

⋮ The Cyber Threats Targeting Your Organization Now

A Cybersecurity Awareness Month Webinar

Presented by

Ed Ko

SVP & COO, CampusGuard

CISA, CISSP, QSA



CAMPUSGUARD®



About the Presenter



Ed Ko
SVP & COO, CampusGuard
CISA, CISSP, QSA





Agenda

- Welcome & Introduction
- Today's Threat Landscape
- How We Got Here
- Top Cyber Threats
- Small Habits, Real Protection
- The Partner Behind Your Readiness
- Q&A



Poll Question #1



● The Stakes Have Never Been Higher

Cybersecurity has become one of the most consequential issues facing organizations of every size; no longer optional, no longer someone else's job.



As organizations adopt AI, cloud, and hybrid work models, attackers are moving just as fast, weaponizing the same technologies to outpace traditional defenses.





How We Got Here

John Draper discovered that a toy whistle from a cereal box made the exact tone phone companies used to grant free long-distance calls, earning him the nickname “Cap’n Crunch.”



1971

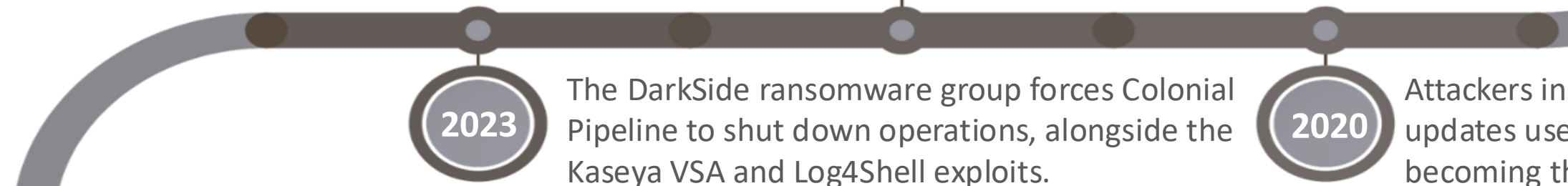
Yahoo suffers one of the largest-scale hacks in history, with over 3 billion user accounts compromised.

2017

The Equifax breach exposes the personal and financial data of 147 million people after attackers exploited an unpatched Apache Struts vulnerability.

The MOVEit breach and the MGM Resorts social engineering attack, which started with a single phone call to a help desk.

2021



2023

The DarkSide ransomware group forces Colonial Pipeline to shut down operations, alongside the Kaseya VSA and Log4Shell exploits.

2020

Attackers insert malicious code into SolarWinds’ Orion software updates used by government agencies and major enterprises, becoming the defining supply-chain attack of the decade.

Ransomware and phishing dominate, with identity-based attacks quietly overtaking technical exploits.

2025



2024

AI-powered attacks accelerate as organizations report AI-related vulnerabilities as their fastest-growing risk.

2026

Attacks now operate at machine speed, converging with global instability to reshape the threat landscape.



... ——— Top Threats Defining 2026 ——— ...

Four threat categories are driving the majority of incidents organizations face this year.



AI-Driven Attacks

Attackers are using AI to launch phishing, malware, and intrusions faster and at greater scale than ever.



Ransomware

Ransomware-related attacks still drive over half of all global cyberattacks, with costs climbing every year.



Identity Attacks

Stolen credentials and session tokens now account for roughly 30% of intrusions, no exploit required.



Evolved Phishing

91% of successful breaches start with phishing, now supercharged by deepfakes and AI-generated lures.





AI-Driven Attacks

- Attackers are using AI to launch phishing campaigns, malware, and intrusion attempts faster and at far greater scale than ever before.
- 87% of organizations now rank AI-related vulnerabilities as their fastest-growing cyber risk.

AI-powered attacks now operate at machine speed and human-only response can't keep up.

AI-Driven Attack Examples



Hyper-personalized spear phishing

- AI-generated phishing attacks that bypass email filters
- Pull from public profiles and company content to mimic a real coworker's writing style



Deepfake videos

- Cybercriminals generate real-time voice and video that convincingly mimic executives or department heads
- Often used in high-pressure situations to request transfers or bypass approval processes.



Deepfake voice calls (vishing)

- Attackers can clone someone's voice using just a few seconds of publicly available audio, like a podcast or conference recording



AI-generated fake identities

- Ghost students who steal financial aid funds
- Fake job postings that steal identity documents or onboarding fees



● Ransomware

- Ransomware-related attacks continue to drive over half of all global cyberattacks.
- Even as some ransomware-as-a-service groups disappear, new and emerging actors are filling the gap, and costs keep climbing every year.

The average data breach now costs organizations more than \$10 million.



Types of Ransomware

- Crypto ransomware
- Locker ransomware
- Leakware/exfiltration-only
- Double extortion
- Ransomware-as-a-Service (RaaS)
- Triple (and quadruple) extortion



Identity-Based Attacks

- Rather than breaking in through technical exploits, attackers are increasingly signing in using stolen credentials, session tokens, or compromised authentication flows.
- Identity-based attacks now account for roughly 30% of all intrusions.

Attackers who steal credentials can move, escalate, and access data while looking like a legitimate user.



Types of Identity-Based Attacks

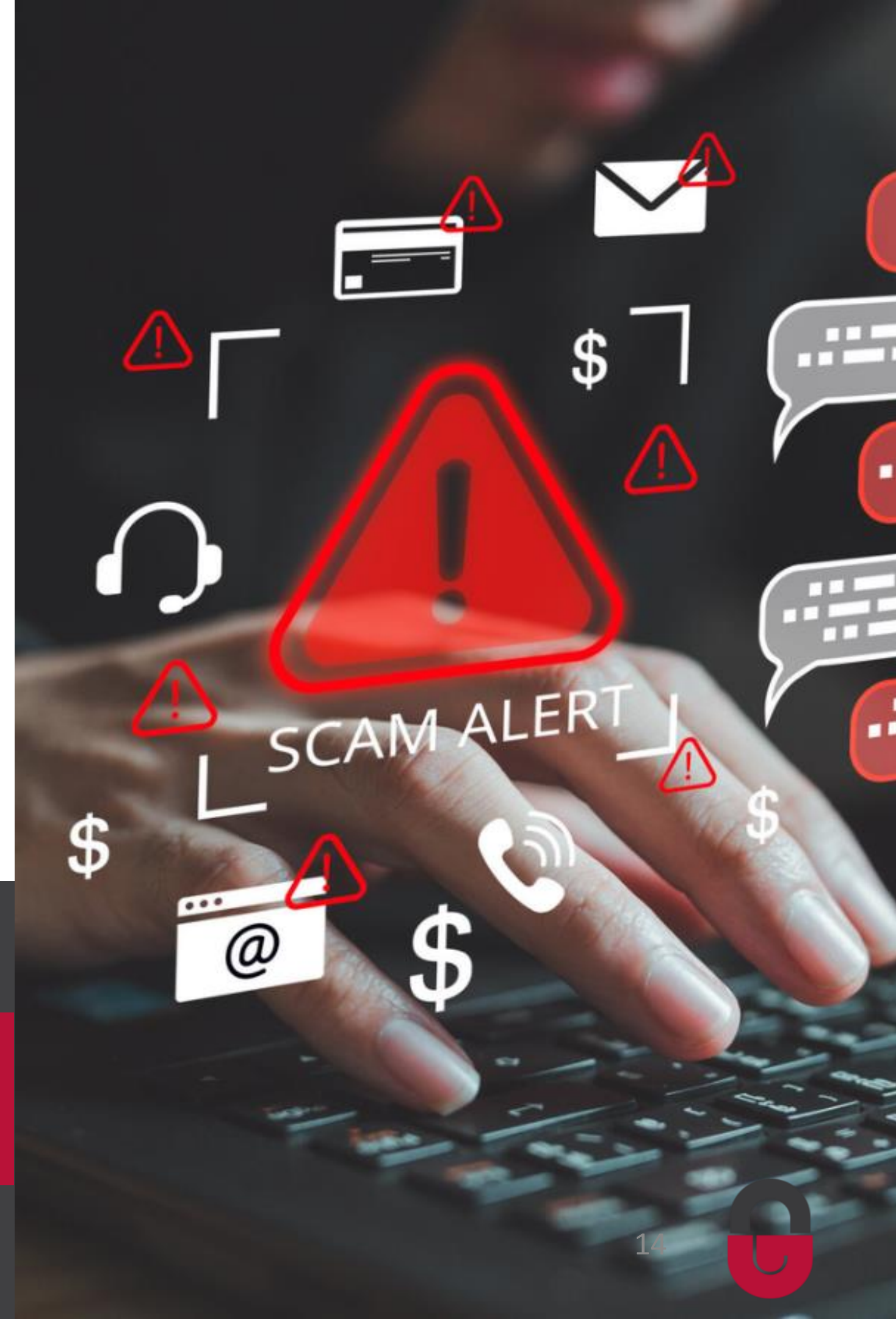
- Credential stuffing
- Session/cookie hijacking
- Voice-phishing into SSO
- API key/machine credential theft
- Deepfake-enabled identity verification failure
- Agentic AI identity hijacking



Evolved Phishing

- Phishing remains the most common entry point for attackers, but the tactics have changed.
- Email phishing is now joined by deepfake audio and video, and AI-generated lures that are harder than ever for employees to spot.

91% of successful breaches still start with phishing.



Types of Evolved Phishing

Growing in sophistication by using AI-powered phishing, deepfakes, and automated malware to evade detection and bypass traditional defenses.

- AI-generated spear phishing
- Deepfake voice phishing (vishing 2.0)
- Deepfake video BEC
- Quishing (QR code phishing)
- Callback phishing
- MFA-bypassing phishing kits (AiTM)
- Recruitment/interview deepfakes



Poll Question #2



Scale, Speed, and Sophistication

The result is a threat landscape defined less by isolated incidents and more by scale, speed, and sophistication, though many attacks still exploit the same fundamental gaps in people, process, and technology.

- Ransomware drives over half of all global cyberattacks
- 91% of successful breaches start with phishing
- Identity attacks account for roughly 30% of intrusions
- Attackers move at machine speed; response can't lag behind



● ● ● Beyond the Headlines

Vendor & Supply Chain Risk



Third-party and vendor risk is an expanding blind spot for many organizations.

The Cost of Distraction



Chasing the “threat of the month” pulls focus from the fundamentals that actually reduce risk.

Everyday Habits Matter



The biggest wins often come from simple, consistent habits practiced institution-wide.

Rising Regulatory Pressure



Tightening frameworks like NIST and PCI DSS are raising the compliance stakes for every organization.



Small Habits, Real Protection

- **Pause Before You Click**
Hover over links and verify sender addresses before clicking, especially on urgent or unexpected requests.
- **Use a Password Manager**
Unique, complex passwords for every account take seconds to generate and stop credential-stuffing attacks cold.
- **Verify Before You Trust**
If a request for money, credentials, or sensitive data feels urgent or unusual, confirm it through a second channel; call, don't reply.
- **Keep Software Updated**
Enable automatic updates on your devices; most exploited vulnerabilities already have a patch available.
- **Report, Don't Ignore**
Flag suspicious emails or calls to IT immediately, even if you're not sure; early reporting stops attacks before they spread.
- **Lock It When You Leave**
Lock your screen any time you step away, on campus or remote; physical access is still one of the easiest ways in.

Security isn't just IT's job. Every employee is a frontline defense.



● ● ● The Partner Behind Your Readiness

Make sure you have a partner to turn these threats into a manageable, ongoing program.

A partner should be equipped to combine compliance expertise with practical, everyday security guidance built specifically for your environment.



Partner Solutions

A layered program should combine training, phishing tests, pen testing, assessments, and incident response.



AI-Driven Attacks

- AI Assessment
- Advisory & vCISO Services
- Pen Testing



Ransomware

- Security Awareness & Compliance Training
- Incident Response Planning/Tabletop Exercises



Identity Attacks

- Compliance Assessments
- Verifiable Credentials



Evolved Phishing

- Phishing Simulator



Questions?



CAMPUSGUARD®

Contact Us



info@campusguard.com



www.campusguard.com

