, June 15, 2015, LastPass posted a blog post indicating that the LastPass team had discovered and halted suspicious activity on their network the previous Friday. Their investigation revealed that LastPass account email addresses, password reminders, server per user salts, and authentication hashes were compromised; however, encrypted user vault data had not been affected. The company blog said, "We are confident that our encryption measures are sufficient to protect the vast majority of users. LastPass strengthens the authentication hash with a random salt and 100,000 rounds of server-side PBKDF2-SHA256, in addition to the rounds performed client-side. This additional strengthening makes it difficult to attack the stolen hashes with any significant speed."[37][38]

2016 security incidents [edit]

In July 2016, a blog post published by independent online security firm Detectify detailed a method for reading plaintext passwords for arbitrary domains from a LastPass user's vault when that user visited a malicious web site. This vulnerability was made possible by poorly written URL parsing code in the LastPass extension. The flaw was not disclosed publicly by Detectify until LastPass was notified privately and able to fix their browser extension.[39] LastPass responded to the public disclosure by Detectify in a post on their own blog, in which they revealed knowledge of an additional vulnerability, discovered by a member of the Google Security Team, and already fixed by LastPass.[40]

2017 security incidents [edit]

ithurtsme.txt quotes.txt

Real life password quotes

- ⭐ “I am so ****ing tired of changing my password all the time.”
- ⭐ “I use the same password for everything. It’s easier.”
- ⭐ “Yeah… I’m not doing that…” (In reference to using a password manager”

MFA.txt hooray.txt

Multifactor Authentication

<we're saved!!!>

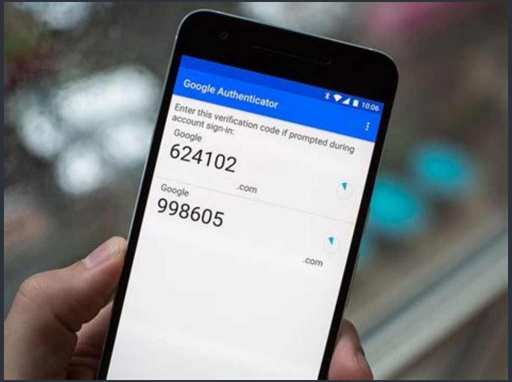
Password + (OTP or Biometric) = WIN

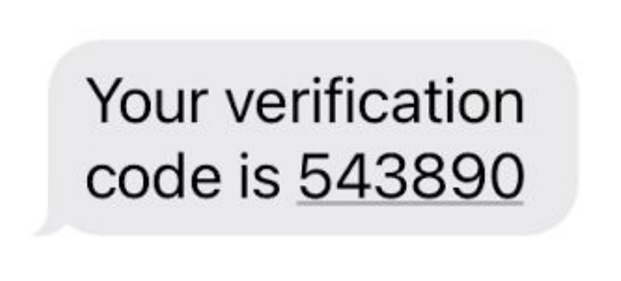
Something you know

Something you have or something you are

Common authentication methods

- ⭐ OTPs - SMS & Authenticator apps
- ⭐ Push notifications
- ⭐ Biometrics


Google Authenticator
Enter this verification code if prompted during account sign-in:
Google
624102
.com
Google
998605
.com


Your verification code is 543890

Challenges with implementing MFA

- ⭐ End-user friction
- ⭐ Increased help desk tickets
- ⭐ Application compatibility + migration

ForgeRock®

onelogin

Ping Identity®

okta

MFA Bypass overview

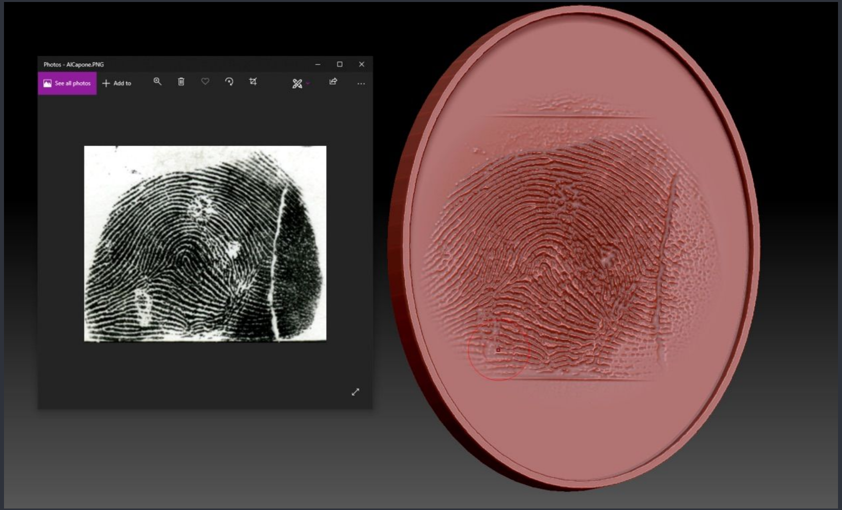
- ⭐ Insecure components
- ⭐ Physical device access
- ⭐ Setup keys - Google & Microsoft Authenticator
- ⭐ Social engineering your OTP
- ⭐ MFA bombing / fatigue
- ⭐ SMS

Physical device access

<it’s not your computer anymore>

Game over

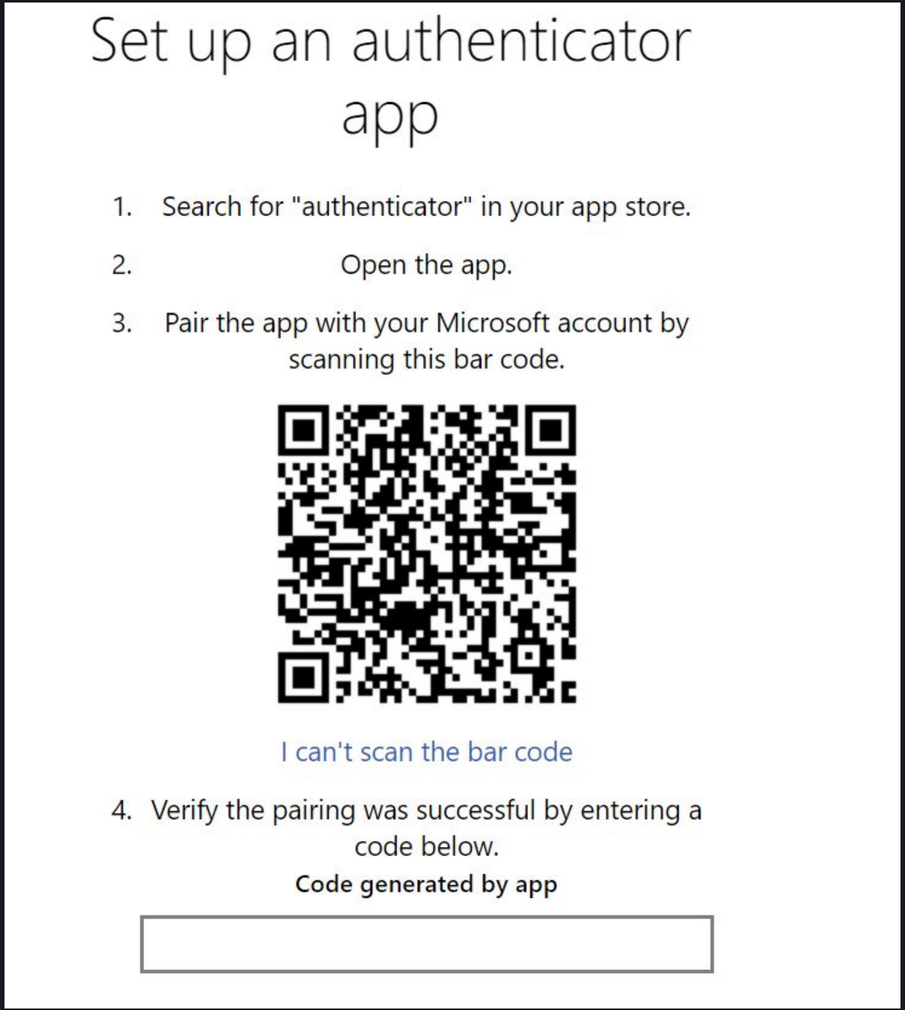
- ⭐ Biometric attacks
- ⭐ Cold boot attacks



Setup keys

<they don’t expire>

SCAN ME!



Set up an authenticator app

1. Search for "authenticator" in your app store.
2. Open the app.
3. Pair the app with your Microsoft account by scanning this bar code.

I can't scan the bar code

4. Verify the pairing was successful by entering a code below.

Code generated by app

Social engineering your OTP

<no OTP? no problem!>

Just ask for it!

⭐ Email or SMS

> Hello Kylie, we noticed a suspicious login to your Google account. To avoid locking out your account, we need to verify your identity. Please respond to this message with the six-digit code you will be receiving momentarily.

bombing.txt

notokaywiththis.txt

MFA Bombing

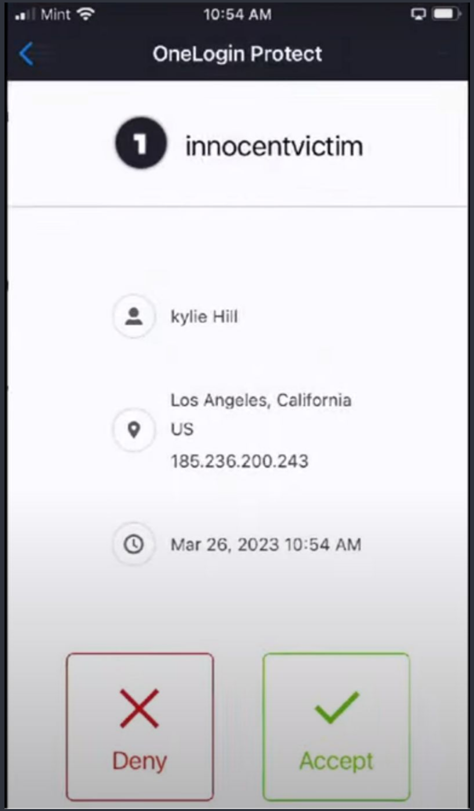
<how to be annoying>

herewego.txt

bombing.txt

MFA Bombing attacks

- ⭐ Compromised username and password
- ⭐ SPAM push notification prompts
- ⭐ User gets annoyed and accepts



innocentvictim

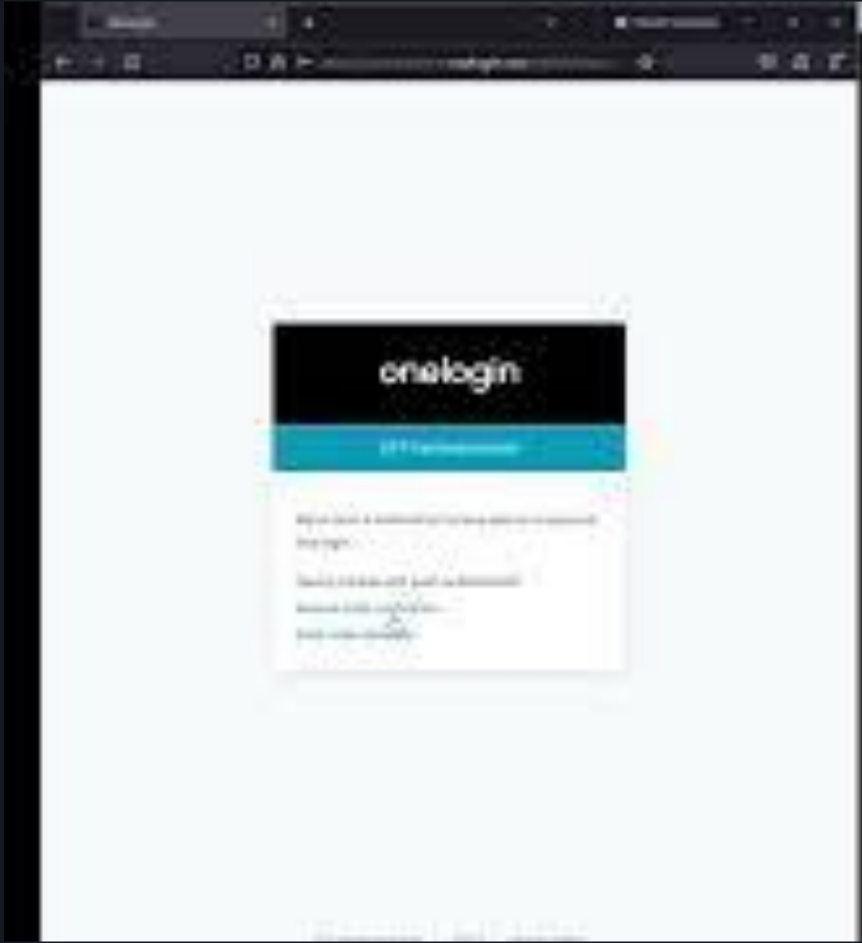
kylie Hill

Los Angeles, California
US
185.236.200.243

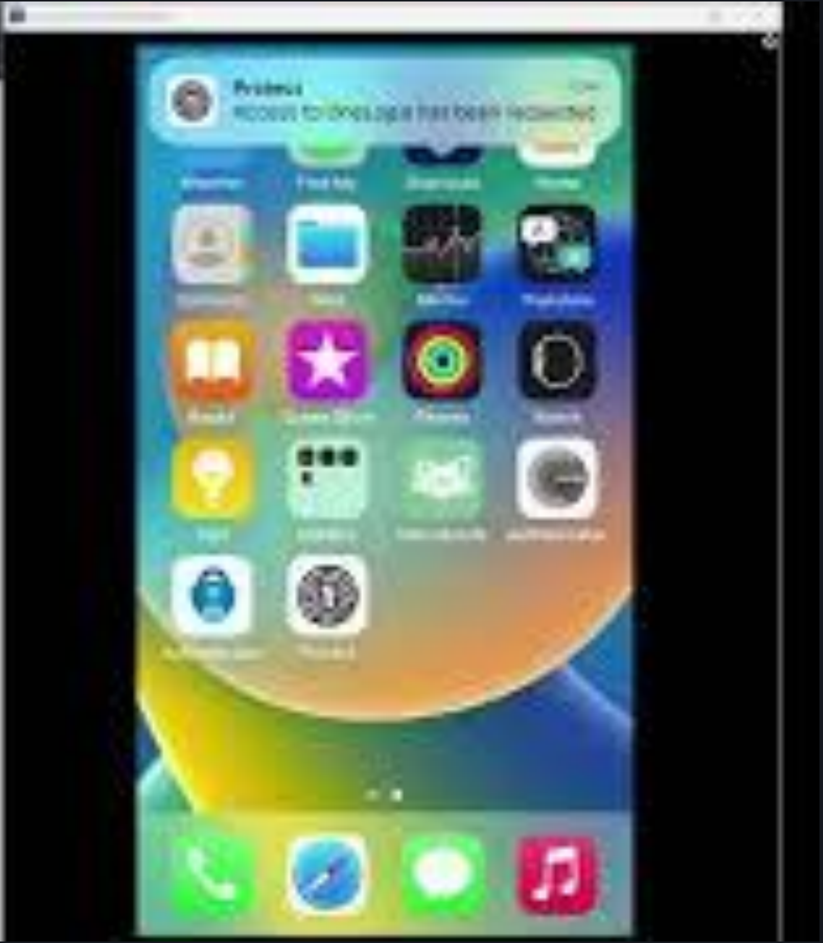
Mar 26, 2023 10:54 AM

kat1na-is-online

Attacker



Victim

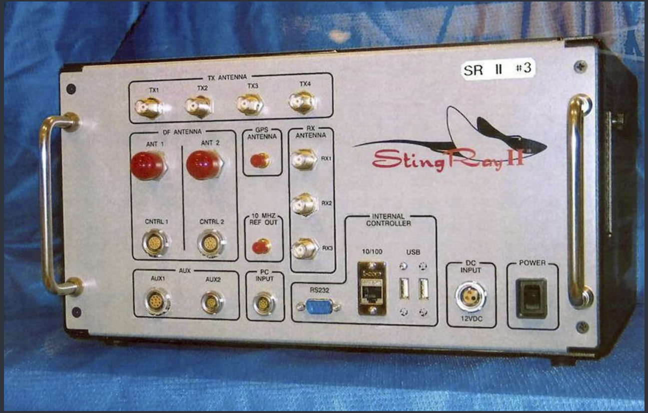


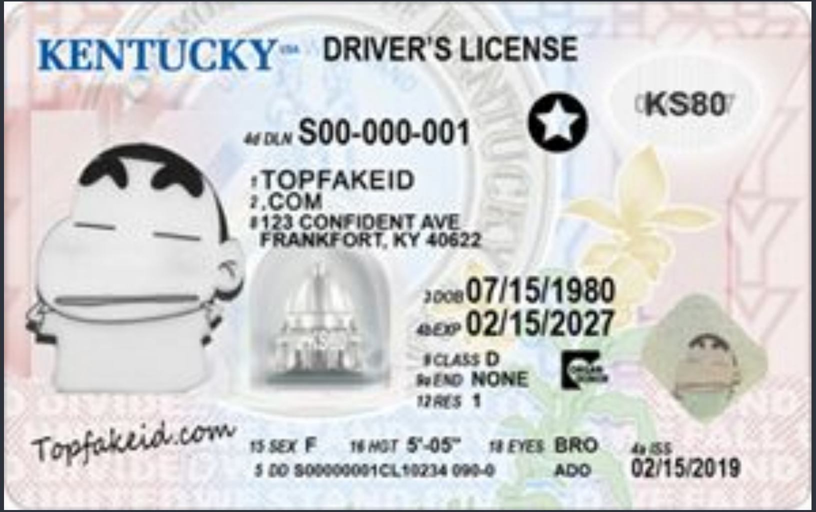
The wonderful insecurities of SMS

<why do we still use this?>

Bypassing SMS MFA

- ⭐ Eavesdropping – SS7 protocol
- ⭐ SIM Swapping – STORYTIME
- ⭐ SMS spoofing




KENTUCKY DRIVER'S LICENSE

KS80

4d DLN S00-000-001

1 TOPFAKEID
2 .COM
8 123 CONFIDENT AVE
FRANKFORT, KY 40622

3 DOB 07/15/1980
4b EXP 02/15/2027
9 CLASS D
9a END NONE
12 RES 1

Topfakeid.com

15 SEX F 16 HGT 5'-05" 18 EYES BRO
5 DD S00000001CL10234 090-0 ADO
4a ISS 02/15/2019

LET’S GO PHISHING!!!

<for $20 or less>

evil.txt phishing.txt

Recipe for evil

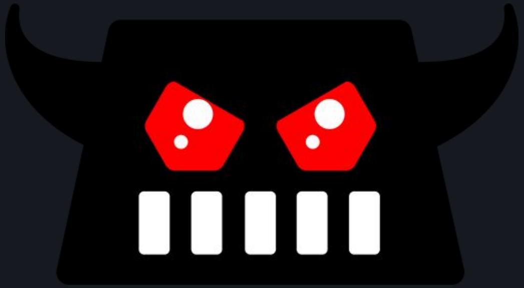
⭐ Convincing domain name (https://mlcrosoff.com)

⭐ Web server

⭐ Get user to click on link and authenticate

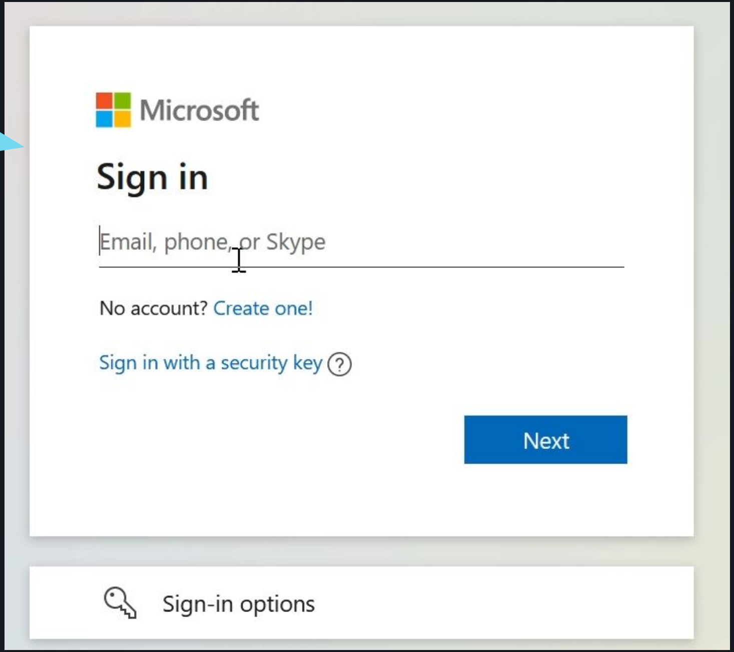
namecheap + aws

Fake web server + Eavesdrop + Relay HTTP Request



Victim POV

- ⭐ Legit-looking login page
- ⭐ Legit-looking URL
- ⭐ Padlock



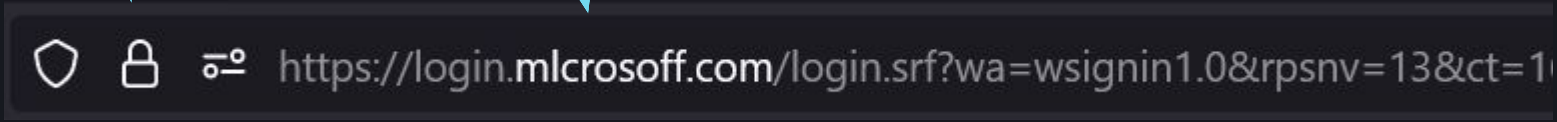
Microsoft

Sign in

Email, phone, or Skype

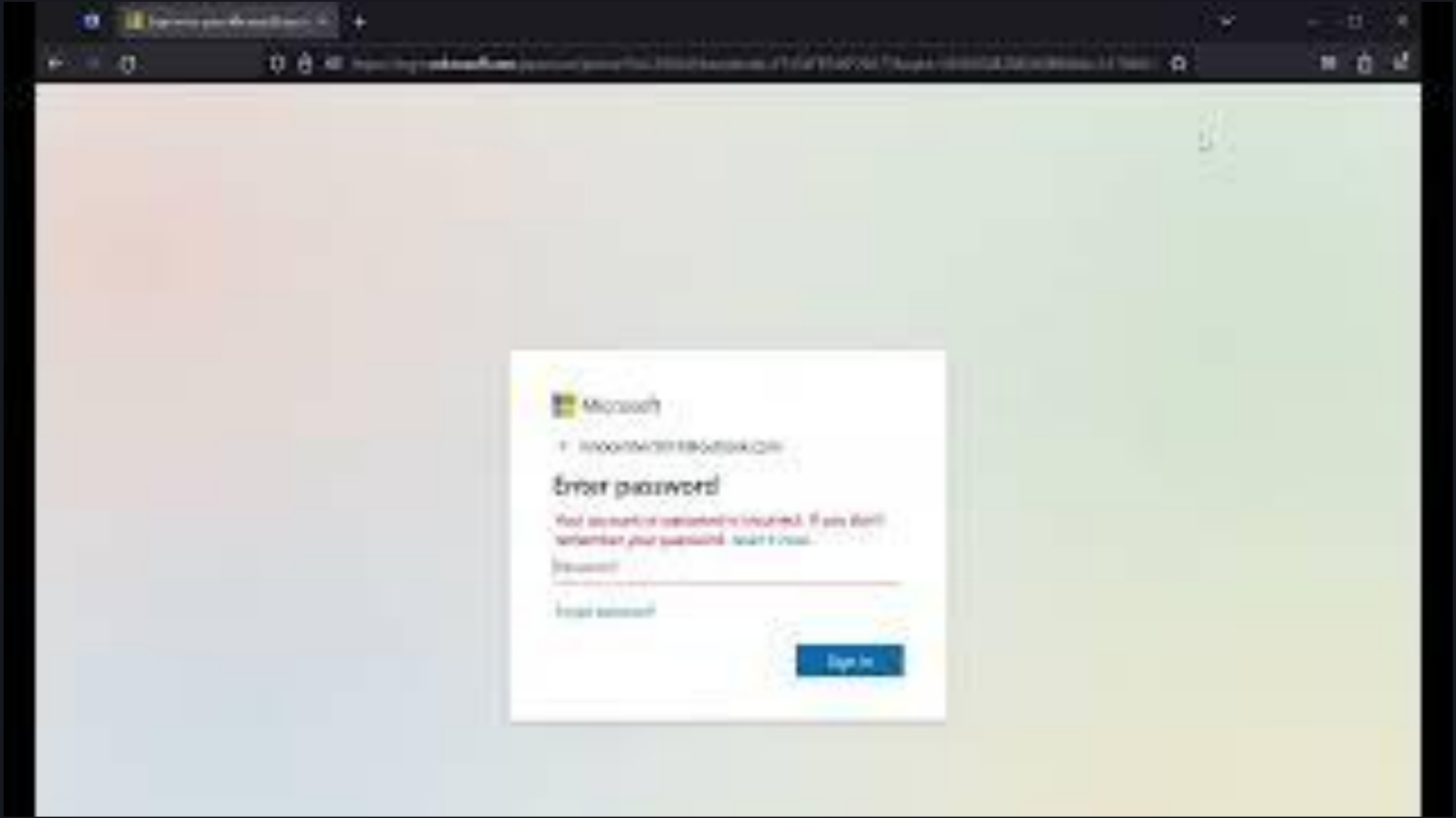
No account? Create one!

Sign in with a security key ?



https://login.mlcrosoff.com/login.srf?wa=wsignin1.0&rpsnv=13&ct=1

Victim POV



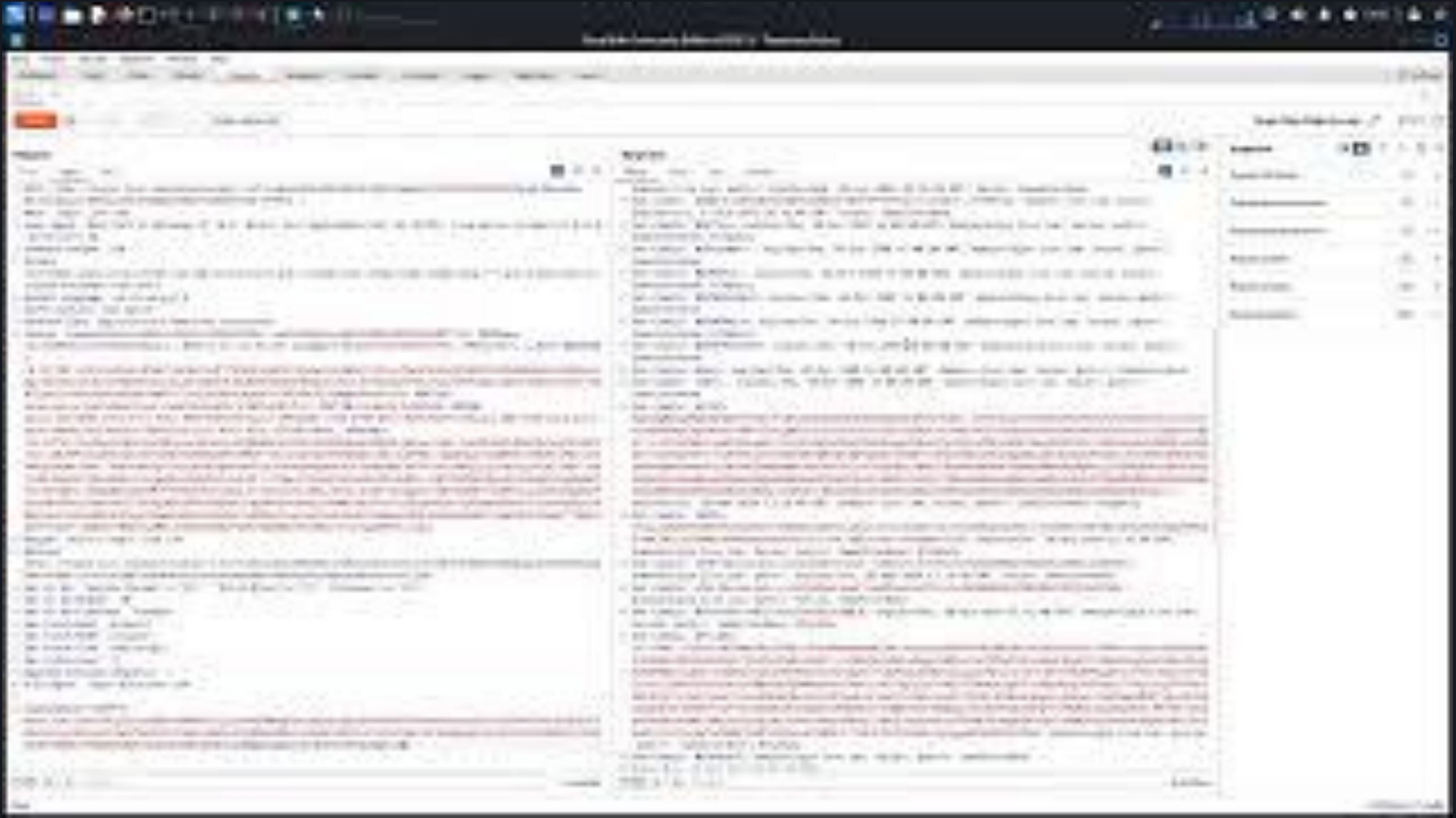
Microsoft

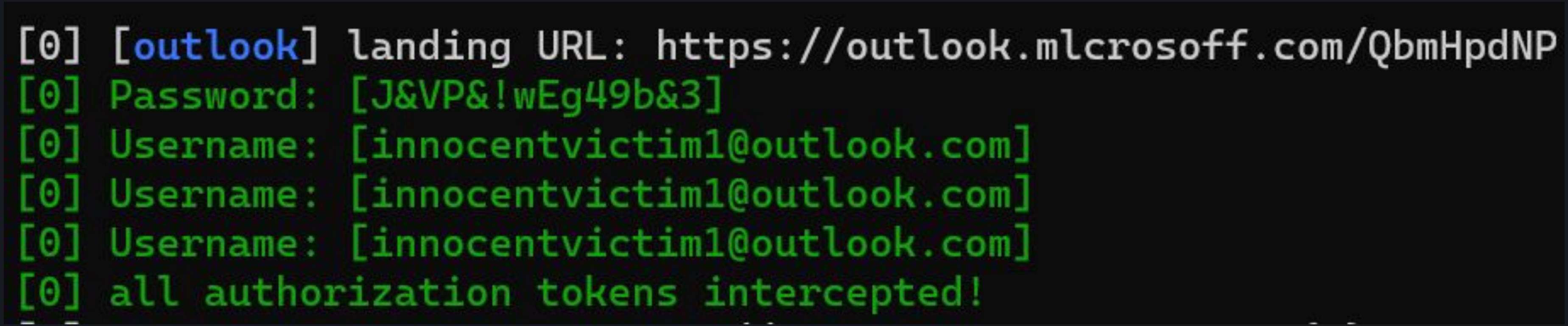
[illegible]OUTLOOK.COM

Enter password

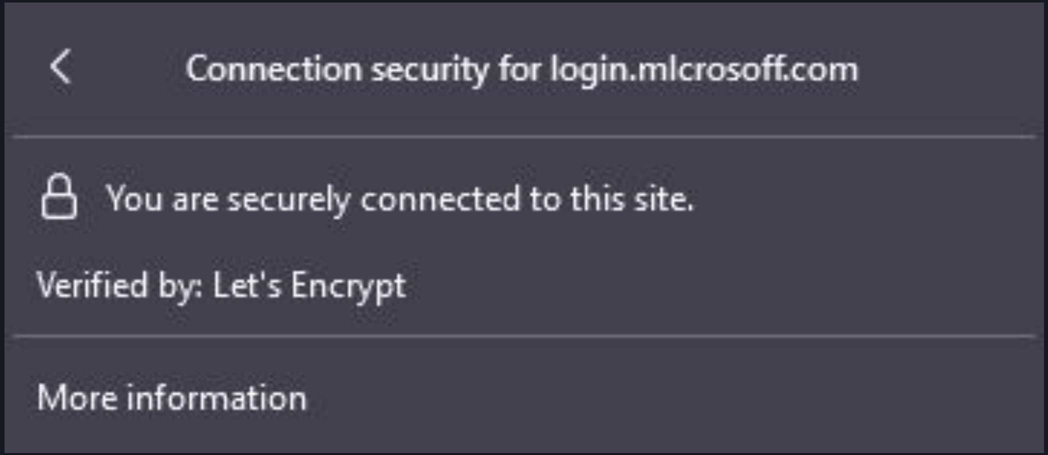
Your account or password is incorrect. If you don't remember your password, reset it now.

Attacker POV





```
[0] [outlook] landing URL: https://outlook.mlcrosoff.com/QbmHpdNP
[0] Password: [J&VP&!wEg49b&3]
[0] Username: [innocentvictim1@outlook.com]
[0] Username: [innocentvictim1@outlook.com]
[0] Username: [innocentvictim1@outlook.com]
[0] all authorization tokens intercepted!
```



Connection security for login.mlcrosoff.com

You are securely connected to this site.

Verified by: Let's Encrypt

More information

An alternative?

+

mitigations.txt

thereishope.txt

Mitigations for MFA attacks

<it’s not hopeless>

users.txt   mitigations.txt

Mitigations

⭐ USER EDUCATION!!!!!

⭐ Avoid SMS where possible

⭐ Security keys in high-risk scenarios

⭐ Rate limiting

⭐ Block suspicious activity

users.txt credits.txt

Credit where credit is due

⭐ “Hacking Multifactor Authentication” by Roger A. Grimes

⭐ Slidesgo.com for slides design

⭐ For more resources visit: https://kat1na.github.io/

questions.txt coolcool.txt

Question Time!