Introductions

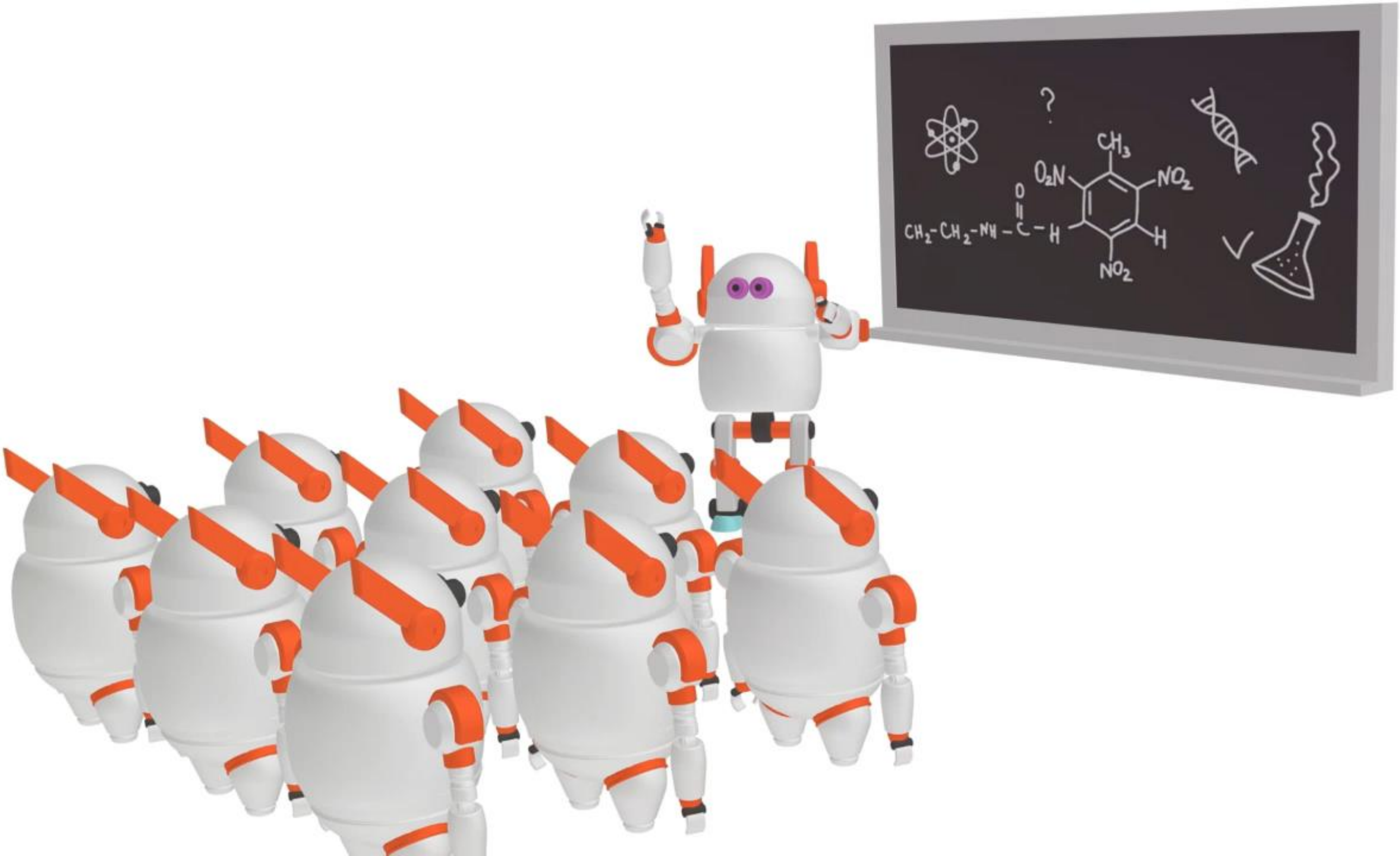
Adam Salameh - Speaker
Sales Executive, The Horton Group

Aaron Turner, CCIC - Speaker
Practice Group Leader – Management Liability and Cyber, The Horton Group

Michael Marassa, Ed.D, CETL
Chief Technology Officer, New Trier Township Dist. 203

Kevin Peronto - Moderator
Employee Management Coordinator, District 230

Artificial Intelligence – Real Life Capabilities


?
CH3
O2N
NO2
O
CH2-CH2-NH-C-H
H
NO2

Artificial Intelligence – How Schools Use

We may have asked Chat GPT this question…

1. **Personalized Learning:** AI algorithms can analyze student data to understand individual learning styles, strengths, and weaknesses. This information can then be used to personalize learning experiences, such as recommending specific resources or adjusting the pace of instruction to suit each student.

2. **Adaptive Learning Platforms:** Adaptive learning platforms use AI to dynamically adjust the difficulty level of content based on students' performance and mastery of concepts. This ensures that students are appropriately challenged and receive targeted support where needed.

3. **Automated Grading:** AI-powered tools can automate the grading of assignments, quizzes, and exams, saving teachers time and providing students with immediate feedback on their work.

Artificial Intelligence – Real Life Capabilities

AI makes us smarter?

1.**Content Creation:** AI can assist teachers in creating educational content, such as lesson plans, presentations, and interactive materials. For example, AI-generated content can be tailored to specific curriculum standards or learning objectives.

2.**Administrative Tasks:** AI can streamline administrative tasks such as scheduling, enrollment management, and resource allocation, freeing up educators' time to focus on teaching and student support.

3.**Virtual Reality (VR) and Augmented Reality (AR) Simulations:** AI-driven VR and AR simulations can create immersive learning experiences, allowing students to explore complex concepts in subjects like science, history, and geography.

Artificial Intelligence – Real Life Capabilities

AI makes us better plagiarizers?

1. **Student Support Services:** AI-powered systems can provide counseling support, career guidance, and mental health resources to students, offering personalized recommendations and interventions based on individual needs and preferences or adjusting the pace of instruction to suit each student.

2. **Adaptive Learning Platforms:** Adaptive learning platforms use AI to dynamically adjust the difficulty level of content based on students' performance and mastery of concepts. This ensures that students are appropriately challenged and receive targeted support where needed.

3. **Automated Grading:** AI-powered tools can automate the grading of assignments, quizzes, and exams, saving teachers time and providing students with immediate feedback on their work.

Artificial Intelligence is Not Only an Opportunity, but Also a Risk

Hackers can use ChatGPT or other LLMs to write perfectly crafted emails

Why does this matter?
How can hackers use LLMs to manipulate us?

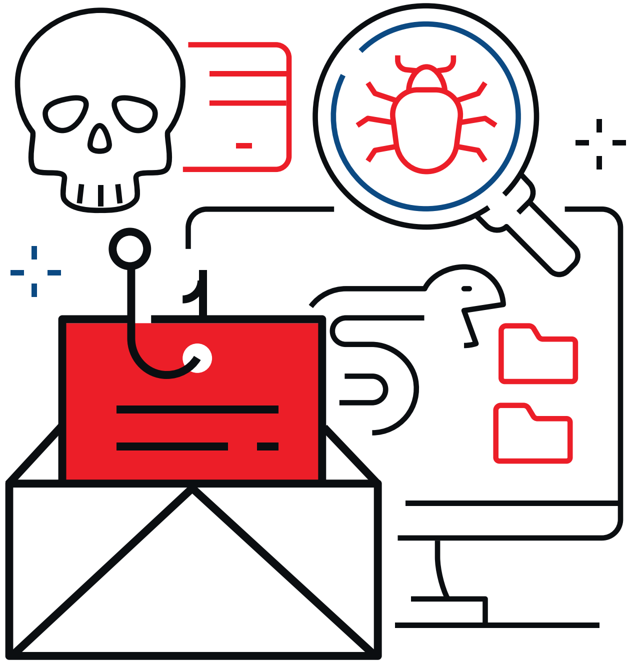
Example of Cyber Claim We See Regularly – Schools are Victims too

Someone in the school’s finance department gets what seems to be a legitimate email requesting a bank account change for a vendor

- The change seems legitimate so it’s processed.
- There is a pending invoice and it gets sent out the new account.
- 30 days later the vendor calls looking for payment
- The school’s finance department shows the paid invoice
- The vendor responds that the funds were not sent to their bank account

Just a Year or Two Ago, You Could Rely on Bad Grammar or Misspellings in Fraudulent Emails

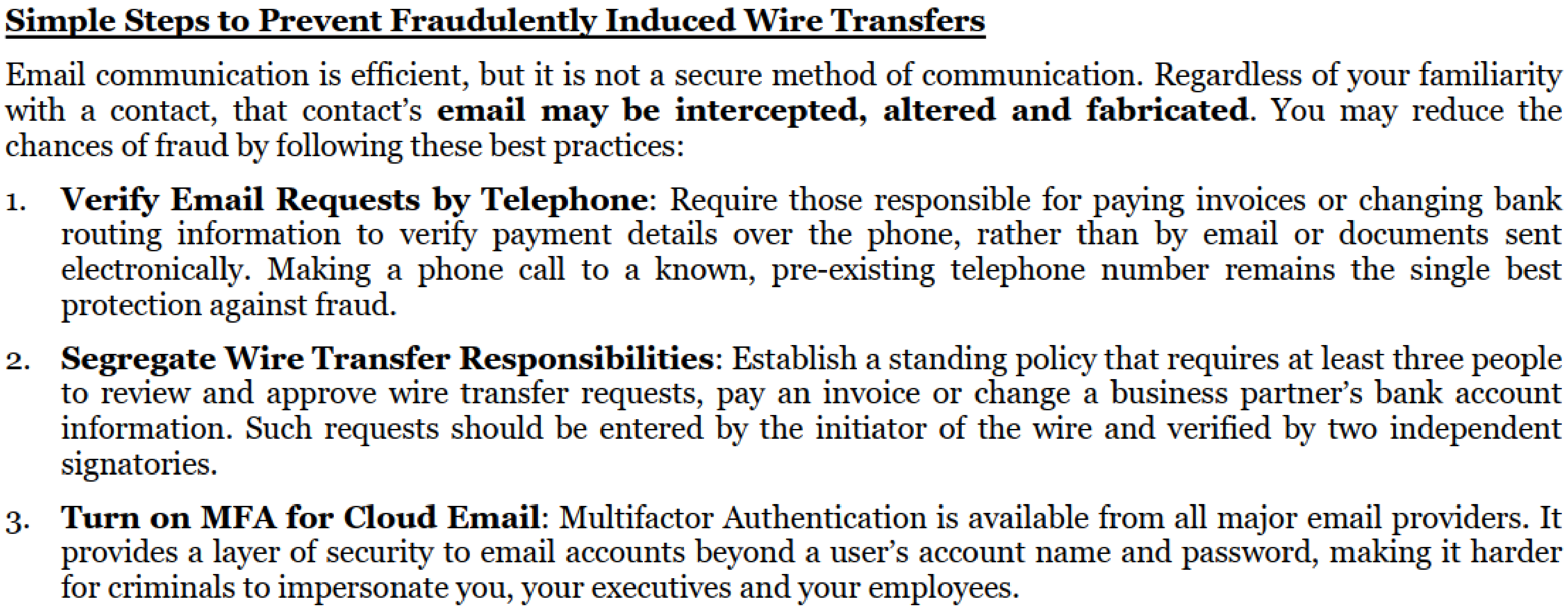
Now the Artificial Intelligence Large Language Models solve this "problem" for fraudulent actors



- LLMs can mimic language that is input into its database
- LLMs can craft responses in real time to keep conversations going
- LLMs eliminate an indication that you are corresponding with a foreign threat actor who may not have a great grasp on English

What is the Resolution?

See tips from Cyber Insurer Chubb to avoid these types of losses



Simple Steps to Prevent Fraudulently Induced Wire Transfers

Email communication is efficient, but it is not a secure method of communication. Regardless of your familiarity with a contact, that contact's **email may be intercepted, altered and fabricated**. You may reduce the chances of fraud by following these best practices:

1. **Verify Email Requests by Telephone**: Require those responsible for paying invoices or changing bank routing information to verify payment details over the phone, rather than by email or documents sent electronically. Making a phone call to a known, pre-existing telephone number remains the single best protection against fraud.
2. **Segregate Wire Transfer Responsibilities**: Establish a standing policy that requires at least three people to review and approve wire transfer requests, pay an invoice or change a business partner's bank account information. Such requests should be entered by the initiator of the wire and verified by two independent signatories.
3. **Turn on MFA for Cloud Email**: Multifactor Authentication is available from all major email providers. It provides a layer of security to email accounts beyond a user's account name and password, making it harder for criminals to impersonate you, your executives and your employees.

ChatGPT and Data Privacy

Many LLMs knowingly collect submitted data for the use of teaching the algorithm

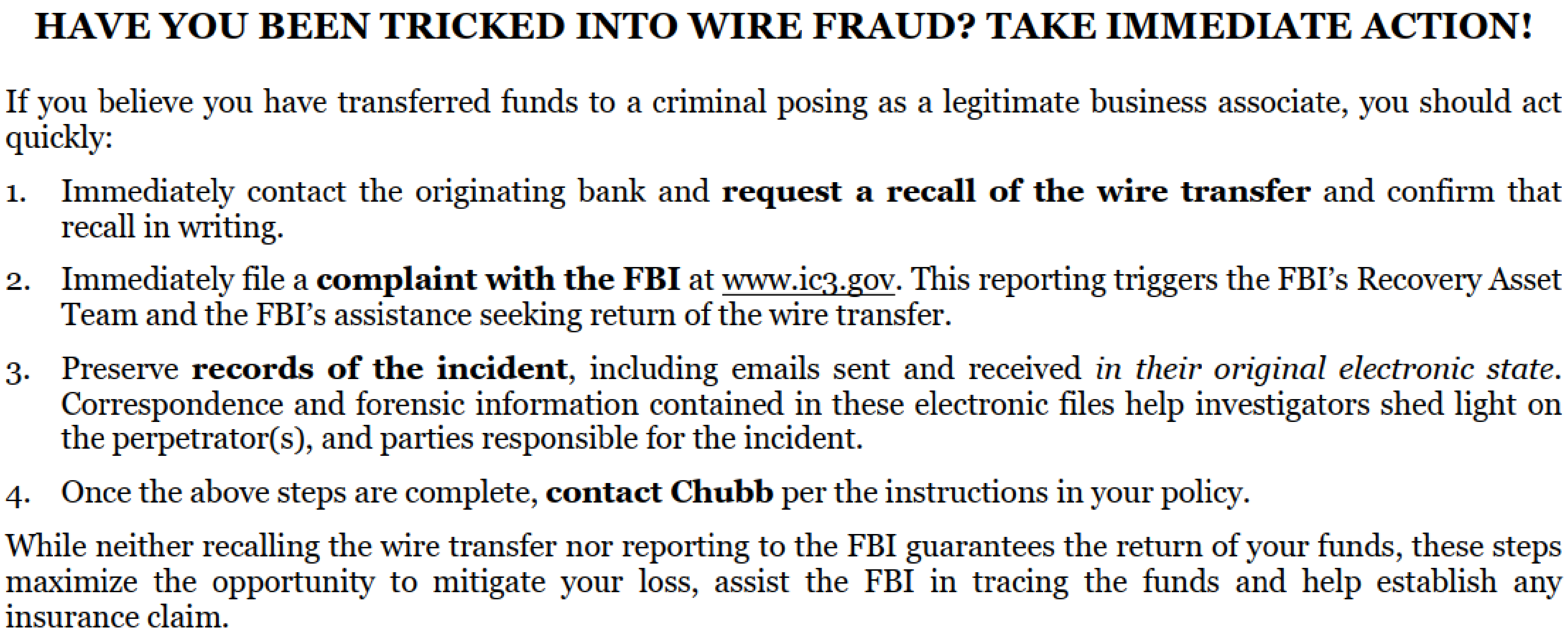
- After careful consideration of data privacy and security concerns and consultation with AI experts, we have decided to use Microsoft Bing Chat rather than ChatGPT as our AI chat platform for all staff

- Our decision is grounded in our commitment to safeguarding the privacy and confidentiality of both our students and staff. While both platforms offer valuable chat capabilities, Bing Chat offers enhanced data privacy features that align more closely with our requirements.

- Regardless of any AI tool you use, it is important that you never enter confidential or personally identifiable information into these AI large language models, especially student or staff information. As we heard during the Institute Day presentation, there is no guarantee that the privacy of such information will be protected. such as generating content, finding information, or having fun conversations. We encourage you to try it out and begin to learn how these tools can be used.

Additionally

See tips from Cyber Insurer Chubb if you've fallen victim to this type of crime:



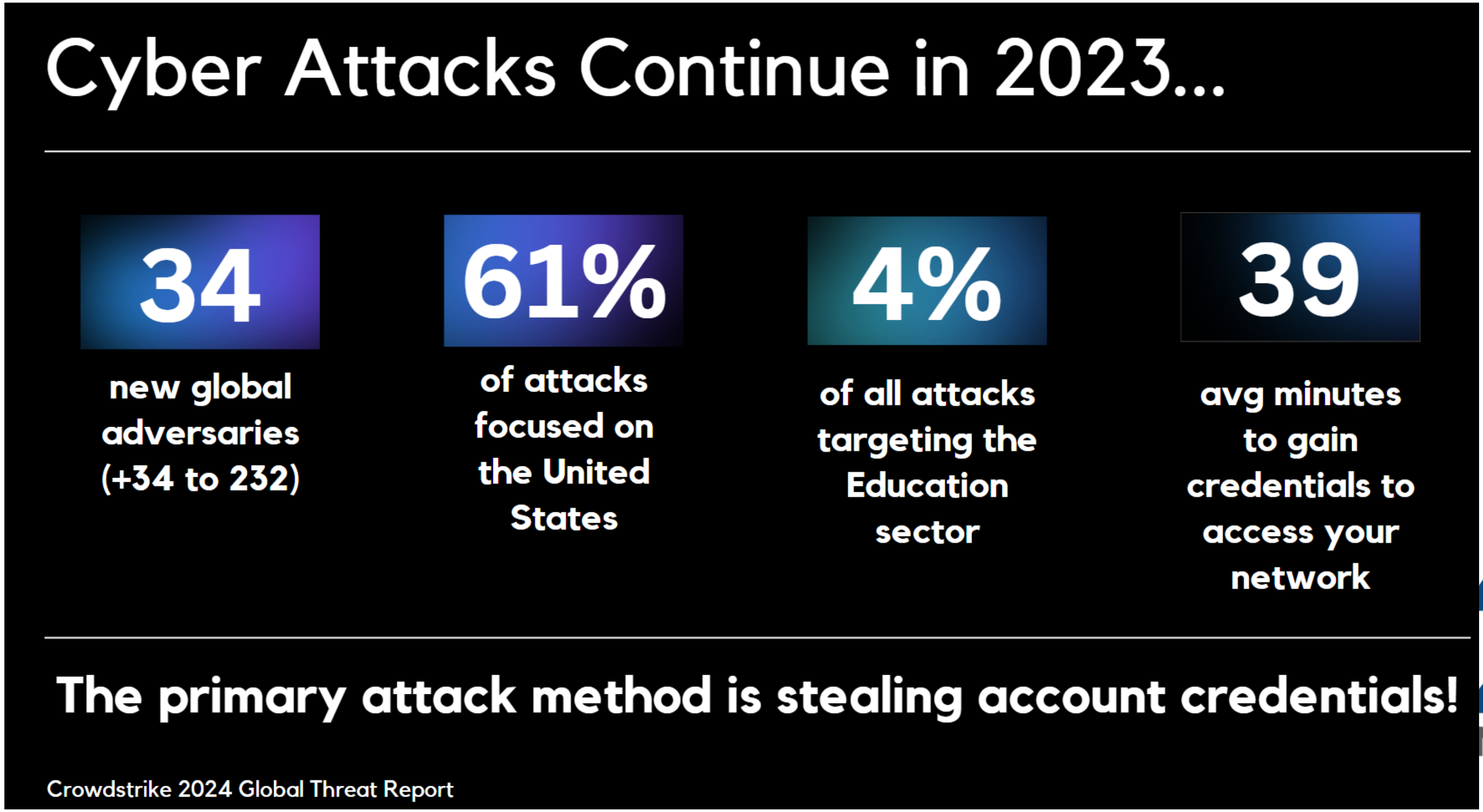
HAVE YOU BEEN TRICKED INTO WIRE FRAUD? TAKE IMMEDIATE ACTION!

If you believe you have transferred funds to a criminal posing as a legitimate business associate, you should act quickly:

1. Immediately contact the originating bank and **request a recall of the wire transfer** and confirm that recall in writing.
2. Immediately file a **complaint with the FBI** at www.ic3.gov. This reporting triggers the FBI's Recovery Asset Team and the FBI's assistance seeking return of the wire transfer.
3. Preserve **records of the incident**, including emails sent and received *in their original electronic state*. Correspondence and forensic information contained in these electronic files help investigators shed light on the perpetrator(s), and parties responsible for the incident.
4. Once the above steps are complete, **contact Chubb** per the instructions in your policy.

While neither recalling the wire transfer nor reporting to the FBI guarantees the return of your funds, these steps maximize the opportunity to mitigate your loss, assist the FBI in tracing the funds and help establish any insurance claim.

Technology Security



Cyber Attacks Continue in 2023...

34	61%	4%	39
new global adversaries (+34 to 232)	of attacks focused on the United States	of all attacks targeting the Education sector	avg minutes to gain credentials to access your network

The primary attack method is stealing account credentials!

Crowdstrike 2024 Global Threat Report

Zero Trust Approach

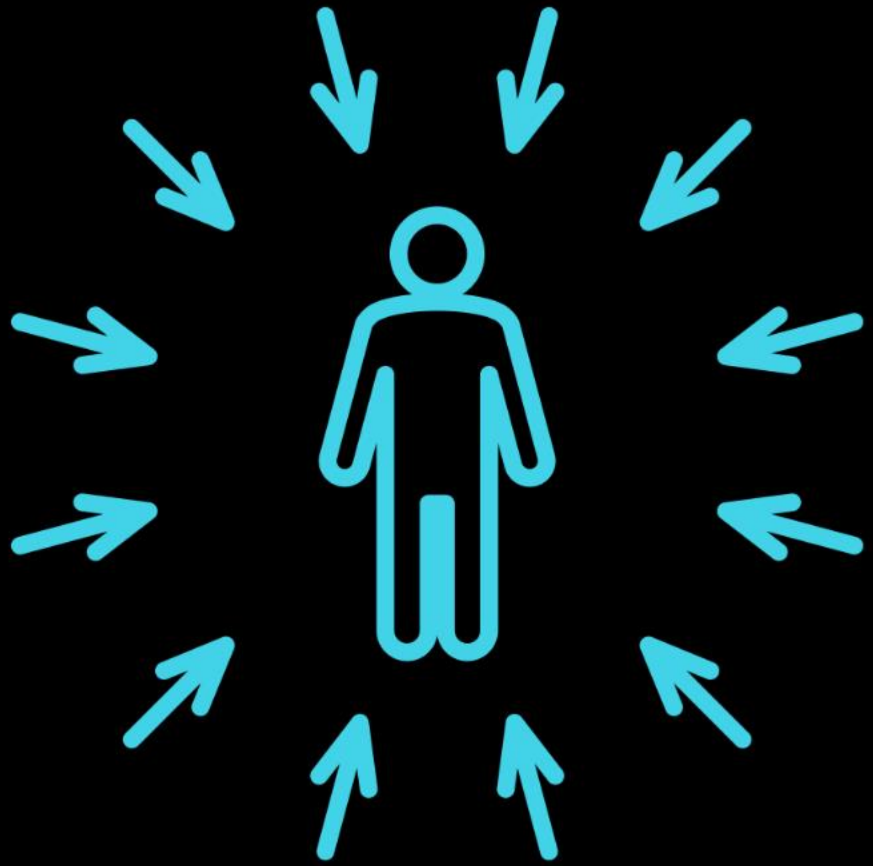
EVERYONE is a target – personally and professionally

Many cyber attacks use compromised login/password credentials to exploit your network

Ransomware and data extraction attacks are a business model for hackers

ZTA is standard in the corporate sector

Effective risk management...



Starts with the CTO

Time

Incident Response Plan

Importance of being prepared

Tabletop exercises with technical teams and administrative teams

Practice drills

Disaster recovery expectations

Recommended Resouces

- FRSecure
- Pileum
- Cosmopolis.io
- CISA

Money

Required Investment

District leaders must ensure adequate resources are available.

Security must be treated the same as other mandatory district expenses.

Considerations...

- Staffing
- Equipment and systems
- Outside experts

Attention

Shared Understanding

Foster a dialogue around security with your entire leadership team.

Shared focus, knowledge, and regular conversations are essential.

Consider CoSN's Trusted Learning Environment program – a great place to start.

Leadership must...

- Accept the circumstances
- Commit to the investment
- Increase preparedness

The CTO Cybersecurity Checklist

IDENTITY

- Require Complex Passwords/Passphrases
- Implement 2FA / MFA
- Require VPN Access for Non-MFA Systems/Software
- Role-based Access

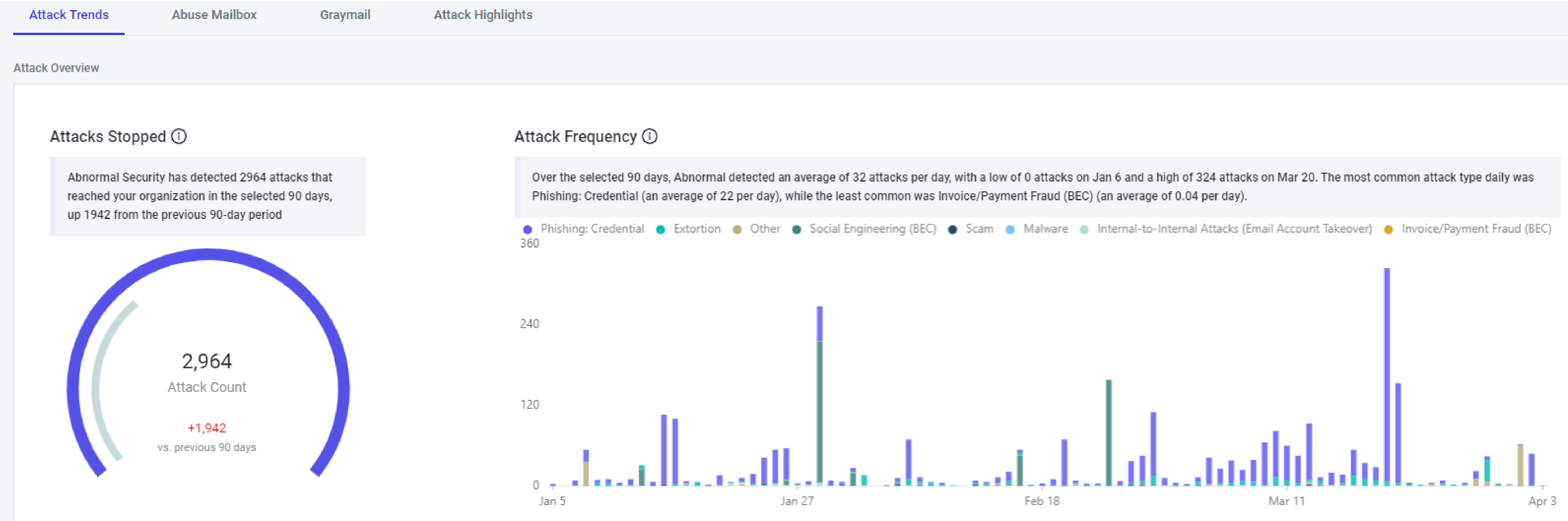
INFRASTRUTURE

- Software Systems Security Patching
- Endpoint Protection for Computers & Servers
- Data Evaluation & Exfiltration
- External Evaluation / Regular Audits
- Third Party Security Partnership
- vCISO / CISO

INCIDENCE RESPONSE

- Disaster Recovery
- Learning Continuity Plan
- Continuous Professional Development

Email Security – 90 day lookback



Attacks Stopped ⓘ

Abnormal Security has detected 2964 attacks that reached your organization in the selected 90 days, up 1942 from the previous 90-day period

Attack Frequency ⓘ

Over the selected 90 days, Abnormal detected an average of 32 attacks per day, with a low of 0 attacks on Jan 6 and a high of 324 attacks on Mar 20. The most common attack type daily was Phishing: Credential (an average of 22 per day), while the least common was Invoice/Payment Fraud (BEC) (an average of 0.04 per day).

● Phishing: Credential
● Extortion
● Other
● Social Engineering (BEC)
● Scam
● Malware
● Internal-to-Internal Attacks (Email Account Takeover)
● Invoice/Payment Fraud (BEC)
360
240
120
0
Jan 5
Jan 27
Feb 18
Mar 11
Apr 3

Questions and Answers

We thank you for your time!

Presenters:

MODERATOR INFO:

Kevin Peronto, EMS Coordinator; District 230
(708) 745-5219; kperonto@d230.org

PANELISTS INFO:

Adam Salameh, Sales Executive; The Horton Group
(123) 456-7890; email

Aaron Turner, Practice Group Leader; The Horton Group
(312) 989-1404; aaron.turner@thehortongroup.com

Michael Marassa, Ed.D. CTO; New Trier 203
(847) 784-2360; marassam@nths.net