NIST Small Business Cybersecurity Webinar

Protecting Your Small Business from Phishing Risks

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

This webinar is being recorded

Notes and Reminders

Attendees are muted: Due to the number of attendees, all participant microphones and cameras are automatically muted.

Webinar recording: This webinar will be recorded and posted to the event page here: https://www.nist.gov/itl/smallbusinesscyber/events
Registrants will be notified via email when the recording is available.

Submitting Questions: Please enter questions and comments for presenters in the Zoom for Government Q&A. Chat has been disabled for this event.

CE/CPE credits: NIST does not provide specific information regarding CE/CPE credits. Attendees are welcome to use their registration confirmation email to self-report to their certification bodies.

This webinar is being recorded

How to spot a phish

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Shanée Dawkins, Ph.D.

NIST Small Business Cybersecurity Webinar
August 14, 2025

Disclaimer

Throughout the presentation, certain commercial companies or products may be identified to foster understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the companies or products identified are necessarily the best available for the purpose.

Presentation Overview

- What we do
- Phishing defense
- Our research
- How to spot a phish

Championing the Human in I.T.

Defending Against Phishing

Phishing Threat Landscape

- Email
- Text messages
- Phone calls
- Social Media

Phishing Threat Landscape

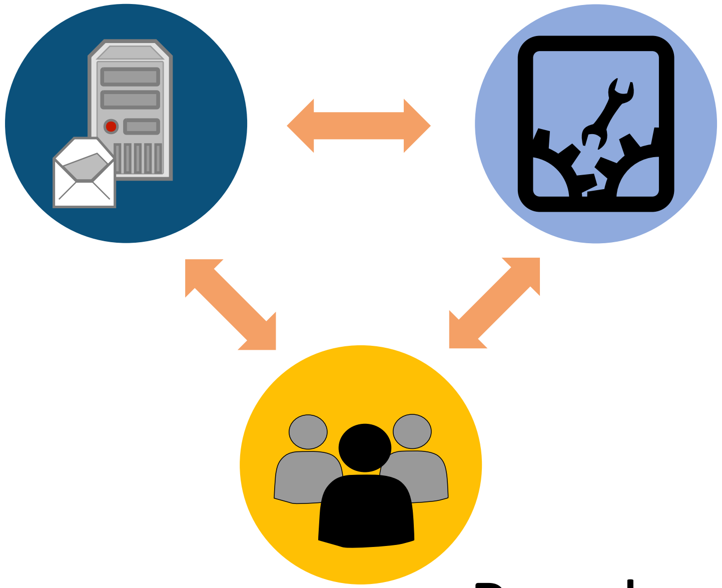
Phishing Threats

Broad cybersecurity
email attacks

Spear Phishing

Direct and targeted
email attacks

Phishing Defense



Technology

- Filtering & built-in tools
- AI & ML
- Multi-factor authentication

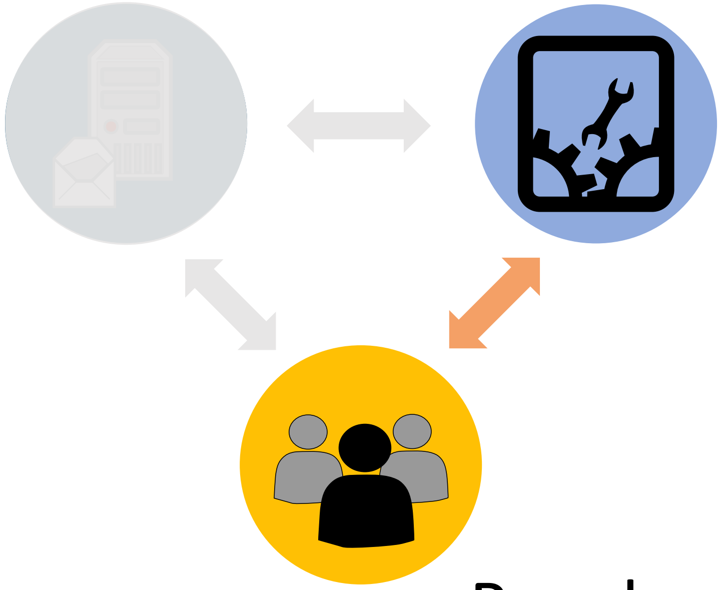
Process

- Identify vulnerabilities
- Limiting publicly available information
- Awareness training
- Easy and clear reporting mechanism
- Meaningful metrics

People

- End users
- IT security staff
- Leadership

Phishing Defense



Technology

- Filtering & built-in tools
- AI & ML
- Multi-factor authentication

Process

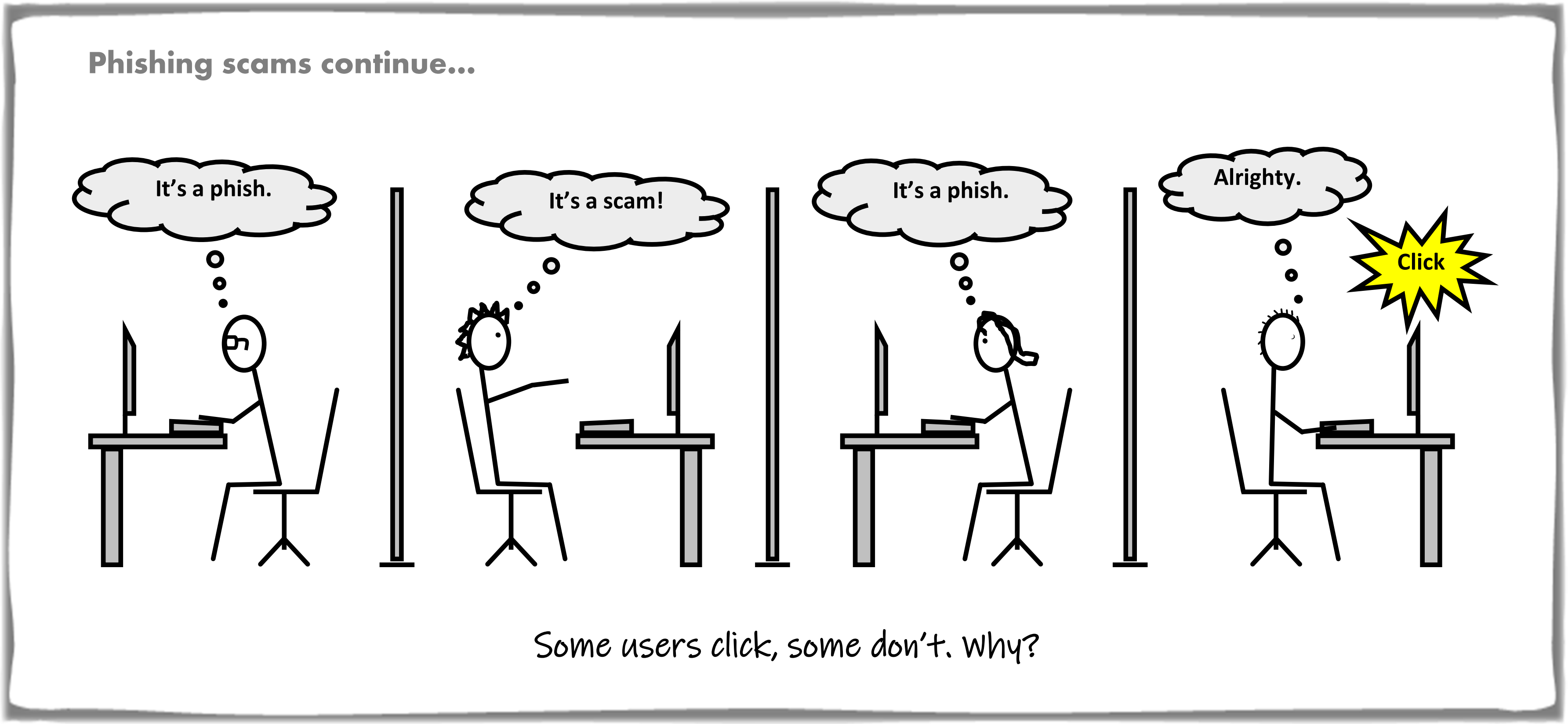
- Identify vulnerabilities
- Limiting publicly available information
- Awareness training
- Easy and clear reporting mechanism
- Meaningful metrics

People

- End users
- IT security staff
- Leadership

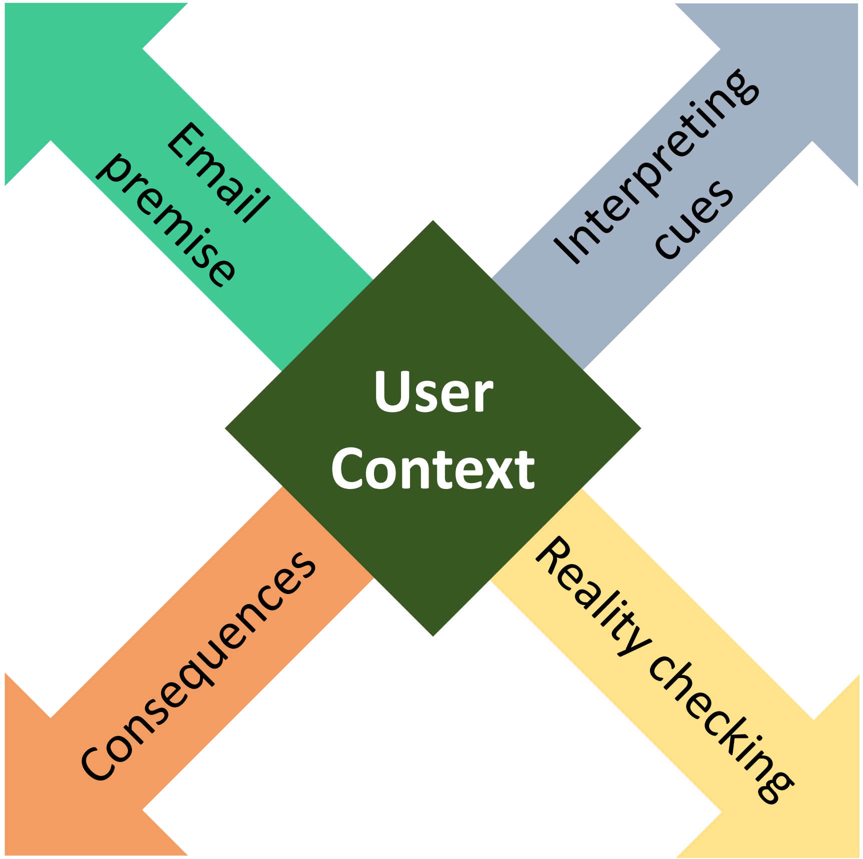
Our Research

Our Research – Phishing Awareness Study



Our Research – Phishing Awareness Study

Alignment vs. misalignment with expectations and external events

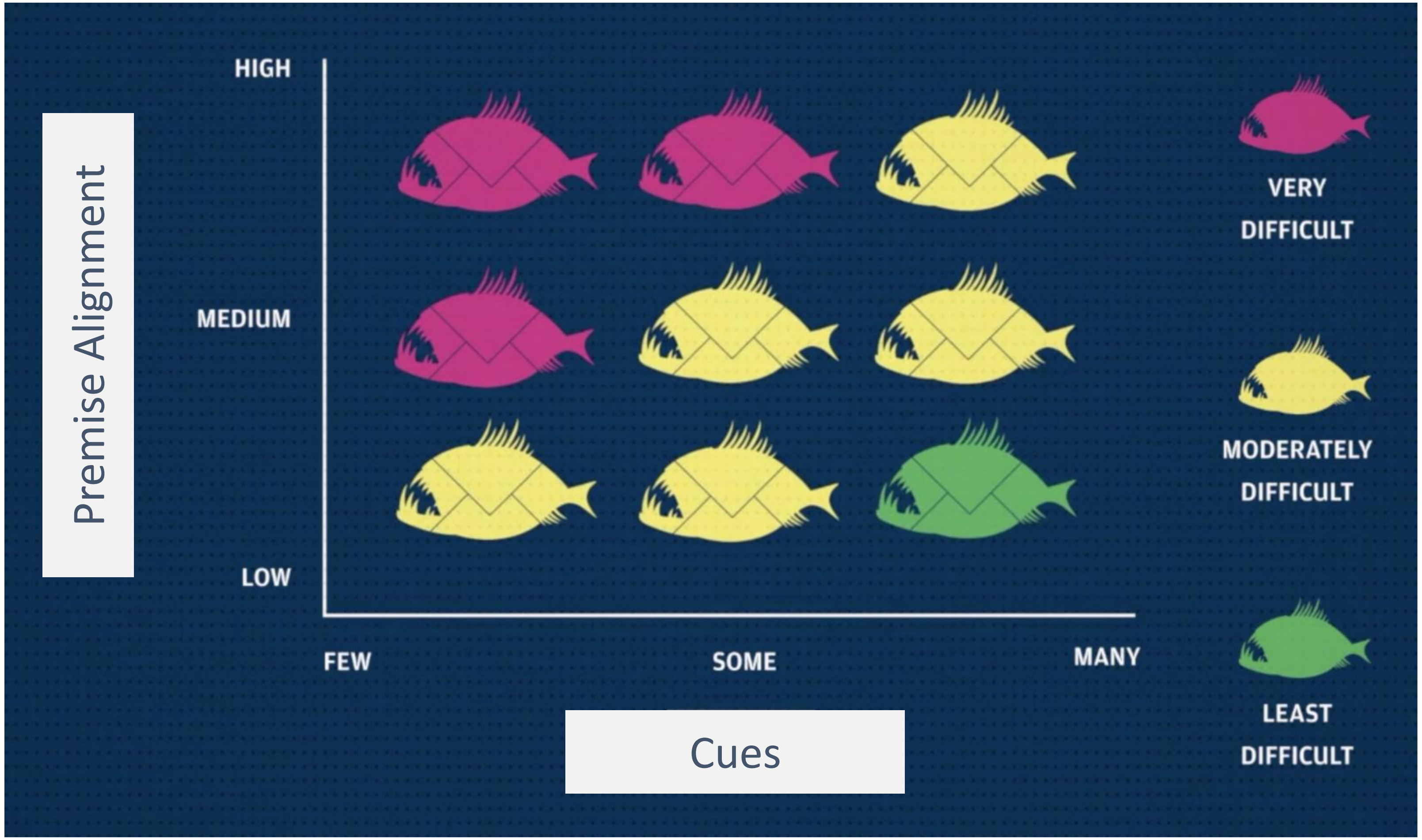


Compelling vs. suspicious cues

Concern over consequences

Reality-checking strategies

NIST Phish Scale



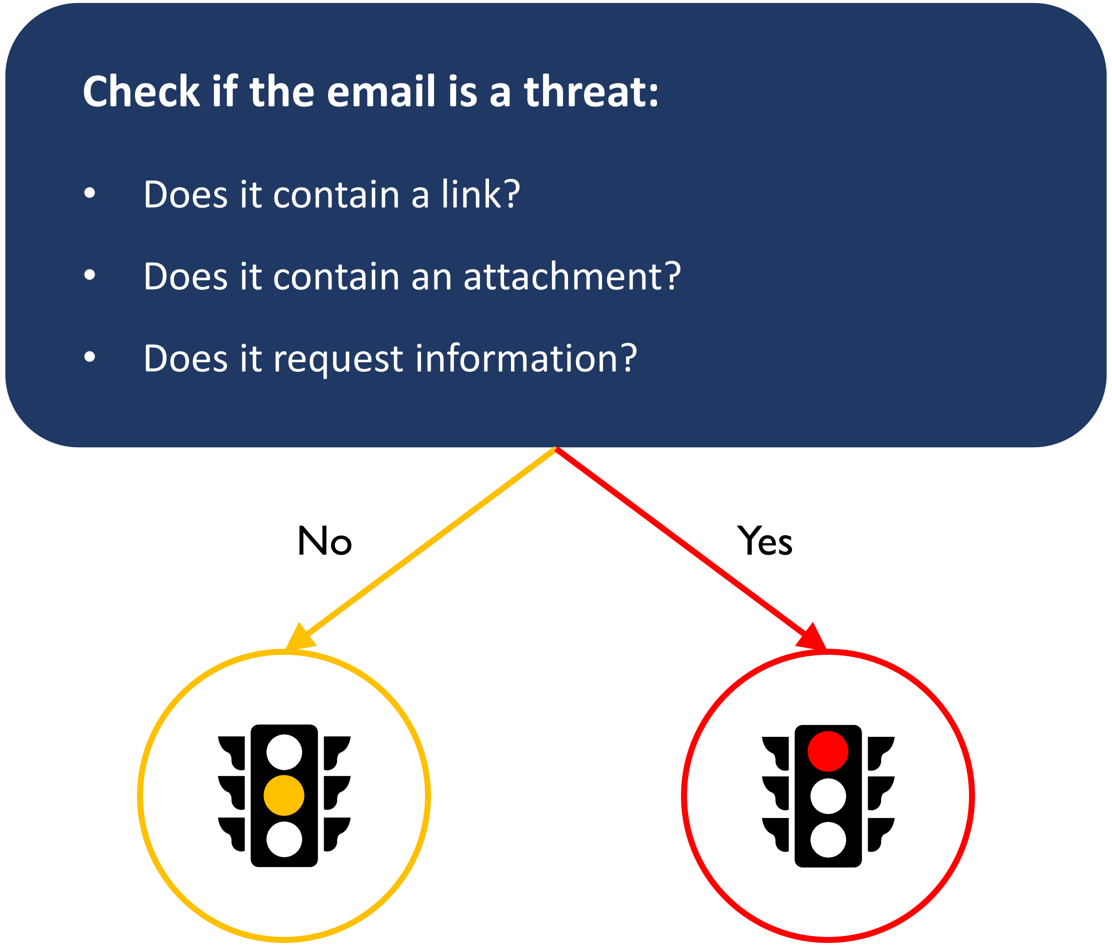
Our Research

Image credit: NIST

https://www.nist.gov/news-events/news/2018/06/youve-been-phished

How To Spot a Phish

How to Spot a Phish – Investigate Email



Check if the email is a threat:

- Does it contain a link?
- Does it contain an attachment?
- Does it request information?

Phishing Cues

WINNER!
CONGRATULATIONS
YOU ARE WON!!!

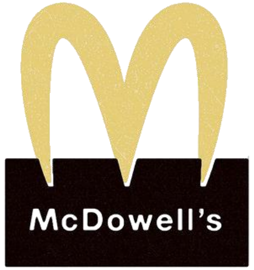
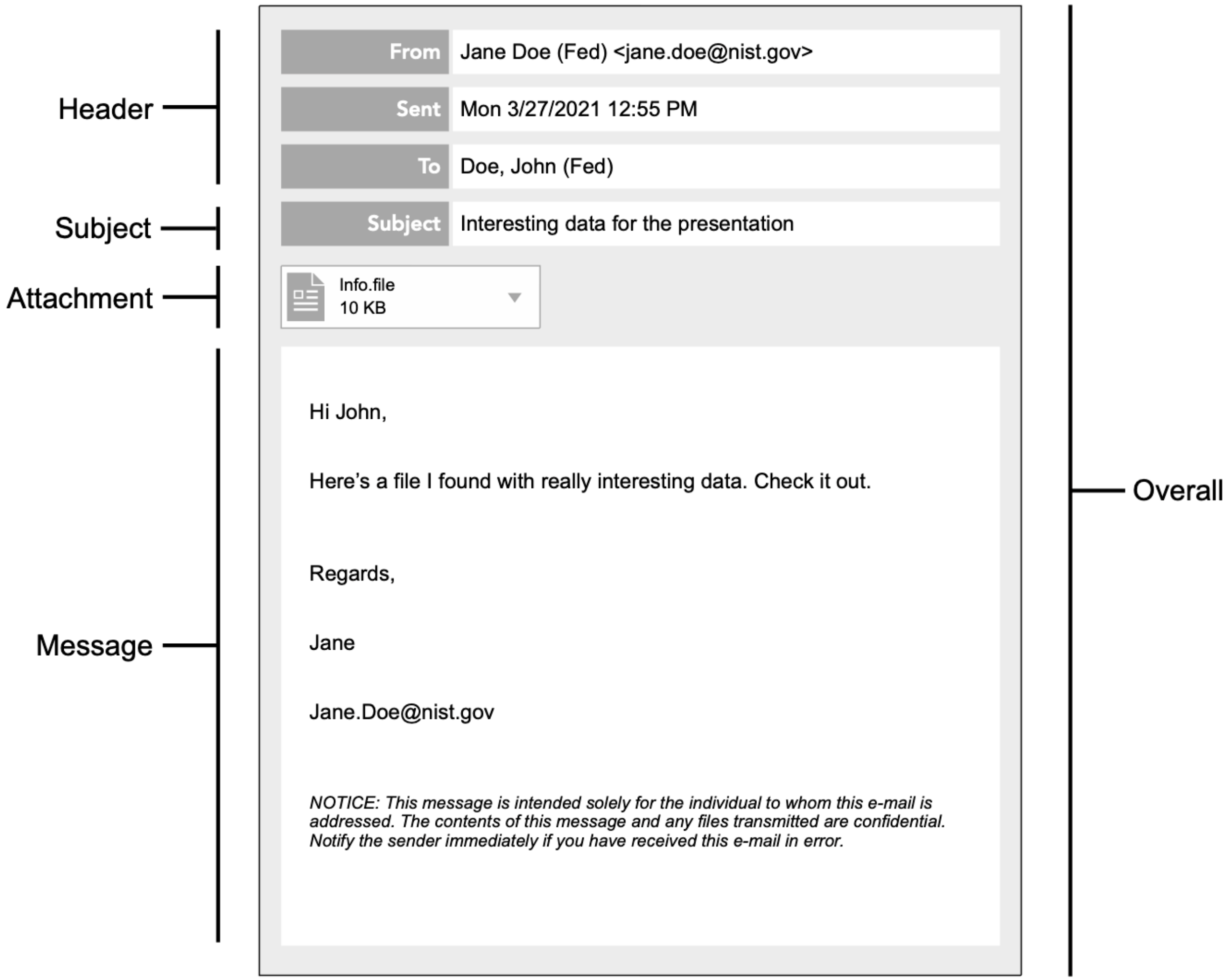


Image credits: Shutterstock; https://retruster.com/blog/phishing-email-scams-with-real-phishing-examples.html

How to Spot a Phish: Where to Find Cues



Header

Subject

Attachment

Message

Overall

From Jane Doe (Fed) <jane.doe@nist.gov>

Sent Mon 3/27/2021 12:55 PM

To Doe, John (Fed)

Subject Interesting data for the presentation

Info.file
10 KB

Hi John,

Here’s a file I found with really interesting data. Check it out.

Regards,

Jane

Jane.Doe@nist.gov

NOTICE: This message is intended solely for the individual to whom this e-mail is addressed. The contents of this message and any files transmitted are confidential. Notify the sender immediately if you have received this e-mail in error.

How to Spot a Phish: What Cues to Look for

- 5 Types of Cues
    - Errors
    - Technical indicators
    - Visual presentation indicators
    - Language and content
    - Common tactics

How to Spot a Phish: Error Cues

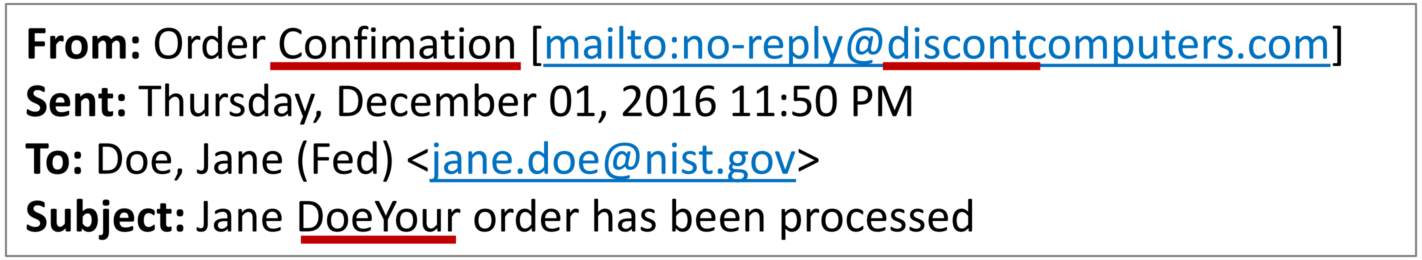
- 5 Types of Cues
  - Errors
  - Technical indicators
  - Visual presentation indicators
  - Language and content
  - Common tactics

Spelling errors

Grammar errors

Inconsistencies

How to Spot a Phish: Error Cues



From: Order Confimation [mailto:no-reply@discontcomputers.com]
Sent: Thursday, December 01, 2016 11:50 PM
To: Doe, Jane (Fed) <jane.doe@nist.gov>
Subject: Jane DoeYour order has been processed

Errors cue type: Grammar error cue

How to Spot a Phish: Technical Cues

- 5 Types of Cues
  - Errors
  - Technical indicators
  - Visual presentation indicators
  - Language and content
  - Common tactics

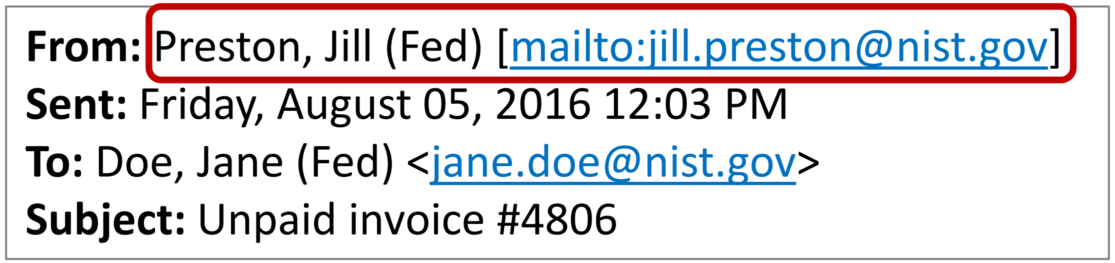
Attachments

Sender’s name and email address mismatch

Displayed link text differs from the actual URL

Domain spoofing

How to Spot a Phish: Technical Cues



From: Preston, Jill (Fed) [mailto:jill.preston@nist.gov]
Sent: Friday, August 05, 2016 12:03 PM
To: Doe, Jane (Fed) <jane.doe@nist.gov>
Subject: Unpaid invoice #4806

Technical indicators cue type: Domain spoofing cue

How to Spot a Phish: Visual Presentation Cues

- 5 Types of Cues
  - Errors
  - Technical indicators
  - Visual presentation indicators
  - Language and content
  - Common tactics

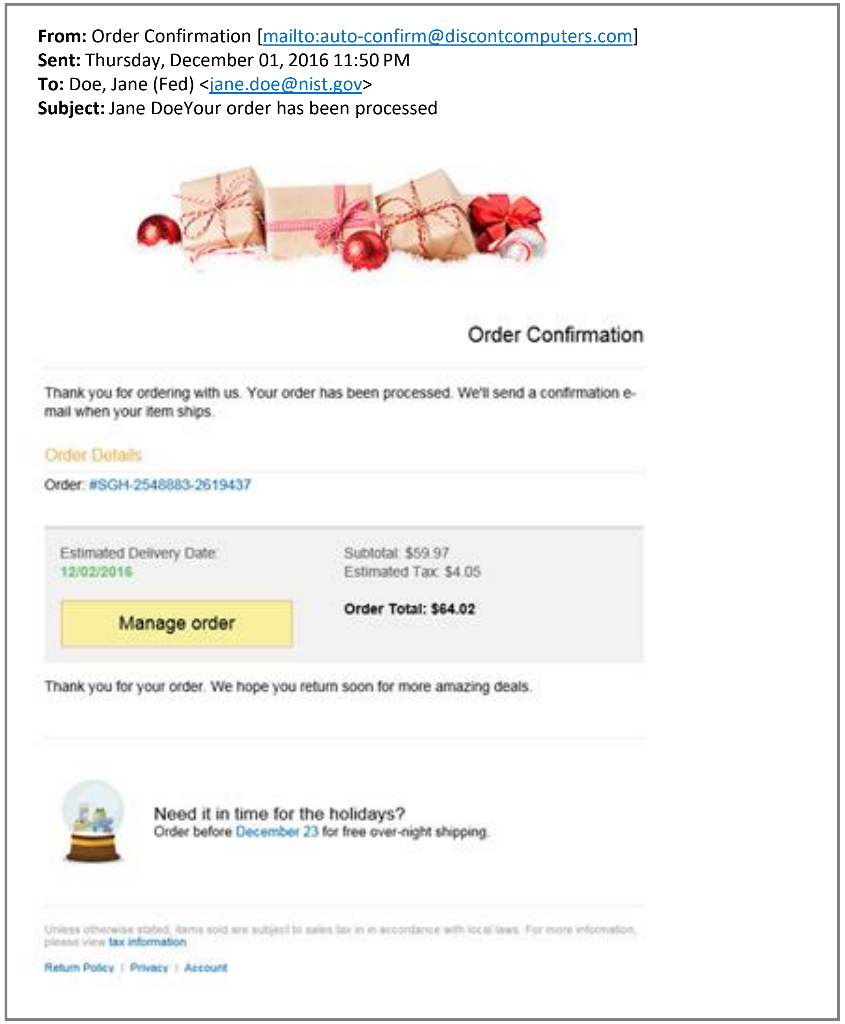
Branding imitation

Outdated logos

Unprofessional formatting

Inappropriate security indicators and icons

How to Spot a Phish: Visual Presentation Cues



From: Order Confirmation [mailto:auto-confirm@discontcomputers.com]
Sent: Thursday, December 01, 2016 11:50 PM
To: Doe, Jane (Fed) <jane.doe@nist.gov>
Subject: Jane DoeYour order has been processed

Order Confirmation

Thank you for ordering with us. Your order has been processed. We'll send a confirmation e-mail when your item ships.

Order Details

Order: #SGH-2548883-2619437

Estimated Delivery Date:
12/02/2016

Subtotal: $59.97
Estimated Tax: $4.05

Order Total: $64.02

Thank you for your order. We hope you return soon for more amazing deals.

Need it in time for the holidays?
Order before December 23 for free over-night shipping.

Unless otherwise stated, items sold are subject to sales tax in in accordance with local laws. For more information, please view tax information

Return Policy | Privacy | Account

Visual presentation indicators cue type: Branding imitation cue

How to Spot a Phish: Language & Content Cues

- 5 Types of Cues
  - Errors
  - Technical indicators
  - Visual presentation indicators
  - Language and content
  - Common tactics

A generic greeting

Legal language/copyright info/disclaimers

Requests for sensitive information

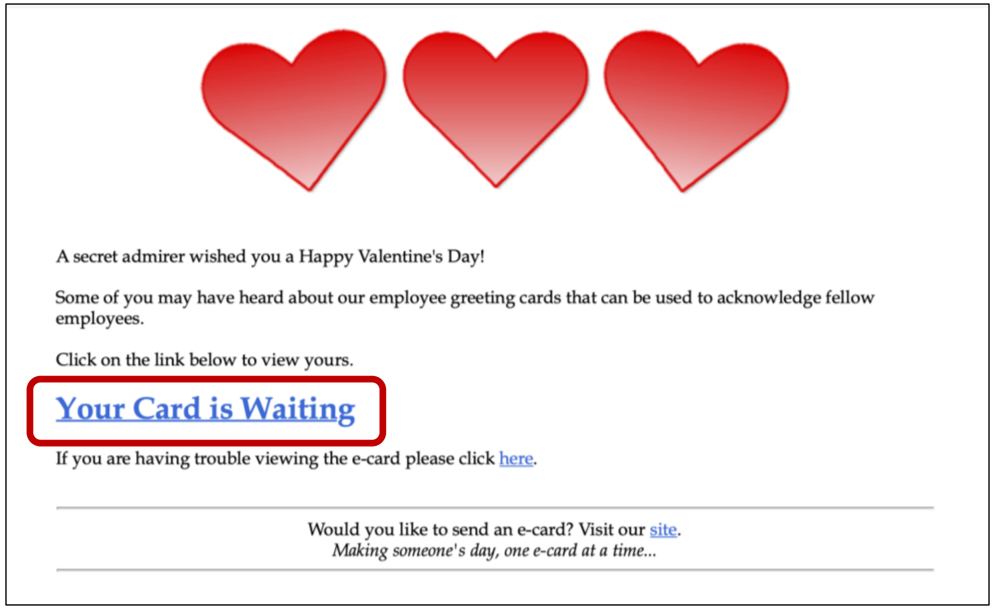
Sense of urgency

Threatening language

Lack of signer details

Distracting details

How to Spot a Phish: Language & Content Cues



A secret admirer wished you a Happy Valentine's Day!

Some of you may have heard about our employee greeting cards that can be used to acknowledge fellow employees.

Click on the link below to view yours.

Your Card is Waiting

If you are having trouble viewing the e-card please click here.

Would you like to send an e-card? Visit our site.
Making someone's day, one e-card at a time...

Language and content cue type: Sense of urgency cue

How to Spot a Phish: Common Tactics Cues

- 5 Types of Cues
  - Errors
  - Technical indicators
  - Visual presentation indicators
  - Language and content
  - Common tactics

Humanitarian appeals

Too good to be true offers

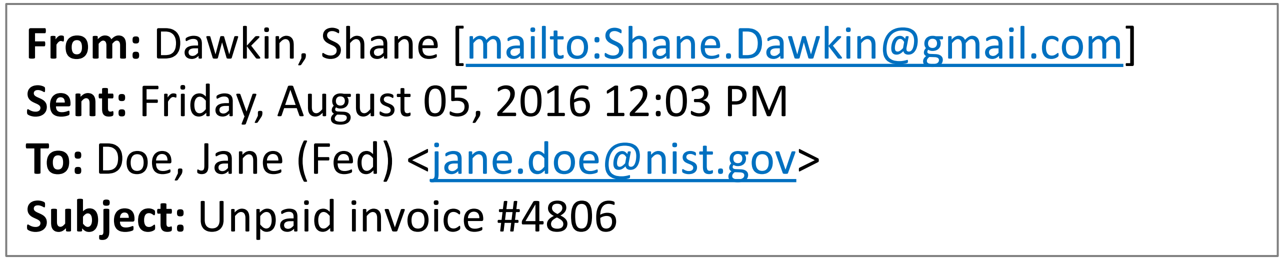
Limited time offer

“You’re special” offer

Mimics work or business process

Poses as colleague or authority figure

How to Spot a Phish: Common Tactics Cues



From: Dawkin, Shane [mailto:Shane.Dawkin@gmail.com]
Sent: Friday, August 05, 2016 12:03 PM
To: Doe, Jane (Fed) <jane.doe@nist.gov>
Subject: Unpaid invoice #4806

Common tactics cue type: Poses as friend, colleague, supervisor, or authority figure cue

Final Tips

- What if you see a potential phish?
  - Be vigilant, considering your context
  - Look for cues
  - Use bookmarked links/favorites instead of clicking
  - Use a search engine, don't click on ads

- Don't:
  - Click on links
  - Download attachments
  - Provide any requested information

- Do:
  - Report suspicious emails
  - Contact sender through an alternative route, like a phone call

Talking about Phishing

- **Understand the threat** – Phishing attacks can be via email, text messages, phone calls, or social media.

- **Empower staff** – Your staff are the detectives and judges of their inboxes.
  - People are the last line of defense against a phishing attack.

- **Consider user context** – Staff should consider their work roles & responsibilities when investigating phishy emails.

- **Be proactive** – Encourage reporting of phishing emails.
  - Be proactive against phishing threats.

Additional Resources

- Shanée Dawkins, dawkins@nist.gov

- https://csrc.nist.gov/Projects/human-centered-cybersecurity
- https://csrc.nist.gov/Projects/human-centered-cybersecurity/research-areas/phishing

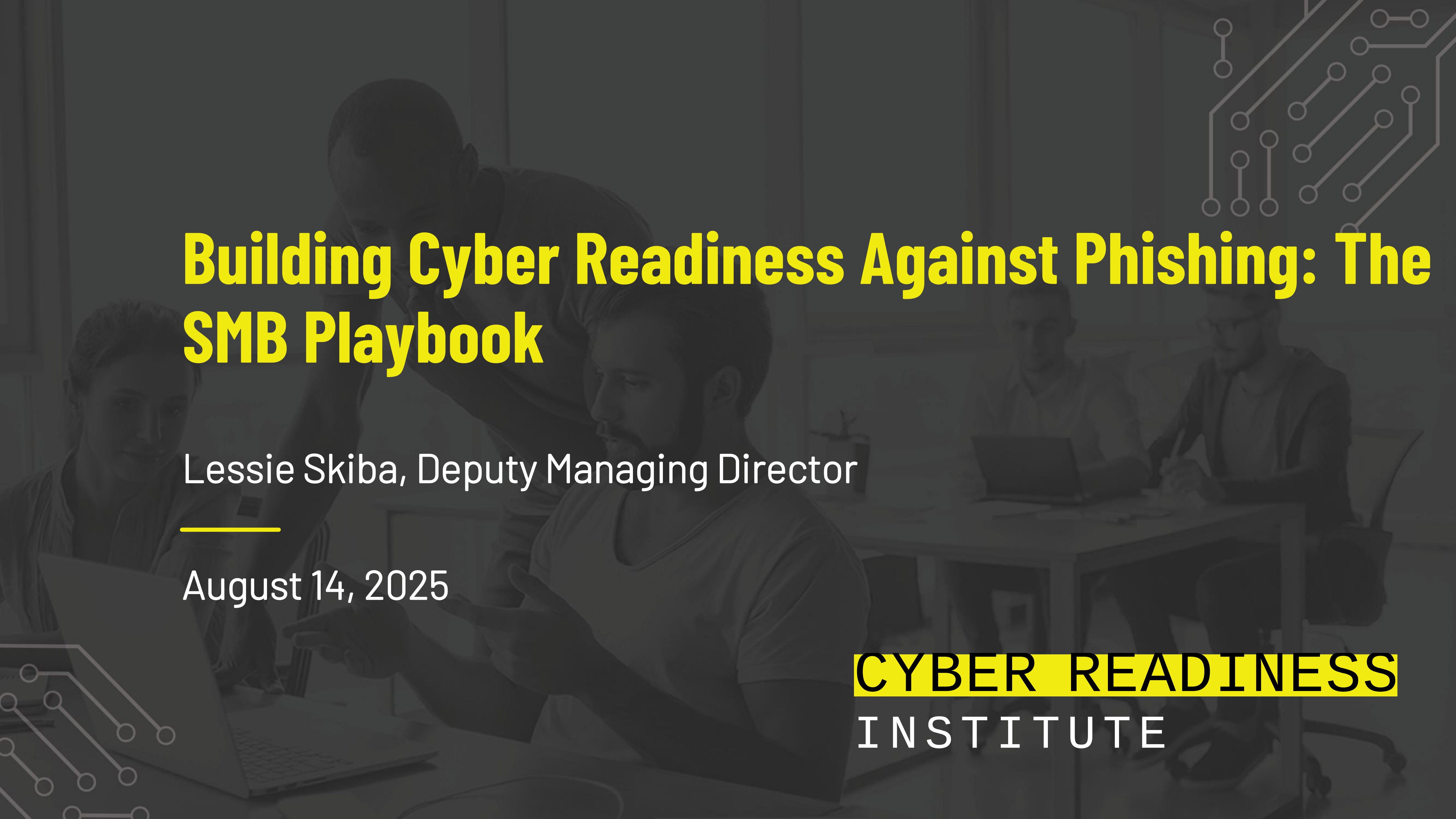
NIST Phishing Research

References

- Anti-Phishing Working Group (APWG) **Phishing Activity Trends Report**, 3rd Quarter 2022 https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf
- Federal Bureau of Investigation Internet Crime Complaint Center (IC3) **Internet Crime Report** https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
- Verizon 2024 **Data Breach Investigations Report** (DBIR) https://www.verizon.com/business/resources/reports/dbir/
- Proofpoint 2024 **State of the Phish Report** https://www.proofpoint.com/us/resources/threat-reports/state-of-phish
- Canham, M., Posey, C., Strickland, D., & Constantino, M. (2021). **Phishing for Long Tails: Examining Organizational Repeat Clickers and Protective Stewards**. SAGE Open, 11(1). https://doi.org/10.1177/21582440211990656

References

- Dawkins, S. and Jacobs, J. (2023). **Phishing With a Net: The NIST Phish Scale and Cybersecurity Awareness**. RSA Conference 2023: Human Element Track, San Francisco, CA, US, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=936343 (Accessed July 2023)
- Barrientos, F., Jacobs, J., and Dawkins, S. (2021). **Scaling the Phish: Advancing the NIST Phish Scale**. In Proceedings of HCII 2021 (23rd International Conference on Human-Computer Interaction). July 24 – July 29, 2021. https://doi.org/10.1007/978-3-030-78642-7_52 (Accessed February 2023)
- Michelle P. Steves, Kristen K. Greene and Mary F. Theofanos. (2020). **Categorizing Human Phishing Detection Difficulty: A Phish Scale**. Journal of Cybersecurity. Published online September 14, 2020. https://doi.org/10.1093/cybsec/tyaa009 (Accessed February 2023)
- Steves, M. , Greene, K. and Theofanos, M. (2019), **A Phish Scale: Rating Human Phishing Message Detection Difficulty**. Workshop on Usable Security and Privacy (USEC) 2019. San Diego, CA, US, [online]. https://doi.org/10.14722/usec.2019.23028 (Accessed February 2023)
- Greene, Kristen & Steves, Michelle & Theofanos, Mary. (2018). **No Phishing beyond This Point**. Computer. 51. 86-89. https://doi.org/10.1109/MC.2018.2701632 (Accessed February 2023)
- Greene, Kristen & Steves, Michelle & Theofanos, Mary & Kostick, Jennifer. (2018). **User Context: An Explanatory Variable in Phishing Susceptibility**. Proceedings of the Network and Distributed Systems Security (NDSS) Symposium, San Diego, CA, US, [online], https://doi.org/10.14722/usec.2018.23016 (Accessed July 2023)



Building Cyber Readiness Against Phishing: The SMB Playbook

Lessie Skiba, Deputy Managing Director

August 14, 2025

CYBER READINESS INSTITUTE

About the Cyber Readiness Institute

The Cyber Readiness Institute (CRI) is a nonprofit institute that brings together business leaders from across sectors and geographic regions to develop free cybersecurity tools for small and medium-sized businesses.

Our mission is to advance the cyber readiness of small and medium-sized businesses by focusing on human behavior to improve the overall security of global value chains and communities.

CRI empowers small and medium-sized businesses with free tools and resources to help them become more secure and resilient.

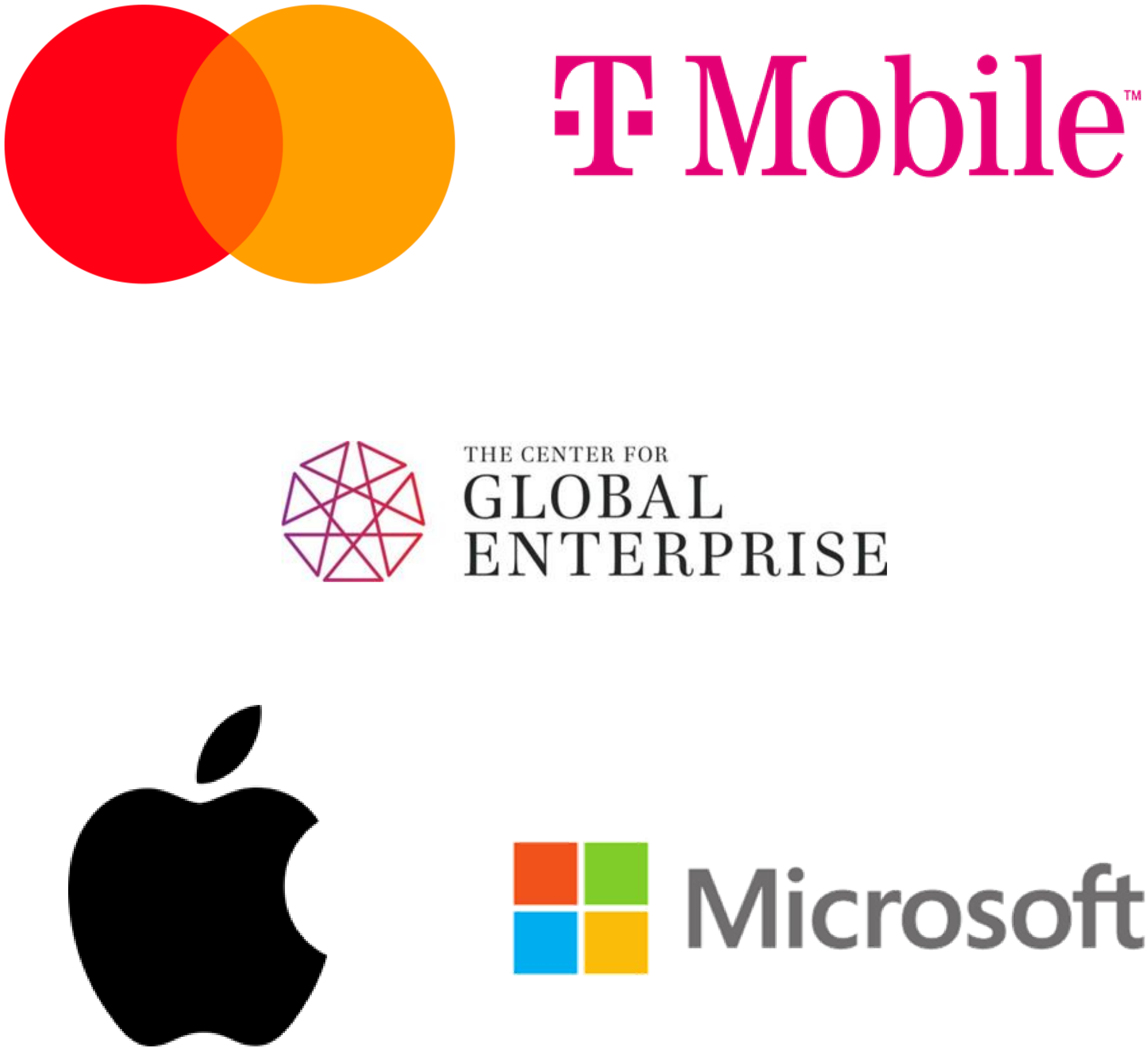
When we're all cyber ready, we're all cyber strong.

Cyber Readiness Institute Members

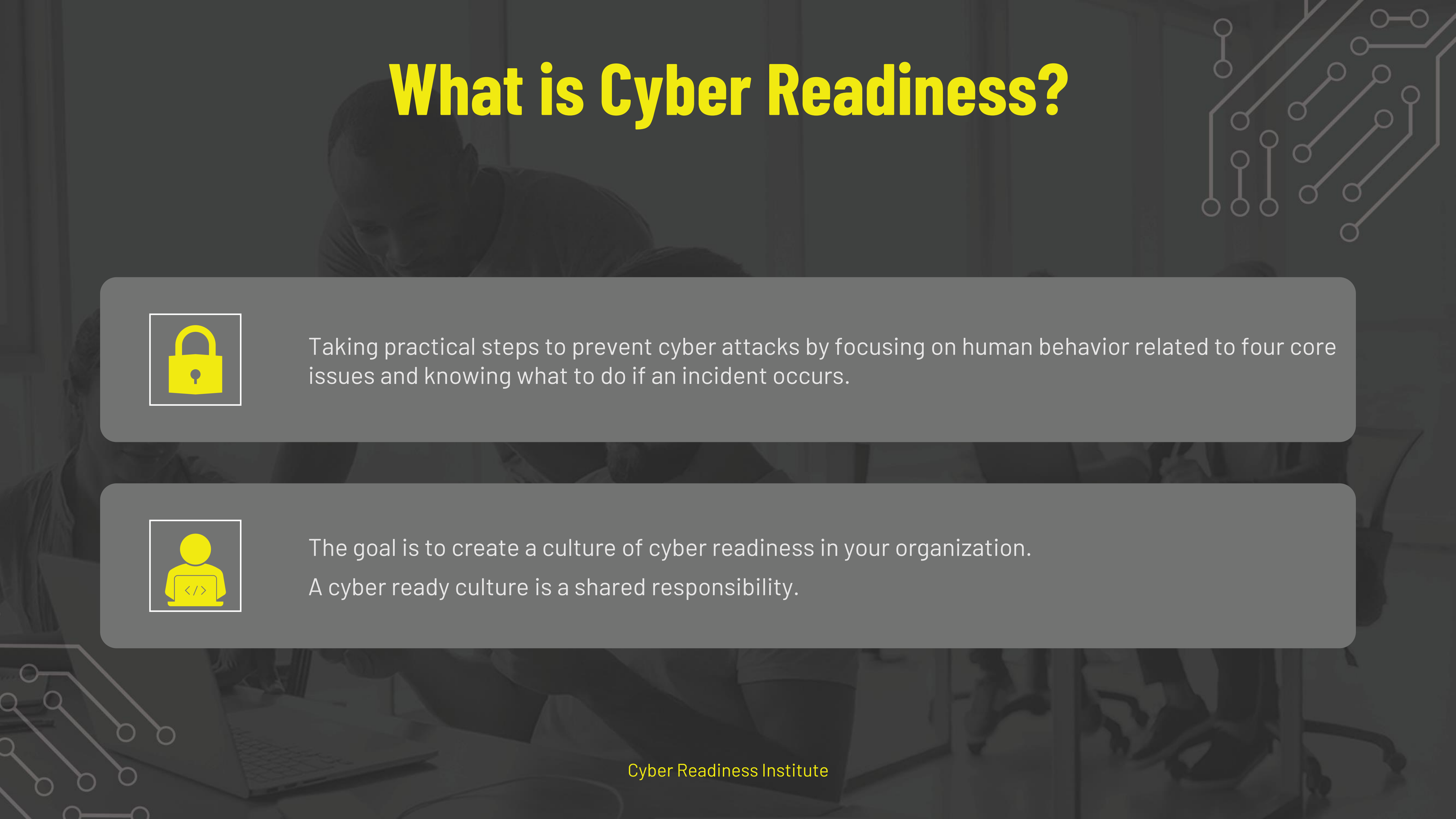
Convenes senior leaders of global companies and supply chain partners

Shares cybersecurity best practices and resources

Develops free content and tools to improve the Cyber Readiness of small and medium-sized enterprises



Cyber Readiness for Small and Medium-sized Businesses (SMBs)

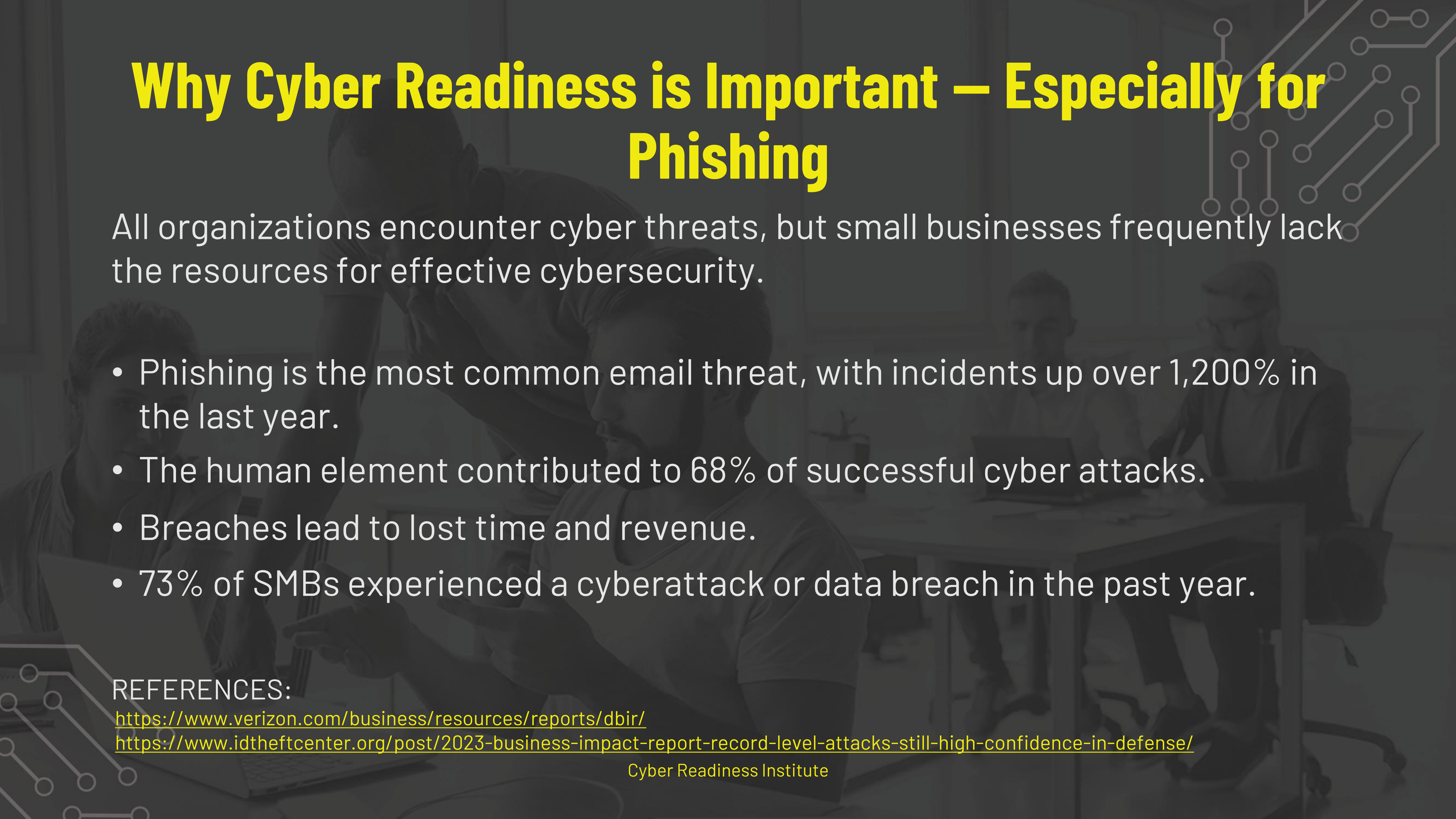


What is Cyber Readiness?

Taking practical steps to prevent cyber attacks by focusing on human behavior related to four core issues and knowing what to do if an incident occurs.

The goal is to create a culture of cyber readiness in your organization.

A cyber ready culture is a shared responsibility.



Why Cyber Readiness is Important — Especially for Phishing

All organizations encounter cyber threats, but small businesses frequently lack the resources for effective cybersecurity.

- Phishing is the most common email threat, with incidents up over 1,200% in the last year.
- The human element contributed to 68% of successful cyber attacks.
- Breaches lead to lost time and revenue.
- 73% of SMBs experienced a cyberattack or data breach in the past year.

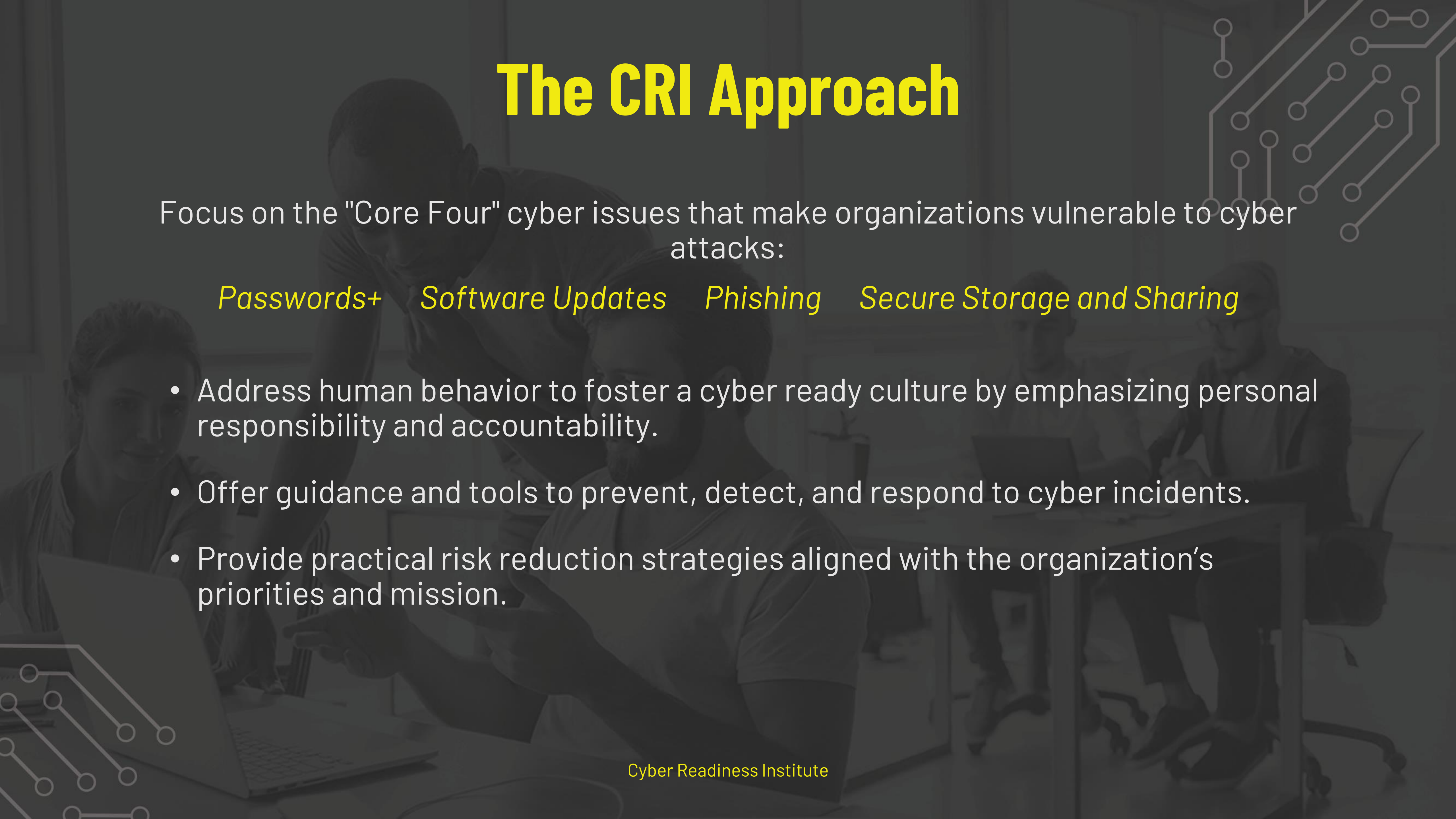
REFERENCES:
https://www.verizon.com/business/resources/reports/dbir/
https://www.idtheftcenter.org/post/2023-business-impact-report-record-level-attacks-still-high-confidence-in-defense/

Building a Cyber Ready Culture

People are the key.

Process needs to be practical and simple.

Technology needs to enhance cybersecurity while enabling job performance.

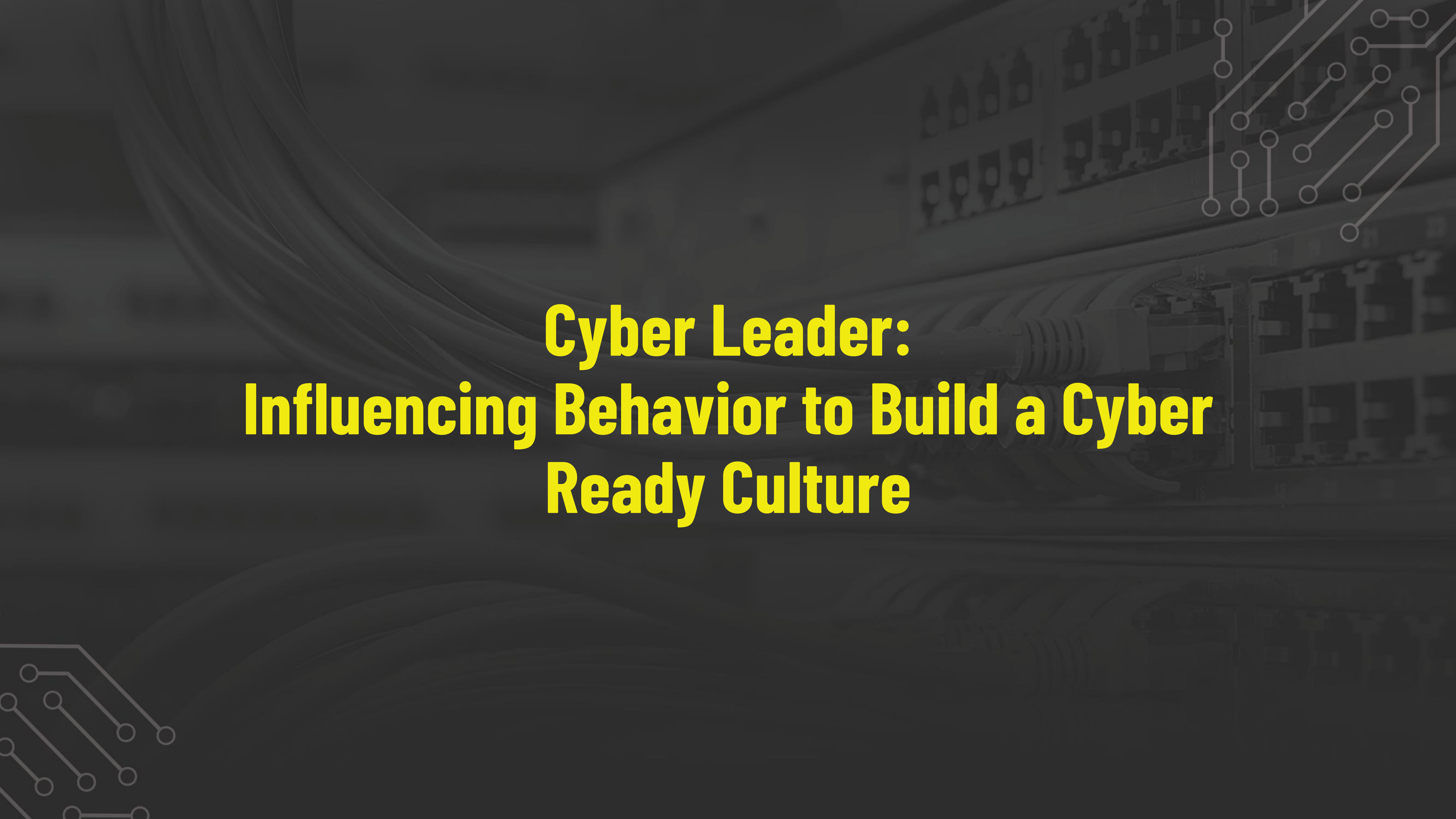


The CRI Approach

Focus on the "Core Four" cyber issues that make organizations vulnerable to cyber attacks:

Passwords+ *Software Updates* *Phishing* *Secure Storage and Sharing*

- Address human behavior to foster a cyber ready culture by emphasizing personal responsibility and accountability.
- Offer guidance and tools to prevent, detect, and respond to cyber incidents.
- Provide practical risk reduction strategies aligned with the organization's priorities and mission.



Cyber Leader:
Influencing Behavior to Build a Cyber Ready Culture

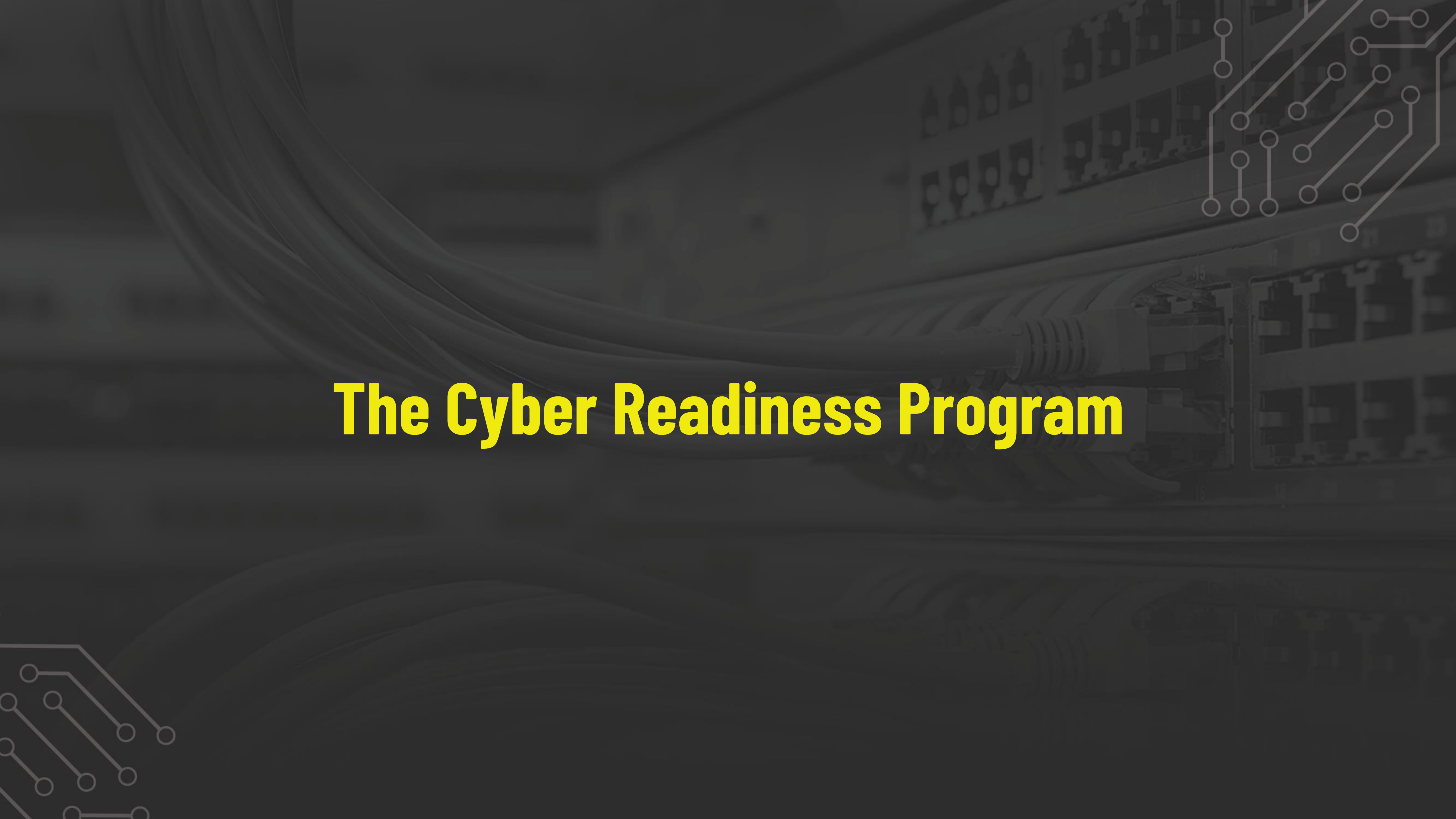
What is a Cyber Leader?

An individual within an organization who leads the development of a cyber ready culture, implements practical policies, and promotes best practices and cyber ready behavior across the organization. The Cyber Leader does not need to have technology expertise.

- Promotes cybersecurity awareness among employees.
- Influences behavior to adopt secure practices across daily operations.
- Cultivates a proactive, cyber ready culture throughout the organization.

A cyber ready culture is a shared responsibility.

Ensure everyone understands their role to protect the organization.



The Cyber Readiness Program

Cyber Readiness Program

A *FREE* self-paced program focused on human behavior to help organizations improve their cyber readiness and resilience, supporting small and medium-sized businesses.

The Program helps SMBs as they implement the following measures:

1. Comprehensive Security Policies
2. Business Continuity Planning
3. Employee Training and Awareness
4. Data Backup and Recovery
5. Incident Response Planning

"The Core Four"

- Passwords+
- Software Updates
- Phishing
- Secure Storage and Sharing

Building Cyber Readiness Against Phishing

Don’t Panic: You’ve Prepared

Prepare (before an incident)

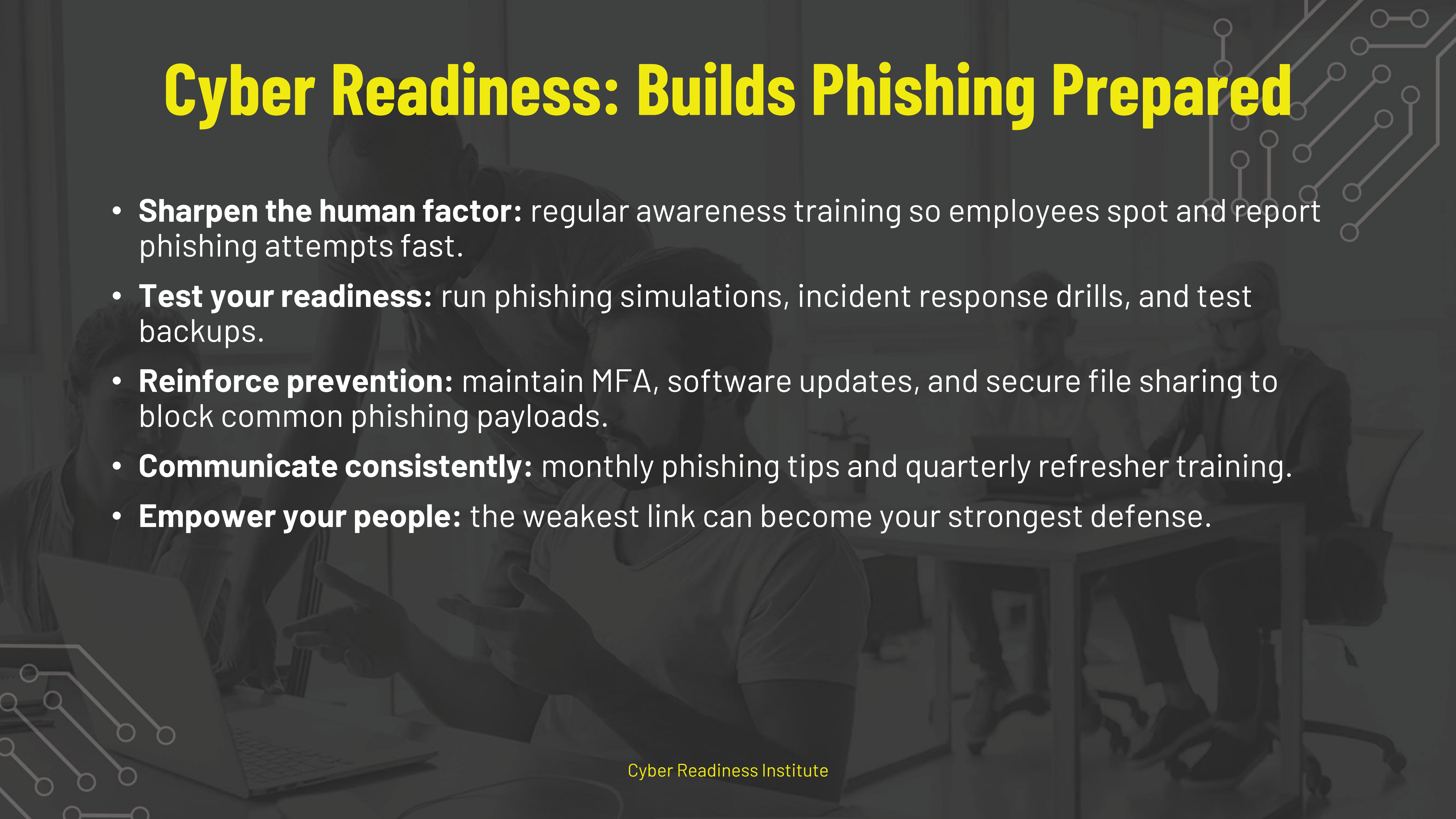
- Identify your Cyber Leader & emergency contacts
- Keep offline/phone contact info handy
- Maintain & test backups regularly

Respond (during the incident)

- Shut down the affected device
- Disconnect from network (Wi-Fi & cable)
- Call your Cyber Leader immediately
- Cyber Leader alerts emergency contacts & coordinates response

Recover (after the incident)

- Notify suppliers/customers if affected
- Reset IDs/passwords for compromised devices
- Patch all devices
- Restore from backups
- Document lessons learned



Cyber Readiness: Builds Phishing Prepared

- **Sharpen the human factor:** regular awareness training so employees spot and report phishing attempts fast.
- **Test your readiness:** run phishing simulations, incident response drills, and test backups.
- **Reinforce prevention:** maintain MFA, software updates, and secure file sharing to block common phishing payloads.
- **Communicate consistently:** monthly phishing tips and quarterly refresher training.
- **Empower your people:** the weakest link can become your strongest defense.

CYBER READINESS
INSTITUTE

Change Behavior.
Be Cyber Ready.

Enroll in the Cyber Readiness Program today!

CYBER READINESS INSTITUTE

Programs Starter Kit Champions About CRI Resources

Be Cyber Ready. Stay Cyber Strong.

Protect Your Business With the Cyber Readiness Program

Cyber risk is on the rise. The Cyber Readiness Program can help you protect your data, your employees, your vendors, and your customers. This free, online program is designed to help small and medium-sized enterprises become more secure against today's most common cyber vulnerabilities.

With just a few hours of time, your organization can become Cyber Ready.

in @cyber-readiness-institute

X @Cyber_Readiness

f @CyberReadinessInstitute

▶ @cyberreadinessinstitute

@cyberreadinessinstitute

BeCyberReady.com

Thank You

Lessie Skiba

lskiba@cyberreadinessinstitute.org

Contact the Cyber Readiness Institute: support@cyberreadinessinstitute.org

Disclaimer

CRI does not provide legal advice, and the information and resources we offer should not be construed as such; instead, all resources, information, and content we offer is for informational purposes only. We make no representation that our content or program will guarantee prevention of cyber incidents and disclaim all liability for actions you take or fail to take based on any content we provide. It is advisable to consult with legal counsel regarding any applicable regulations or legal matters.

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

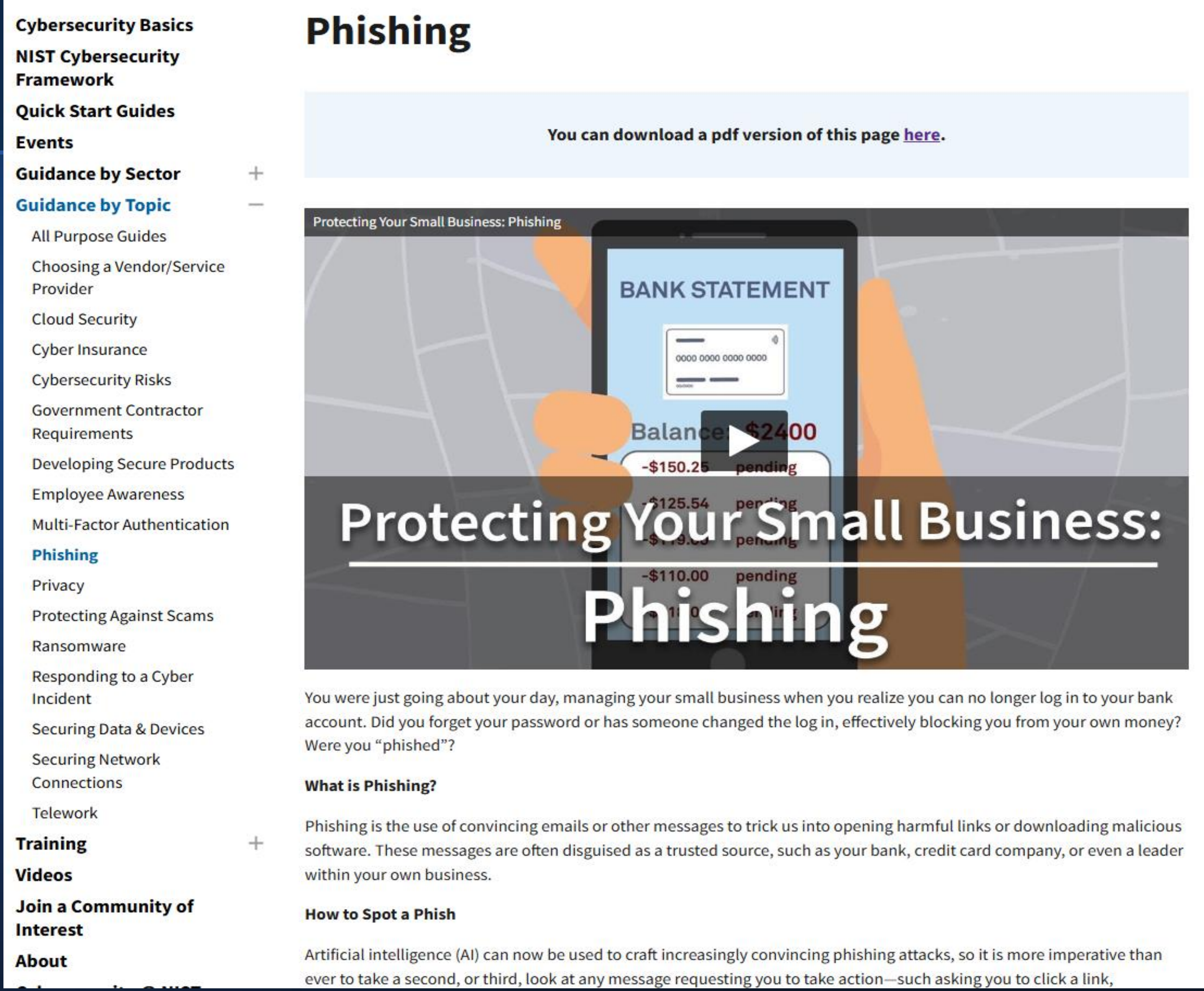
Related Webinar Recording: Ransomware Prevention, Detection, Response, and Recovery :

NIST Small Business Cybersecurity Webinar: Ransomware Prevention, Detection, Response, and Recovery

August 15, 2024

This webinar is being recorded

nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware



Phishing

You can download a pdf version of this page here.

You were just going about your day, managing your small business when you realize you can no longer log in to your bank account. Did you forget your password or has someone changed the log in, effectively blocking you from your own money? Were you "phished"?

What is Phishing?

Phishing is the use of convincing emails or other messages to trick us into opening harmful links or downloading malicious software. These messages are often disguised as a trusted source, such as your bank, credit card company, or even a leader within your own business.

How to Spot a Phish

Artificial intelligence (AI) can now be used to craft increasingly convincing phishing attacks, so it is more imperative than ever to take a second, or third, look at any message requesting you to take action—such asking you to click a link,

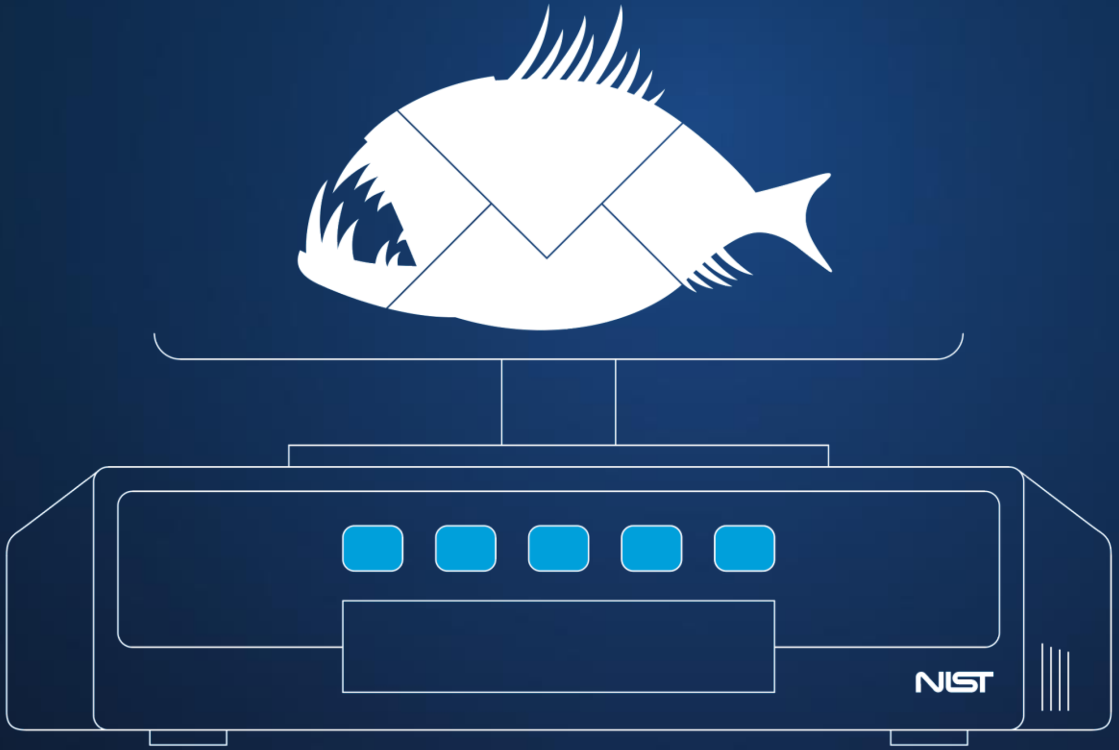
nist.gov/itl/smallbusinesscyber/guidance-topic/phishing

Seeking Comments

NIST Interagency Report (NIST IR) 8374 Revision 1, Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile

https://doi.org/10.6028/NIST.IR.8374r1.ipd

- Seeking comment through September 11, 2025
- You can send feedback about this draft publication to ransomware@nist.gov



Q&A

Thank You for Joining Today's Webinar!

FOR FURTHER INFORMATION AND/OR QUESTIONS ABOUT NIST'S SMALL BUSINESS CYBERSECURITY RESOURCES:

Email: smallbizsecurity@nist.gov

Visit Us Online: https://www.nist.gov/itl/smallbusinesscyber