RSAConference™2023
San Francisco | April 24 – 27 | Moscone Center

SESSION ID: HUM-T01

Phishing With a Net: The NIST Phish Scale and Cybersecurity Awareness

Shanée Dawkins, Ph.D.
Computer Scientist
National Institute of Standards and Technology

Jody Jacobs, M.S.
Computer Scientist
National Institute of Standards and Technology

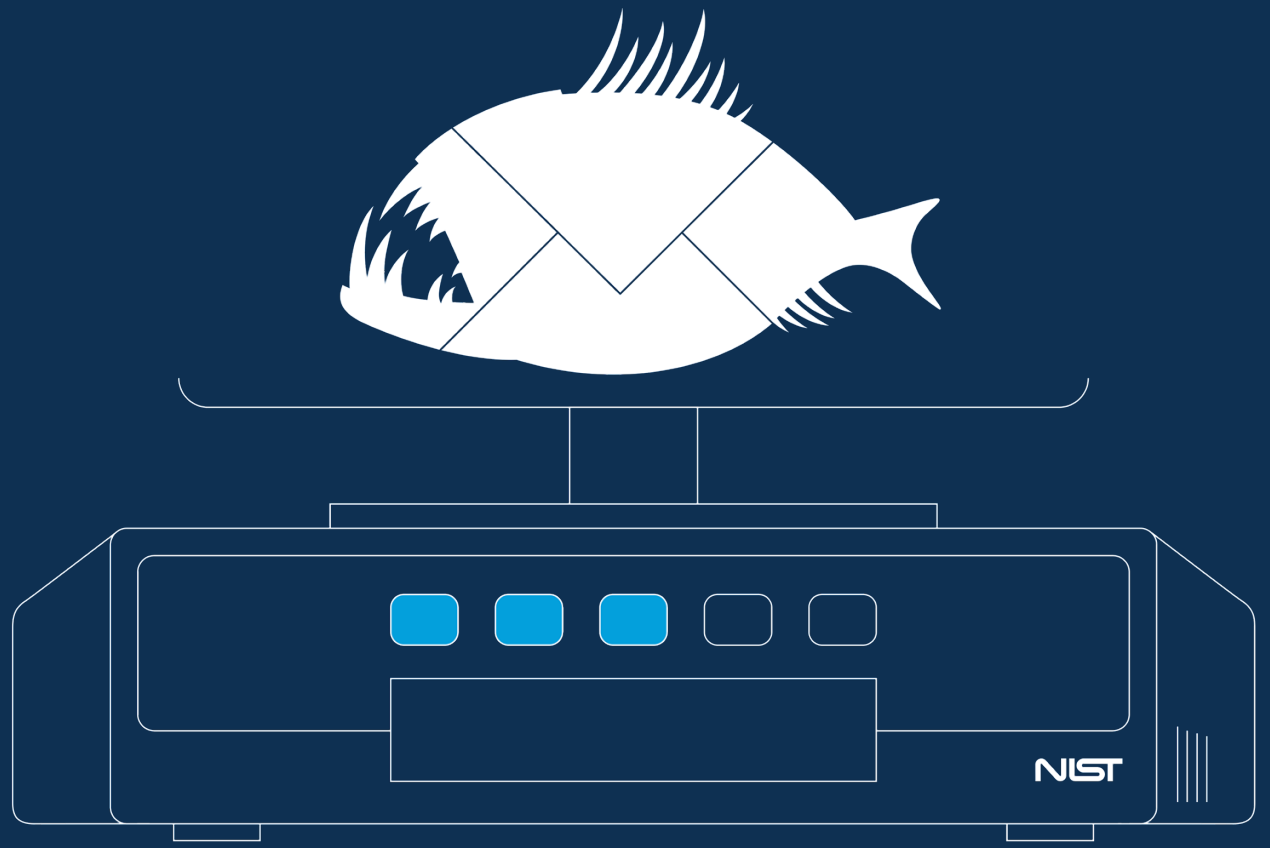
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

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.

The NIST Phish Scale and the Human Element



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

Image credit: NIST

The Big Picture

Phishing Landscape

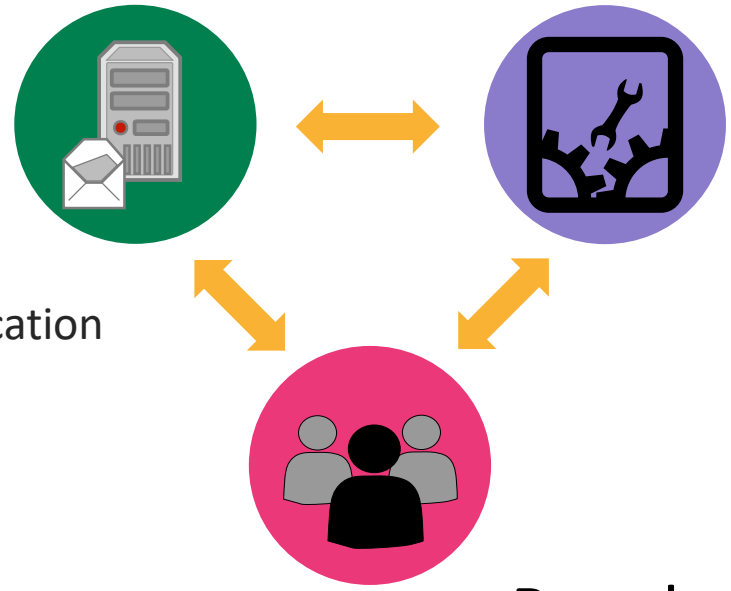
↑5x	Phishing attacks have quintupled since 2020.[1]
$10.2B	Victim losses in 2022.[2]
82%	Breaches involved the human element in 2021.[3]
74%	Reported spear phishing attacks in 2022.[4]

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

Phishing Defense

Technology

- Filtering
- DMARC, DKIM
- AI & ML
- Multi-factor authentication



Process

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

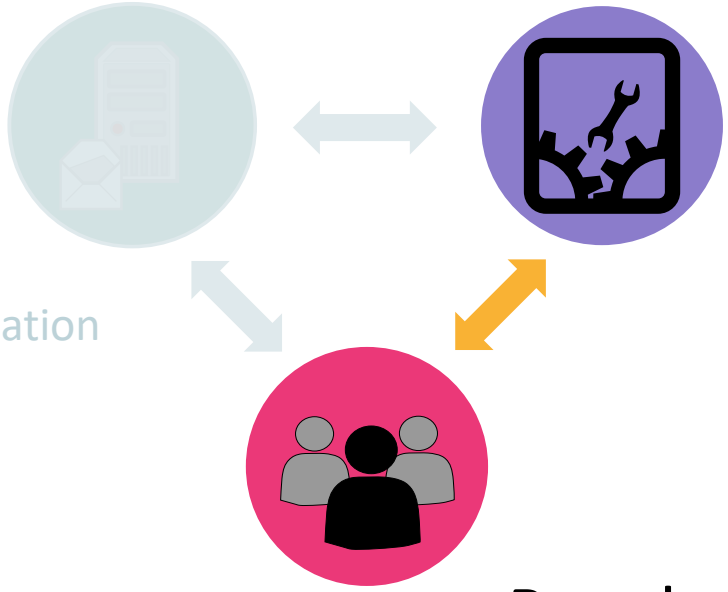
People

- End users
- IT security staff
- Leadership

Phishing Defense

Technology

- Filtering
- DMARC, DKIM
- AI & ML
- Multi-factor authentication



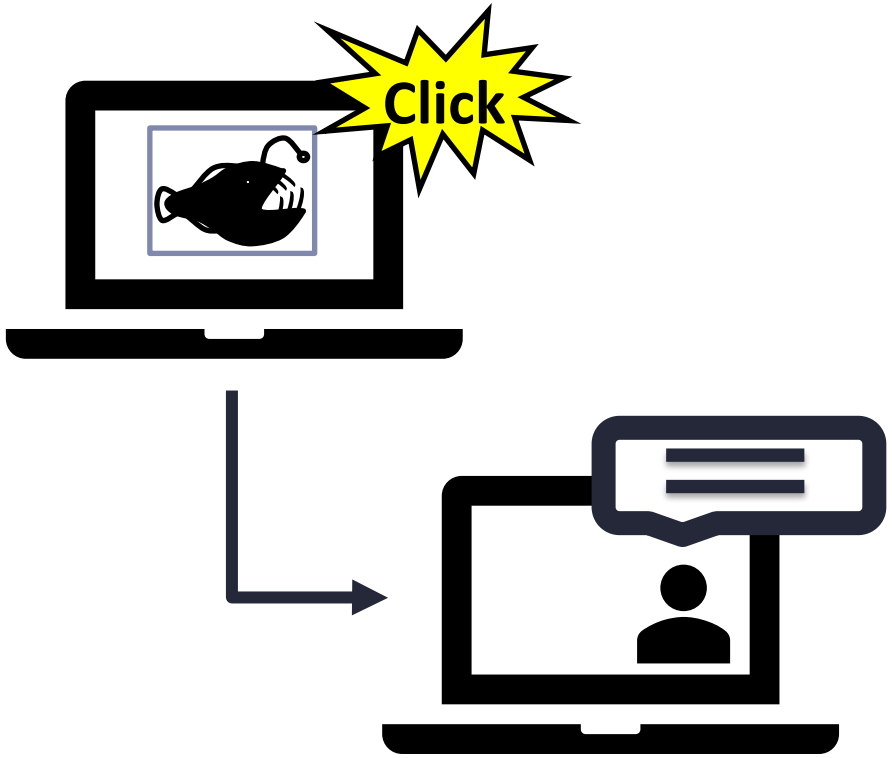
Process

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

People

- End users
- IT security staff
- Leadership

Phishing Awareness Training



Training in Practice

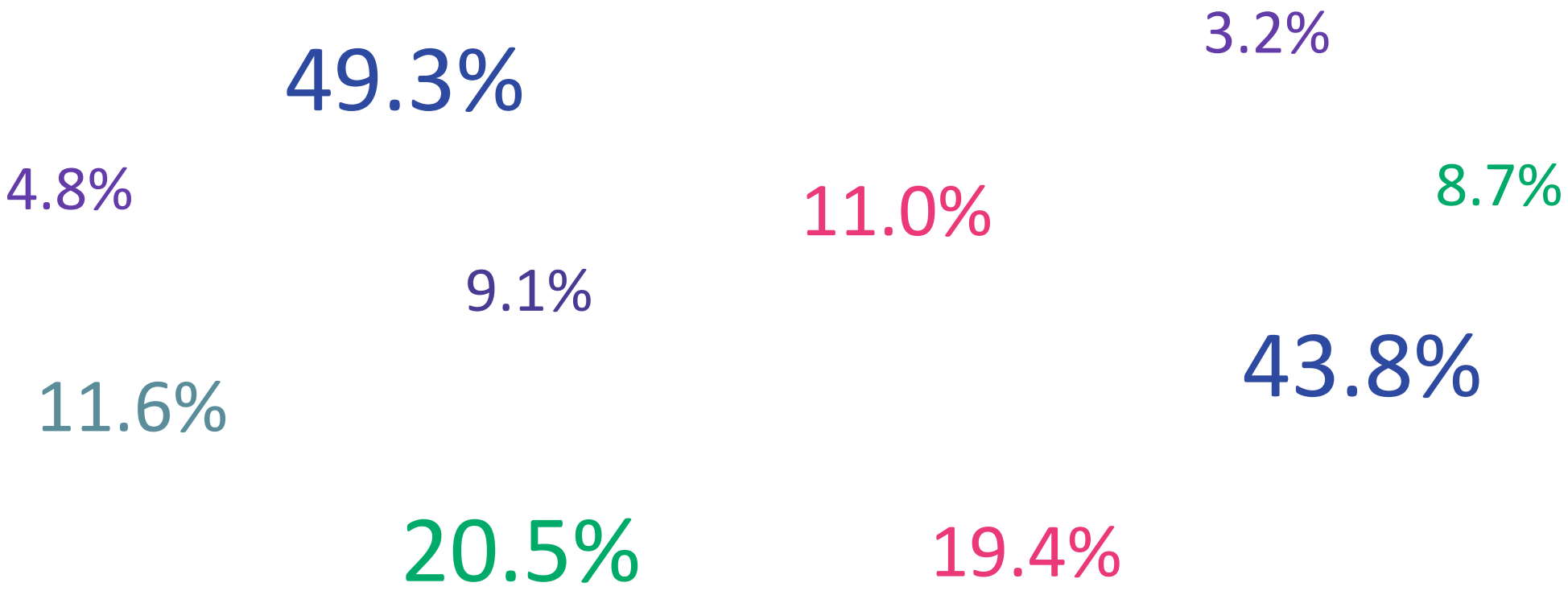
- Simulated phishing emails
- Gamifying phishing
  - e.g., phish hunting badges, shark awards
- Staff profiles

Common Metrics and Behaviors

- Click rates
- Reporting rates
- Repeat clickers
- Protective stewards

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

Variability in Click Rates

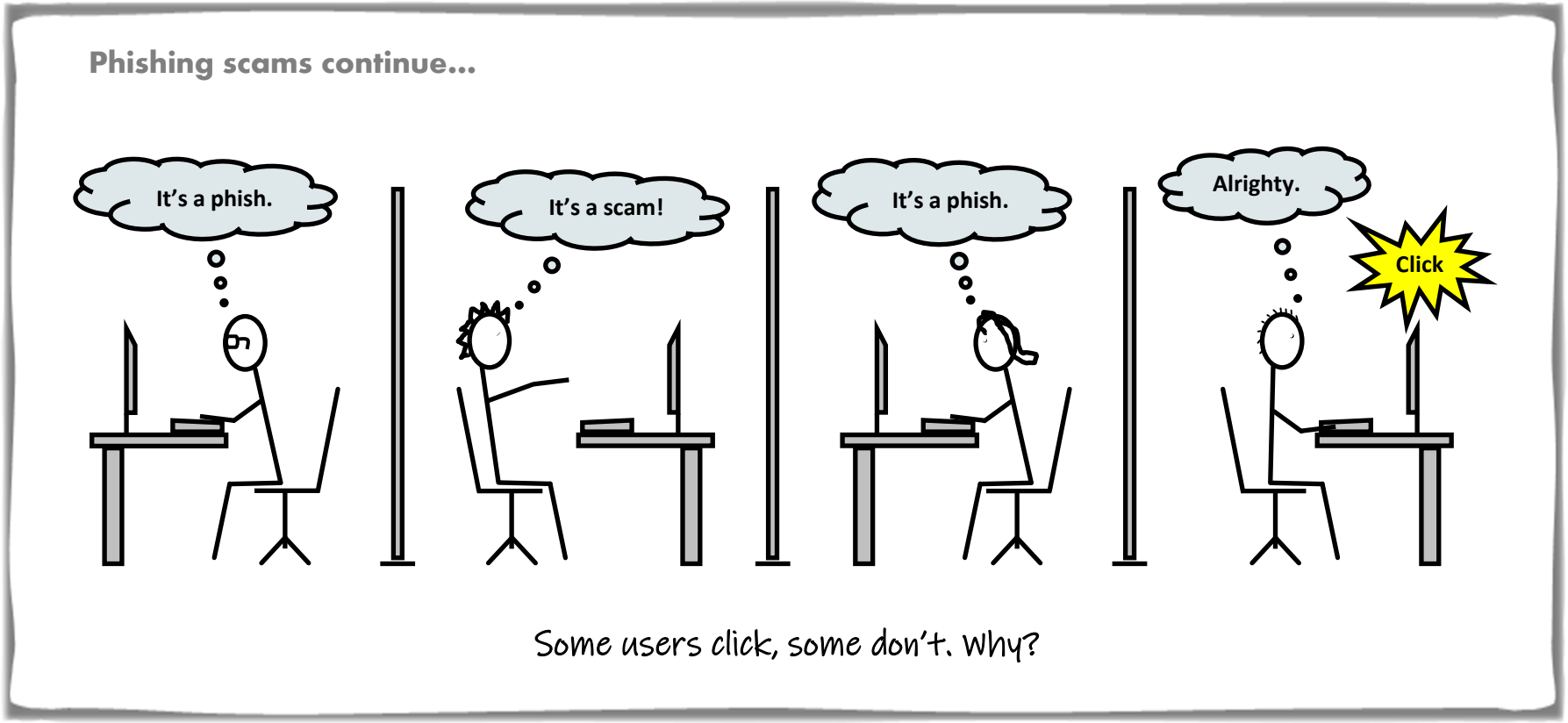


Click rates don't tell the whole story

RSAConference™2023

The Human Element

Phishing Awareness Study

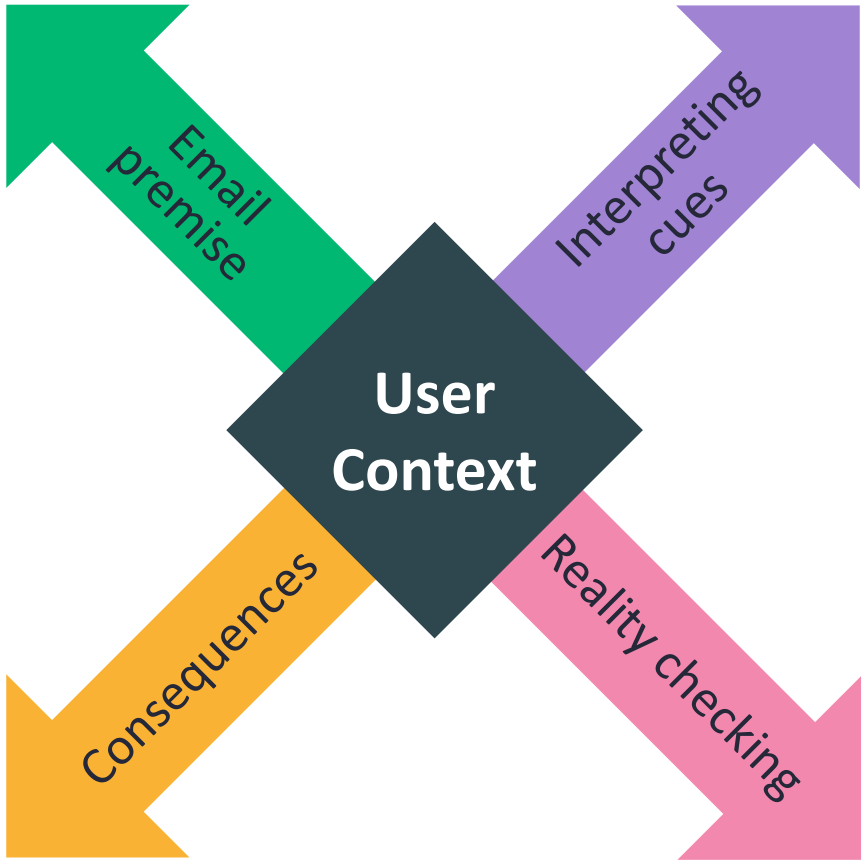


NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Image credit: NIST

User Context

Alignment vs. misalignment with expectations and external events



Compelling vs. suspicious cues

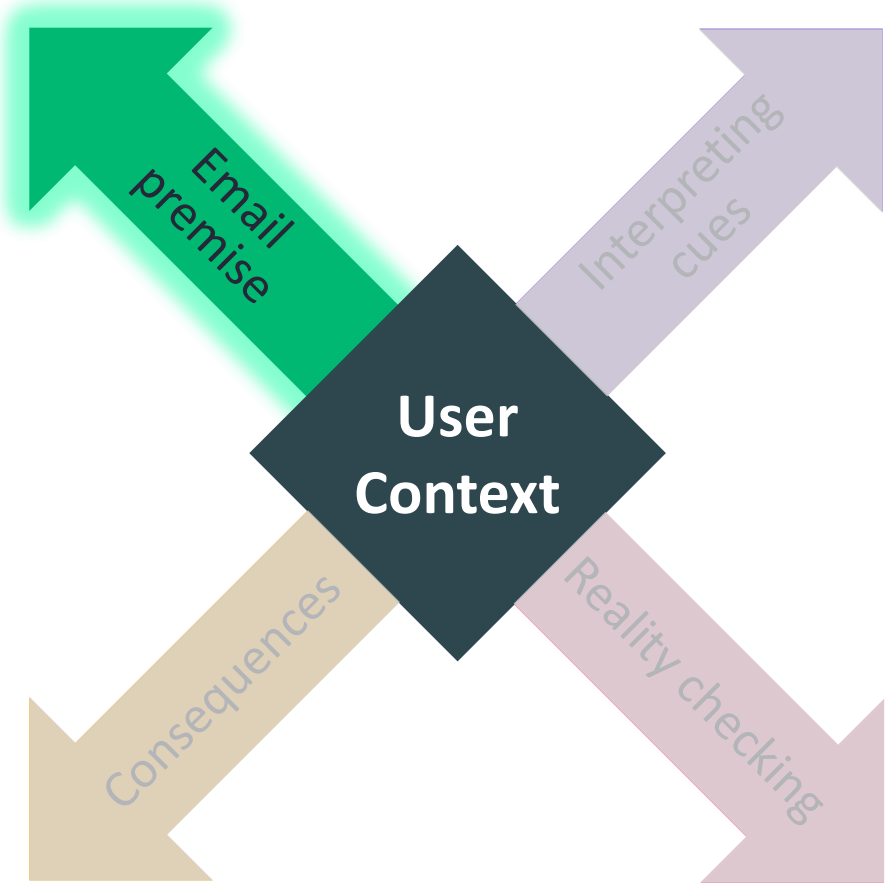
Concern over consequences

Reality-checking strategies

Participants Said…

Clicker

I pay invoices so I was wondering what invoice this was that did not get paid.



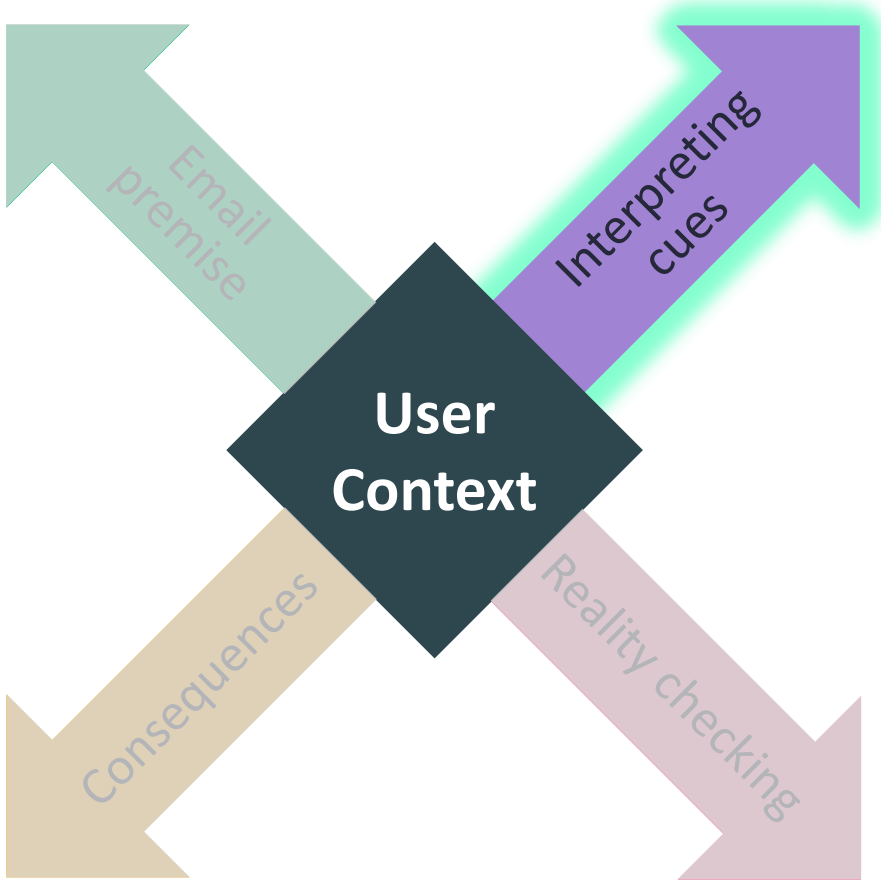
Non-clicker

I don't deal with invoices or anything having to do with accounts payable or accounts receivable.

Participants Said…

Clicker

The unfamiliar email is common at work, and generally not a problem. Did not trigger anything in my brain that would indicate that it was harmful.



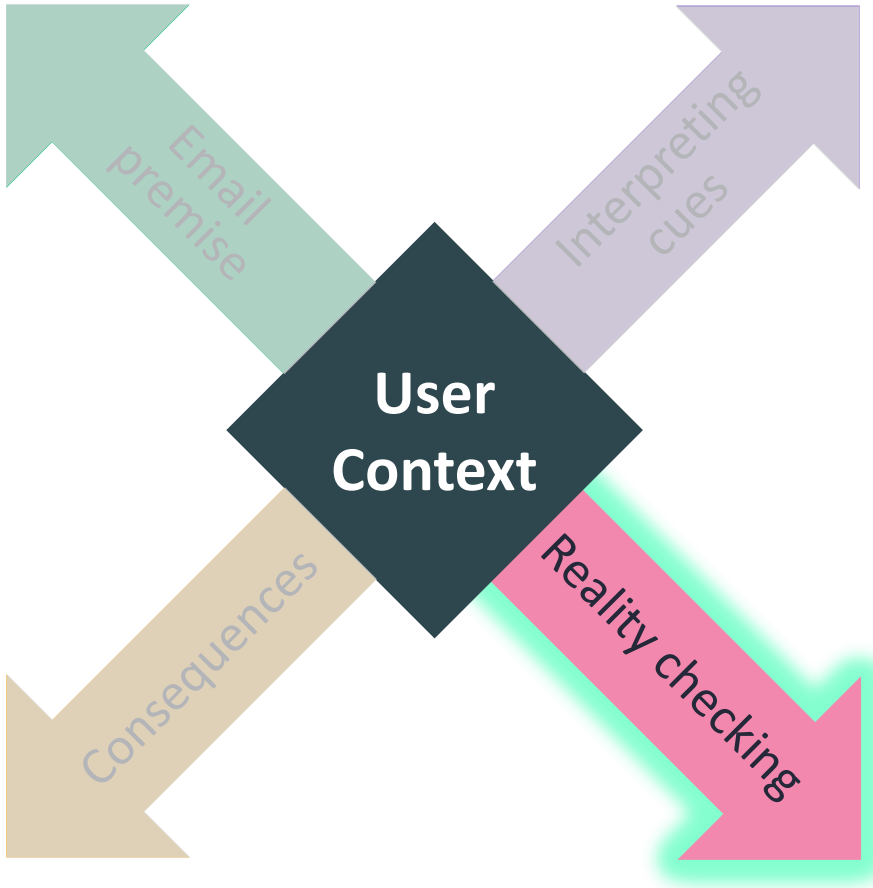
Non-clicker

Upon re-reading the email I became very suspicious. The email references a .doc attachment, but the attachment was a .zip file.

Participants Said…

Clicker

[The email was] from a NIST employee, figured she worked in AR and/or finance.



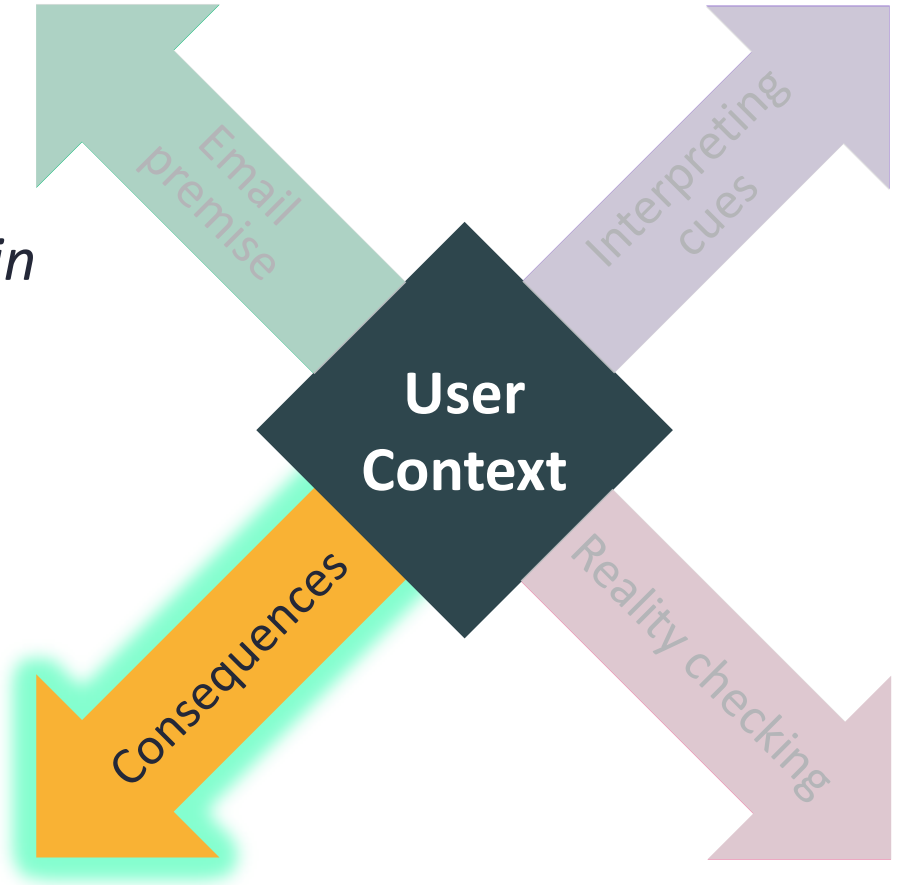
Non-clicker

I didn't think I had any unpaid invoices and then I looked up Jill Preston in the NIST user directory and the person didn't exist.

Participants Said…

Clicker

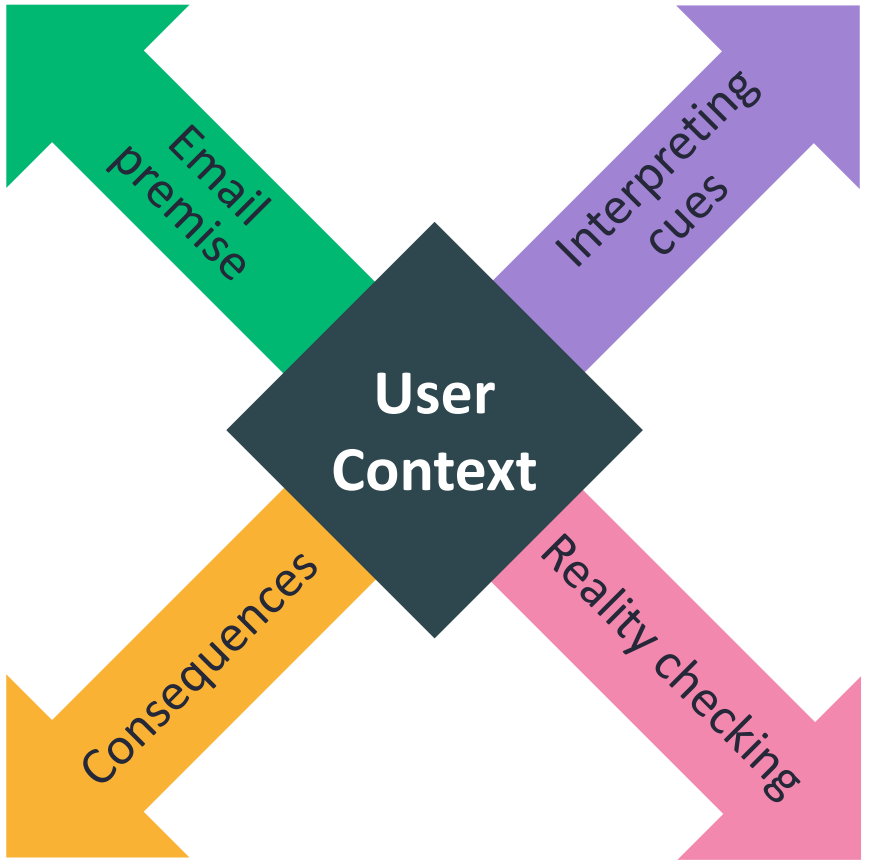
I am always interested in ensuring that I get any messages and act on them.



Non-clicker

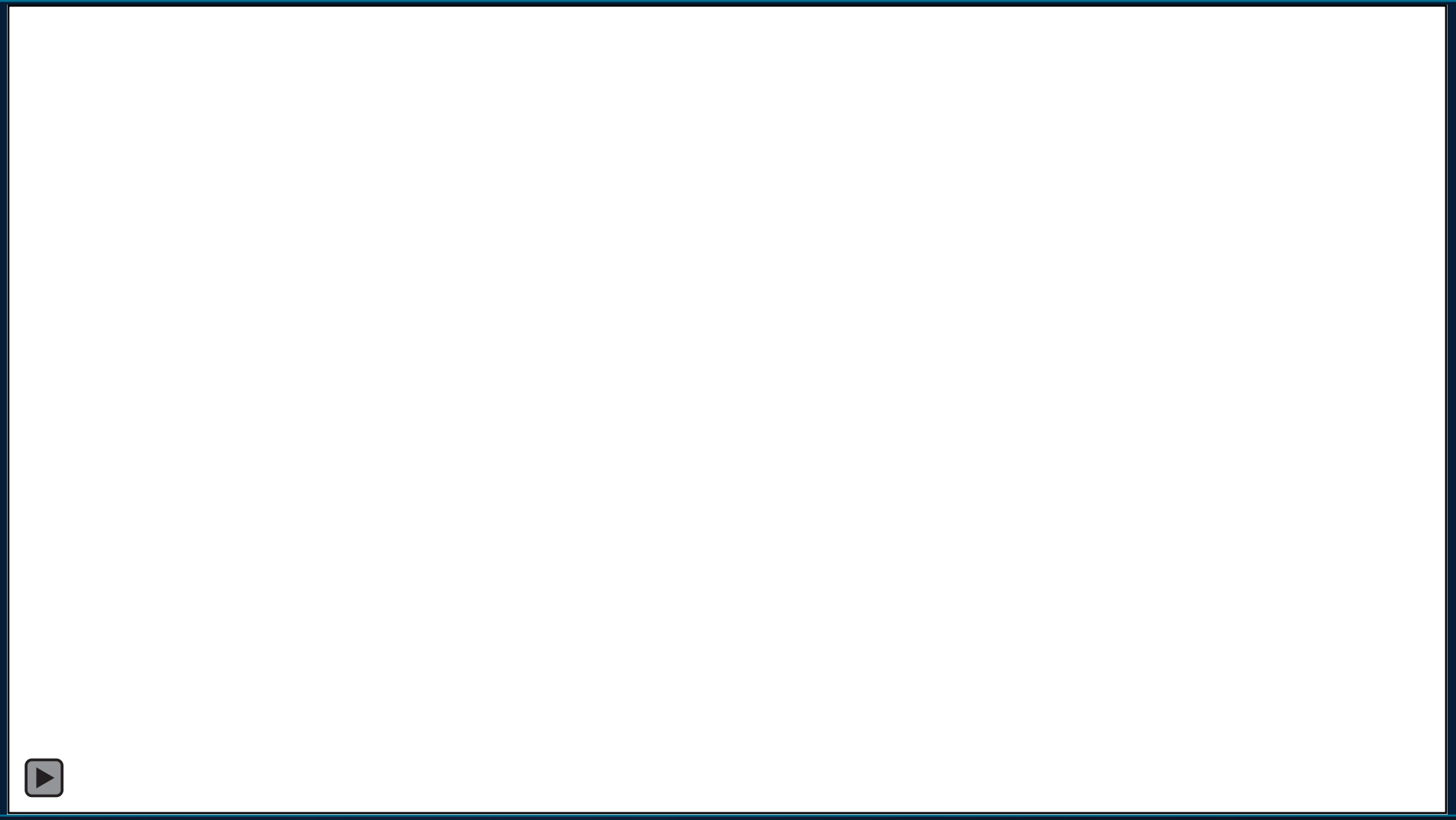
I was concerned something might be downloaded onto my computer or I could get a virus.

User Context



Now what?

NIST Phish Scale



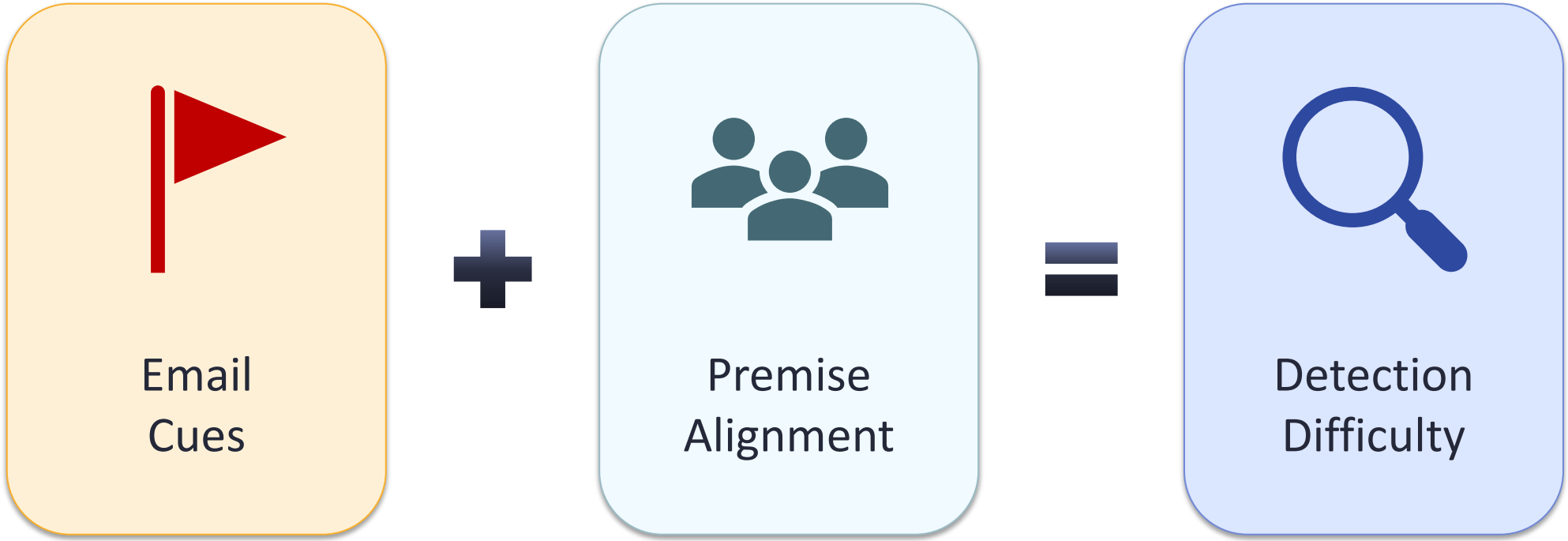
https://www.nist.gov/video/introducing-phish-scale

Image credit: NIST

The NIST Phish Scale

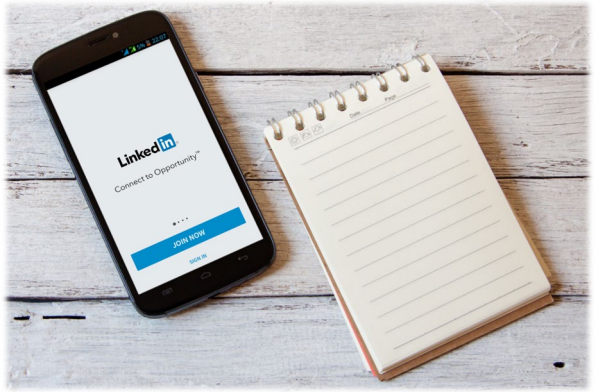
- Created in 2019 using real-world empirical data
- A metric that incorporates the human element to contextualize click rates
- Two components
  - Email cues
  - Premise alignment
- NIST Phish Scale output: detection difficulty rating

NIST Phish Scale Components



NIST Phish Scale Components

NIST Phish Scale – Cues



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

Images credit: Shutterstock *"McDowell's" credit: https://retruster.com/blog/phishing-email-scams-with-real-phishing-examples.html*

NIST Phish Scale Components

NIST Phish Scale – Premise Alignment

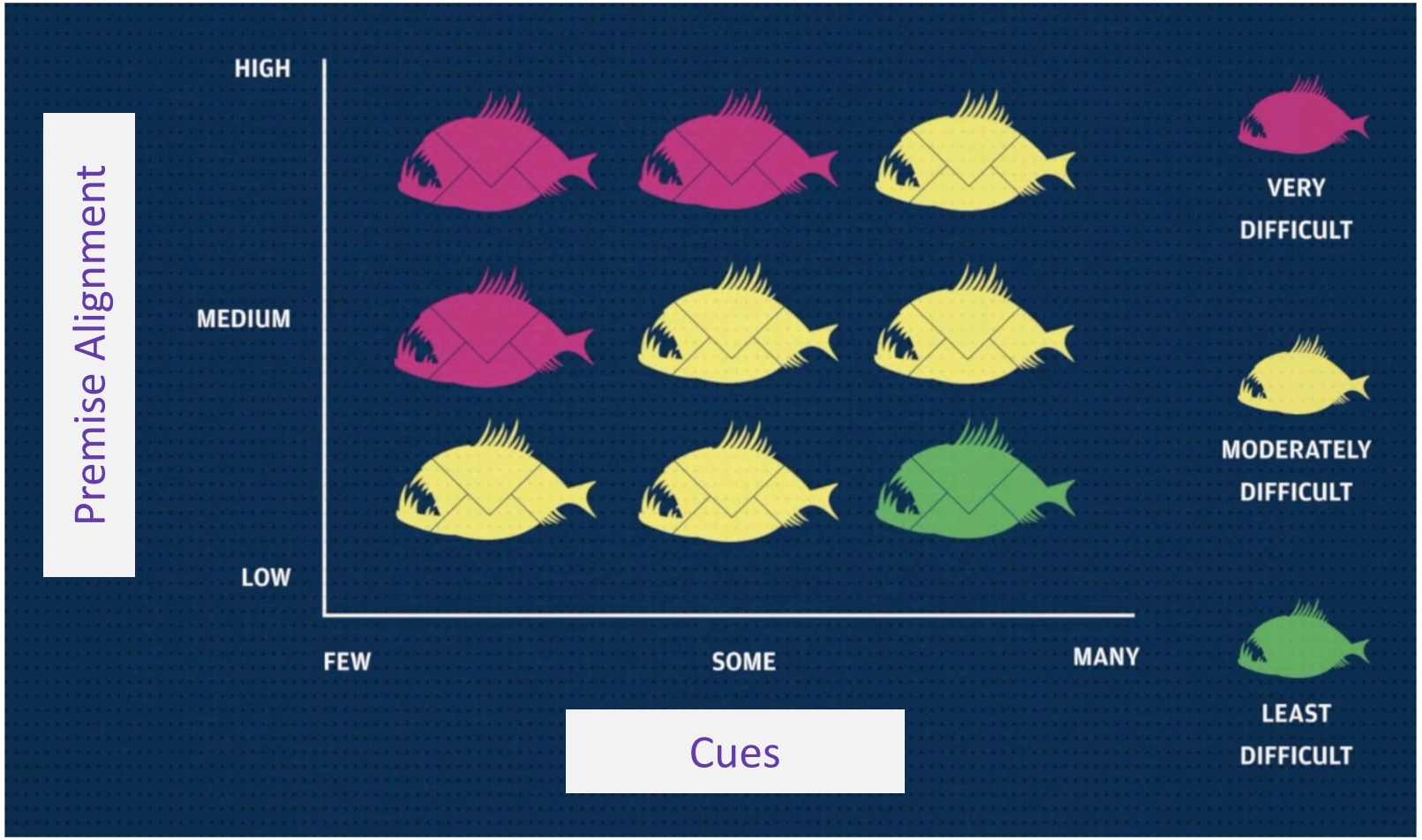
- Characterize relevancy of the email premise for the target audience
  - Based on workplace responsibilities and culture, business practice plausibility, staff expectations
  - Knowledge of target population context of work is crucial for accurate categorization

NIST Phish Scale – Premise Alignment

1. Mimics a workplace process or practice
2. Has workplace relevance
3. Aligns with other situations or events, including external to the workplace
4. Engenders concern over consequences for NOT clicking
5. Has been the subject of targeted training, specific warnings, or other exposure

NIST Phish Scale Components

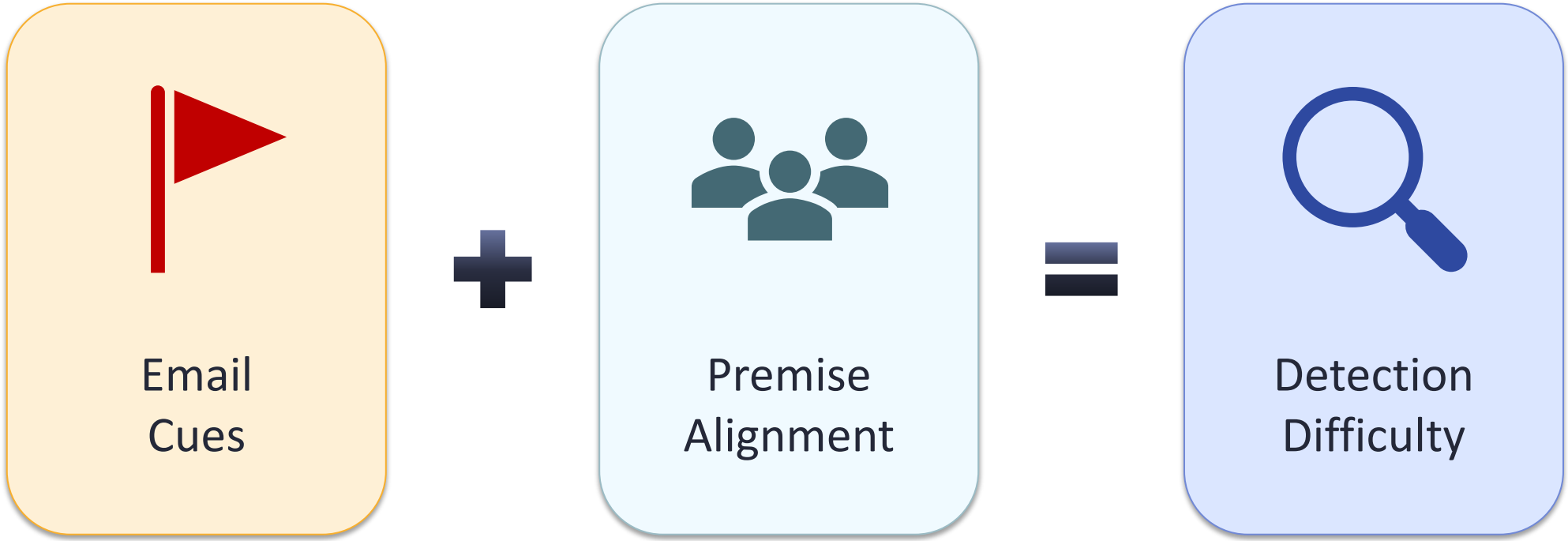
The NIST Phish Scale – Detection Difficulty



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

Image credit: NIST

NIST Phish Scale Components



Applying the NIST Phish Scale

- Applying NIST Phish Scale to NIST simulated phishing emails

From: Jones, Richard F. [mailto:richard.jones1@gmail.com]
Sent: Friday, August 31, 2012 8:00 AM
To: Doe, John E.
Subject: PLEASE READ THIS

Dear colleagues -

I highly encourage you to read this.

Safety Requirements

Best regards,

Rich

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

Dear Jane Doe,
Please see the attached invoice (.doc) and remit payment according to the terms listed at the bottom of the invoice.

Let us know if you have any questions.

We greatly appreciate your prompt attention to this matter!

Jill Preston

invoice_S-37644806.zip
3KB

Applying the NIST Phish Scale

From: System Administrator [mailto:notice@nist.gov]
Sent: Friday, February 21, 2014 1:00 PM
To: Doe, John <john.doe@nist.gov>
Subject: Unauthorized Web Site Access

This is an automated email

Our regulators require we monitor and restrict certain website access due to content. The filter system flagged your computer as one that has viewed or logged into websites hosting restricted content. The system is not fool-proof, and may incorrectly flag restricted content. The IT department does not investigate every web filter report, but disciplinary action may be taken.

Log into the filter system with your network credentials immediately and review your logs to see which websites triggered this alert.

Web Security Logs

Do not reply to this email. This email was automatically generated to inform you of a violation of our security and content policies.

Applying the NIST Phish Scale Broadly

- Designed to use a target audience
- Many organizations conduct phishing training and exercises as a one-size-fits-all approach
- Question: How to apply NIST Phish Scale to whole organization accurately?

Image credit: Shutterstock

Applying the NIST Phish Scale – Workplace Relevance

- How pertinent is the email to the work of the target audience?
- Different detection difficulty ratings for different job families:
  - Administrative support
  - Core mission employees
  - Facilities – field
  - Facilities – office
  - Legal
  - Management
  - Organization support staff

Applying the NIST Phish Scale – Workplace Relevance

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

Dear Jane Doe,
Please see the attached invoice (.doc) and remit payment according to the terms listed at the bottom of the invoice.

Let us know if you have any questions.

We greatly appreciate your prompt attention to this matter!

Jill Preston

invoice_S-37644806.zip
3KB

Whole Organization Application

Workplace Relevance: Low
Premise Alignment: Low
Detection Difficulty: Least to Moderate

Applying the NIST Phish Scale – Workplace Relevance

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

Dear Jane Doe,
Please see the attached invoice (.doc) and remit payment according to the terms listed at the bottom of the invoice.

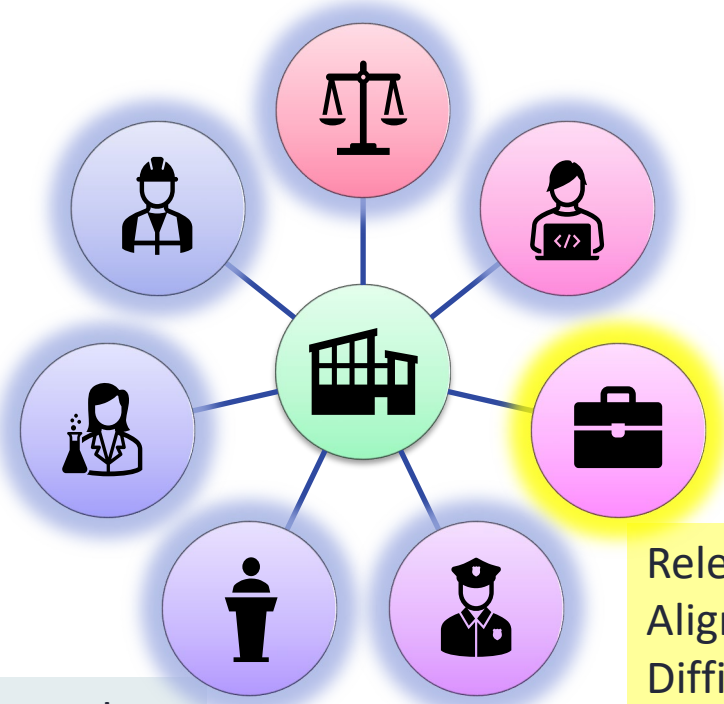
Let us know if you have any questions.

We greatly appreciate your prompt attention to this matter!

Jill Preston

invoice_S-37644806.zip
3KB

Job Family Application



Relevance: High
Alignment: High
Difficulty: Very

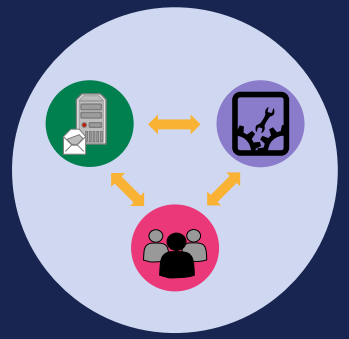
Relevance: Low
Alignment: Low
Difficulty: Least

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

RSAConference™2023

Final Parting Thoughts

Summary



Multi-Pronged

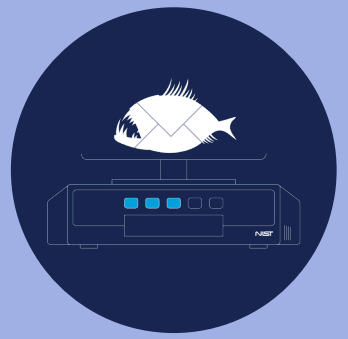
Organizational phishing defense

Click rates

Click rates will not go to zero! (and stay there)

User context

Understand human element to contextualize click rates



NIST Phish Scale

Don't fish without a net!

Apply What You've Learned

- Next week you should:
  - Bring members of cybersecurity awareness team up-to-date on premise alignment and phishing cues
  - If you *do* already have a phishing awareness program:
    - examine the context and premise alignment of the phishing emails that have been used
  - If you *don't* already have a phishing awareness program:
    - consider simulated phishing training or training about phishing cues and user context

- In the first three months following this presentation you should:
  - Tailor phishing awareness program to current threats your organization faces
  - Contextualize training data results – consider email premises that align with staff roles and responsibilities
  - Reassess impact of phishing program in your organization

Big Takeaway

In an organization’s phishing defense, consider the **human elements** of phishing training

Contacts and Additional Resources

Shanée Dawkins, Jody Jacobs
usability@nist.gov

https://csrc.nist.gov/usable-cybersecurity/phishing

NIST Phishing Research

The NIST Phish Scale is free to use for academic purposes. For any commercial use, companies will need to reach out to our partnership office for a license.

References

1. Anti-Phishing Working Group (APWG) **Phishing Activity Trends Report**, 3rd Quarter 2022 https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf (Accessed March 15, 2023)

2. Federal Bureau of Investigation Internet Crime Complaint Center (IC3) **Internet Crime Report** https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf (Accessed March 15, 2023)

3. Verizon 2022 **Data Breach Investigations Report** (DBIR) https://www.verizon.com/business/resources/reports/dbir/ (Accessed March 15, 2023)

4. Proofpoint 2023 **State of the Phish report** https://www.proofpoint.com/us/resources/threat-reports/state-of-phish (Accessed March 15, 2023)

References

- Haney, J. , Jacobs, J. and Furman, S. (2022), **Approaches and Challenges of Federal Cybersecurity Awareness Programs**, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8420A (Accessed February 9, 2023)
- 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/10.1177/2158244021990656 (Accessed February 9, 2023)
- National Cybersecurity Alliance (NCSA) **Oh, Behave! The Annual Cybersecurity Attitudes and Behaviors Report** 2022. https://staysafeonline.org/online-safety-privacy-basics/oh-behave/ (Accessed February 9, 2023)
- Greene, Kristen & Steves, Michelle & Theofanos, Mary & Kostick, Jennifer. (2018). **User Context: An Explanatory Variable in Phishing Susceptibility**. https://www.ndss-symposium.org/wp-content/uploads/2018/07/usec2018_01-2_Greene_paper.pdf (Accessed February 9, 2023)

References

- Michelle P. Steves, Kristen K. Greene and Mary F. Theofanos. **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 9, 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 9, 2023)
- Barrientos, F., Jacobs, J., and Dawkins, S., **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 9, 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 9, 2023)