Phishers of Men: How Cybercriminals Target the Human Psyche

If you think social engineering is just about greedy princes and clumsy scam emails, I’ve got bad news: the con artists have been hitting the books (and your inbox), and your humans are their favorite lab rats. Forget those cringey password reminders, today’s cybercriminals are pulling off psychological magic tricks that would make Houdini jealous.

In this session, we’ll take you on a whirlwind tour through the modern carnival of social engineering, where neuroscience meets mischief and emotional triggers are more powerful than malware. From manufactured urgency to laser-targeted flattery, you’ll see how attackers turn basic human instincts into their best tools.

Let’s chat about how attackers hijack emotions (and why your stressed-out staff are their favorite targets), the cognitive shortcuts and blind spots that make even us IT pros fall for “just this once”, and how to use psychology for you, not against you, and build human defenses that actually stick.

If you’re tired of playing bait in this digital fishing derby, this session will help you flip the script and outsmart the con artists at their own game. Let’s make the phishers wish they never clicked “send.”

The session will cover:

- The behavioral science behind social engineering
- How AI tools are making things easier
- Defensive measures that can actually help

knowbe4

Phishers of Men

How Cybercriminals Target the Human Psyche

Erich Kron / CISO Advisor

Erich Kron

CISO Advisor, Florida USA

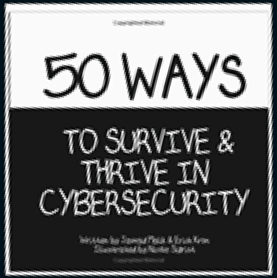
30+ Years in Cybersecurity and IT

QUICK BIO

- Former Security Manager for the US Army 2nd Regional Cyber Center
- U.S. Navy Veteran
- Former Director of Member Relations and Services for (ISC)2
- Bachelor of Science, IT - Networks Administration
- Background in medical, aerospace manufacturing, military and IT fields
- First evangelist for KnowBe4

PRESENCE

- Author
- Podcaster
- 750+ quotes in industry publications
- Advisory Board - Keiser University
- Mentor - Tampa Bay Wave Accelerator



CERTIFICATIONS

CISSP
Certified Information Systems Security Professional
CISSP
Certified Information Systems Security Professional
ISSAP Architecture

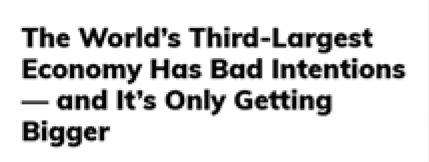
H LAYER CREDENTIALING
CERTIFIED
Security Awareness and Culture Professional (SACP)™

+ Many more

This Is Not What the Adversary Looks Like

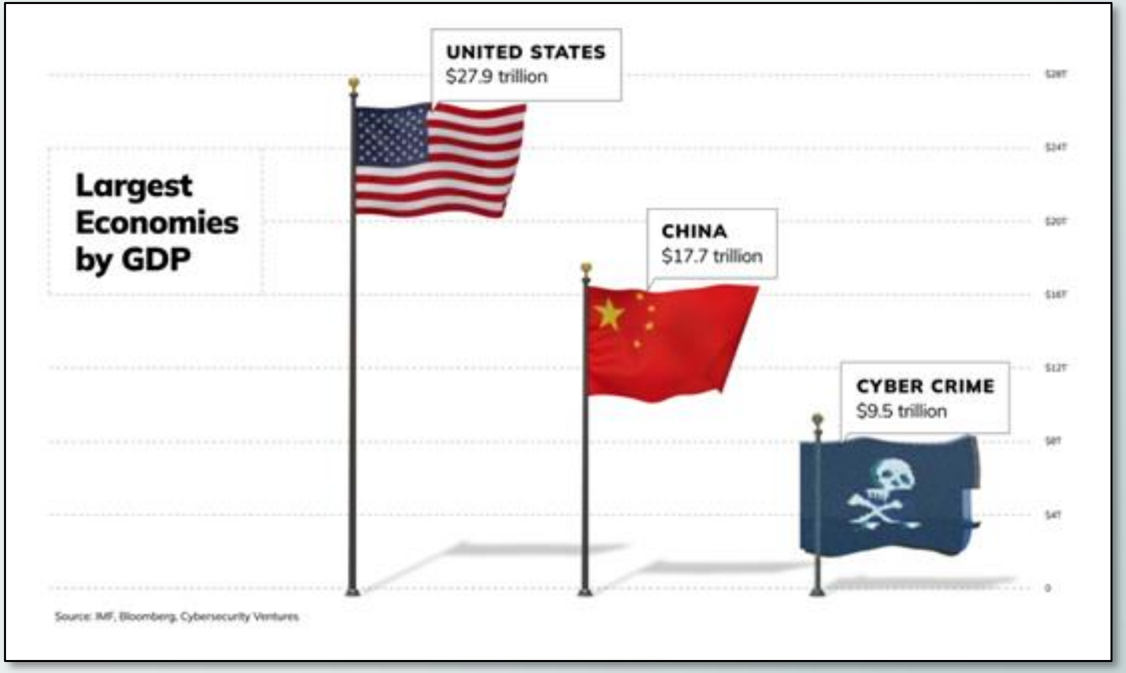
- We are not dealing with just some kids in their parent's basement hacking for fun.
- Many cybercrime groups run as if they are a business, allowing them to grow and expand.
- We cannot underestimate them.

There Is BIG Money in Cybercrime



The World's Third-Largest Economy Has Bad Intentions — and It's Only Getting Bigger

"The global cyber crime economy – a $9.5 trillion behemoth – represents the world's third-largest economy by GDP, according to Cybersecurity Ventures, trailing only the US and China."

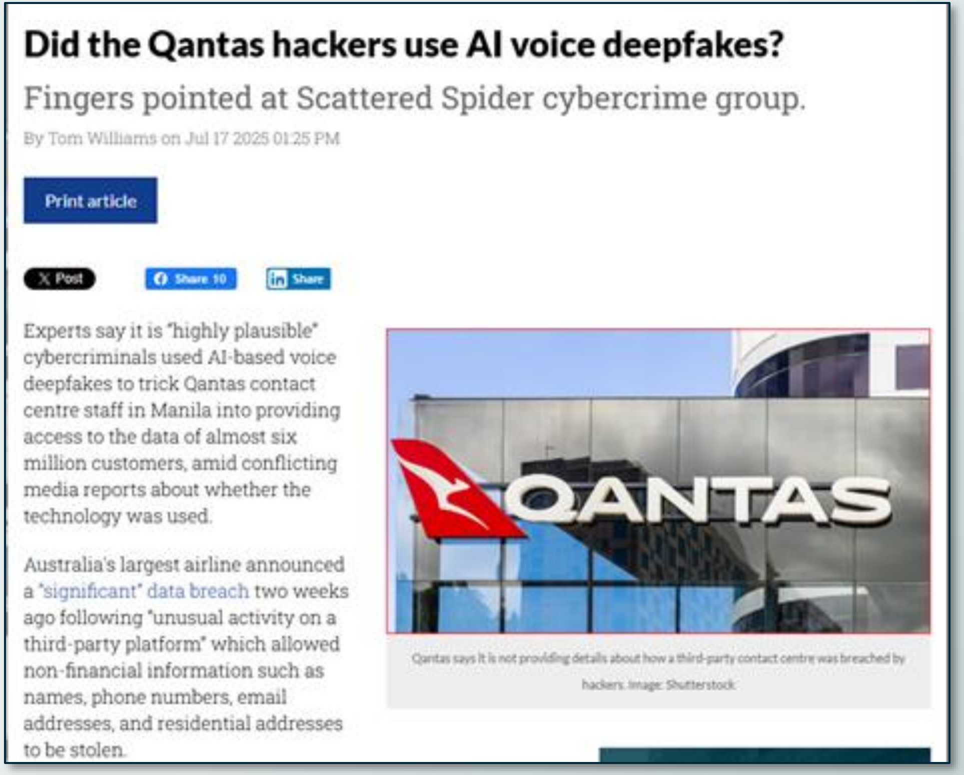


Source: IMF, Bloomberg, Cybersecurity Ventures

https://sponsored.bloomberg.com/quicksight/check-point/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger

Let’s Talk About the Qantas Attack

- The consensus is that this was Scattered Spider
- They often target customer service centers in vishing calls in an effort to get passwords and MFA options reset.
- We are not sure if they use AI-generated voice or not, but it really doesn’t matter in the end.



Did the Qantas hackers use AI voice deepfakes?

Fingers pointed at Scattered Spider cybercrime group.

By Tom Williams on Jul 17 2025 01:25 PM

Experts say it is "highly plausible" cybercriminals used AI-based voice deepfakes to trick Qantas contact centre staff in Manila into providing access to the data of almost six million customers, amid conflicting media reports about whether the technology was used.

Australia's largest airline announced a "significant" data breach two weeks ago following "unusual activity on a third-party platform" which allowed non-financial information such as names, phone numbers, email addresses, and residential addresses to be stolen.

Qantas says It is not providing details about how a third-party contact centre was breached by hackers. Image: Shutterstock.

Secretary of State Faked

- An "unknown actor" created a Signal account and used AI to impersonate Secretary of State Marco Rubio and contact government and foreign officials
- The individual contacted at least five non-Department individuals, including three foreign ministers, a U.S. governor, and a U.S. member of Congress. The actor left voicemails on Signal for at least two targeted individuals, and in one instance, sent a text message inviting the individual to communicate on Signal.

Rubio impersonation campaign underscores broad risk of AI voice scams

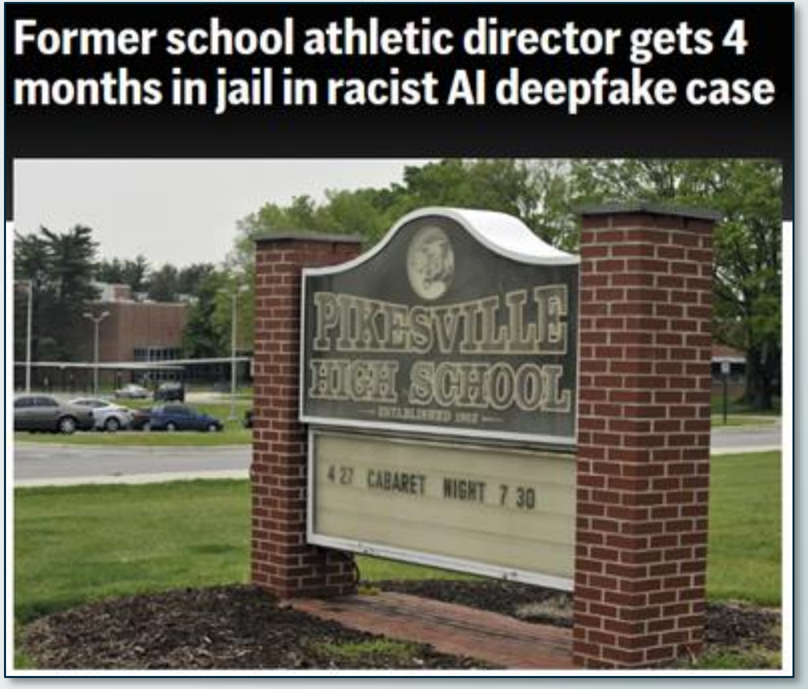
Avery Lotz, Sam Sabin

https://www.axios.com/2025/07/08/rubio-ai-impersonation-voice-cloning-risk

Revenge Against the Boss

- A former high school athletic director in Baltimore was told his contract wouldn’t be renewed the following semester because of concerns over poor job performance

- He got back at the principal by creating a deepfake video of him saying racist and antisemitic things, then spreading the video through the community



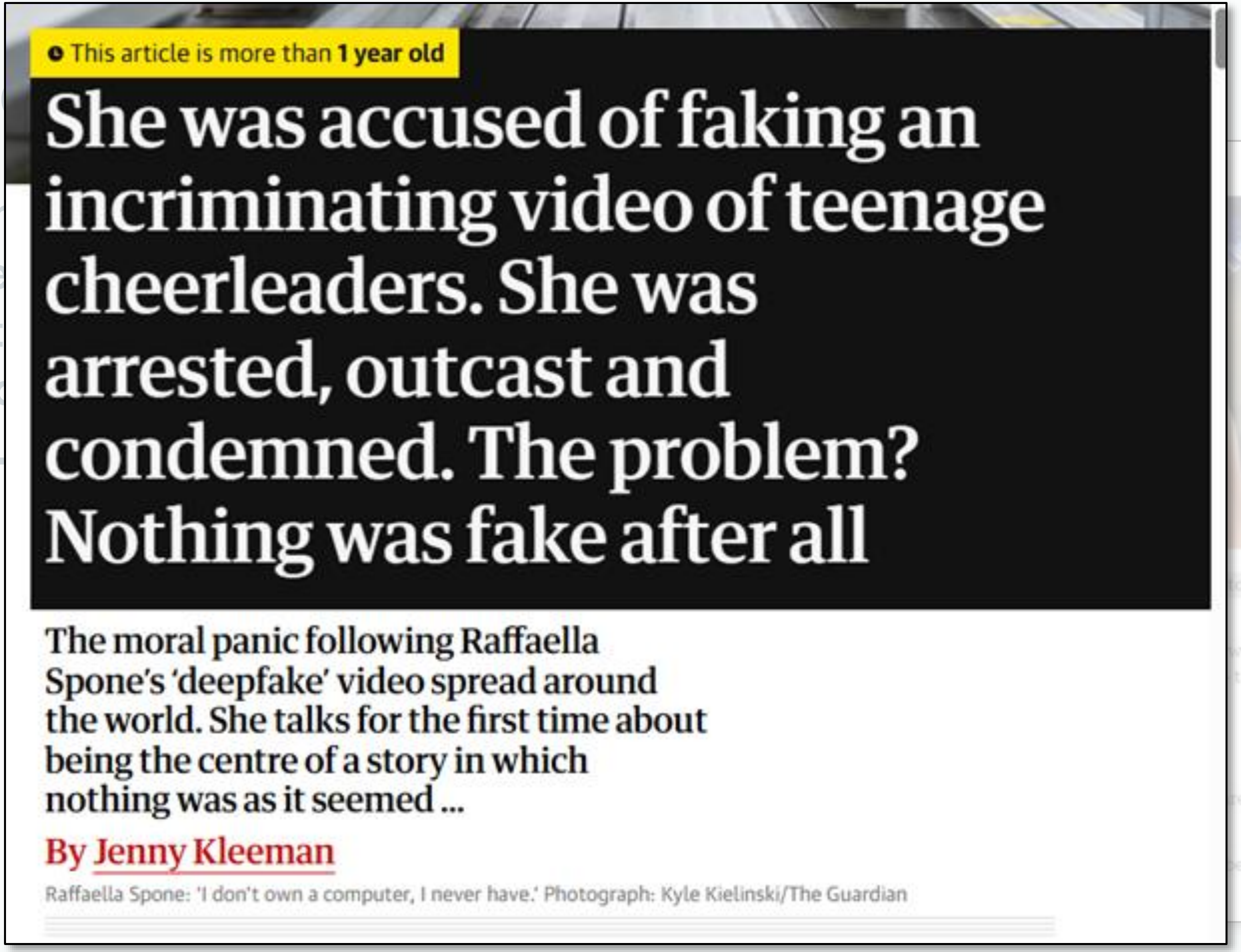
Former school athletic director gets 4 months in jail in racist AI deepfake case

https://apnews.com/article/racist-ai-recording-maryland-high-school-487ea673b0449077cb23e7970546cb9f

Reveng

- A mother
  deepfake
  try to get
  cheerlead
  the team.

- **Turns out, it wasn't a fake after all!**



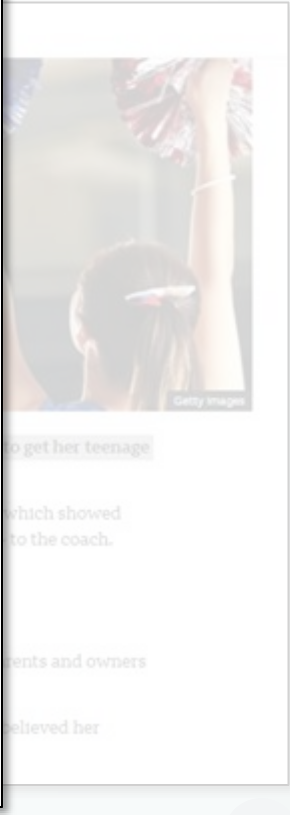
This article is more than **1 year old**

She was accused of faking an incriminating video of teenage cheerleaders. She was arrested, outcast and condemned. The problem? Nothing was fake after all

The moral panic following Raffaella Spone's 'deepfake' video spread around the world. She talks for the first time about being the centre of a story in which nothing was as it seemed ...

By Jenny Kleeman

Raffaella Spone: 'I don't own a computer, I never have.' Photograph: Kyle Kielinski/The Guardian



Getty Images

o get her teenage

which showed
to the coach.

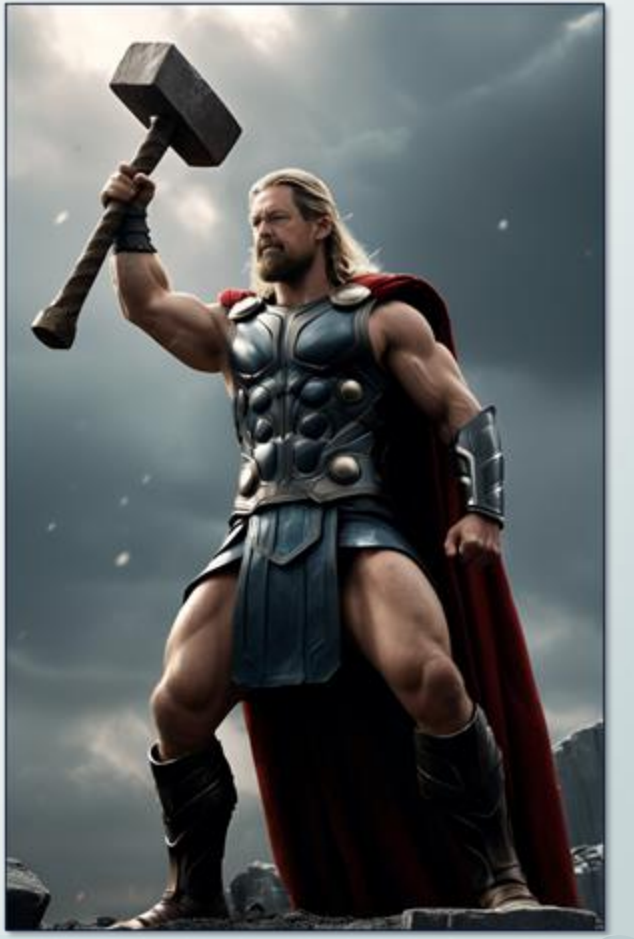
ents and owners

elieved her

What Is Real Anymore?

I'm pretty sure none of us think this is real, but what if it was something that we were already prepared to believe?

Deepfake videos from the L.A. protests and the Air India crash circulated almost instantly.



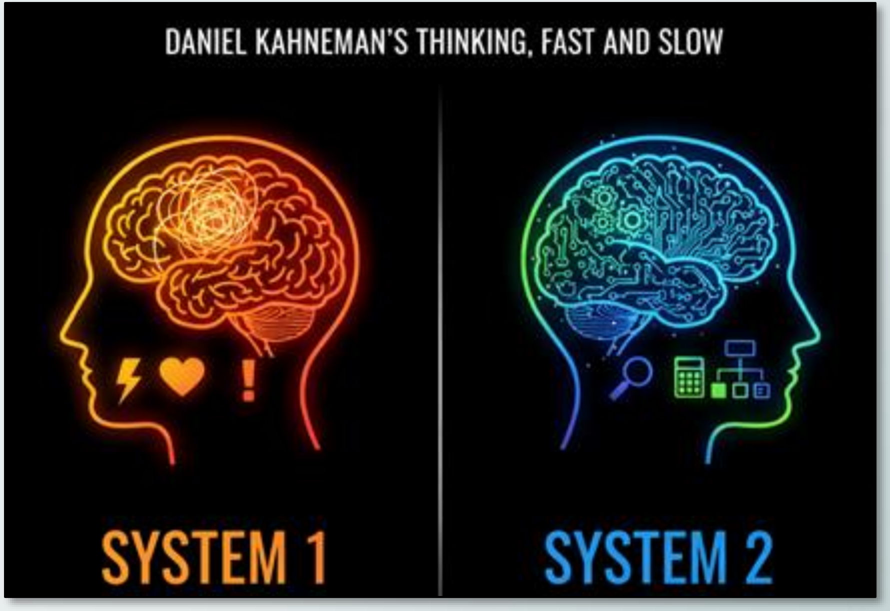
How They Get Into Your Head

- Pressure, stress, and other emotions are used to get us to make mistakes.
- Fear and urgency are tools being used to get us to miss otherwise obvious signs of deception.
- Blending in with daily tasks can catch people when their guard is down.

Processes of Thought

- System 1 is fast, automatic, unconscious and low effort. It handles everyday tasks and provides quick, emotional, and intuitive judgments.

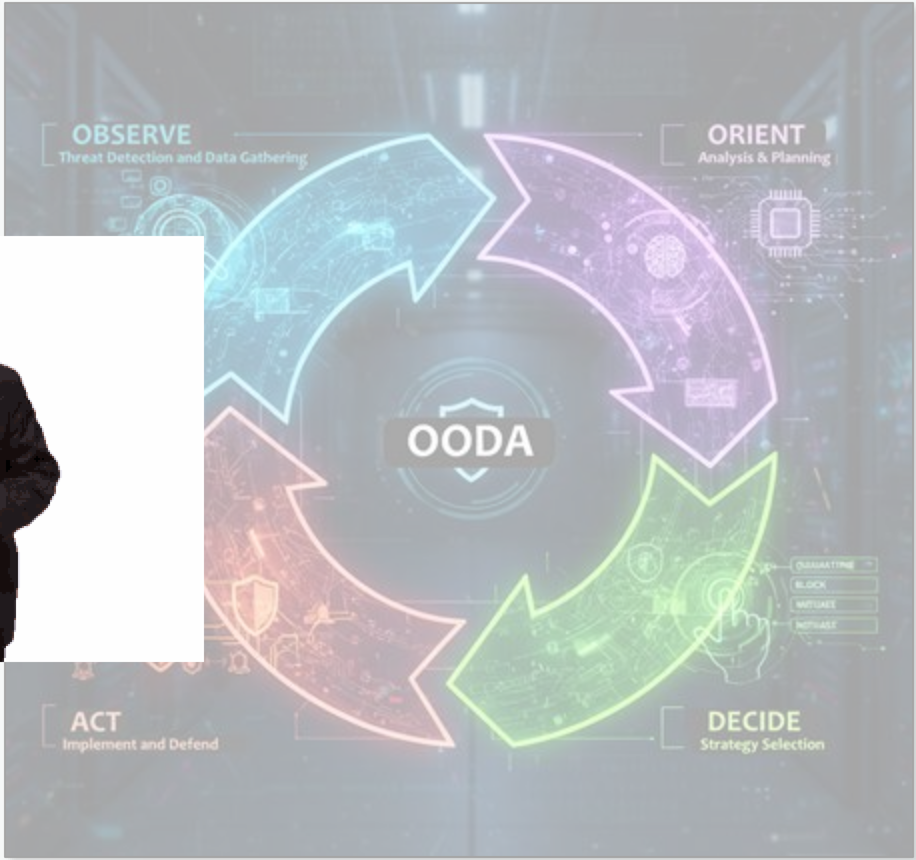
- System 2 is slow, conscious, takes effort, and logical. Engaged for complex, abstract, and analytical tasks that require sustained focus and rational thinking.



The OODA Loop

Created by U.S. Air Force Colonel John Boyd

- Observe - Gather information understand the situation
- Orient - Position yourself to understand the situation
- Decide - Based on your orienta choose the best course of action
- Act - Execute the chosen decision, then observe the results



So, What Do We Do?

"You can't patch human nature, but you can train people to recognize when it's being exploited."

– Me

(According to ChatGPT)

Defense Is a Combination of Tech and Humans

- There is simply no silver bullet to deal with cybercrime. It involves a combination of technical and non-technical controls.

- Since most breaches start with a human action, it makes sense to have an HRM program in place.

- This is more than just awareness and phishing training. It is an approach that looks at addressing the entire human element.

What Can We Teach People To Do?

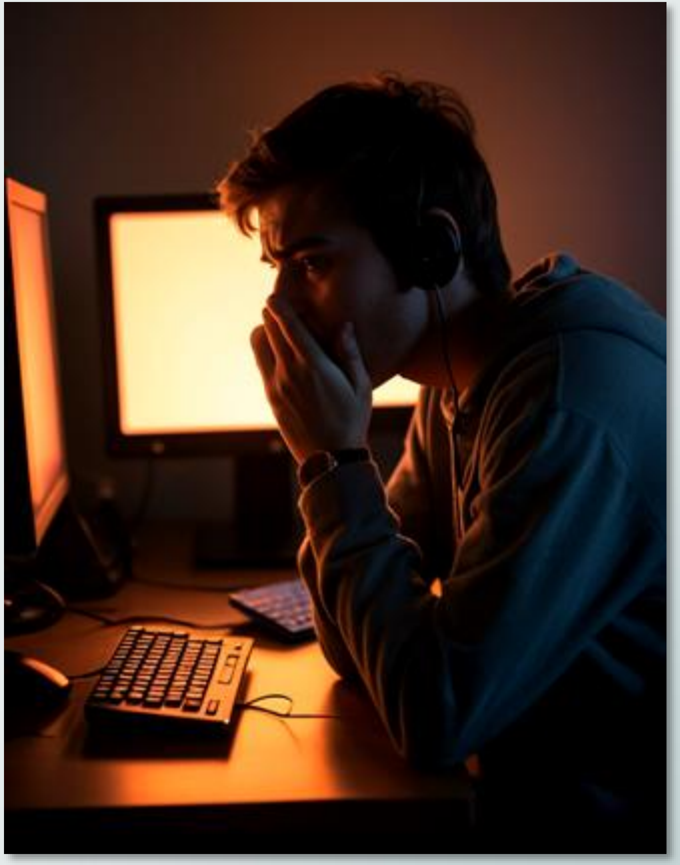
- Pay attention to the request. Is it strange?
- Listen to intuition and emotions
- Ensure there are policies in place to avoid scams, such as calling to confirm some requests, and follow them every time
- Teach how the scams work and the red flags around phishing/vishing and smishing

Believe Nothing (Without Checking)

- Audio, photos and video can’t be taken at face value.
- Careful scrutiny is now needed, and we need to start trusting our instincts a little more and pay attention to our emotions.

Understand Emotions

- Teach them that if they feel a strong emotional response to a phone call, email or text message, pay careful attention to whatever triggered it.
- Take a deep breath and force themselves into System 2 thinking.



Use Unique and Strong Credentials

- Reusing passwords, or using weak passwords makes things much easier for the attackers.

- Attackers will often use credentials stolen from other breaches or from tricking a person, to log into other sites

Technical Controls

- Patch regularly in case there is a mistake.
- Use MFA everywhere you can, It’s not a fix for bad/stolen passwords, but can help.
- Use DLP to watch for data being stolen.
- Have good EDR controls in place.
- Make sure the basics are covered such as network segmentation, regular permissions auditing, etc.

In Summary

- Cybercrime is big business and the adversaries have funds.
- Psychology is being used heavily in social engineering.
- You can’t believe anything you heard or see anymore.
- AI is making attackers much more efficient.
- It takes tech and human controls to defend against attacks.

THANK YOU

Erich Kron – Security Awareness Advocate

Erich Kron

Cybersecurity Keynote Speaker | Author | Security Awareness Advocate | Technical Ev...