# TEST YOUR TEAM BEFORE THE ATTACKERS DO
# CAMPUSGUARD PHISHING SIMULATOR

CAMPUSGUARD®

May 13, 2026

Katie Johnson, PCIP
AVP, Product
Senior Manager, Operations Support

# AGENDA

CAMPUSGUARD AWARENESS TRAINING

COMMON PHISHING ATTACKS

WHY PHISHING WORKS

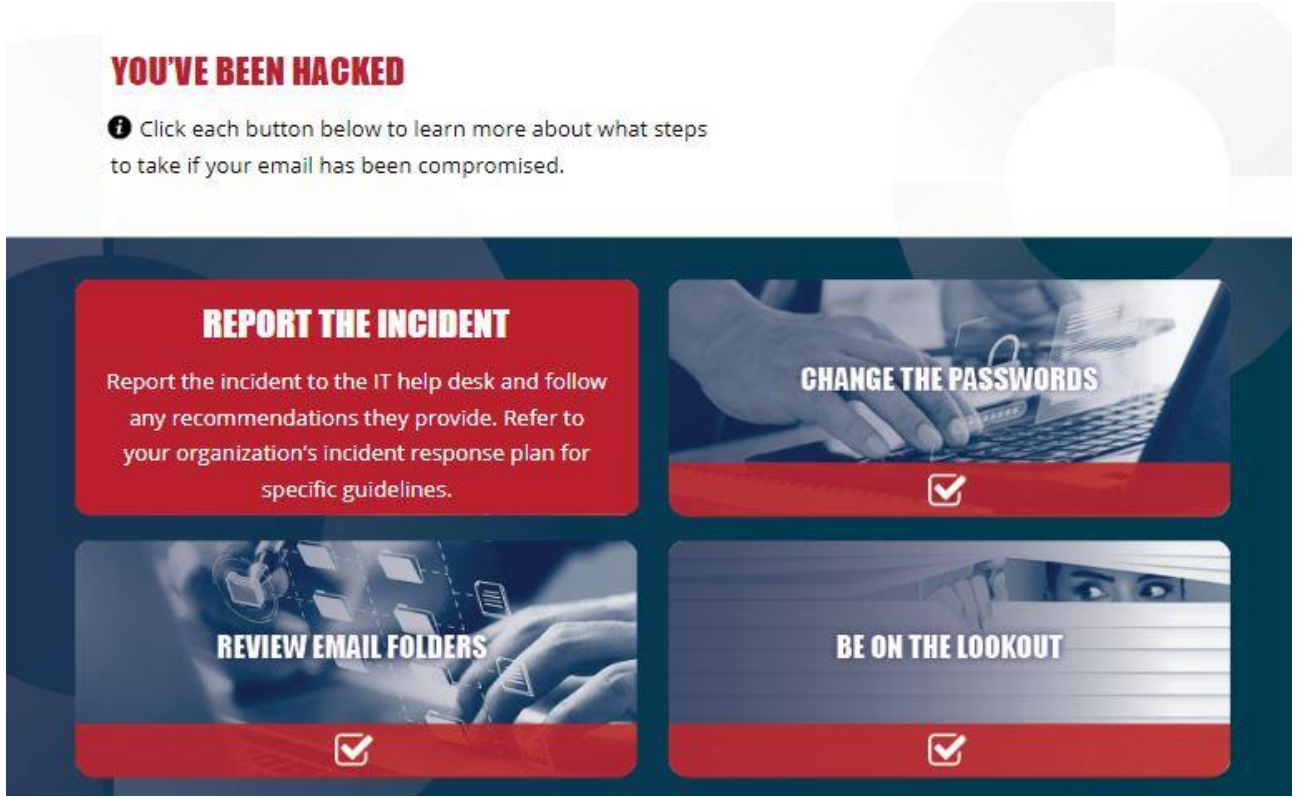
PREVENTION

PHISHING SIMULATOR DEMO

QUESTIONS AND FEEDBACK

CAMPUSGUARD

# INFORMATION SECURITY AND COMPLIANCE AWARENESS TRAINING




- Providing online training since 2016
- All content created by credentialed CampusGuard experts
- All courses updated annually
- Delivered in SCORM format or hosted

CAMPUSGUARD

# CAMPUSGUARD COURSE LIBRARY

## Information Security Awareness

- Information Security
- Data Classification and Protection
- Social Engineering
- Email Security
- Password Management
- Remote Work Environments
- Incident Management
- Internal Controls
- Security Components
- Physical Security
- Cyber Crime
- Internet Usage
- Security at Home
- Data Breaches and Compromise
- Third-Party Risks
- AI Risks
- Travel Security
- Help Desk Security

## Phishing Awareness

- Phishing 101
- Rules for Spotting Phishing
- Phishing Practice
- Student Phishing

## PCI DSS Compliance

- PCI for Merchants
- PCI for IT
- PCI for Executives
- PCI for Students/Cashiers
- PCI DSS v4.0 Overview
- Device Inspections

## FERPA

- FERPA Overview
- Common Scenarios

## GLBA

- Introduction to GLBA
- Privacy Rule and Safeguards Rule

## Federal Tax information (FTI)

- Safeguarding FTI

## FACTA Red Flags

- FACTA Red Flags

## HIPAA Compliance

- Introduction to HIPAA
- Protected Health Information
- Who is Required to Comply with HIPAA
- HIPAA Privacy Rule
- HIPAA Security Rule
- Security of PHI
- Data Breaches and Reporting
- HIPAA Compliance

# EXPANDED OFFERING

## Information Security Awareness

- Cryptocurrency Risks
- Identity Theft
- Insider Threats
- Managing AI Risks
- Database/System Admin
- Web/Application Development
- New Employee
- Board/Executives
- Personally Identifiable Information*
- Identity and Access Management*
- Using AI the Right Way*

## CMMC/CUI/Research Data

- CMMC Overview
- Accessing and Safeguarding CUI
- Protecting Sensitive and Regulated Data

## GDPR

- GDPR Overview
- Complying with GDPR

## Data Privacy

- Introduction to Data Privacy
- Data Privacy Best Practices
- Common Scenarios
- Privacy Regulations at a Glance
- Impact of Emerging Technologies on Privacy

## Payments Security*

- Cash Handling
- Check Handling
- Revenue Approval
- Electronic Payments
- Evolving Payment Technologies
- Common Payment Fraud Examples
- Payment Fraud in Higher Ed
- Bank Secrecy Act/Anti-Money Laundering

## Student Information Security*

- Phishing/Social Engineering
- Keeping personal information private
- Understanding and using privacy settings
- Password Security
- Respectful behavior online
- Online scams/preventing fraud
- Securing personal devices
- Managing your digital footprint
- Safe social media habits

*currently in development

# I SHOULDN’T HAVE CLICKED THAT…

# POLL QUESTION

- How confident are you that your employees can spot phishing emails?

CAMPUSGUARD

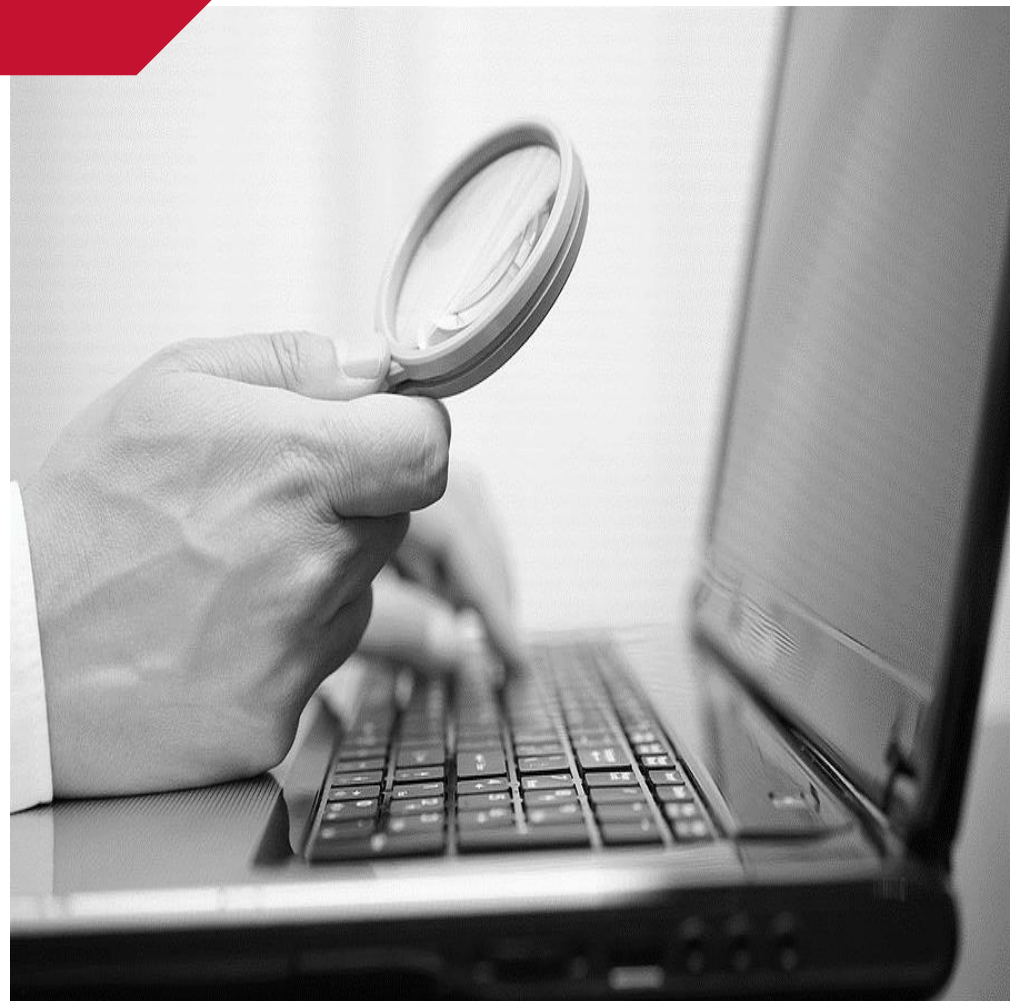
# HIGHER ED EXAMPLE

- A staff member in the bursar's office receives an email that looks like it's from IT—branding is perfect, tone is professional. It says their session expired and they need to log back in.
- They click. They enter credentials. Nothing seems wrong.
- Within 30 minutes, an attacker is logging into their real account, setting up forwarding rules, and targeting student refund processes.

CAMPUSGUARD

# ANATOMY OF AN ATTACK

1. **RECON:** attackers research your institution or staff.
2. **DELIVERY:** sends phishing email or message.
3. **ENGAGEMENT:** someone clicks.
4. **EXPLOITATION:** credentials captured or malware installed.
5. **IMPACT:** financial fraud, data exposure, or ransomware entry.



CAMPUSGUARD

# INCREASING COSTS

Breaches caused by phishing cost organizations an average of $4.88 million.

Business Email Compromise (BEC) attacks average $150,000 per incident.

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

CAMPUSGUARD


# ESCALATING CONSEQUENCES

- Financial loss (tuition funds re-directed, vendor payment fraud)
- Operational disruption (systems taken offline, classes impacted)
- Regulatory exposure (FERPA violations, GLBA concerns for financial data)
- Research data theft
- Reputational damage (student and donor trust)

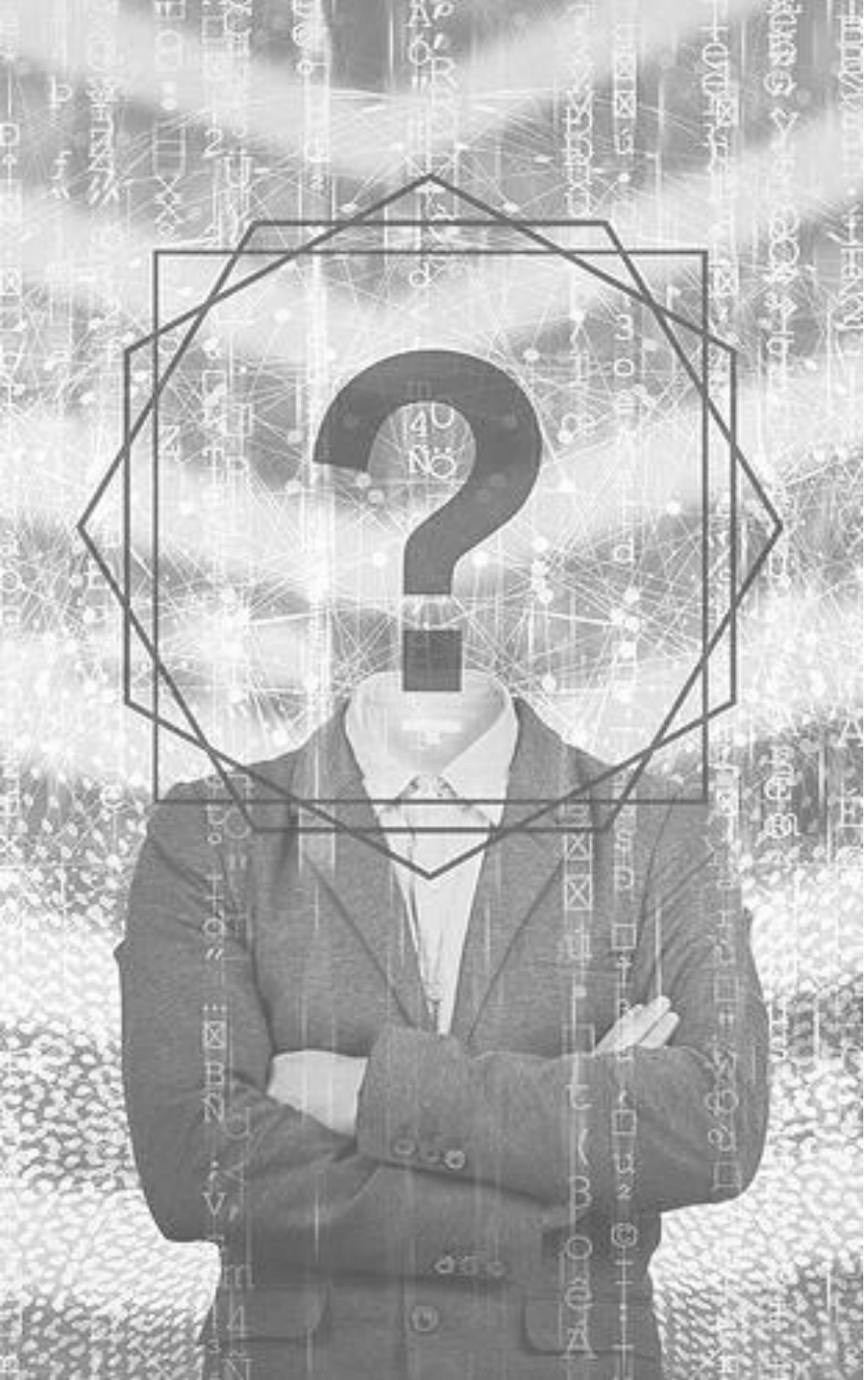
**Faculty are high value targets – public profiles, access to research data, grants/funding, student information.**

**Phishing can expose pre-publication research, intellectual property, federal contract data.**

CAMPUSGUARD

# EVOLUTION OF PHISHING

IT’S NOT GOING AWAY.



# EVOLUTION OF PHISHING

- No longer obvious or poorly written emails
- Personalized targeting
- Multi-channel (email, SMS, QR codes, deepfakes, etc.)

**Phishing emails have increased 1,265% driven by generative AI. Attacks are 192x faster, with AI reducing effective campaign creation time from 16 hours to 4 minutes.**

CAMPUSGUARD

# WHY PHISHING WORKS

**Phishing attacks don't succeed because of technical flaws in your systems. They succeed because they exploit human behavior.**

- **Pressure/Urgency**
  - Action needed (expiring account, process a refund)
- **Authority**
  - This is from the Dean or IT/Security
- **Familiarity**
  - Access file in LMS, DropBox, DocuSign request
- **Curiosity**
  - Updated student list, salary adjustment

*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*

# PREVENTION

LIMIT THE RISK OF PHISHING

# IDENTIFYING RED FLAGS

- Is the email addressed to you/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 you to immediately open an attachment that you 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?

CAMPUSGUARD

# 5 SECOND RULE

**Before clicking…**

- Check sender
- Hover over links
- Ask: Was I expecting this? Is this urgent or unusual? Does it make sense?

**A small pause can stop a huge percentage of attacks.**


# REPORTING PHISHING

- Be sure all staff know how and to whom to report fraudulent emails or phishing attempts. Reminders are good.
- It's okay to be unsure.
- Make it easy to report.
- Reporting is better than ignoring or deleting!
- Encourage users to report if they think they might have clicked/responded.
- Offer possible incentives for users that successfully identify phishing emails.

CAMPUSGUARD

# POLL QUESTION

- How do you currently measure phishing risk?

CAMPUSGUARD

# PHISHING TESTS

**Conduct Phishing Tests – monitor improvement from users**

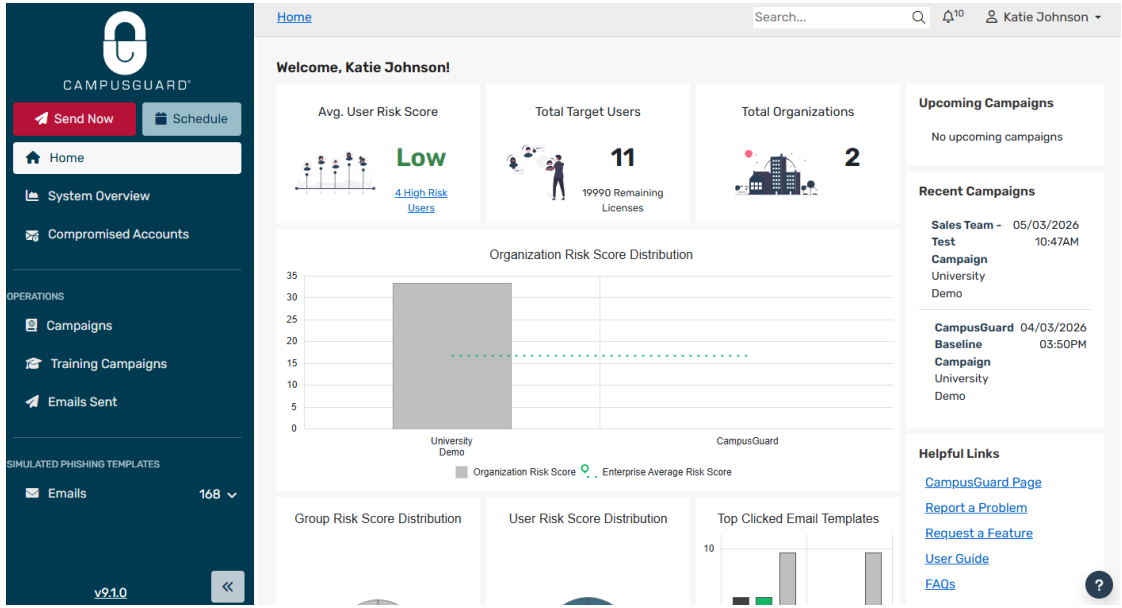
- Educate users on the different methods used by attackers
- Increase employee engagement
- Identify potential areas of weakness
- Provide immediate feedback to users
- Helps analyze if training is working

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

# CAMPUSGUARD PHISHING PLATFORM

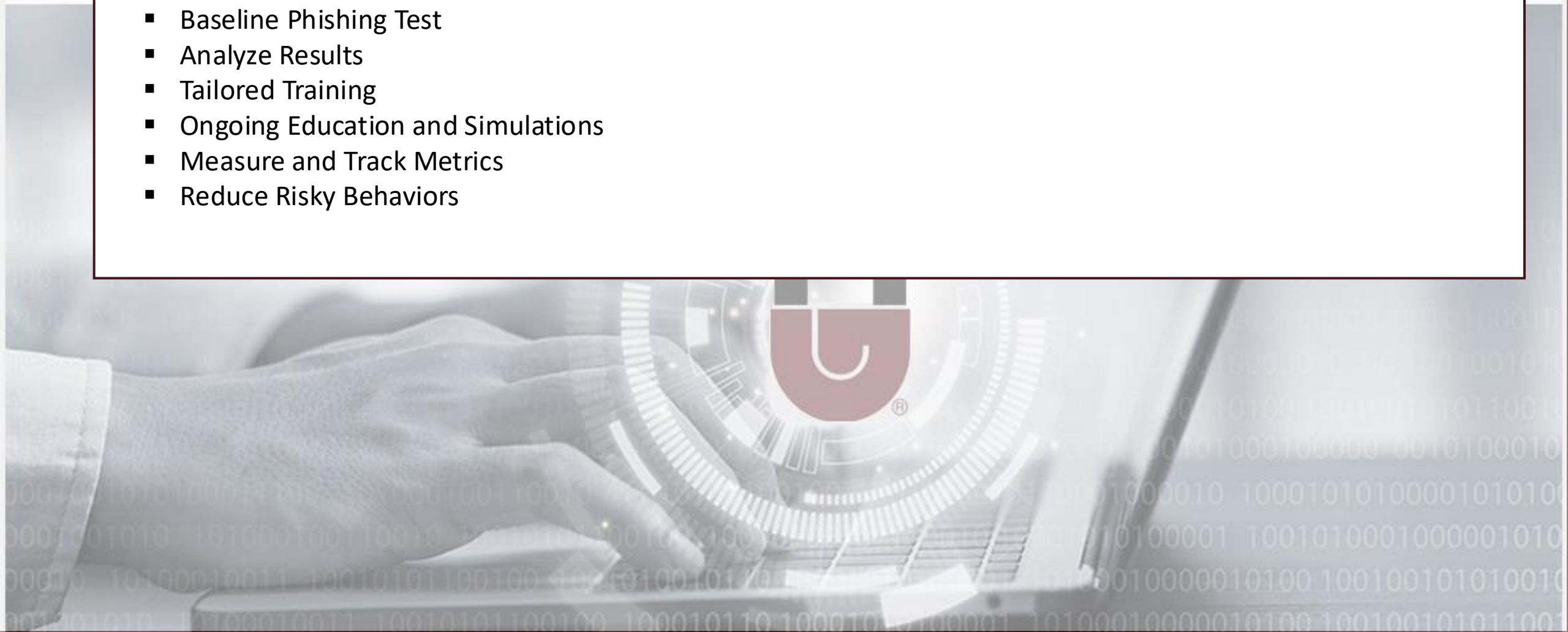
Accelerate and test your organization's cybersecurity awareness education program with CampusGuard’s full-featured phishing simulation software powered by Red Herring.

- Improve user awareness with ongoing training
- Reduce successful phishing attacks
- Easily identify employees susceptible to phishing emails
- Keep your organization safe and resilient against phishing and other social engineering attacks
- Meet cybersecurity insurance and compliance requirements (PCI, HIPAA, etc.)



# Phishing Platform Demo

- Baseline Phishing Test
- Analyze Results
- Tailored Training
- Ongoing Education and Simulations
- Measure and Track Metrics
- Reduce Risky Behaviors



# POLL QUESTION

- What feature would be MOST valuable in a phishing simulator?

CAMPUSGUARD

# IMPLEMENTATION/PRICING

- 25% discount for first 50 customers
- Stand-alone phishing tool or bundled with CampusGuard's Information Security Awareness Training Package
- Priced per user subscription / unlimited phishing emails

CAMPUSGUARD

# QUESTIONS?

Katie Johnson

kjohnson@campusguard.com

CAMPUSGUARD