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....

Charlotte ISSA
Information Systems Security Association

KnowBe4

Neural Networks & Criminal Networks

From Reactive to Predictive, Leveraging AI to stay Ahead of Intelligent Ransomware

James R. McQuiggan, SACP, CISSP
Security Awareness Advocate

Ransomware is the outcome of unauthorized access

When It Happens, You Need Response Plans & Backups

Ransomware has moved past brute force. It’s now using AI.
We need to shift from waiting for alarms to predicting the storm.

James R. McQuiggan
CISSP, SACP, OSC

Security Awareness Advocate, KnowBe4 Inc.

Professor, Cyber Threat Intelligence, Full Sail

ISC2 North American Advisory Council

Past President, ISC2 Central Florida Chapter

Cyber Security Awareness Lead, Siemens

Product Security Officer, Siemens Gamesa

CISSP Certified Information Systems Security Professional
ISC2 Certification

H LAYER CREDENTIALING
CERTIFIED
Security Awareness and Culture Professional (SACP)

OSC
OPEN-SOURCE
CERTIFIED

About KnowBe4

We help over 70,000 organizations build a strong security culture to manage the ongoing problem of social engineering and human risk.

Top 100 Global Software Companies BEST SOFTWARE AWARDS 2024

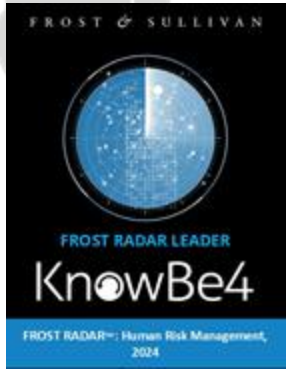
Trusted by 47 of the world's top 50 cybersecurity companies, and the largest human risk management platform

Gartner Magic Quadrant Leader

Global Sales, Courseware Development, Customer Success, and Technical Support teams worldwide

TrustRadius Top Rated 2024

CEO, leadership and Knowsters are industry veterans in cybersecurity



Office in the USA, UK, Canada, France, Netherlands, India, Germany, South Africa, United Arab Emirates, Singapore, Japan, Australia, and Brazil

Our mission

To help organizations manage the ongoing problem of social engineering

We do this by

Empowering your workforce to make smarter security decisions every day.

Outcomes for the next 267 minutes… (and 579 slides)

How do we prevent it from happening?

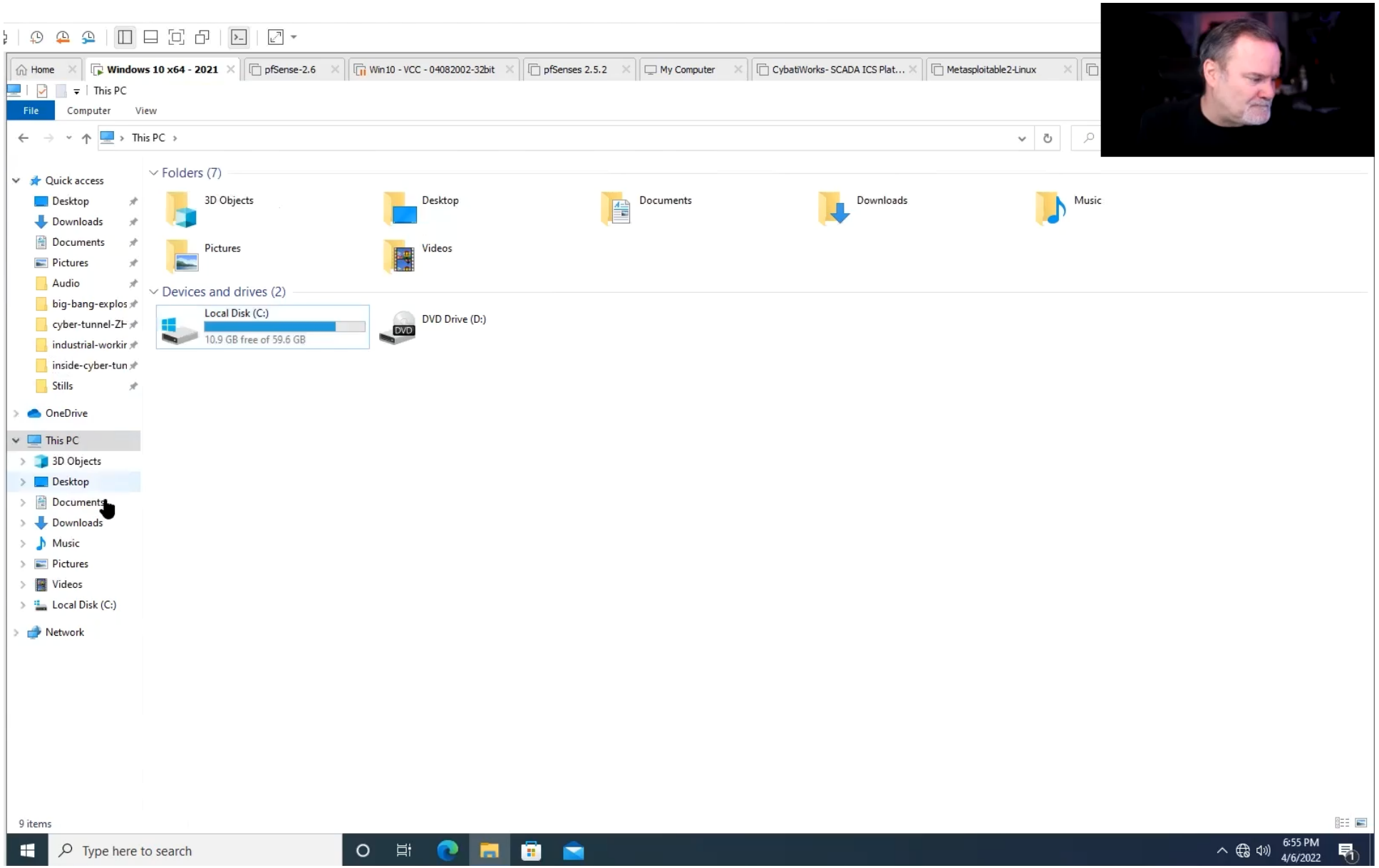
Ransomware is the outcome, how is AI helping the attack?

How do we prepare and reduce the human risk?

KnowBe4

Ransomware Right Now

RANSOMWARE ATTACK!



Common Attack Vectors

- Phishing Emails: Primary initial access vector with increasingly sophisticated social engineering.
- Supply Chain Attacks: Compromising trusted third-party software to distribute ransomware.
- RDP Exploitation: Targeting exposed Remote Desktop Protocol services with weak credentials.
- Unpatched Vulnerabilities: Exploiting known security flaws in software and systems.

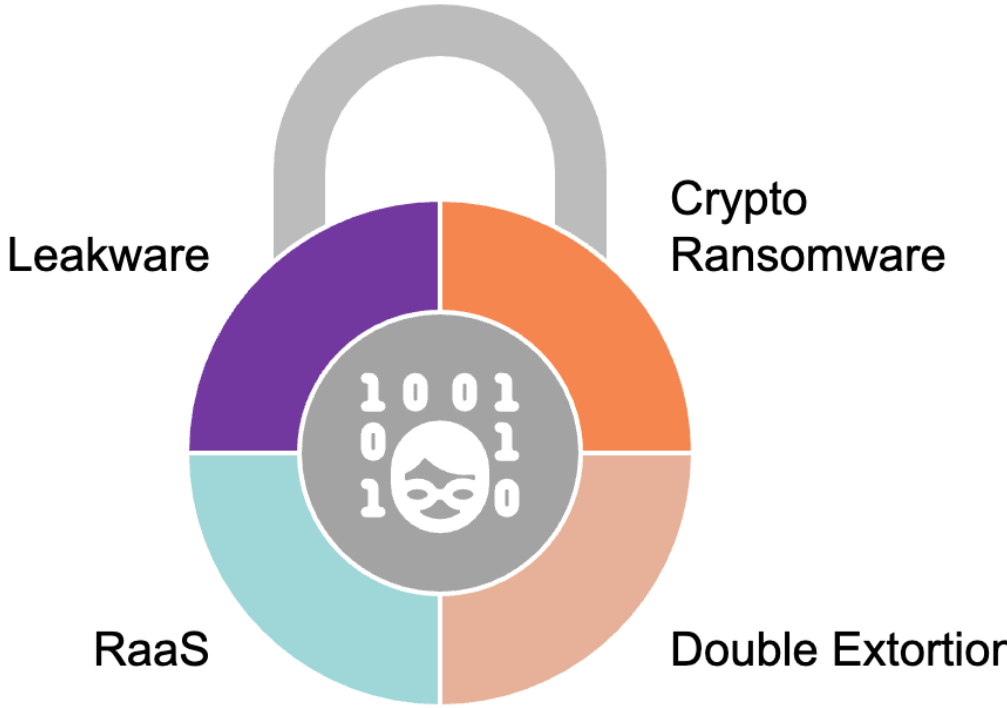
Ransomware Styles

Crypto Ransomware
- Encrypts files and demands cryptocurrency for decryption.
- Often undetected until access is lost.

Double Extortion Ransomware
- Encrypts and exfiltrates data, threatening public release.
- Adds legal and reputational risk beyond operational disruption.
- Protections: monitoring for both encryption and data leaks.

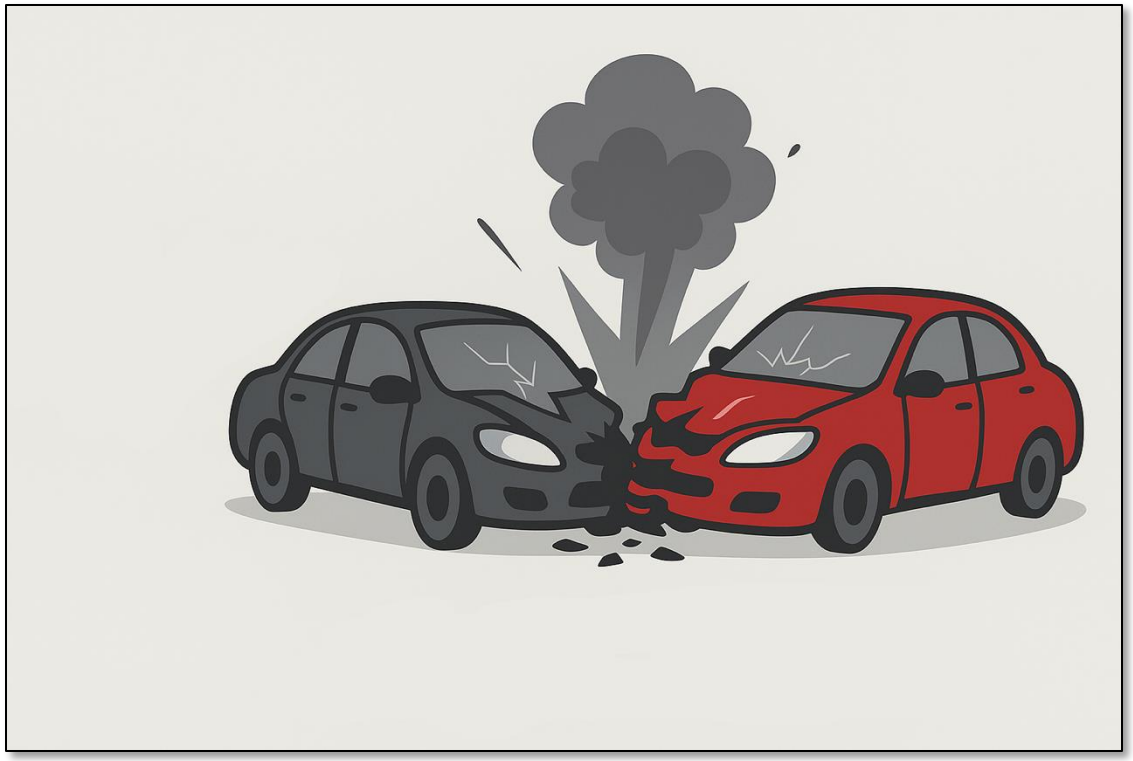
Ransomware-as-a-Service (RaaS)
- Enables non-experts to launch ransomware using purchased kits.
- Copies legitimate software operations.
- Protections: zero-trust, threat intel, and security culture / awareness.

Leakware
- Steals sensitive data and threatens to leak it if ransom isn't paid.
- High risk for organizations handling private or regulated data.
- Protections: encryption, DLP tools, and regular access audits.



The Aftermath of Attacks

- Marks & Spencer (M&S) - A loss exceeding £650 million in market value.
- Change Healthcare - Revenue losses up to $100 million per day
- British Library – Recovery cost ~£6–7 million (about 40% of their financial reserves)



Current Ransomware Impact

59% Organizations Impacted

>$1b Payments Exceeded

32% Access via Unpatched Known Vulnerability

96% Delete Backups before Encryption

70% Resulted in Data Encryption

x2 Average Recovery Costs ($4.5m)

Top Ransomware Groups

1. LockBit 3.0
2. BlackCat/ALPHV
3. Black Basta
4. Akira
5. Hunters International

Evaluate Your Responses

- Restore from a recent backup
- Decrypt your files using a third party decrypter
- Do nothing (lose your data)
- Negotiate / Pay the ransom

FINALLY...

Rid Your Computer of All Ransomware & Malware

- Wipe the Machine & Reload
- Possible remaining malware artifacts undetectable to EDR
- Consider the risks of unknown remnants for future attack
- Organizations have been known to be hit twice!

KnowBe4

AI & Ransomware

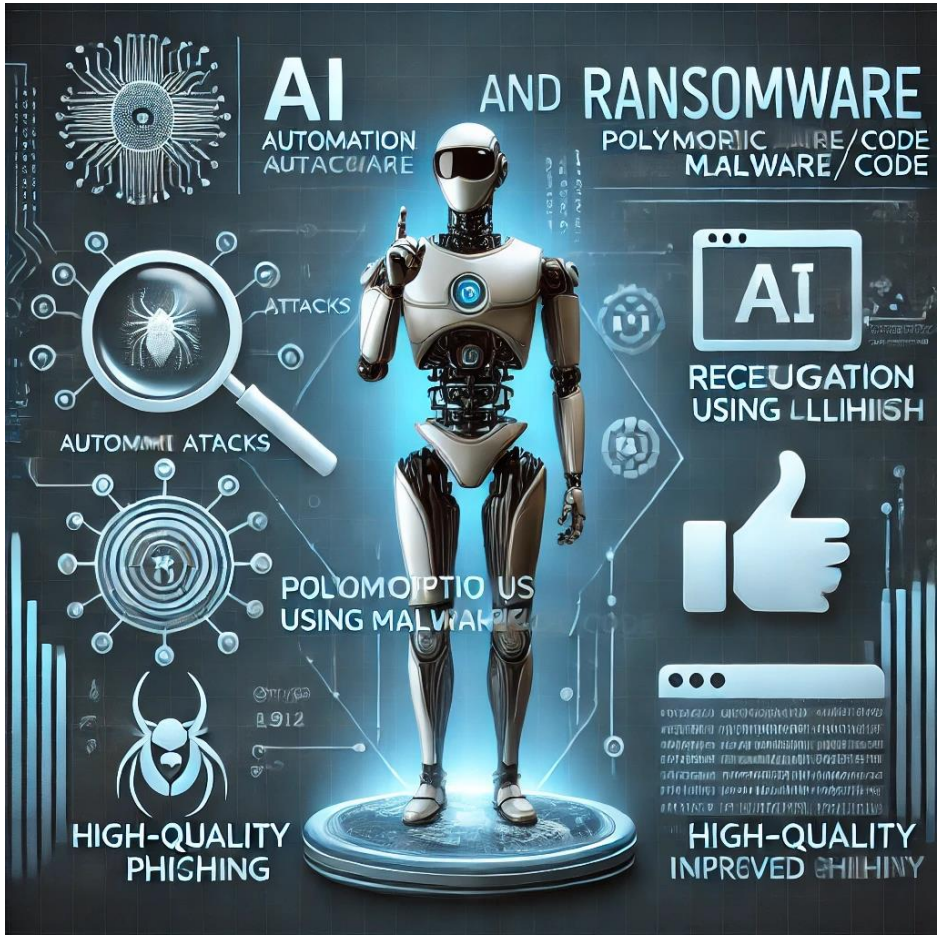
AI & Ransomware – Improved Efficiency

Automated Attacks

Polymorphic Malware / Code

Reconnaissance (LLMs for research)

Phishing Quality (grammar / spelling)



Ransomware and AI

Is AI Helping Ransomware?

Yes, but it's minor right now, but will absolutely be more over time

Bruce Schneier: "AI Will Increase the Quantity—and Quality—of Phishing Scams"

A recent report by the UK's National Cyber Security Centre (NCSC) warned that malicious attackers are already taking advantage of AI to evolve ransomware attacks, posing significant risks to individuals, businesses, and even critical infrastructure. Threat actors such as APT28 have been busy using large language models (LLMs) in elaborate moves to avoid detection and run advanced reconnaissance.

NCSC Warns That AI is Already Being Used by Ransomware Gangs

Posted on January 25, 2024

Artificial intelligence (AI) is making ransomware faster and easier to use as the online crime hits record levels, experts said at a House Financial Services subcommittee hearing Tuesday.

AI-Enabled Malware Is Getting Better

Singaporean cybersecurity company Group-IB, which has been tracking the e-crime actor since January 2023, described the crimeware solution as a "sophisticated AI-powered phishing-as-a-service platform" capable of targeting users of more than 36 Spanish banks, governmental bodies, and 30 institutions worldwide.

Among the other services advertised by the threat actor on a dedicated Telegram channel are AI-infused voice calling tools that allow its customers to generate voice calls to prospective targets based on a series of prompts directly from the phishing kit.

The phishing kit is priced anywhere between $150 and $900 a month,

Source: https://thehackernews.com/2024/07/spanish-hackers-bundle-phishing-kits.html

Everything hackers do today, now automatic, better, and faster

AI-Enabled Malware Is Getting Popular

About 82% of phishing toolkits that Egress researchers found being advertised on forums and other parts of the dark web marketplace mentioned deepfakes and 74.8% referenced AI, according to a recent report by the software maker on the state of phishing.

According to the Phishing Threat Trends Report by Egress, nearly 71% of AI detectors fail to identify phishing emails generated by AI chatbot software[1].

Source: https://www.msspalert.com/analysis/ai-now-a-staple-in-phishing-kits-sold-to-hackers
Source: https://www.ajg.com/uk/news-and-insights/the-rise-of-hyper-realistic-ai-powered-phishing/

It's getting harder to detect phishing emails written by LLMs

Agentic AI Malware Is Getting Better

In March 2025, **AI was 24% more effective** than humans

AI agents can now out-phish elite human red teams, at scale.

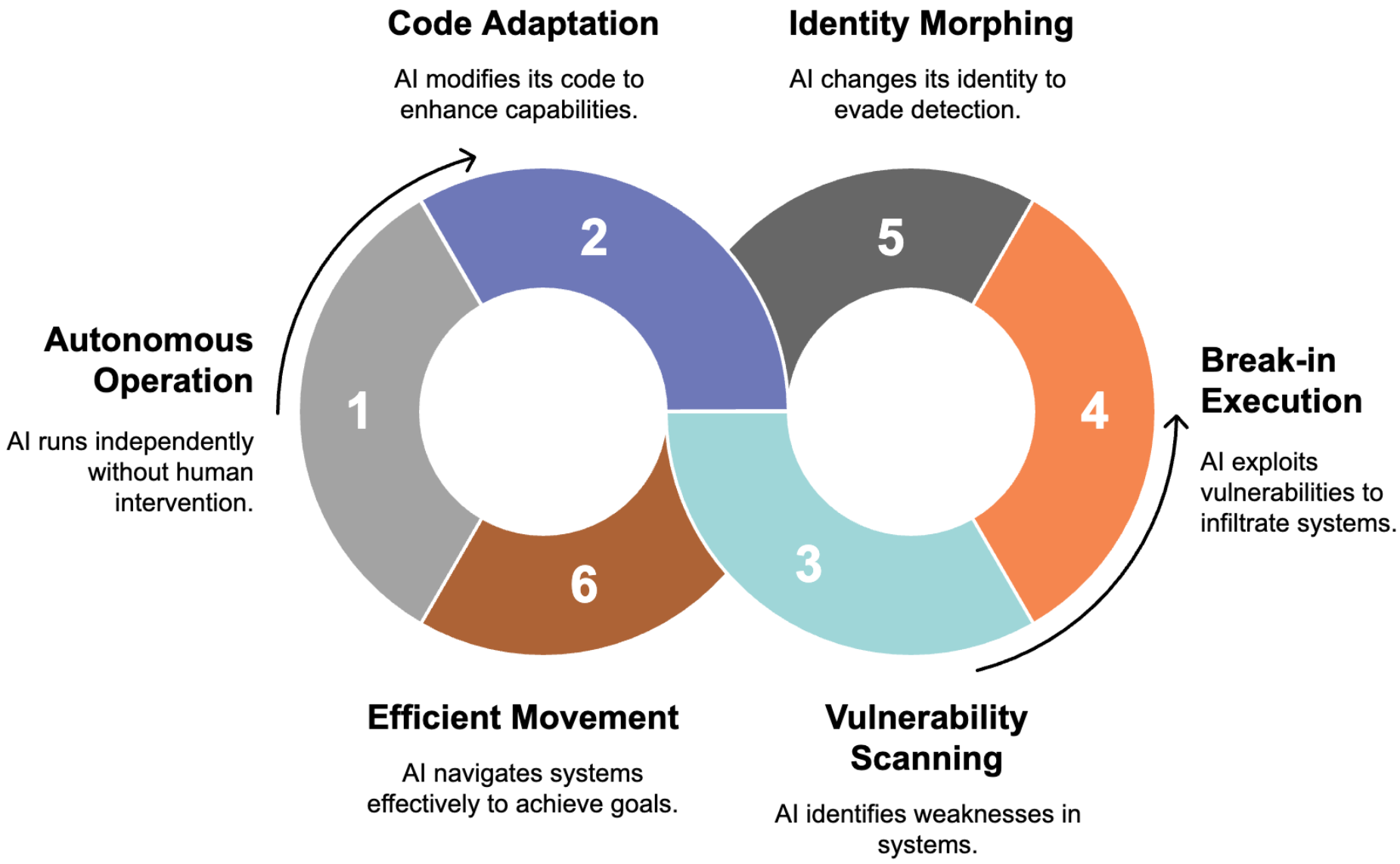
AI AGENT vs HUMAN RED TEAM FAIL RATES

	2023 Failure rate	Nov 2024 Failure rate	March 2025 Failure rate	Total % change
AI	2.9% *	2.1%	2.78%	
Human	**4.2%**	2.3%	2.25%	
AI to Human relative performance	-31% less effective than humans	-10% less effective than humans	+23.8% more effective than humans	+55% improvement

AI-Powered Spear Phishing Can Now Outperform Human Attackers

Source: https://blog.knowbe4.com/ai-powered-spear-phishing-can-now-outperform-human-attackers
Source: https://hoxhunt.com/blog/ai-powered-phishing-vs-humans

Malicious Agentic AI Deepfake Threats



What Is Agentic AI Malware?

Highly Autonomous Malware

Not Here Yet… But

It Will Be Soon

Social Engineering Agent

Less than 0.1% of email attacks are spearphishing, but are involved in 66% of all successful attacks – Mandiant

https://www.action1.com/patching-insights-from-kevin-mandia-of-mandiant/

Agent Summary

It will customize each phishing attack for the exact victim

- It will research them on the Internet and socials
- Then construct a spearphishing attack with a high chance of success
- It will use your existing relationships (e.g., family, business, partners, group memberships, etc.) and interests against you

When Agentic AI Ransomware?

MIT Technology Review

Featured Topics Newsletters Events Audio SIGN IN

ARTIFICIAL INTELLIGENCE

Cyberattacks by AI agents are coming

Agents could make it easier and cheaper for criminals to hack systems at scale. We need to be ready.

By Rhiannon Williams

CYBERCRIME | NEWS

New AI "agents" could hold people for ransom in 2025

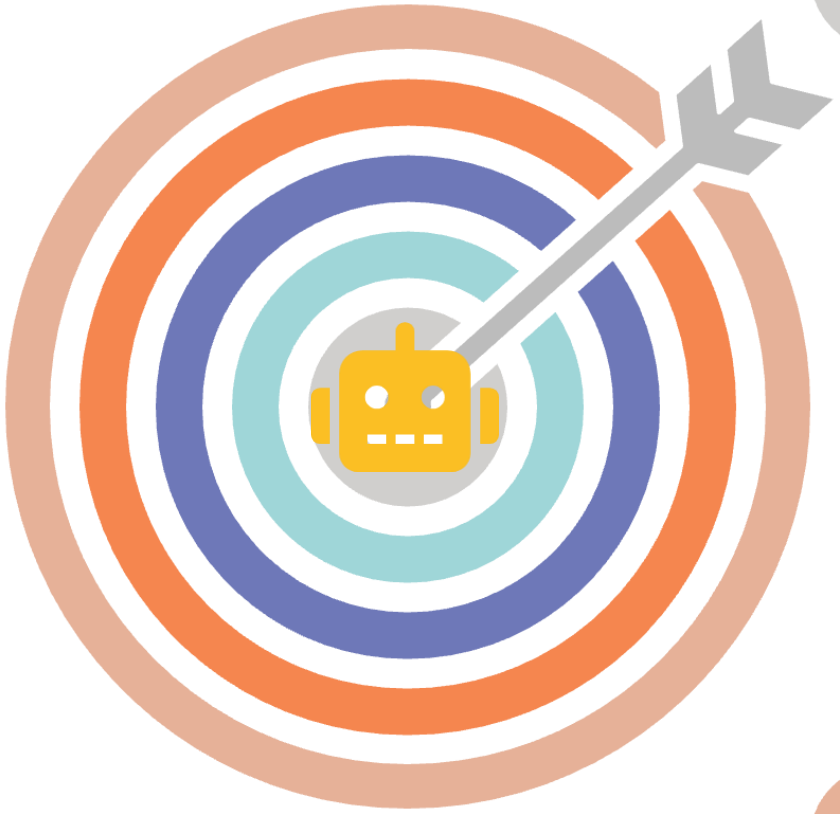
Posted: February 4, 2025 by David Ruiz

Experts are still unsure when agent-orchestrated attacks will become more widespread. Stockley, whose company Malwarebytes named agentic AI as a notable new cybersecurity threat in its 2025 State of Malware report, thinks we could be living in a world of agentic attackers **as soon as this year**. Apr 4, 2025

MIT Technology Review
https://www.technologyreview.com › 2025/04/04 › cybe...

Cyberattacks by AI agents are coming - MIT Technology Review

AI's Role in Ransomware



AI

Core technology enabling various attacks

Autonomous Malware

Adapts to environments and evades detection

Deepfake Social Engineering

Impersonates executives for fraud

AI-Powered Password Cracking

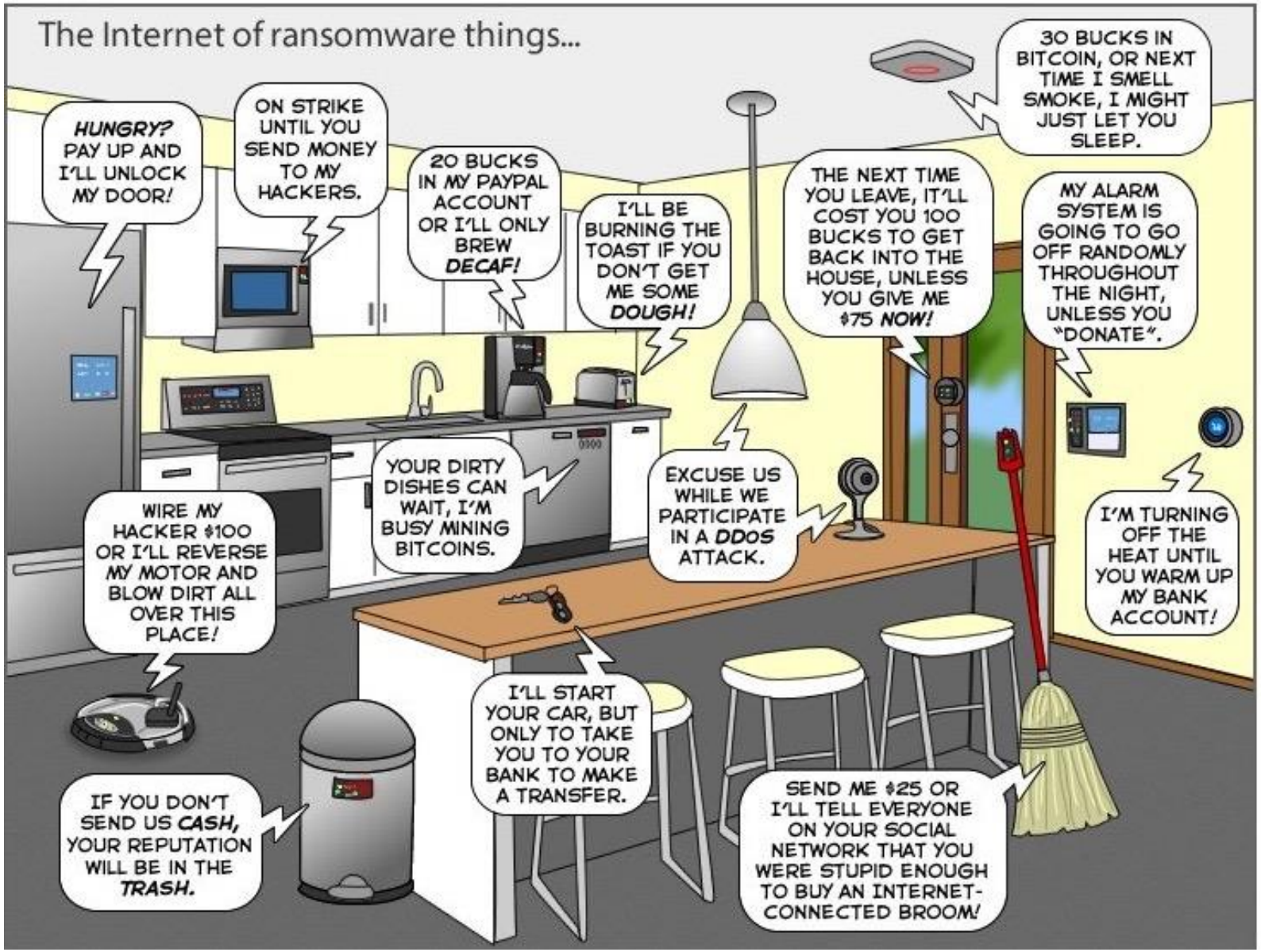
Predicts and breaks passwords quickly

AI-Powered RaaS

Automates target selection and ransom negotiation


An Algo-rithim

Is this next for us with ransomware?



Source: joyoftech.com

KnowBe4

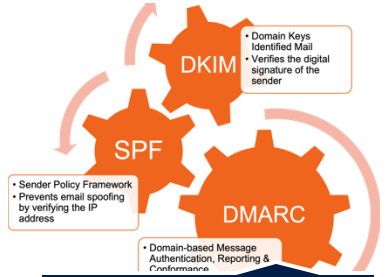
Proactive Defense

Ransomware Best Practices

Backups

Segment the network

Principle of least privilege / MFA



DKIM/SPF/DMARC

Protect RDP

Keep up with Patches

Insurance

IR/TTX

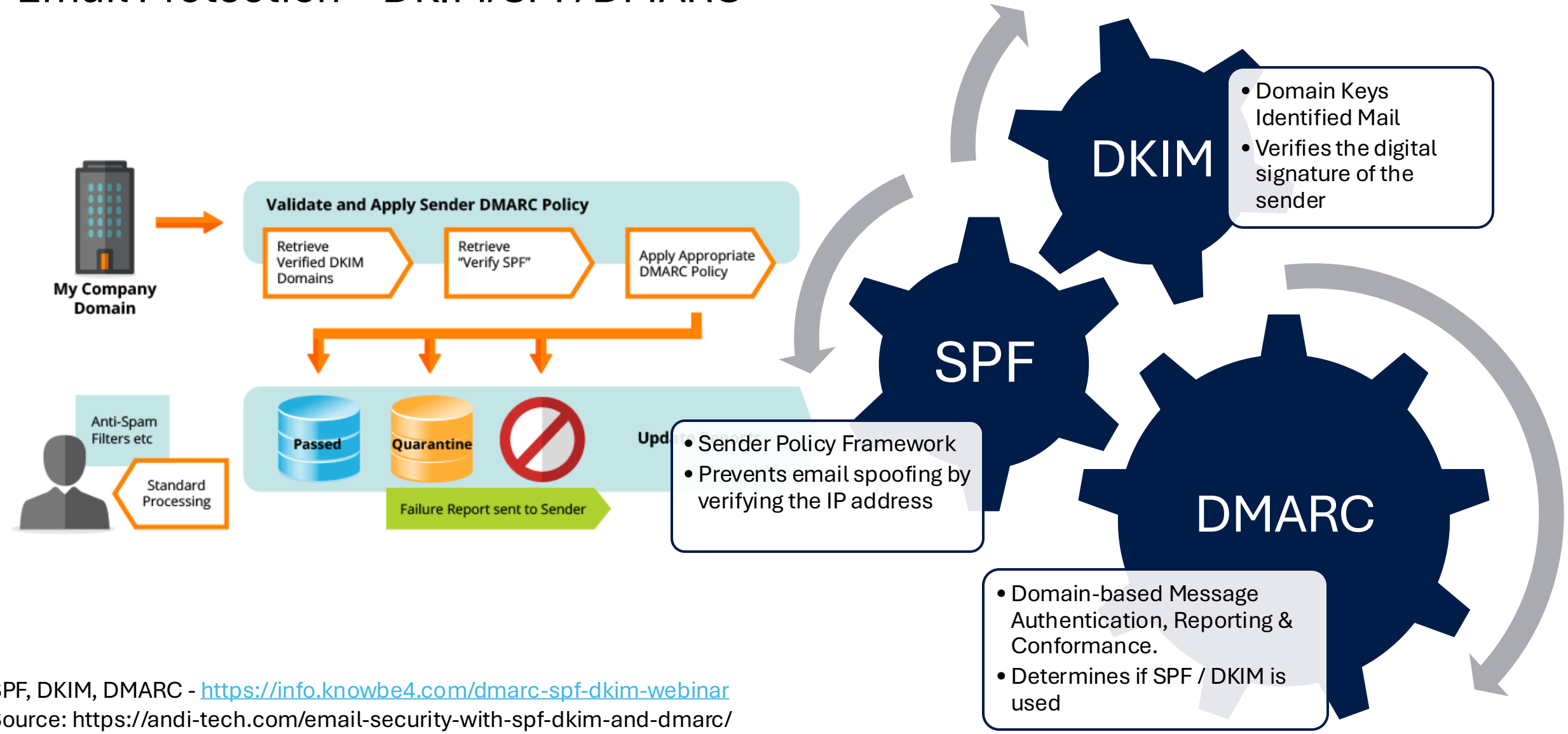
Threat Intel

Experts

Law Enforcement

Train your users

Email Protection – DKIM/SPF/DMARC



SPF, DKIM, DMARC - https://info.knowbe4.com/dmarc-spf-dkim-webinar
Source: https://andi-tech.com/email-security-with-spf-dkim-and-dmarc/

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)

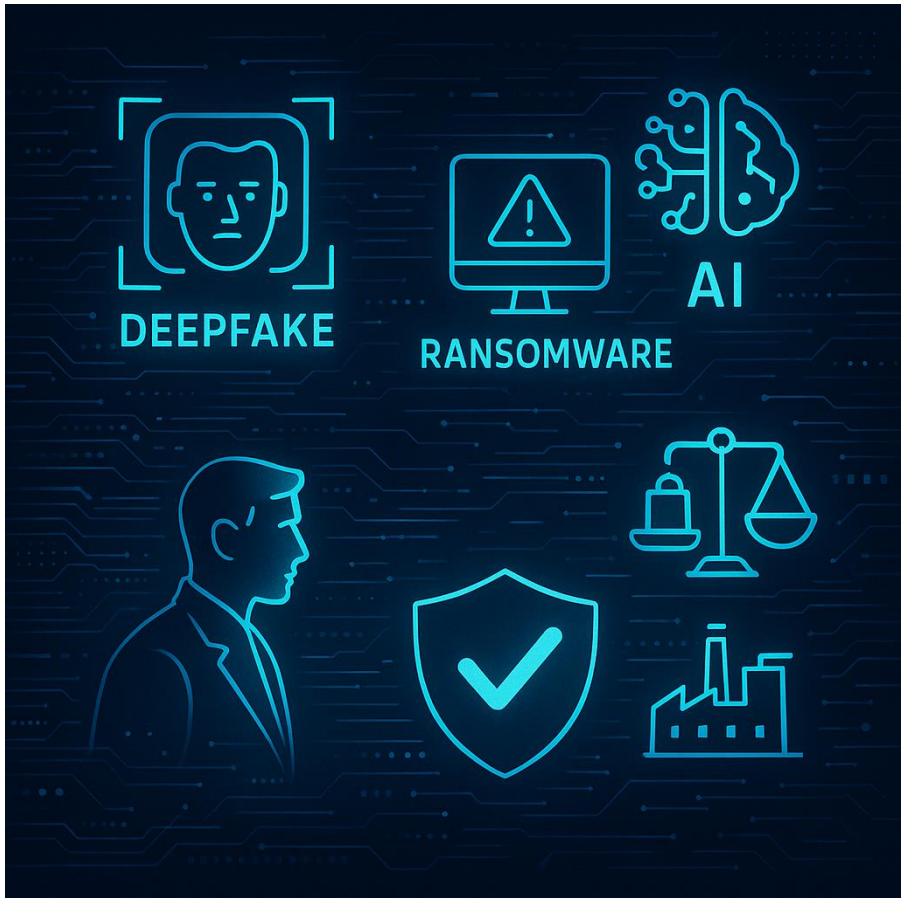
- Code Generated in App
- Make sure you can back them up

Hardware (FIDO Approved)

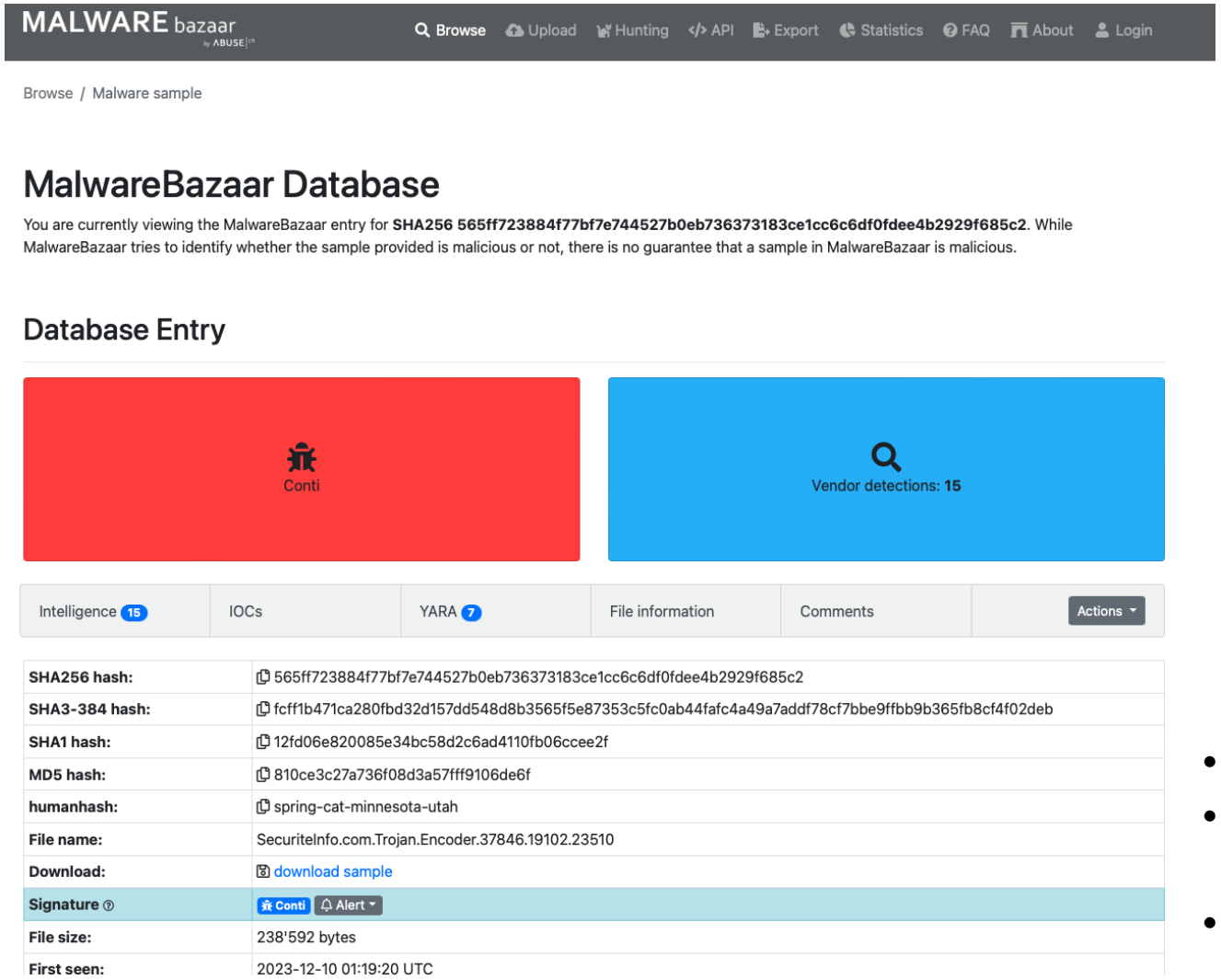
- Uses a hardware token, like a Yubikey or your smartphone
- Can be inconvenient when forgotten or damaged

Bring In the Experts

- **Coveware -** Specializes in ransomware incident response, negotiation, and data recovery and tracks ransomware groups
- **Mandiant (now part of Google Cloud) -** Rapid incident response and threat intelligence. Offers end-to-end support
- **Palo Alto Networks – Unit 42 -** DFIR, Threat Intelligence.
- **Kroll -** Negotiation, breach response, and forensic recovery.
- **Arete -** Threat containment, negotiations, and rebuilding compromised systems with cyber insurance support
- **CrowdStrike -** Strong EDR/XDR platform with ransomware detection, isolation, and forensic capabilities.
- **Sentinel One -** AI-driven endpoint protection and rollback capabilities post-infection.
- **Sophos (Rapid Response Team) -** Works well for mid-sized businesses with limited in-house security teams.
- **IBM Security X-Force -** Combines threat intelligence, IR, and threat actor profiling.



Ransomware Repositories



- https://bazaar.abuse.ch
- https://github.com/Da2dalus/The-MALWARE-Repo/tree/master
- https://github.com/Endermanch/MalwareDatabase

Email Protection

To check if your website and email can be spoofed, please visit

https://www.knowbe4.com/domain-spoof-test/

For the Domain Spoof Test
It's FREE!

Security Awareness & Training

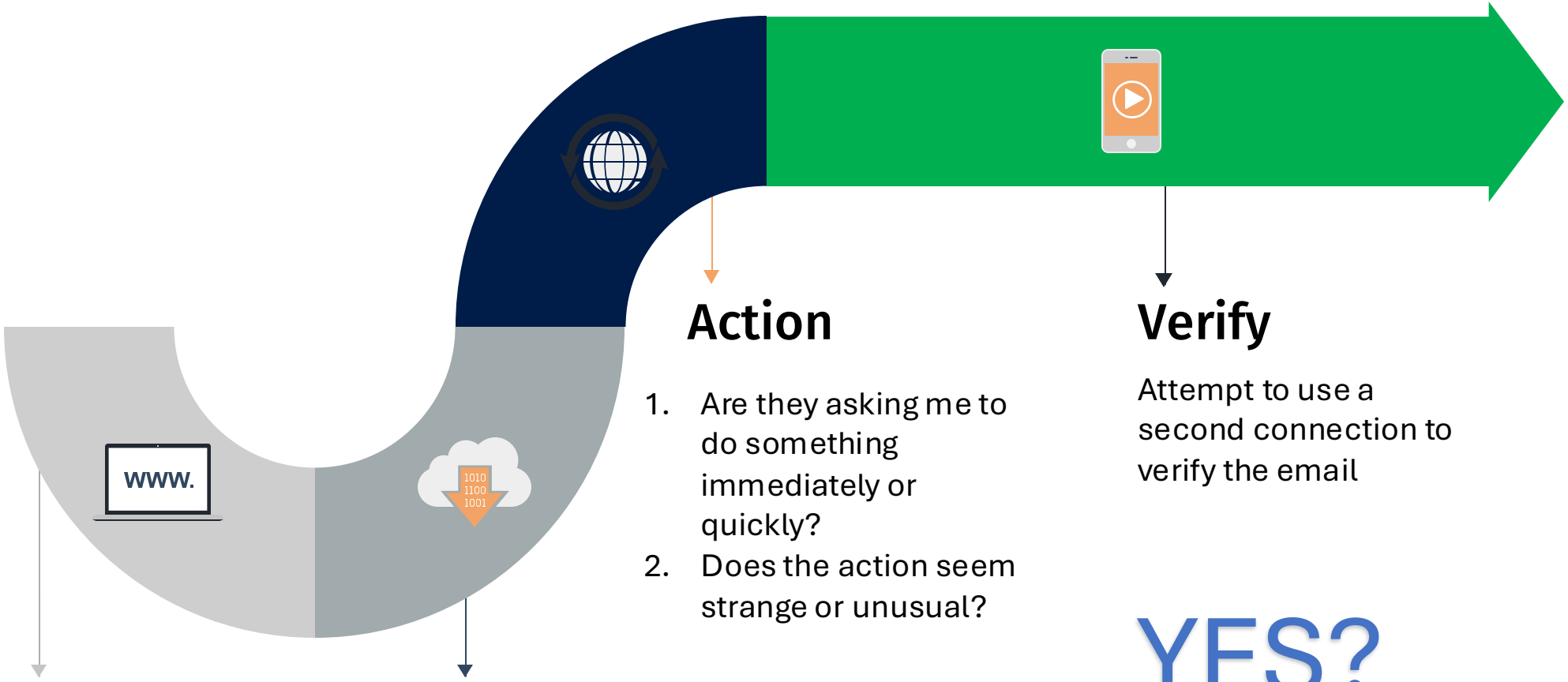
Baseline Testing
We provide baseline testing to assess the Phish-Prone™ percentage of your users through a free simulated phishing attack.

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 training and phishing, ready for management. Show the great ROI!

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?

Zero Trust Mindset

- Not trusting anything by default
- Verifying everything

- Applied to humans it calls for:
  - Politely Paranoid
  - Be skeptical
  - Constant verification

- Mindfulness practices encourage to:
  - pause before reacting
  - engage intentionally and thoughtfully.

Human Risk Management (TEAM)

Technology
Implementing technical controls and threat intelligence to prevent malicious content

Education
Providing personalized training and real time coaching to enhance security awareness

Action
Integrating tools and technology for automated responses and augmented defense

Motivation
Encouraging Leadership and recognition to foster a security conscious culture

Social Engineering Defense in Depth

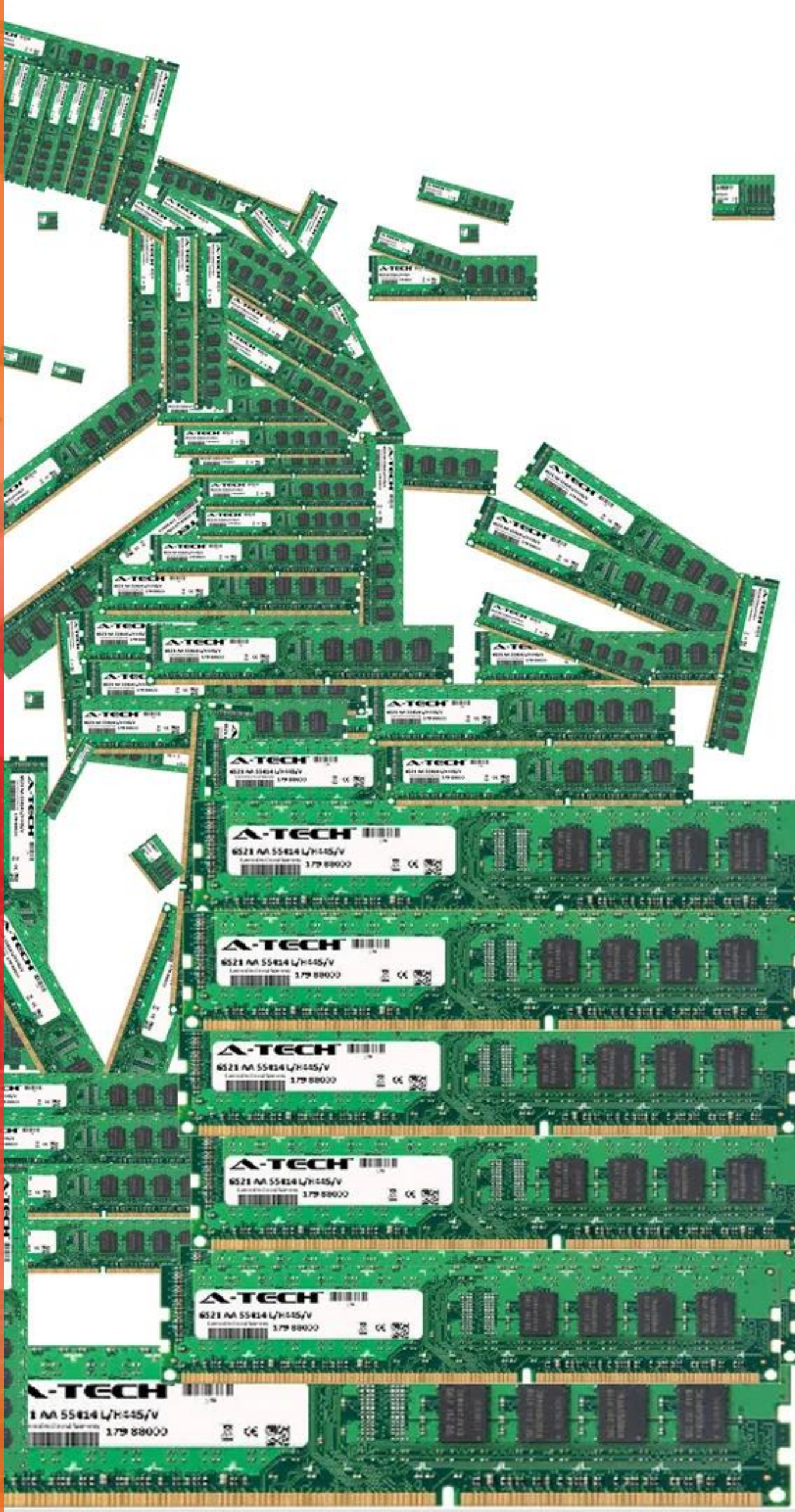
Mitigate	• Aggressively Mitigate Social Engineering • People, Processes, Technology
Patch	• Patch Exploited Software & Firmware • Monitor the CISA KEV Catalog (Known Exploited Vulnerabilities)
MFA	• Use MFA Wherever Possible • Non-phishable MFA too, Avoid SMS and verify all requests that you didn't initiate
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

People, Process and Technology (PPT)

People
- Security Awareness Programs
- Changing their behaviors, culture
- Tabletop Exercises (Ransomware)

Processes
- VPNs for remote work
- External Banners
- Policy for education / training
- Incident Response for Attack

Technology
- Email Filtering
- Threat Detection & Response
- DMARC (SPF/DKIM)
- MFA




amazon
b services
aws

KnowBe4

3 Tips from CyberCriminals

Ransomware Operator

- 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

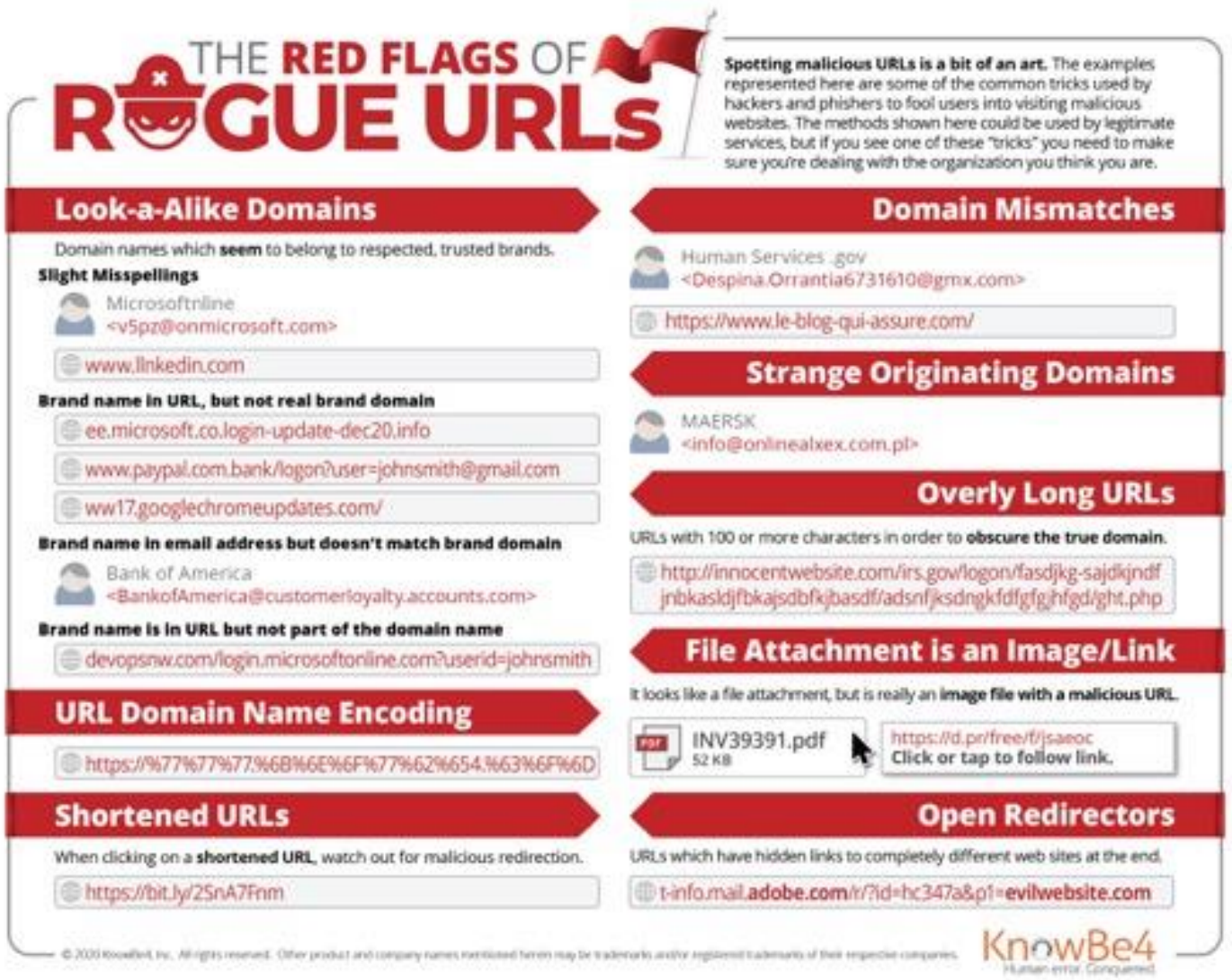
Source: https://papers.vx-underground.org/papers/Other/Interviews/RWO-09-26.html

3 Tips from Cybercriminals (with a bonus tip)

- Patch
- Isolate Backup
- Check the links
- Credential Stuffing

Check for Rogue URLs

- 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)



Most Secure Woman?

Emma Faye

MFA

Multifactor Authentication

KnowBe4

Wrap-up

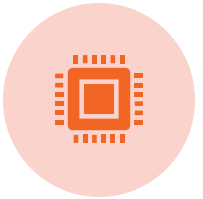
"Ransomware has moved past brute force. It's now using AI. We need to shift from waiting for alarms to predicting the storm."

Humans are the
number one attack vector and
a critical layer of of your security program.

Advice from Conti

Restrict access to servers for regular users

Use different passwords



Check admins' activity on servers once a week

Install EDR on every computer

Set up a more complex storage system

Protect LSASS dump on all computers

Takeaways

Human Compromise

Ransomware relies on exploiting human vulnerabilities, not just technical weaknesses.

AI Social Engineering

Artificial intelligence enhances social engineering, blurring the line between real and fake communication.

Insufficient Training

Traditional security awareness training is inadequate for combating AI-driven threats.

Verification Cultures

Organizations should prioritize verification cultures over simple awareness campaigns.

KnowBe4 Ransomware Resources

- **Ransomware Portal**
  https://www.knowbe4.com/ransomware
- **Ransomware Hostage Rescue Manual**
  https://info.knowbe4.com/ransomware-hostage-rescue-manual-0
- **Ransomware Response Step-by-Step Checklist**
  https://www.knowbe4.com/ransomware#ransomwarechecklist
- **Ransomware Simulator (Ransim)**
  https://www.knowbe4.com/ransomware-simulator

SCREENSHOT


on Edge
Never relaxed?
Edge
Edge
Edge
Edge
Edge
Microsoft
Microsoft

Thank You For Your Attention

James R. McQuiggan, CISSP, SACP

Email: jmcquiggan@knowbe4.com

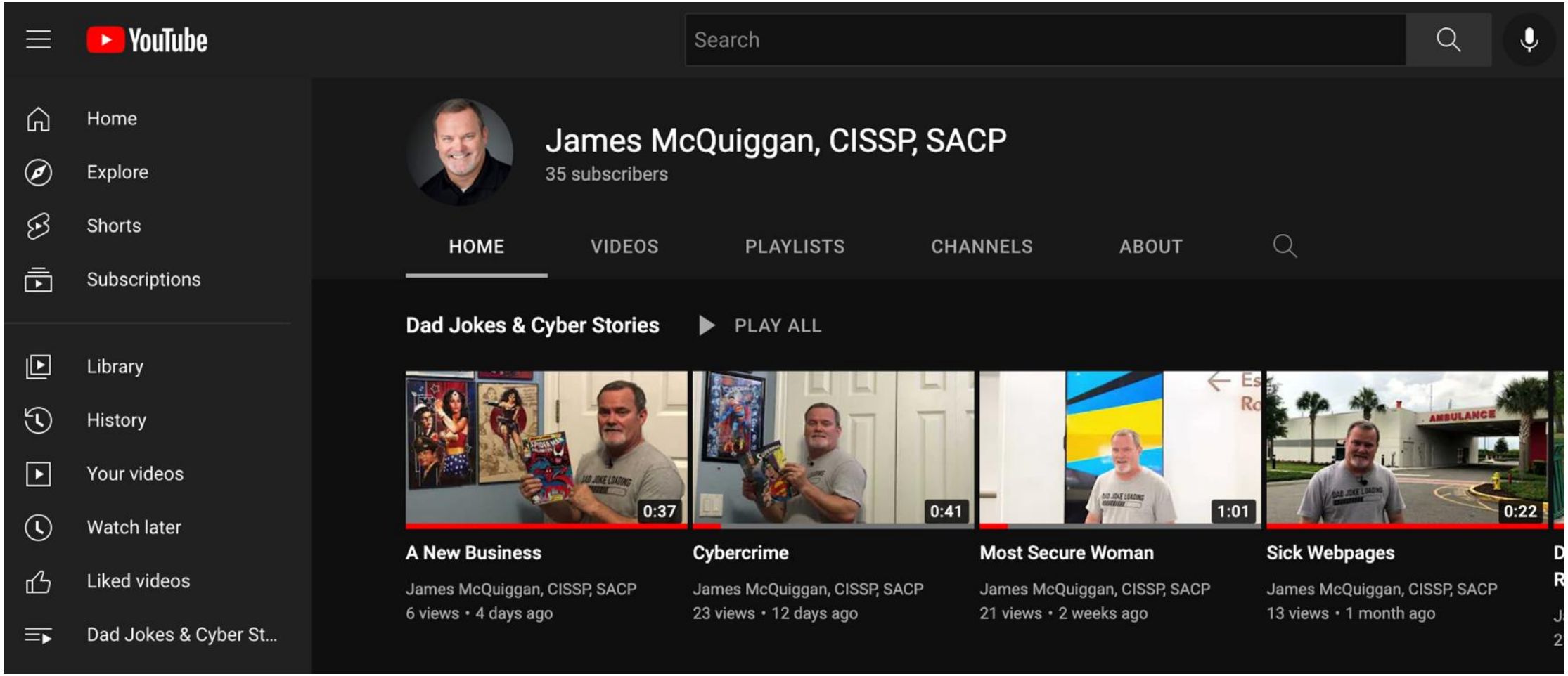
KnowBe4 Blog: blog.knowbe4.com

Connect with Me!

LinkedIn jmcquiggan

X @james_mcquiggan

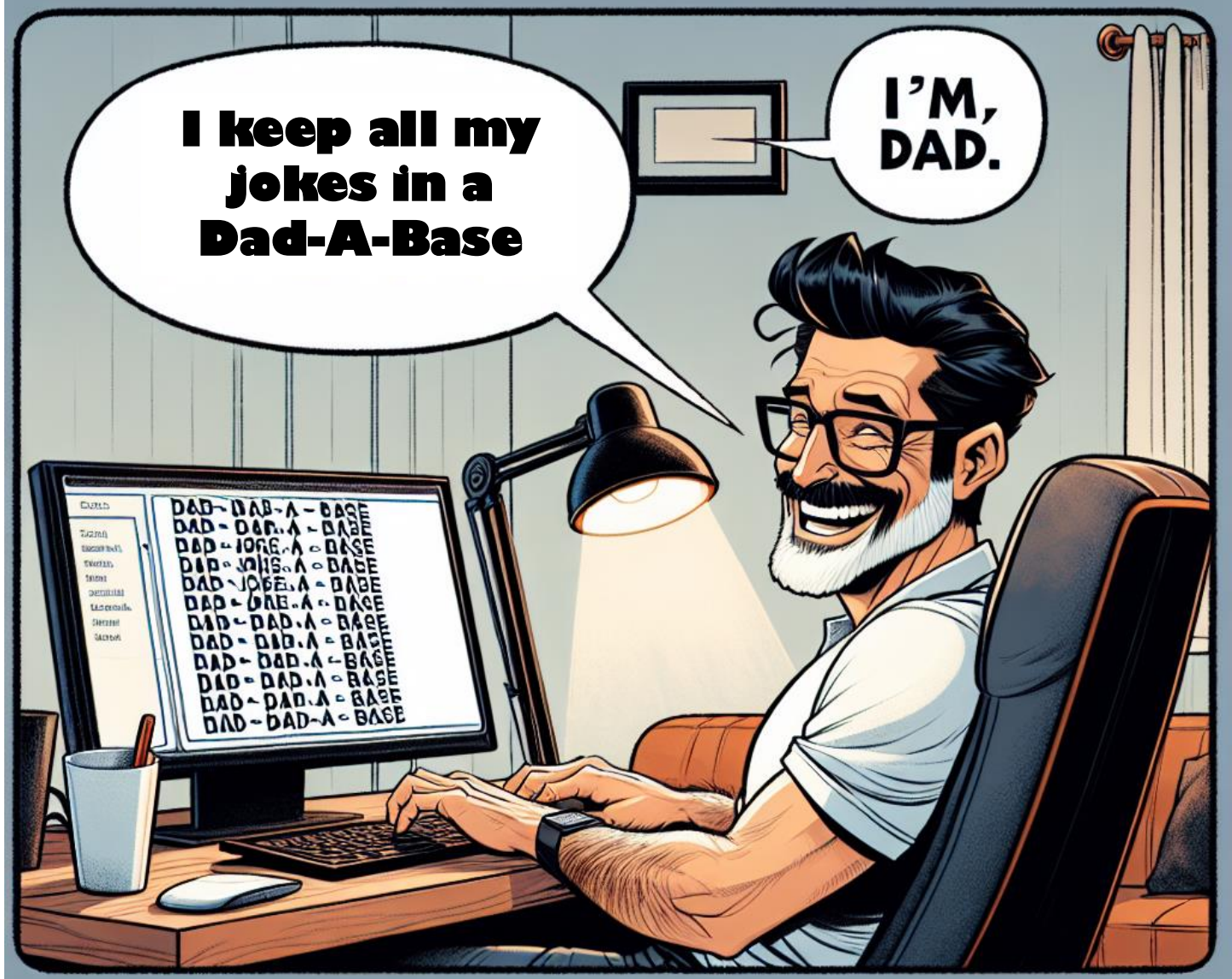
Website jamesmcquiggan.com



YouTube: James McQuiggan and Dad Jokes

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

Yes… I have a way of keeping track of my **Dad Jokes**



KnowBe4

THANK YOU!