After The Action Movie Ends



Bryan Seely

Cybersecurity Expert | Ethical Hacker

Former U.S. Marine

Professional Keynote Speaker

Cofounder of Blackhat conference in Riyadh KSA

Host of the @BlackhatMEA Podcast *launched Q2 2022*

Advisor to the Late John McAfee

How I Got Here

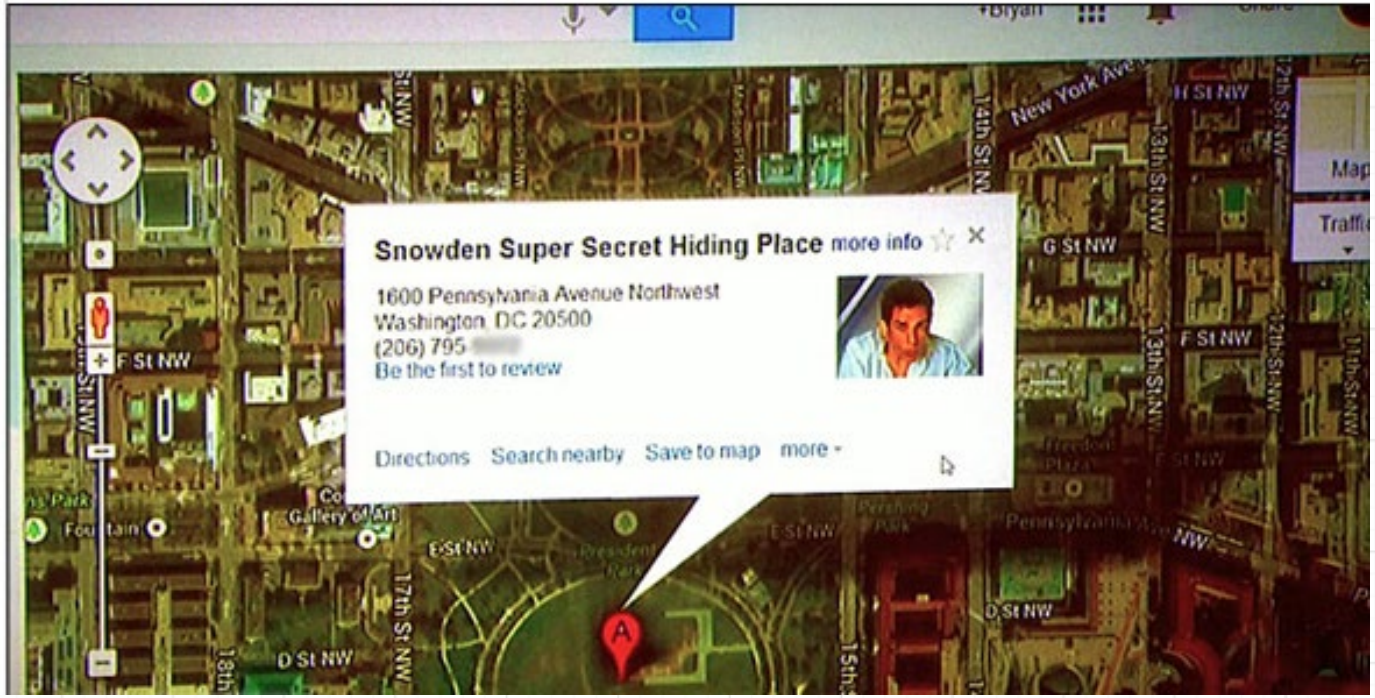


KOMOnews.com

Insider: Google 'map jacking' is rampant, a threat to public safety

By Matt Markovich | Published: Feb 25, 2014 at 10:48 PM PDT | Last Updated: Feb 26, 2014 at 6:33 PM PDT

Recommend 192 | g+1 21 | Tweet 39 | Print | Email



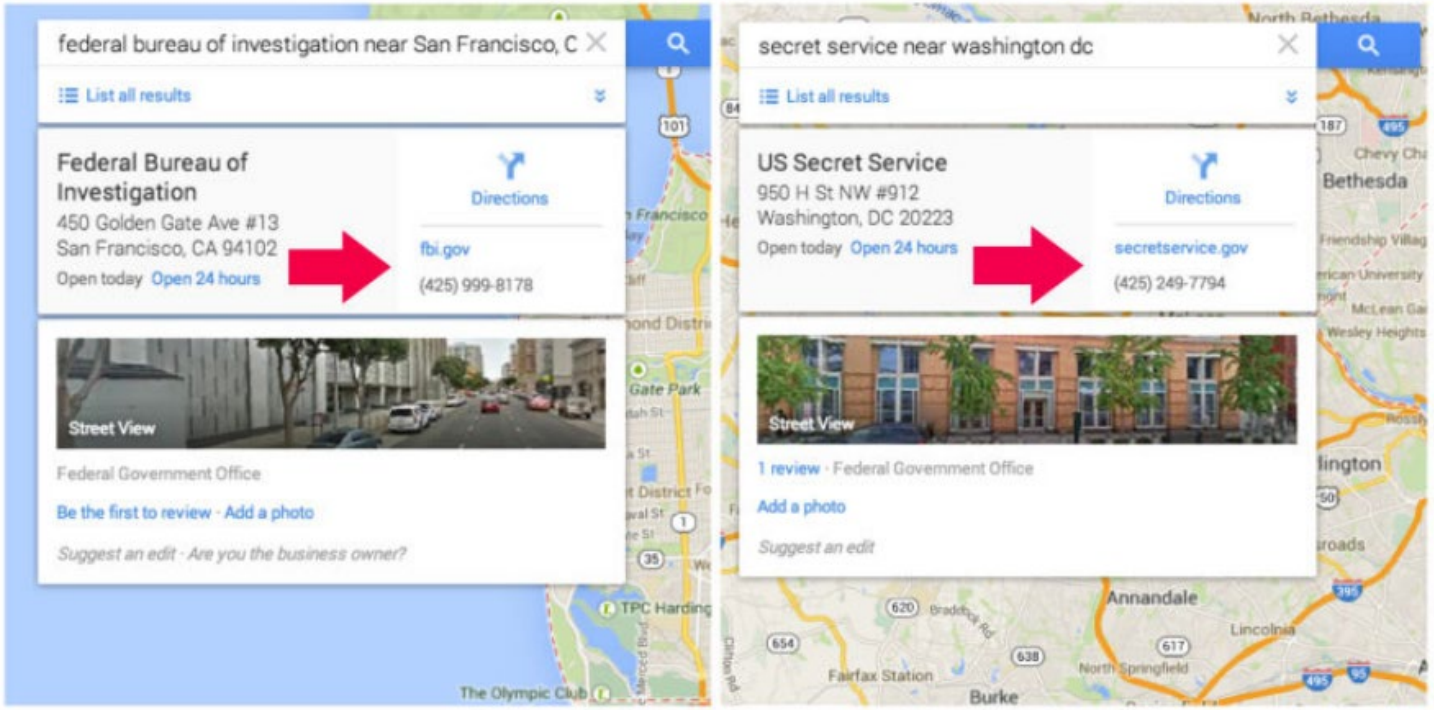
VALLEYWAG

How a Hacker Intercepted FBI and Secret Service Calls With Google Maps

Nitasha Tiku

02/27/14 06:00PM Filed to: GOOGLE

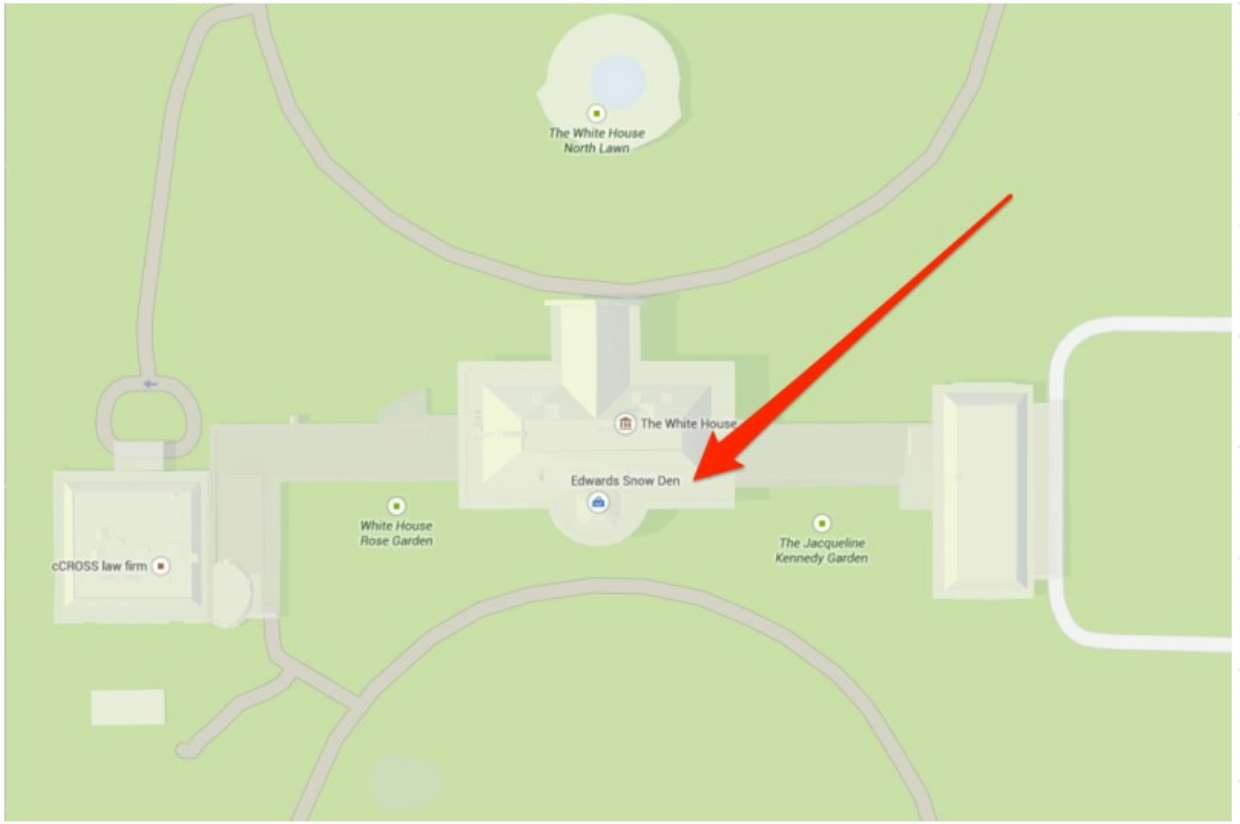
195.44K



Google Maps Shows Edward Snowden In The White House

A sign that the whistleblower and President Obama are talking? No. Ironically, it's likely due to a security failure with how Google monitors local listings.

Danny Sullivan on April 13, 2015 at 5:33 pm | Reading time: 2 minutes



John McAfee's firm hires ethical hacker Bryan Seely to new Hacker Advisory Board

Published: June 13, 2016 at 10:58 a.m. ET



Scientology Seeks Captive Converts Via Google Maps, Drug Rehab Centers

June 27, 2016 79 Comments

Fake online reviews generated by unscrupulous marketers blanket the Internet these days.

Mailing List

What is OSINT?


OSINT SOURCES
with EXAMPLES
1
News articles/ Media reports
(nytimes.com)
2
Published research
(scholar.google.com)
3
Books and similar references
(archiveofourown.org)
4
Social media posts
(twitter.com)
5
Census data
(census.gov)
6
Phone directories
(whitepages.com)
7
Court filings
(pacer.uscourts.gov)
8
Arrest records
(uscourts.gov)
9
Public trading data
(sec.gov)
10
Public surveys
(statista.com)
11
Contextual location-related data
(ipify.org)
12
Breach/ Compromise disclosure information
(privacyrights.org)
13
Publicly shared IoCs
(otx.alienvault.com)
14
Certification/ Domain registration data
(lookup.icann.org)
15
Application/ System vulnerability data
(nvd.nist.gov)

OSINT SOURCES

with EXAMPLES




1
News articles/ Media reports
(nytimes.com)
2
Published research
(scholar.google.com)
3
Books and similar references
(archiveofourown.org)
4
Social media posts
(twitter.com)
5
Census data
(census.gov)
6
Phone directories
(whitepages.com)
7
Court filings
(pacer.uscourts.gov)
8
Arrest records
(uscourts.gov)
15
Application/ System vulnerability data
(nvd.nist.gov)
OSINT SOURCES
with EXAMPLES

OSINT Sources

1. News Media
2. Published Research
3. Books etc
4. Social Media
5. Census Data
6. Phone Directories
7. Court Fillings
8. Arrest Records

OSINT Sources

9 Public Trading Information

10 Public Surveys

11 Contextual Location Related Data

12 Breach Data

13 Public ioCs

14 Certification / Domain Registrations

15 Vulnerability Data

Why is it Important?

Russian soldier gave away his position with geotagged social media posts

Cell phones and combat zones don't mix.

BY JEFF SCHOGOL | PUBLISHED JAN 3, 2023 12:34 PM EST

NEWS



Support the Guardian
Fearless, independent, reader-funded
Support us

GPS

This article is more than 5 years old

Fitness tracking app Strava gives away location of secret US army bases

Data about exercise routes shared online by soldiers can be used to pinpoint overseas facilities

Latest: Strava suggests military users 'opt out' of heatmap as row deepens

Alex Hern
@alexhern
Sun 28 Jan 2018 16.51 EST



A military base in Helmand Province, Afghanistan with route taken by joggers highlighted by

Social Media OSINT

Social Media & Forums

1. Facebook
2. Instagram
3. Linkedin
4. Twitter
5. Snapchat
6. Youtube
7. Reddit
8. Dating Apps

Investigations: *Don't* Do This

1. Use your own device
2. Reusing Accounts & Passwords
3. Mix devices or accounts
4. Privacy Overkill

Use of AI in OSINT

Who is She?

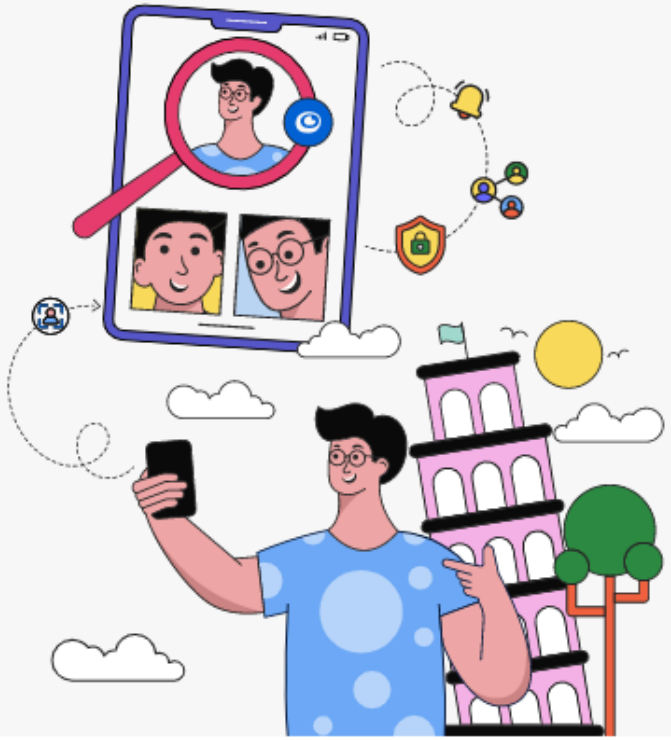


Face Search Engine
Reverse Image Search

UPLOAD PHOTO AND FIND OUT WHERE IMAGES ARE PUBLISHED

Upload a photo

Or you can take a photo with the device's camera. Don't worry, we will not store it!



„It's quick, it's accurate, it's facial recognition on steroids"

BBC

„PimEyes, a search engine that's handy for reverse image searching and facial recognition."

VICE

„The facial recognition site PimEyes is one of the most capable face-searching tools on the planet."

The Washington Post

„For $29.99 a month PimEyes offers a potentially dangerous superpower from the world of science fiction"

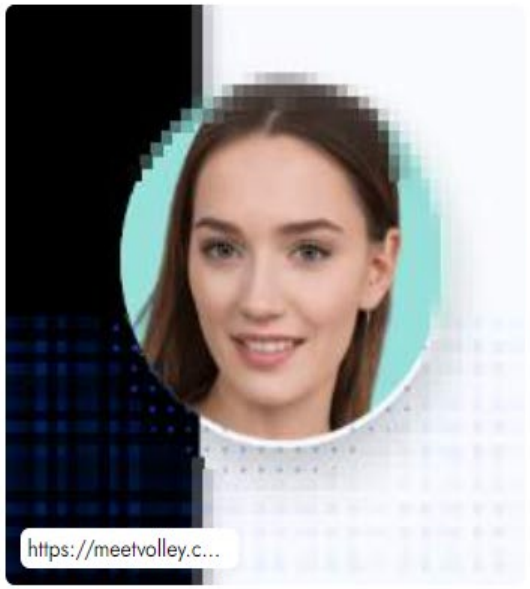
New York Times

PimEyes

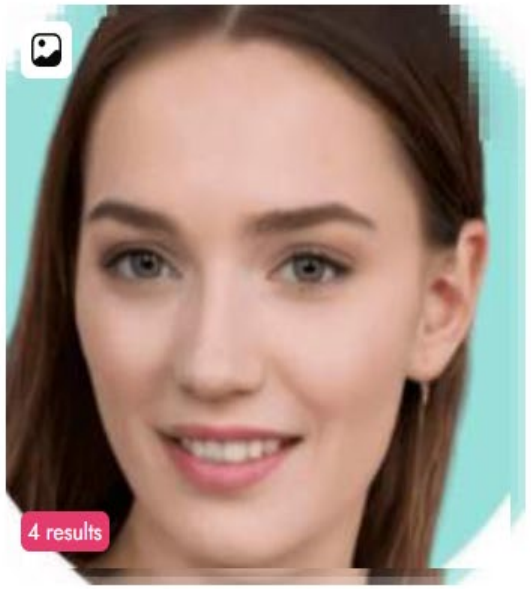
Search Pricing Blog News Opt-Out FAQ

Premium Search
About 249 results in 3.16s

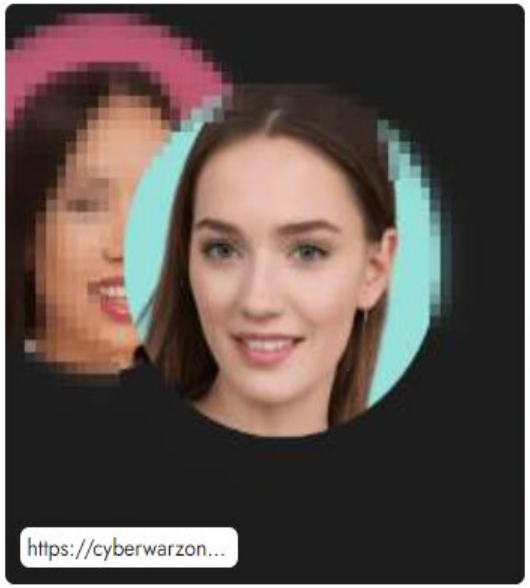
New Search

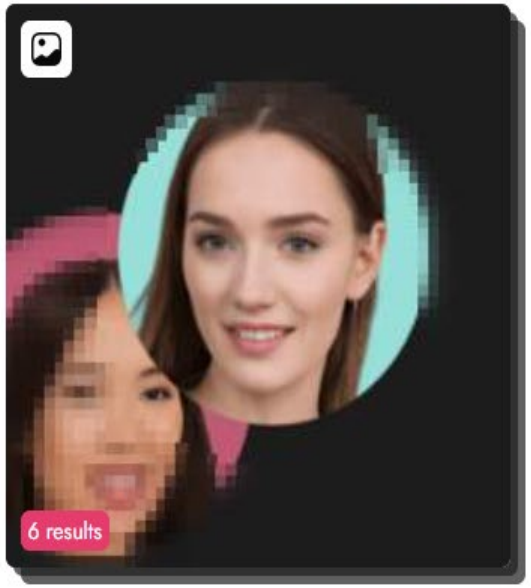




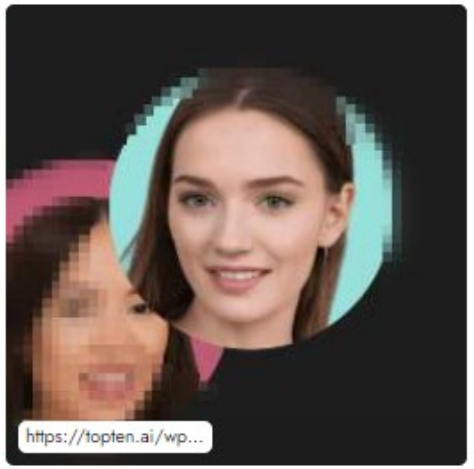


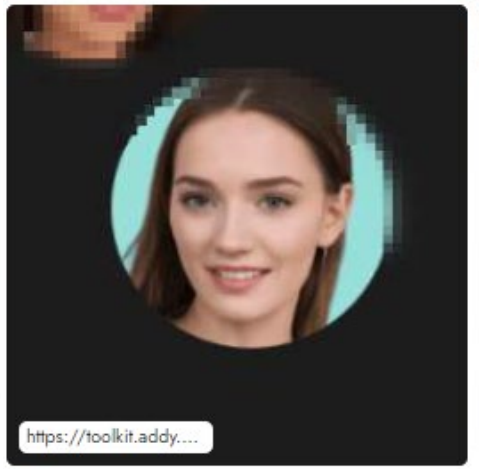


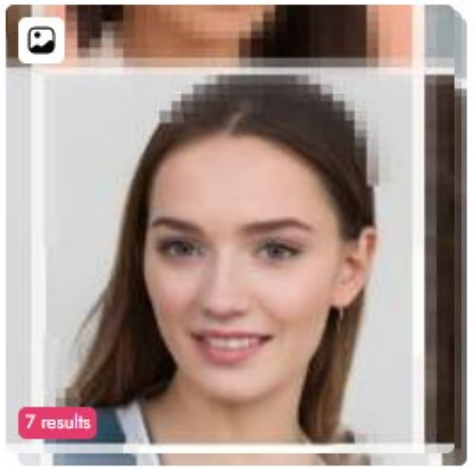


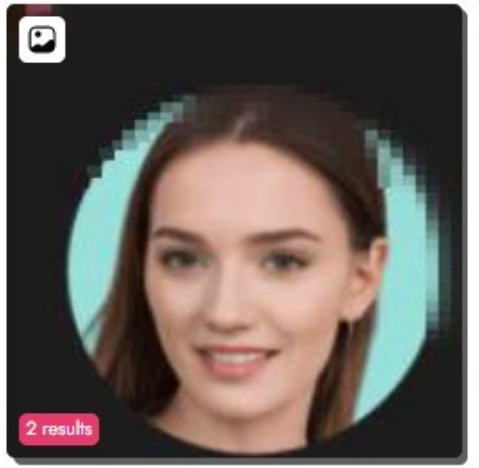


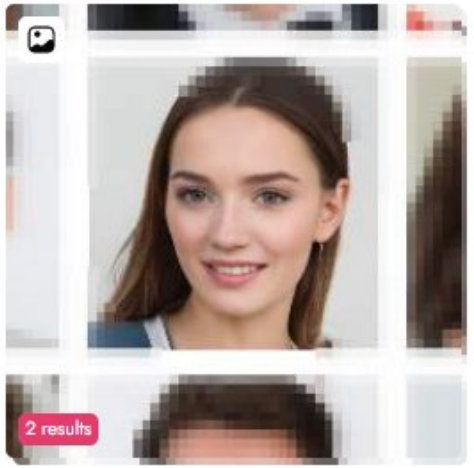




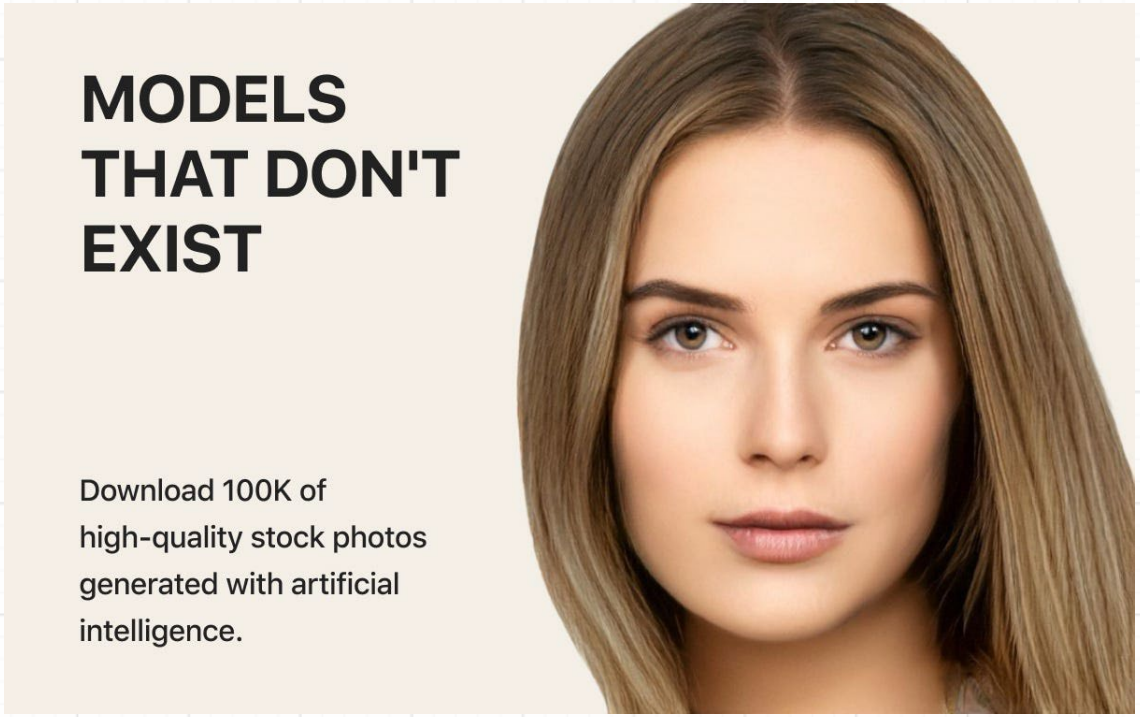








AI Generated Images





Story Time

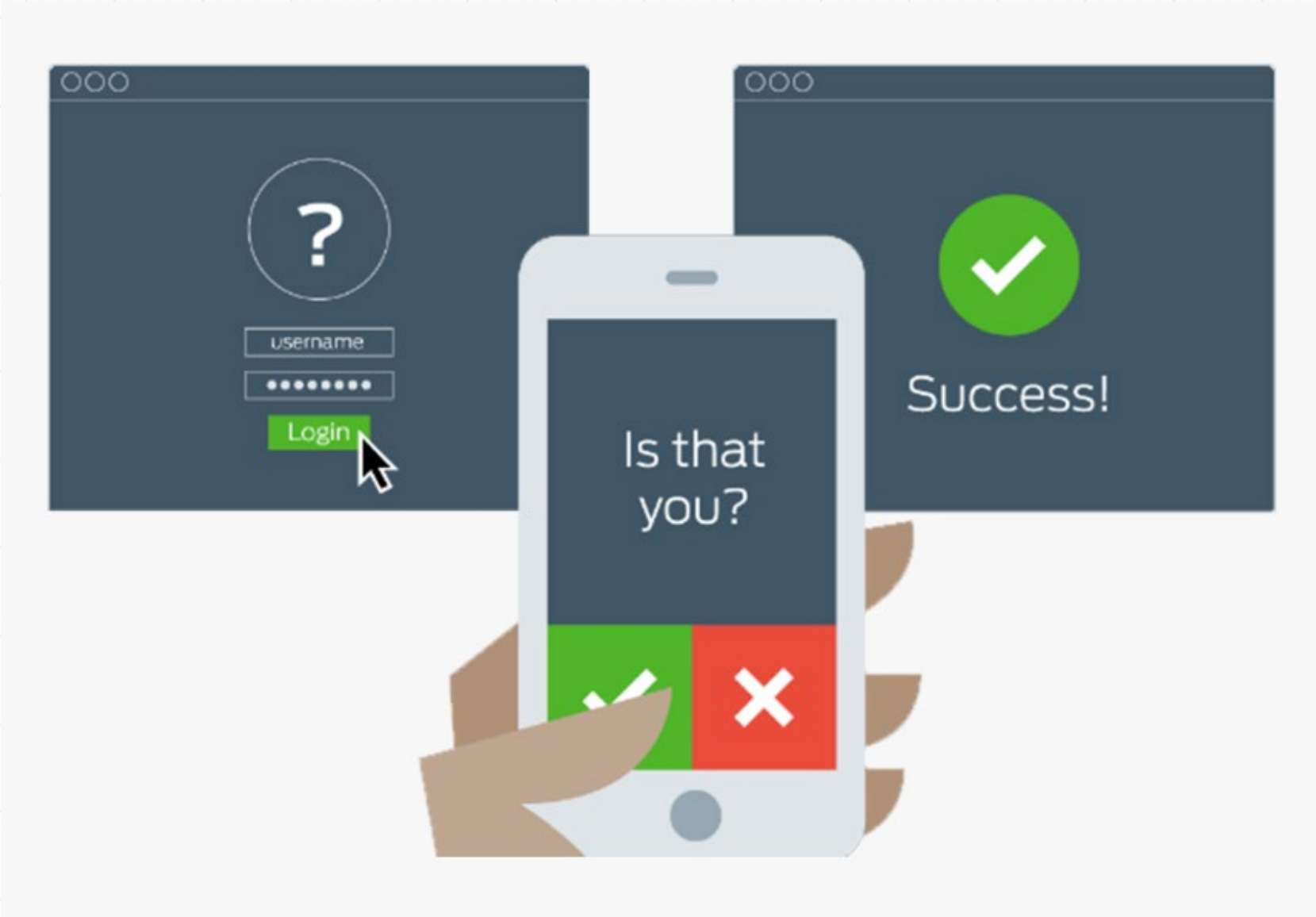

Google

OSINT Links

1. https://inteltechniques.com/tools/
2. https://www.varonis.com/blog/best-sources-of-business-data-in-2019/
3. https://github.com/infomaven/personal-osint/blob/master/resources.md
4. www.reddit.com/r/osint

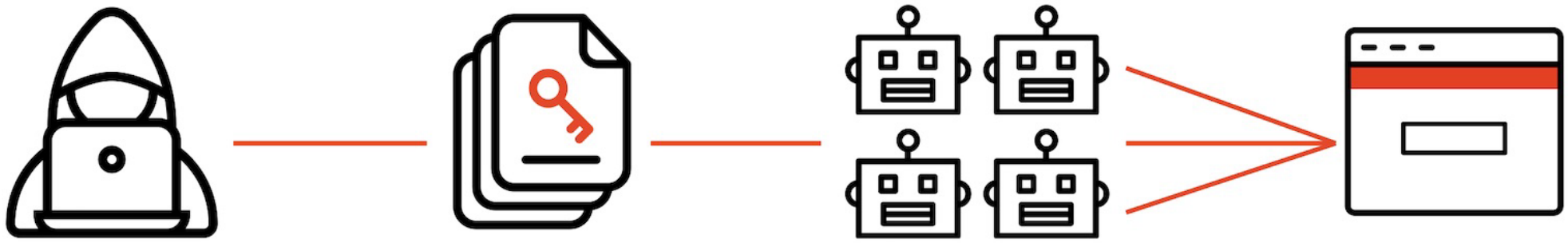
LAPSUS$

Advanced Hacking Group Profile


?
username
Login
Is that you?
Success!



Anatomy of a credential stuffing attack



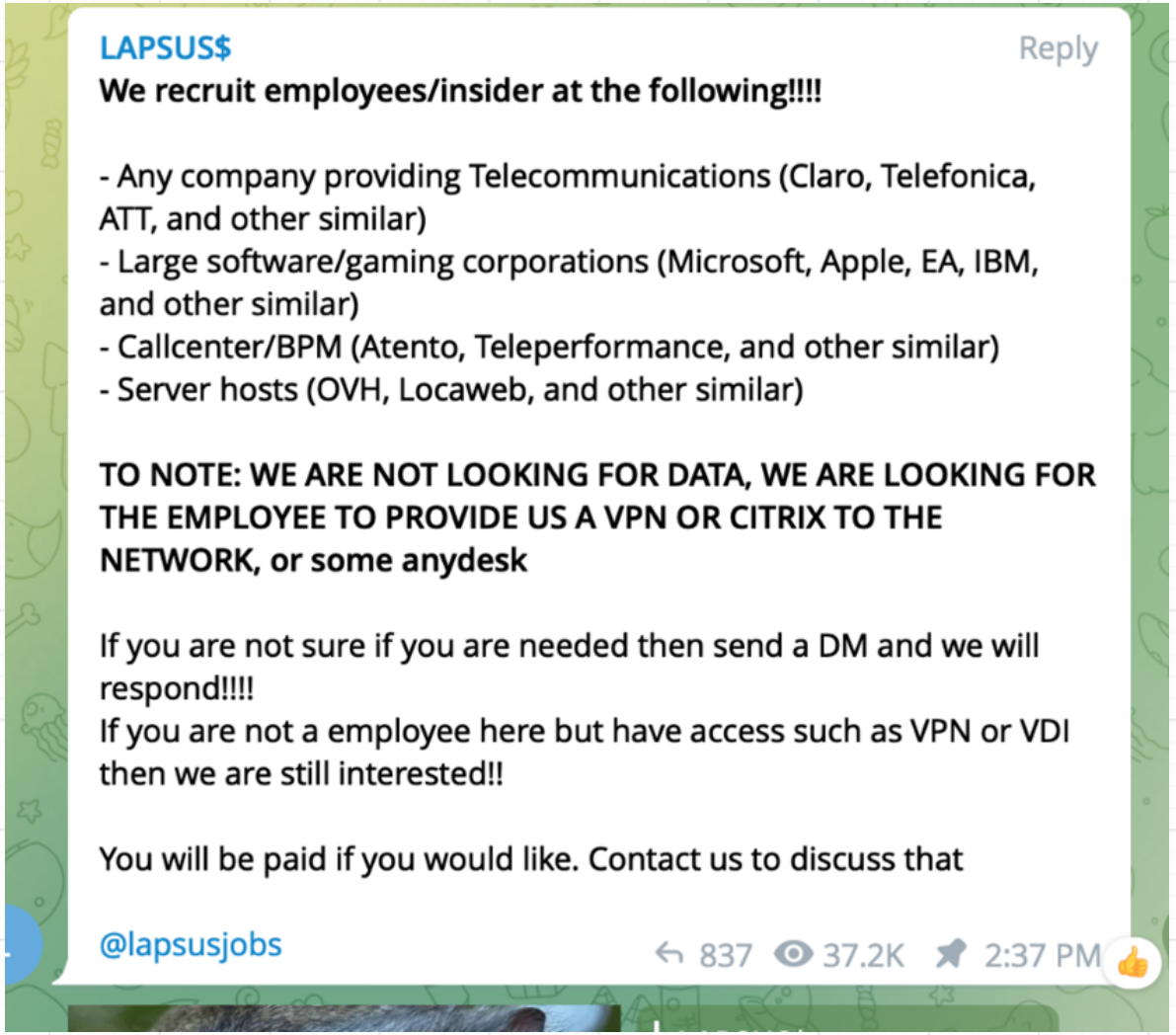
Attacker

Compromised credentials

Botnet

Victim site


REDLINE
@REDLINESUPPORTS_BOT
Powered by © Redline 2021 | Official channel | Officaial chat
12:44
RedLine[Month] #1
RedLine[Week] #2
RedLine[LifeTime] #3
Add balance
MyProfile
Support


LAPSUS$
Reply
We recruit employees/insider at the following!!!!
- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)
TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk
If you are not sure if you are needed then send a DM and we will respond!!!!
If you are not a employee here but have access such as VPN or VDI then we are still interested!!
You will be paid if you would like. Contact us to discuss that
@lapsusjobs
837
37.2K
2:37 PM

Social Engineering Tactics to Watch For

Knowing the red flags can help you avoid becoming a victim.



Your ‘friend’ sends you a strange message.



Your emotions are heightened.



The request is urgent.



The offer feels too good to be true.



You’re receiving help you didn’t ask for.



The sender can’t prove their identity.

Solutions

Security Controls & Mitigations

Action Items

01 Require MFA for all users from all locations

02 Use FIDO Tokens / Yubikey

03 Never use SMS / text messages when possible

04 Have Backup Super Admin Accounts stored in firesafe

05 Never store work credentials in browser

06 Applocker / application whitelisting

07 Advanced Monitoring Solutions

Action Items

08 Automated Alerts / SIEM

09 Immutable Backups

10 MFA Service with number matching vs allow/deny

11 Company password manager / proper training

12 Use dual credentials: User vs Admin.

13 Disable local admin or use LAPS on windows

14 Have a dedicated Admin Workstation or VM

Action Items

15 Minimum password length 15 or more

16 Clean your room

17 Secure DNS Services

18 Someone needs to be in charge of patching / updates.

19 Learn how to use all available security options

20 Audit C-level personal data exposure / google yourself.

21 Need help? Ask. Just generalize and don’t leave clues.

Helpful Links

Some useful tools to keep you safe

Check if your data has been leaked
https://cybernews.com/personal-data-leak-check/

DeHashed is the largest & fastest data breach search engine. You can search for IP address, email, username, name, phone, VIN, address, and more! We have true wild card, dork usage, and we offer a real search engine experience! It's also free!
https://www.dehashed.com/

Have I been pwned? Website repository that checks what sites your email address was used on were compromised
https://haveibeenpwned.com/

Privacy.com Make a unique debit card number for every single purchase online with just 1 click. Never worry again about credit card breaches, shady merchants, or sneaky subscription billing.
https://privacy.com/

MySudo Send private messages, manage multiple phone numbers and email addresses, and create custom personal identities that last as long as you need them.
https://mysudo.com/

ProtonVPN High-speed Swiss VPN that safeguards your privacy.
https://alternativeto.net/outgoing/software/protonvpn

KrebsOnSecurity.com – One of the best cybersecurity news sites out there.

After The Action Movie Ends



Behind The Scenes

Lynnwood father, FBI search for missing teen believed to be caught up in sex trafficking

by Suzanne Phan | Friday, January 13th 2017



Bryan Seely believes he found his missing 17-year-old daughter on an escort ad on Backpage.com. (Photo: KOMO News)

LYNNWOOD, Wash. - A Lynnwood dad, who also happens to be a cyber security expert, is desperate to find his missing child. He believes he found his teenage daughter in an escort ad on Backpage.com. But, his search has gotten more complicated because of the website's shutdown.

"One day you will tell your story of how you overcame what you went through and it will be someone else's survival guide."

-Brene Brown

LAWRENCE lady boss PROJECT

Mental Health

Forbes – *of 1000 security professionals surveyed - June 2022*

1. 50.8% take medications for mental health
2. 51% of infosec professionals self-identified as burnt out
3. 65% were considering leaving the industry entirely

Top 10 Common Life Stressors

1. Death of Spouse
2. Divorce
3. Marital Separation
4. Incarceration
5. Death of Family Member
6. Major personal Injury or Illness
7. Marriage
8. Being fired or laid off from work
9. Marital reconciliation
10. Retirement

Therapy

1. Red Team: Identifying your issues safely
2. Blue Team: Fixing what you found
3. Easily a top 3 “saved my life”activity

Self Care

1. Exercise Daily
2. Learn How to Eat Healthy
3. The Importance of Sleep

Professional Help

1. Treating your specific issues
2. Taking medications consistently
3. Leave emotion / judgement / shame out of it.

Additional Items of Note

1. Join a group / community ; a discord / slack channel / and participate.
2. Find a way to be of service to others.
3. Find a way to laugh every day. I prefer standup comedians.
4. Don’t treat depression and loneliness with isolation.
5. If you are white knuckling it through life / coping, that’s not a good sign.
6. Call a friend everyday.
7. Your ego isn’t your friend. Be humble or humility will be brought to you.

Ideas For People & Podcasts to Follow

1. Brene Brown – *Tedx, Podcast, Books. Pretty much anything she does.*
2. Huberman Podcast
3. RichRoll Podcast
4. The Diary of A CEO
5. Taylor Tomlinson on Netflix / Daniel Sloss on Netflix or Amazon Prime.
6. Your ego isn’t your friend. Be humble or humility will be brought to you.

Most Importantly
You Are Not Alone.

Questions?

Feel free to ask me anything now or use the info below later since asking questions in front of a crowd can be daunting.

Bryan Seely

Email: bryan@bryanseely.com

Cell: 425 835 3397

Linkedin: bryanthemapsguy

Twitter: bryanthemapsguy

Website: www.bryanseely.com