EDUCATING END USERS ON EVOLVING PHISHING ATTACKS

CAMPUSGUARD®

October 30, 2024

Katie Johnson, PCIP
Manager, Operations Support

AGENDA

INTRODUCTION

CAMPUSGUARD OVERVIEW

PHISHING STATISTICS

REASONS USERS CLICK

COMMON ATTACKS

STRATEGIES FOR TRAINING

PREVENTION

CAMPUSGUARD®

CAMPUSGUARD OVERVIEW

InfoSec

- IT Security Assessments
- Pen Testing
- Vulnerability Scans
- Social Engineering
- Phishing Exercises
- Policy Reviews
- Incident Response Plan Testing
- Vendor Reviews

Compliance

- PCI DSS
- GLBA
- CMMC
- GDPR
- HIPAA
- ACH/Nacha
- FERPA
- FACTA Red Flags
- LADMF

Other Services

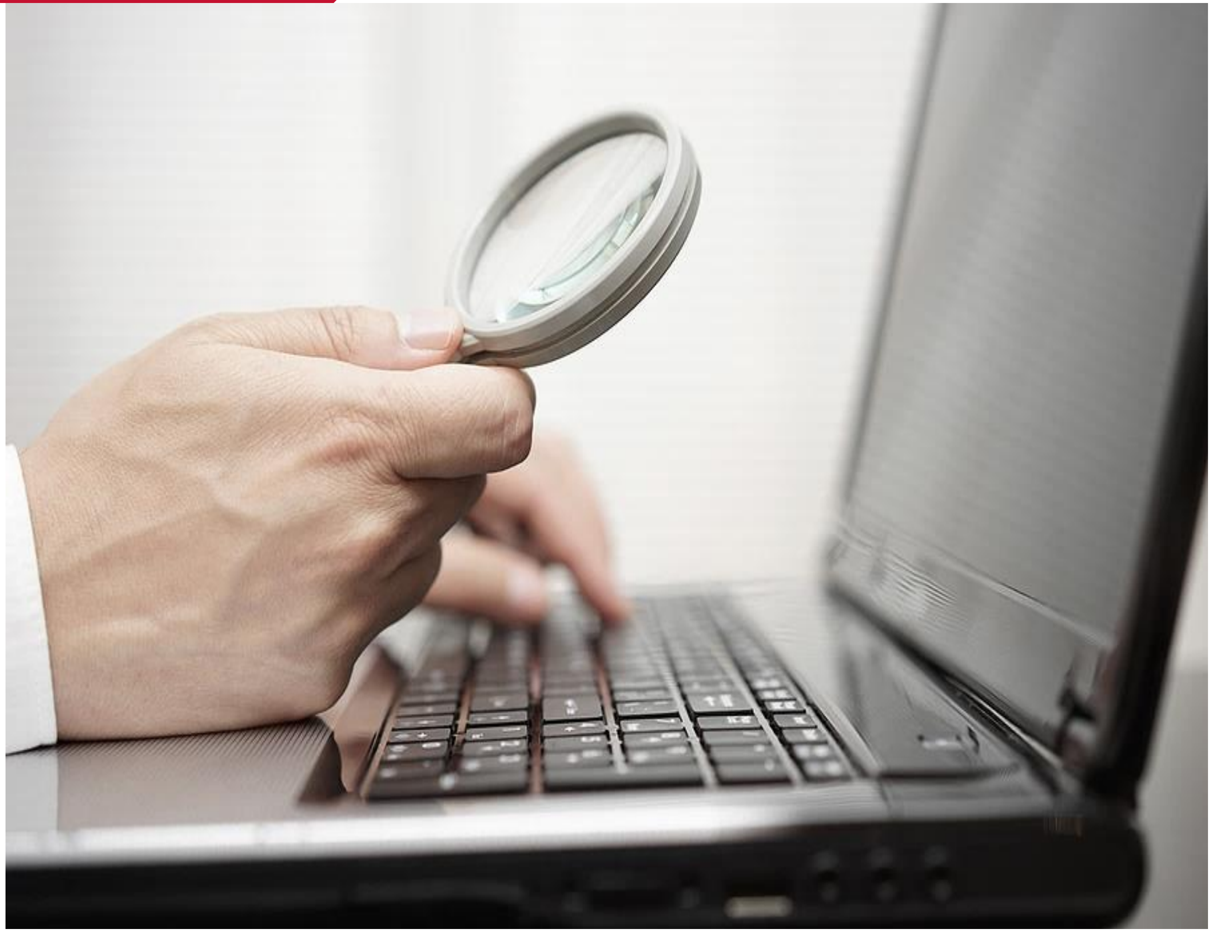
- Annual Support Services
- Customer Compliance Portal
- Online Training
- Treasury Solutions

WHAT IS PHISHING?

CYBERATTACK THAT ATTEMPTS TO TRICK PEOPLE INTO REVEALING SENSITIVE INFORMATION, SUCH AS PASSWORDS, ACCOUNT INFORMATION, OR CREDIT CARD NUMBERS.

AN INCREASING RISK

- **96%** of phishing attacks come from email
- Initial action in **24%** of data breaches is stolen credentials
- **94%** of organizations reported experiencing phishing attacks
- Over **3.4 billion** phishing emails sent daily
- Phishing emails have increased **1,265%** since the release of ChatGPT

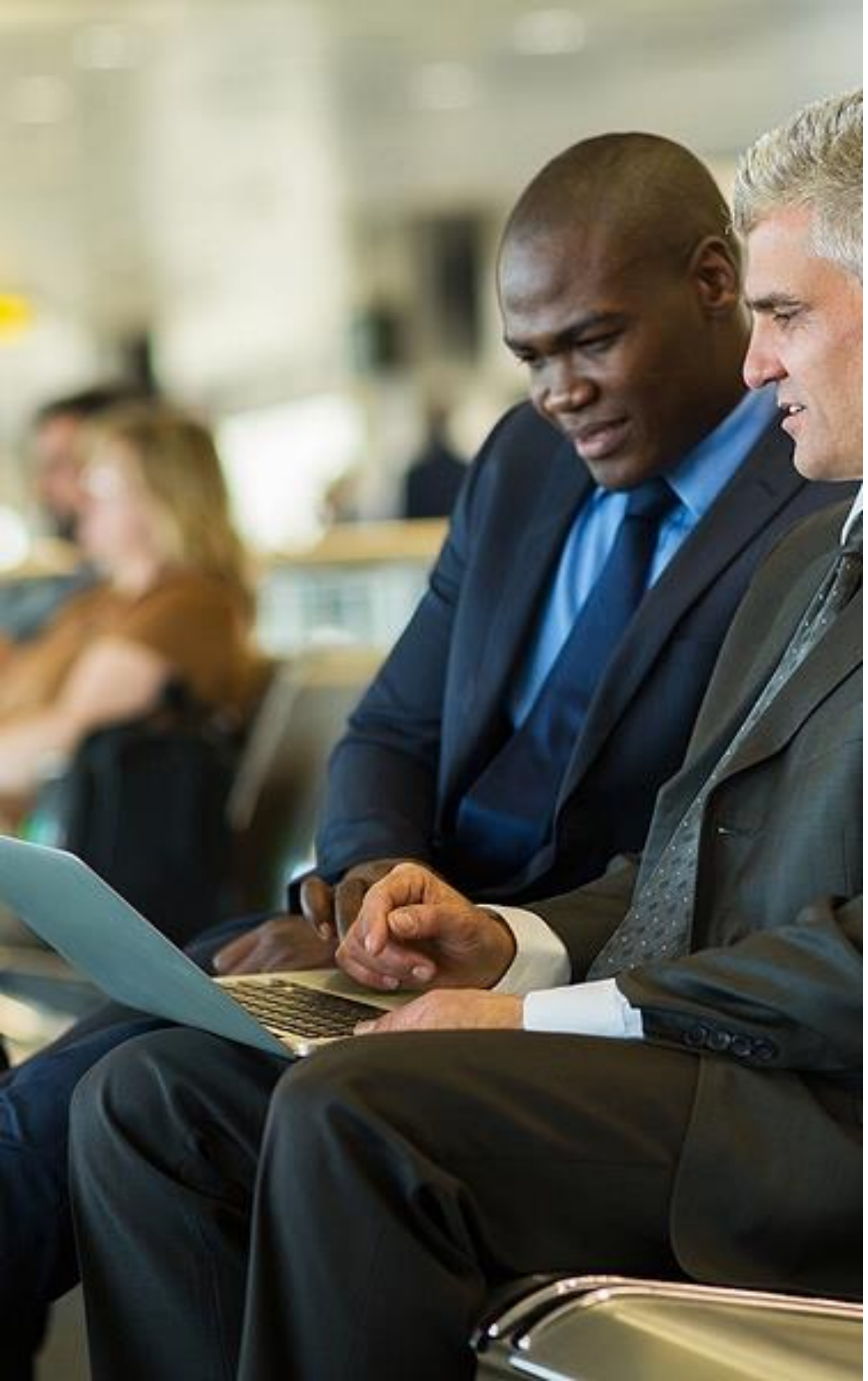


ESCALATING CONSEQUENCES

- Breaches caused by phishing cost organizations an average of $4.88 million
- IT teams spend about 28 minutes and $31 to address a single phishing email
- A typical organization with 25 IT and security professionals may spend over $1M annually to manage phishing attacks
- Phishing incidents have also contributed to a notable increase in cyber insurance premiums

END USERS

NO MATTER HOW MUCH TIME, MONEY, AND TECHNOLOGY AN ORGANIZATION INVESTS INTO THEIR CYBERSECURITY PROGRAM, IF A USER CLICKS A LINK OR FAILS TO FOLLOW AN ESTABLISHED PROCEDURE, A COMPROMISE IS MORE LIKELY TO OCCUR



WHY USERS CLICK

- Perceived Authority/Trustworthy Sources
- Curiosity/FOMO
- Urgency
- Situational Factors
- Lack of Awareness

19% of end users admit to clicking on links or downloading attachments from contacts they didn't know, with 9% providing credentials to an untrustworthy source

RESPONDING TO PHISHING

“Hey! This is an active email account!”

Consequences:

- Download malware/ransomware
- Expose credentials

Additional Risks:

- Information from email signatures
- Out of office replies
- Training your email system

COMMON ATTACKS

EVOLUTION OF PHISHING

PHISHING EMAILS

Hackers use a variety of tactics to lure users into doing what they want through email:

- Pressure/Urgency
- Action needed (expiring account)
- Access file in DropBox
- DocuSign request
- Pay an invoice
- Unusual account activity
- Process a refund
- Send sensitive information (tax information)
- Restart a service (Netflix, Amazon, etc.)

SPEAR PHISHING

Targets a specific employee, or group of employees, within an organization.

Organizations have lost thousands of dollars when a spear phishing email, fraudulently written as if it were from the CEO, is sent to a staff member requesting an urgent transfer of funds and the employee complied.

Prevention:

- Verify requests
- Establish procedures
- Separate job duties

SUPPLY CHAIN PHISHING

Attack that uses phishing emails to gain access to a third-party supplier or vendor’s customers.

Prevention:

- Beware of attacks to send payments to new accounts
- Call the vendor/partner directly to confirm payment information

VOICE PHISHING

Attackers use phone calls to manipulate users into revealing sensitive information.

Beware of these common warning signs:

- Unsolicited calls asking for personal or financial information
- Calls from unknown numbers
- High pressure/urgent demands for immediate action or access

Prevention:

- Verify the caller’s identity
- Test help desk procedures

SMISHING

Phishing attack conducted via SMS or text messages. Beware of requests for personal information and/or unknown links.

Prevention:

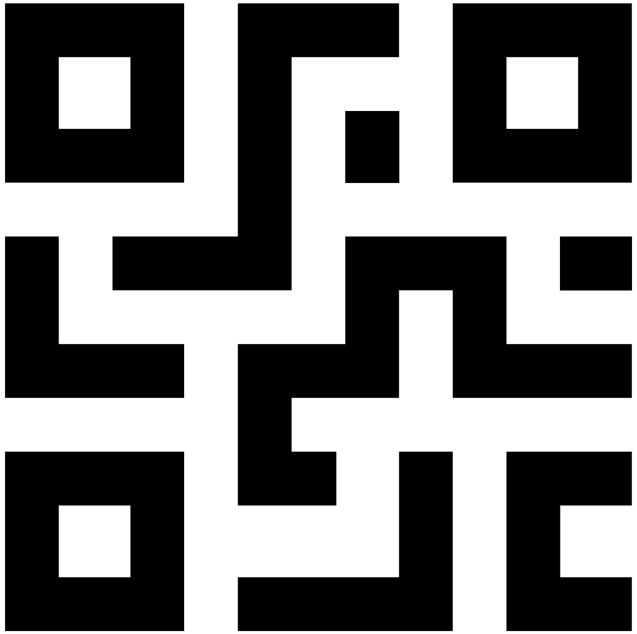
- Verify the sender before taking any action

QUISHING

QR code phishing is when hackers post physical images of fake QR codes in high traffic locations or send them via email, embedded in PDF documents, or within text message.

Prevention:

- Always verify the QR code source before visiting the link or entering



SOCIAL MEDIA

Using social media platforms for phishing attacks

Common techniques include:

- Fake login pages
- Malicious links or downloads within posts
- Impersonation/fake profiles

Prevention:

- Be cautious of requests on social media
- Review and adjust social media security and privacy settings
- Limit personal information
- Disable location tracking

ARTIFICIAL INTELLIGENCE

Deepfake phishing in which hackers can create realistic, but fake audio, video, or images to trick people into giving away sensitive information.

Prevention:

- Exercise due diligence
- Follow multi-step authentication processes
- Verify requests before transferring funds

POLL

ONGOING TRAINING

DON'T JUST CHECK THE BOX

IDENTIFYING RED FLAGS

Is the email addressed to them/personalized?

What is the sender or caller asking the user to do?

Is there a request for sensitive or personal information like passwords, payment card numbers, SSNs?

Are they asking for sensitive information about other individuals or colleagues?

Does the message ask them to immediately open an attachment they weren't expecting?

Does the message ask you to click a link to visit another site or provide information?

Were you not expecting an email or call of this nature (e.g. password reset, travel confirmation, etc.)?

Do the URLs not match the domain?

STRATEGIES FOR TRAINING

- Not a once a year check the box activity
- Repeated, micro training at regular intervals
- Ensuring employees have and remember to take time to think about if a request seems legitimate
- Keep up to date with the latest scams
- Provide updates and alerts
- Targeted, tailored training

REAL-WORLD EXAMPLES

Finishing kick
Hackers hit
"What's been taken is bits of data that the
put together into an identity."

Sharing examples of phishing seen in the real-world can be helpful.

- Student Loan Forgiveness
- Scholarships/Grants
- Potential Job or Internship Opportunities
- Election Updates
- Donations to Natural Disasters

MIX IT UP

Reinforce awareness training through different mediums:

- Online training
- Posters/infographics
- Email campaigns
- Newsletters
- Social media

PREVENTION

LIMIT THE RISK OF PHISHING

REPORTING PHISHING

Continuous reminders to report suspicious messages

Prevention:

- Be sure all staff know how and where to report fraudulent emails or phishing attempts
- Make it easy to report
- Offer possible incentives for users who successfully identify phishing emails
- Encourage users to report if they think they might have clicked/responded

PHISHING TESTS

Conduct Phishing Tests – monitor improvement from users

- Complement to awareness training
- Increase employee engagement
- Helps analyze if training is working
- Identify potential areas of weakness
- Educate users on the different methods used by attackers
- Provide immediate feedback to users

- Track results over time in phishing click rates, employee engagement, increases in reporting, and reduction in system downtime, decrease in help desk requests

POLL

TOOLS FOR PREVENTION

Top-level buy-in for training is critical.

It is also helpful to share what additional steps your organization is taking to limit the risk of phishing and other cyberattacks.

- Antivirus software
- Antispam filters
- Regular browser and software updates
- Multi-factor authentication (MFA)
- Network penetration testing
- Limiting employee directory information
- Align training with policy

COMPLIANCE ON YOUR SIDE

HIPAA: The HIPAA Security Rule requires covered entities to implement a security awareness training program. This includes training on how to identify phishing emails and prevent data breaches.

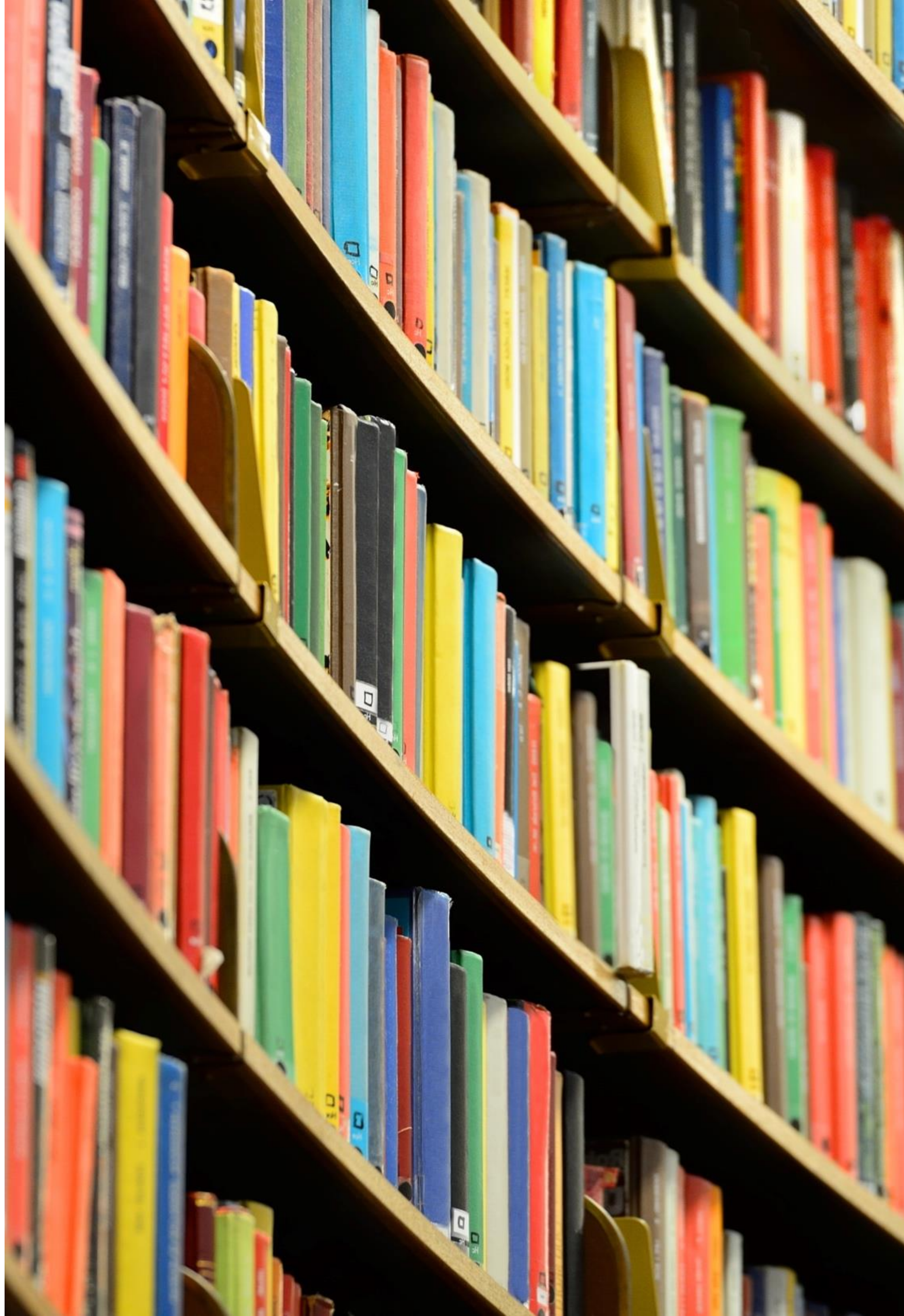
Gramm-Leach-Bliley Act (GLBA): Requires training on how to recognize and respond to fraud and identity theft schemes, computer security, and how to properly dispose of customer information.

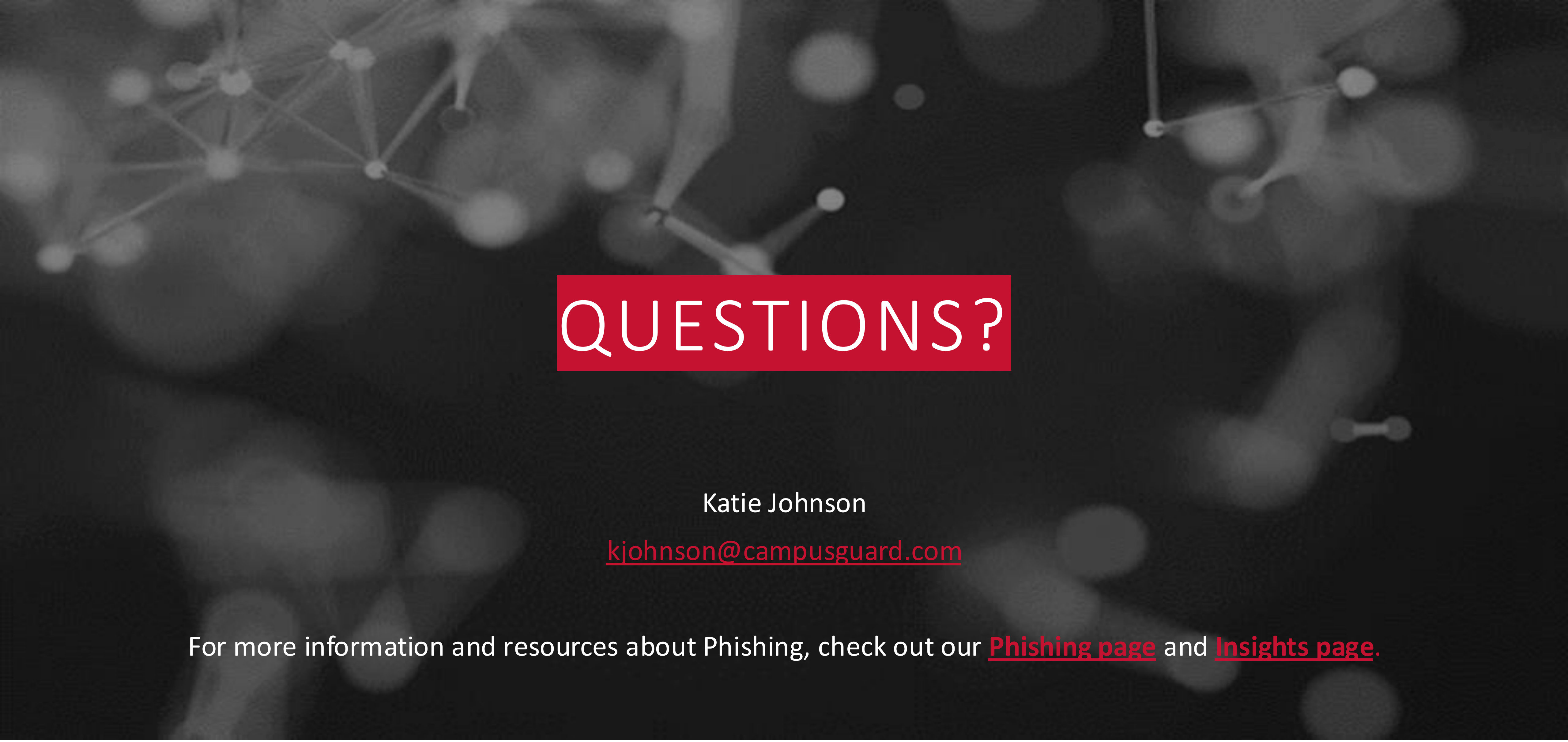
PCI DSS: Requires annual security awareness training; PCI DSS version 4.0 specifically mentions training users on social engineering and phishing.

Red Flags and GDPR: Require security awareness training within the organizational programs.

RESOURCES

- Phishing Infographic
- Student Phishing Module – Request by October 31!
- CampusGuard Phishing Awareness Training
- Have I Been Pwned? Has your email address been used in a data breach?
- Oh, Behave! Annual Cybersecurity Attitudes and Behaviors Report 2024-2025
- 2024 EDUCAUSE Horizon Report: Cybersecurity and Privacy Edition
- The latest news to help you stay informed of evolving cyber threats:
  - CampusGuard Threat Intel Updates Email – Sign up!
  - Security Week
  - Security Weekly Podcast
  - KrebsonSecurity
  - Bleeping Computer





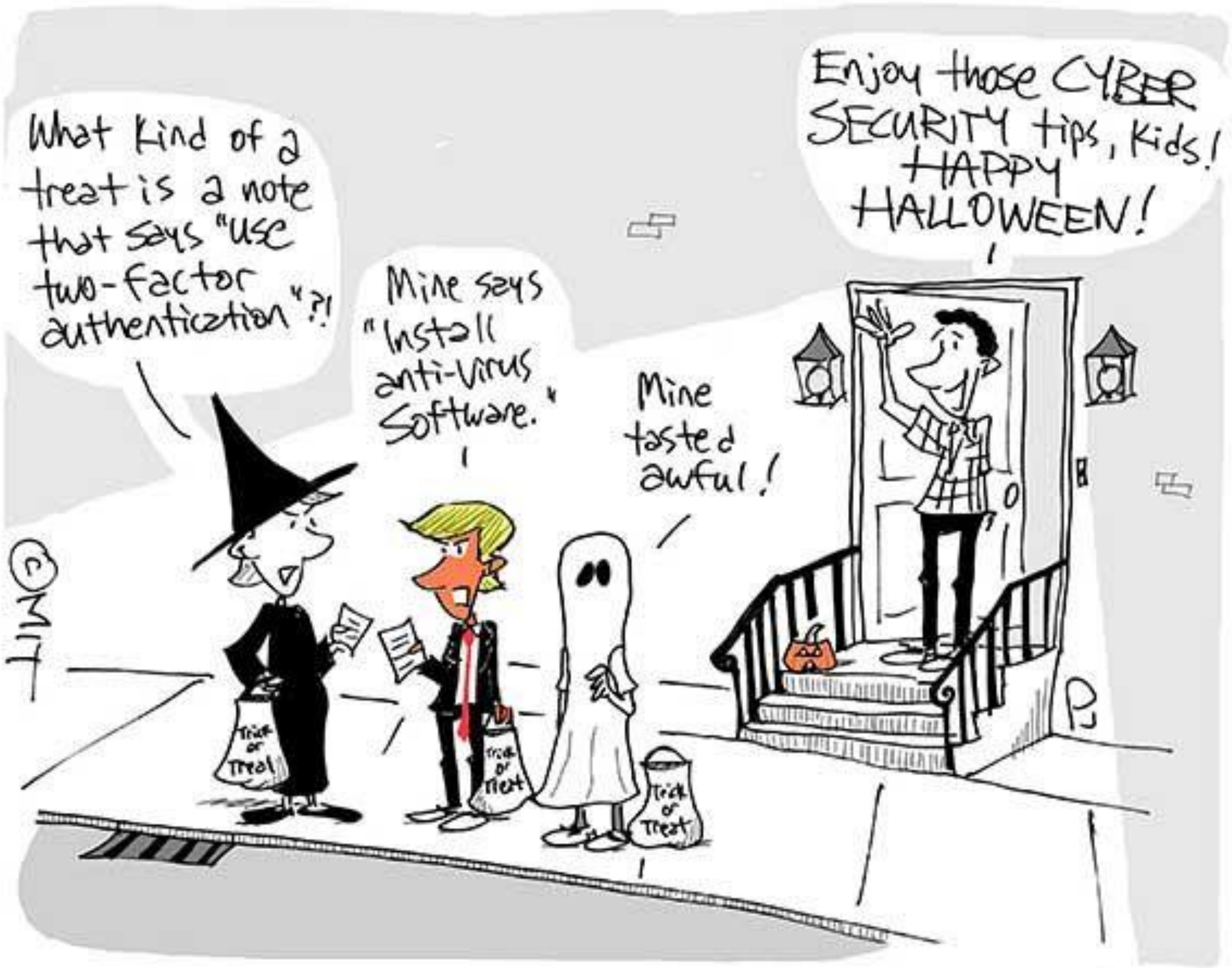
QUESTIONS?

Katie Johnson

kjohnson@campusguard.com

For more information and resources about Phishing, check out our **Phishing page** and **Insights page**.

HAPPY HALLOWEEN!


What kind of a treat is a note that says "use two-factor authentication"?!
Mine says "Install anti-Virus Software."
Mine tasted awful!
Enjoy those CYBER SECURITY tips, Kids! HAPPY HALLOWEEN!
Trick or Treat
Trick or Treat
Trick or Treat
©MIT

CAMPUSGUARD®