

Phishing for User Context: Understanding the NIST Phish Scale

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.

- Who we are
- Phishing threat landscape
- Our research & the NIST Phish Scale

Championing the Human in I.T.

NIST



PHISHING THREAT LANDSCAPE

Phishing Landscape

↑ 5x

Phishing attacks have quintupled since 2020.¹

\$10.2B

Victim losses in 2022.²

82%

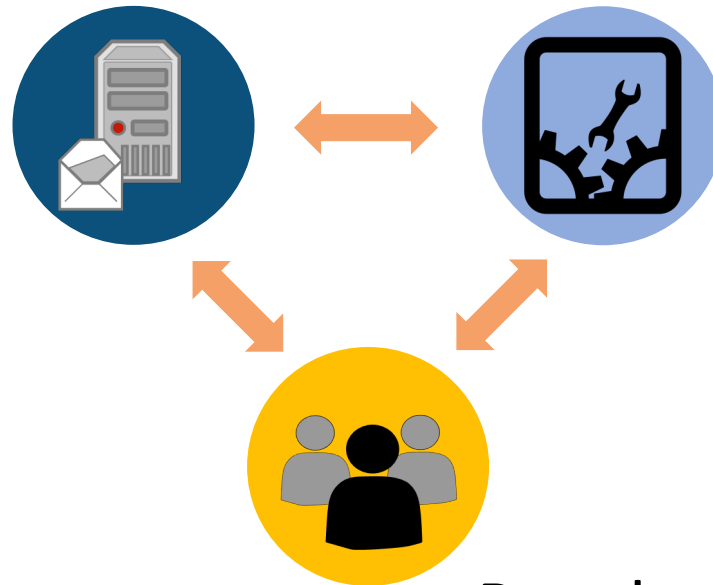
Breaches involved the human element in 2021.³

74%

Reported spear phishing attacks in 2022.⁴

Technology

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



Process

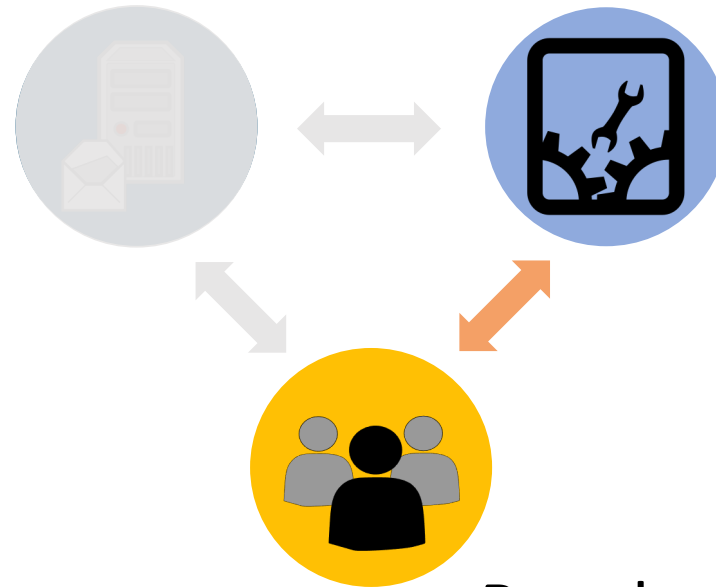
- Identify vulnerabilities
- Limiting publicly available information
- Awareness training
- Easy and clear reporting mechanism
- Meaningful metrics

People

- End users
- IT security staff
- Leadership

Technology

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

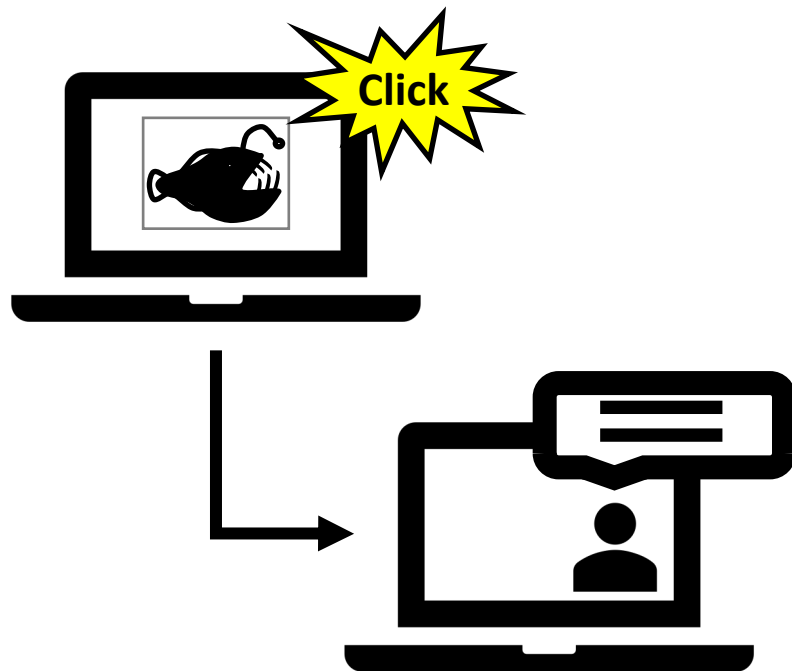


Process

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

People

- End users
- IT security staff
- Leadership



Training in Practice

- Simulated phishing emails
- Gamify phishing
 - e.g., phish hunting badges, shark awards
- Staff Profiles

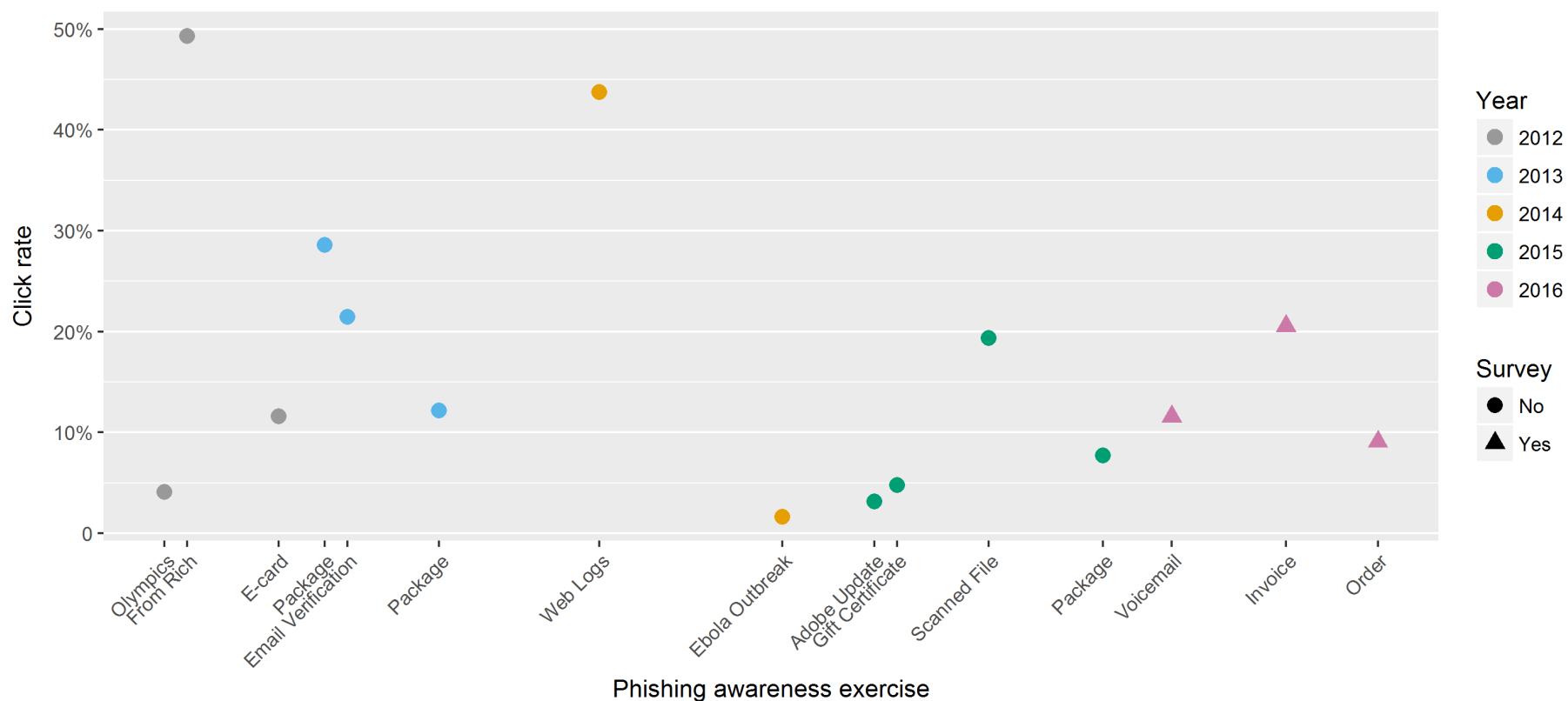
Common Metrics and Behaviors

- Click rates
- Reporting rates
- Repeat clickers
- Protective stewards⁵

OUR RESEARCH

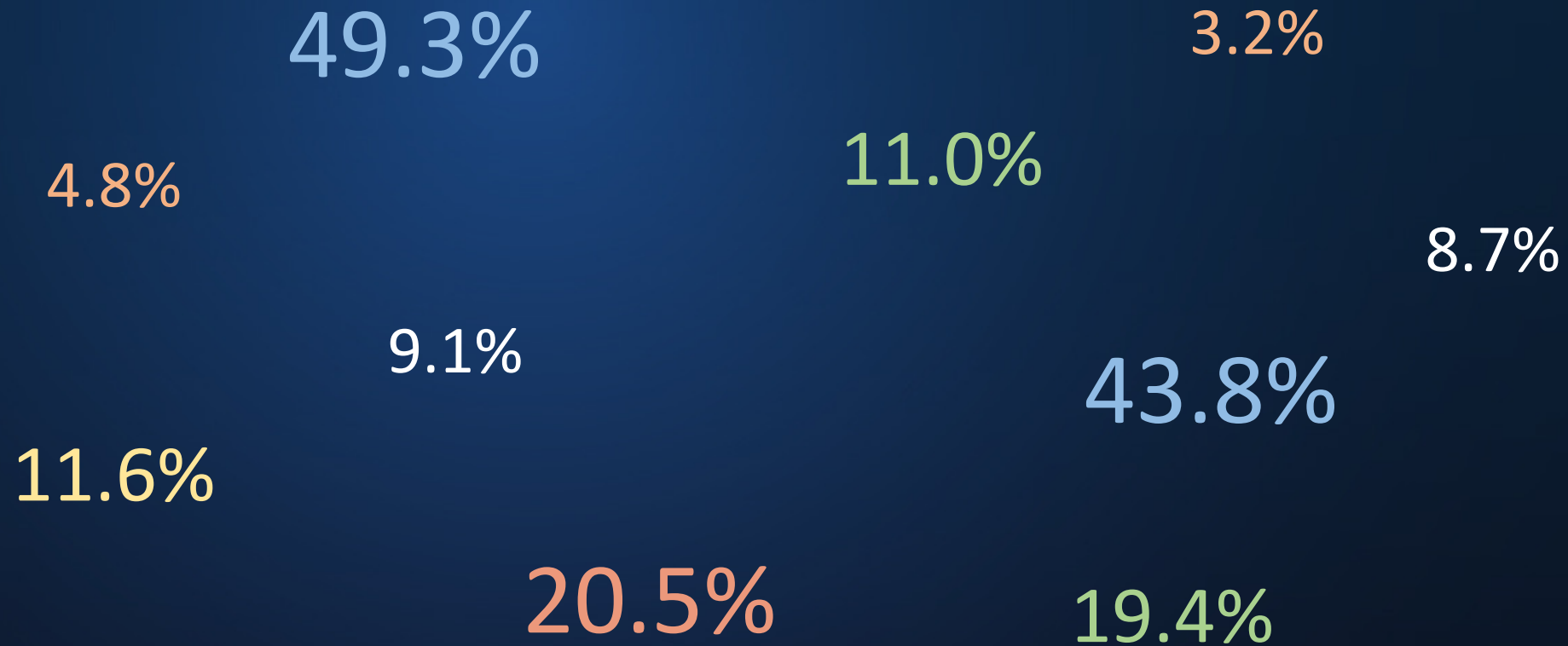
Our Research – Phishing Awareness Study

- 15 training exercises over 4.5 years

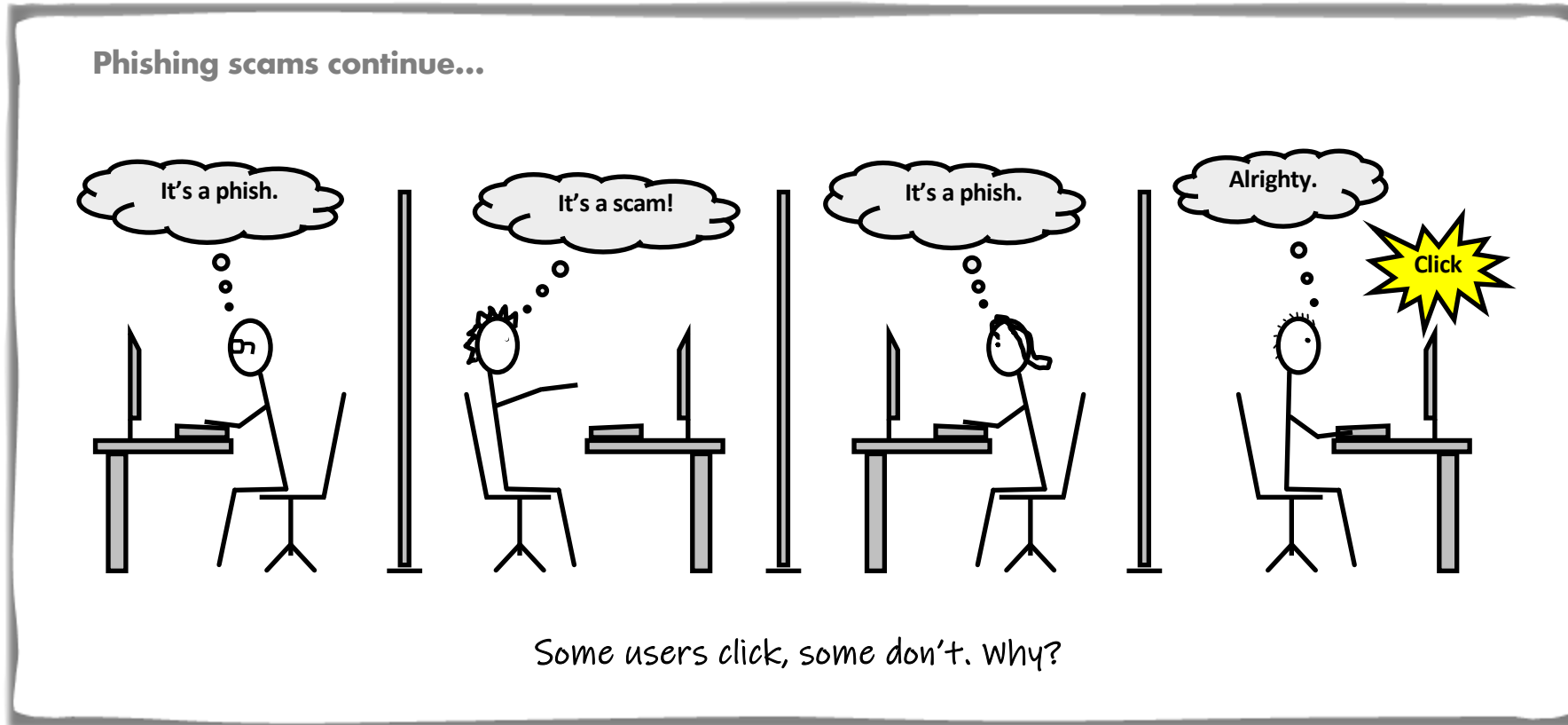


Our Research – Phishing Awareness Study

NIST

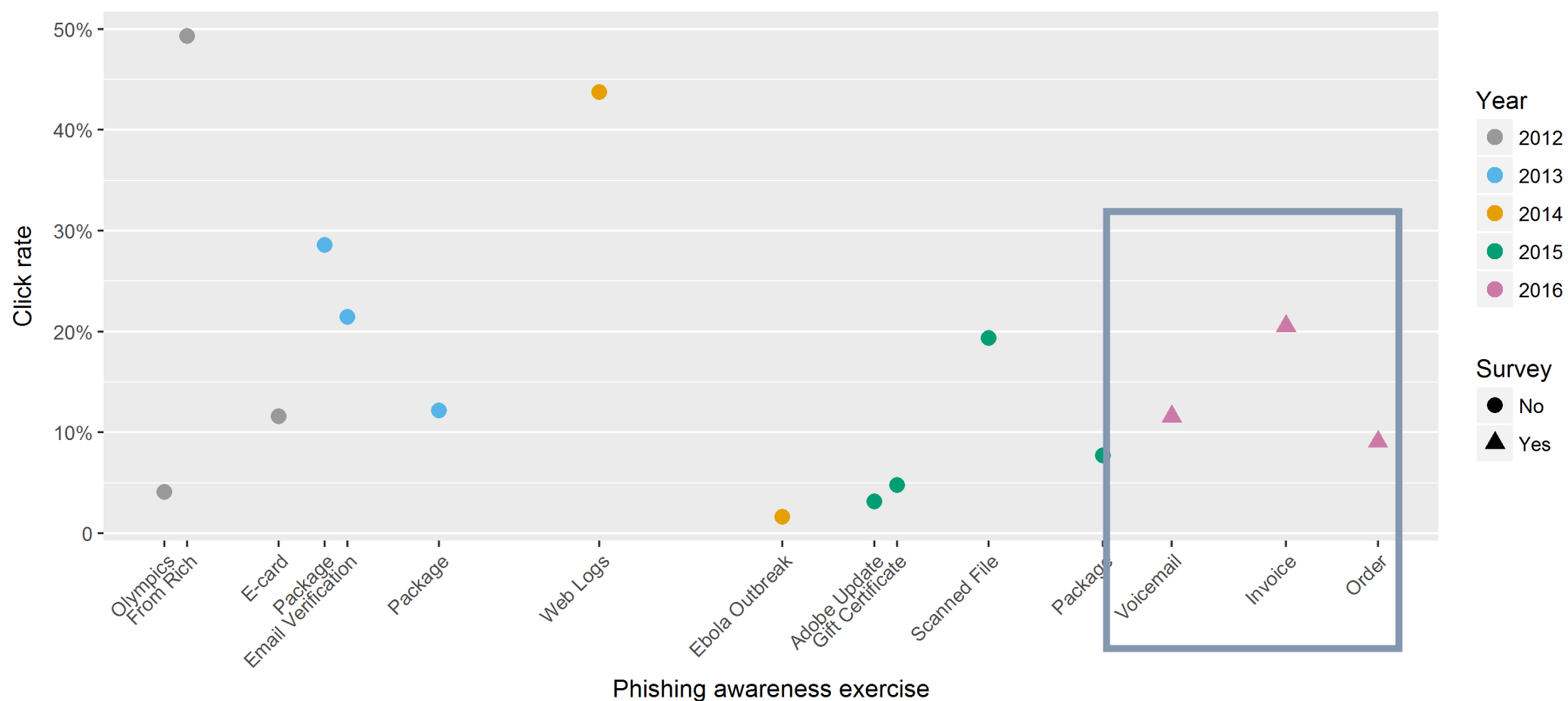


Our Research – Phishing Awareness Study



Our Research – Phishing Awareness Study

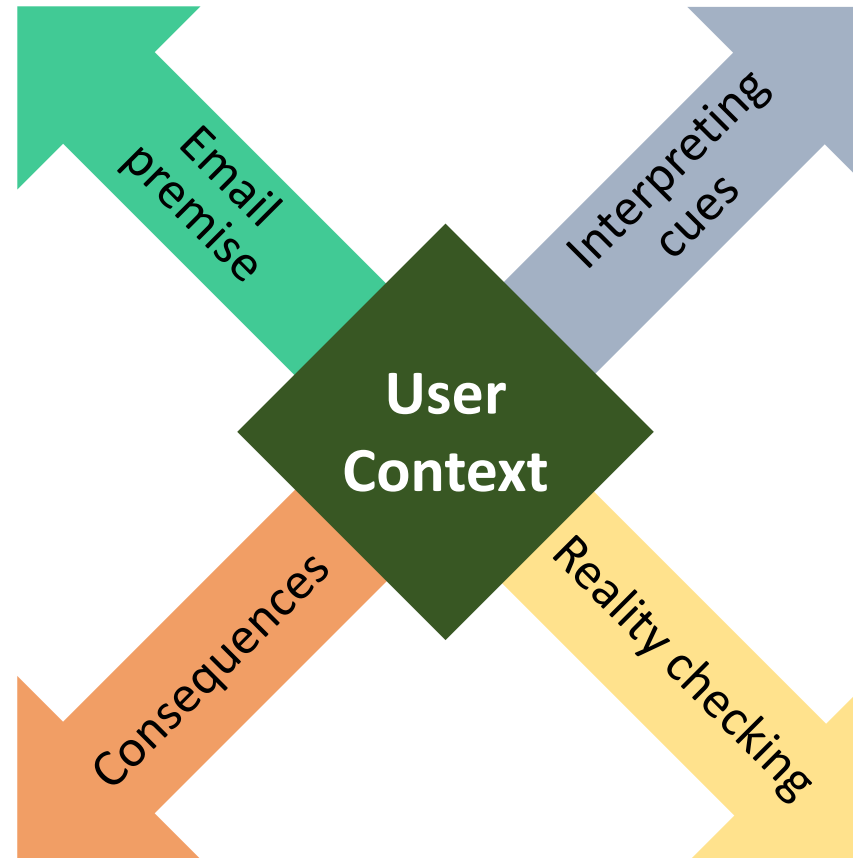
- 15 training exercises over 4.5 years
- Corresponding survey data for last 3 exercises



Our Research – Phishing Awareness Study

Alignment vs.
misalignment with
expectations and
external events

Concern over
consequences



Compelling vs.
suspicious cues

Reality-checking
strategies

Our Research – NIST Phish Scale

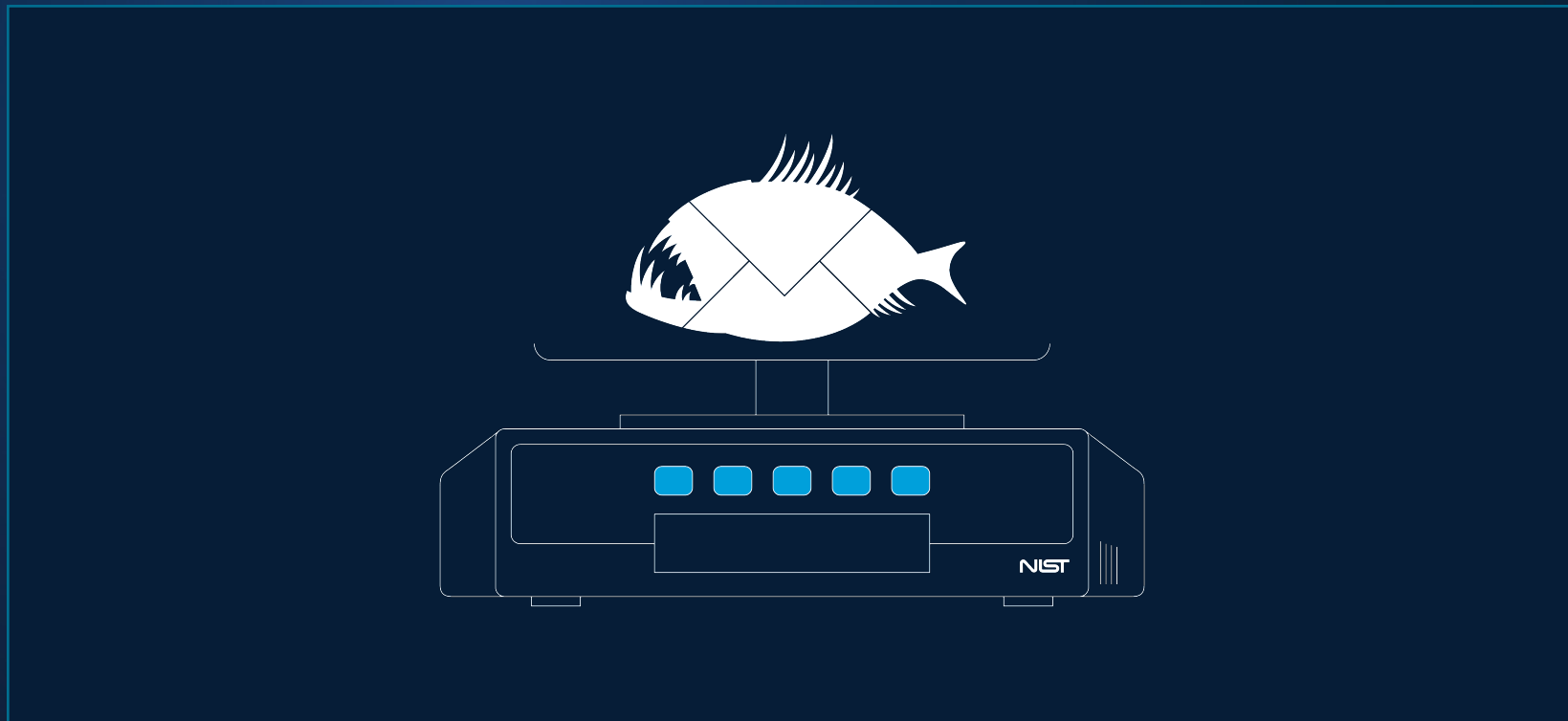
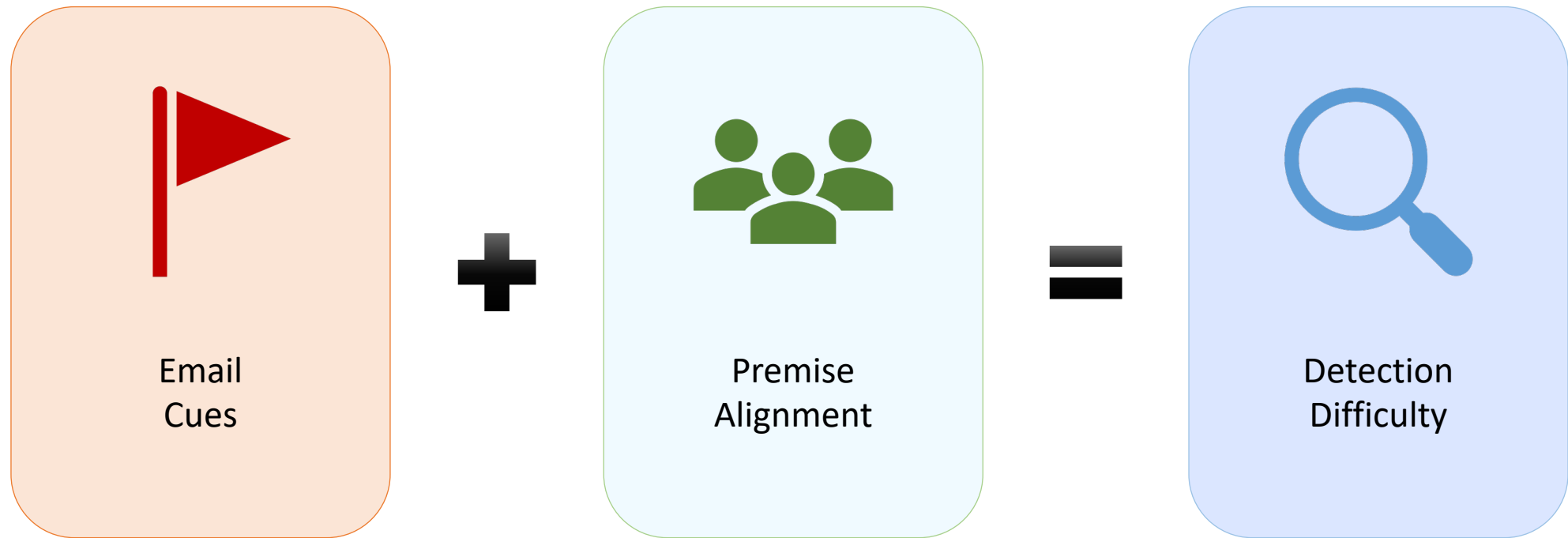


Image credit: NIST

<https://www.nist.gov/video/introducing-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



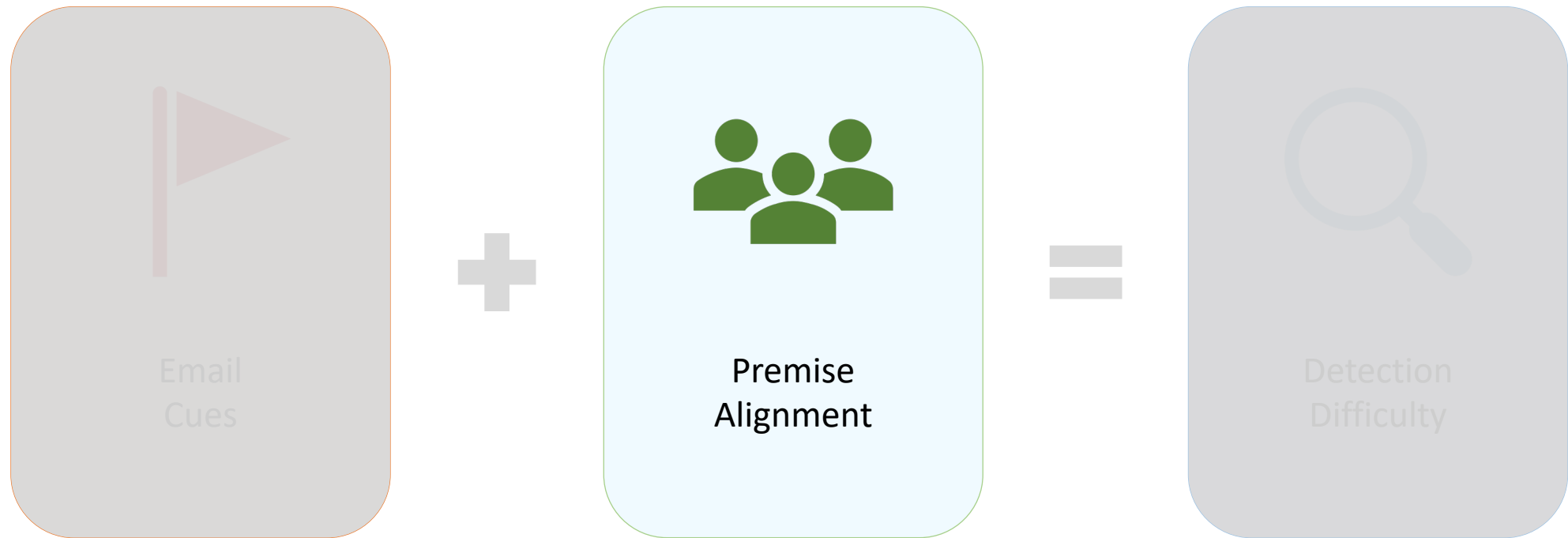
NIST Phish Scale Components



NIST Phish Scale – Cues



NIST Phish Scale Components



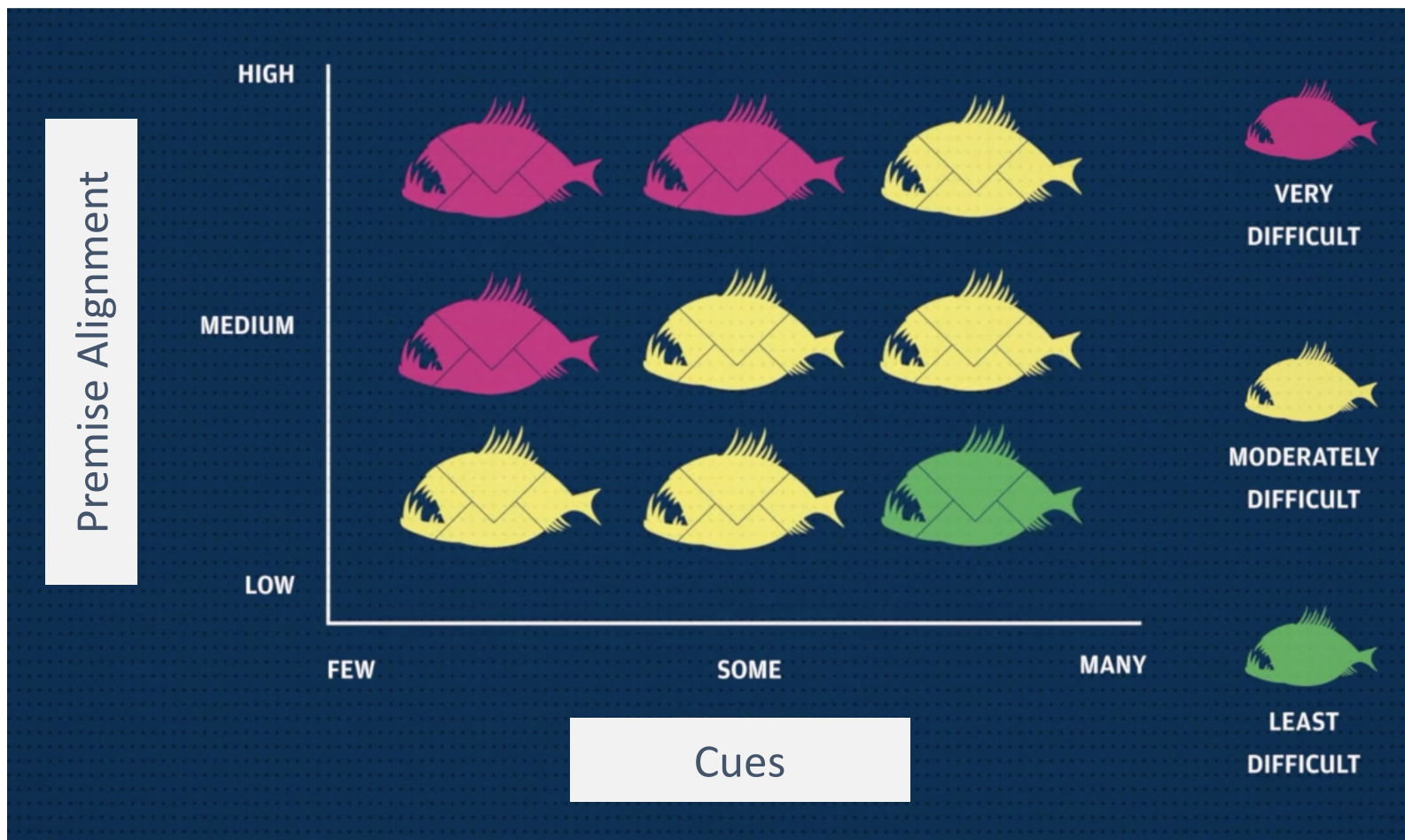
- Characterize relevancy of the email premise for the target audience
 - Based on workplace responsibilities and culture, business practice plausibility, staff expectations
 - Knowledge of target population context of work is crucial for accurate categorization

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

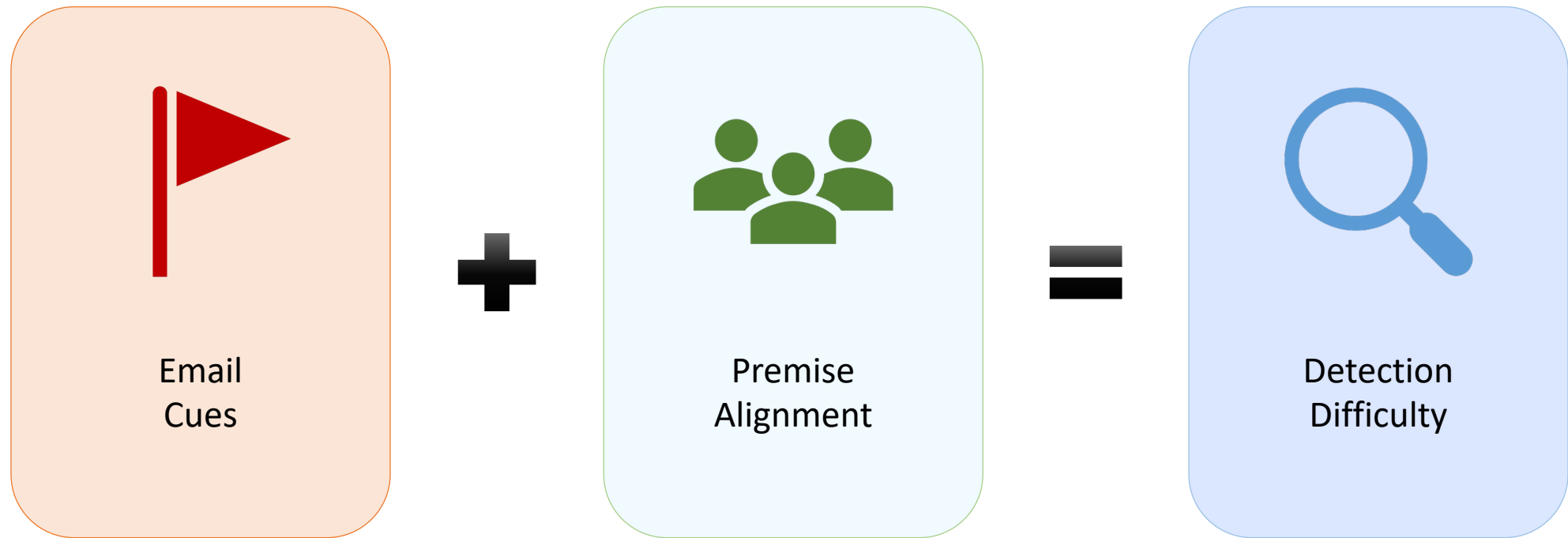
NIST Phish Scale Components



The NIST Phish Scale – Detection Difficulty



NIST Phish Scale Components



APPLYING THE NIST PHISH SCALE

Applying the NIST Phish Scale

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.

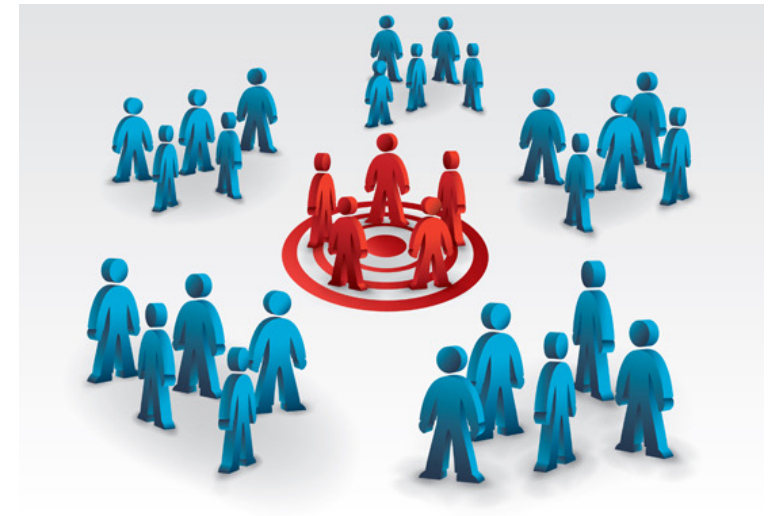
Log into the filter system with your network credentials immediately and review your logs to see which websites triggered this alert.

[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?



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

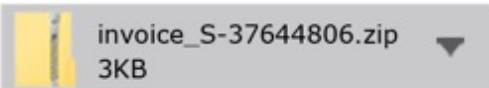
From: Preston, Jill (Fed) [<mailto:jill.preston@nist.gov>]
Sent: Friday, August 05, 2016 12:03 PM
To: Doe, Jane (Fed) <jane.doe@nist.gov>
Subject: Unpaid invoice #4806

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



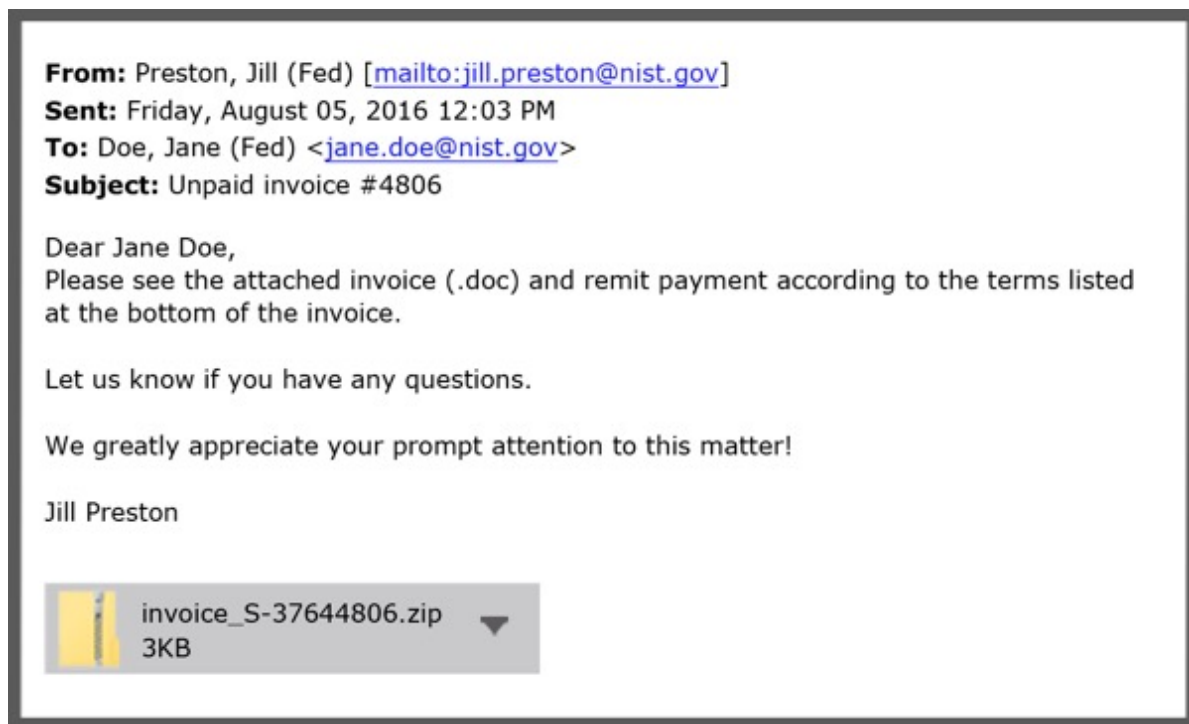
Whole Organization Application

Workplace Relevance: Low

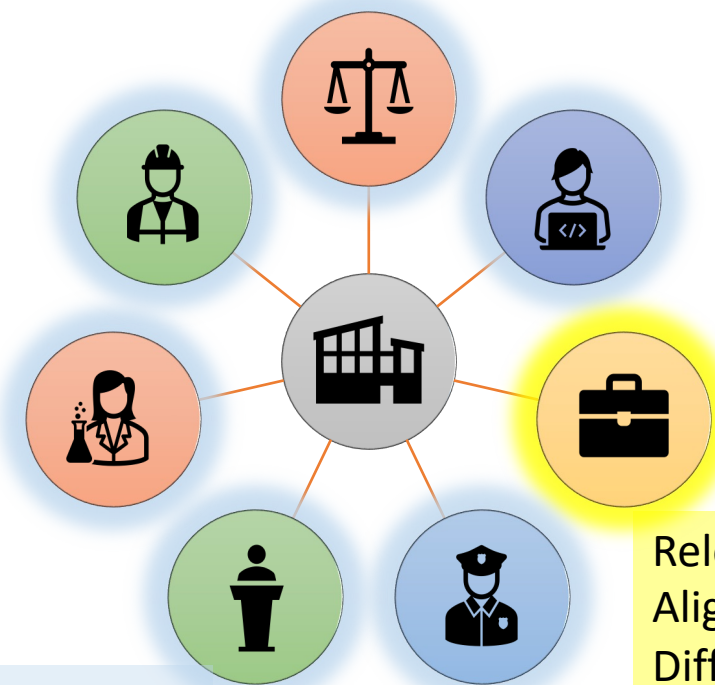
Premise Alignment: Low

Detection Difficulty: Least to Moderate

Applying the NIST Phish Scale – Workplace Relevance



Job Family Application



Relevance: Low
Alignment: Low
Difficulty: Least

Relevance: High
Alignment: High
Difficulty: Very



Multi-Pronged

**Organizational
phishing defense**



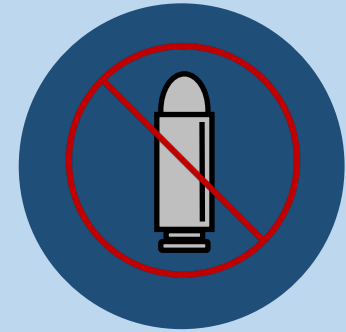
Click rates

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



User context

**Understand
human element
to contextualize
click rates with the
NIST Phish Scale**



No silver bullet

**Awareness training
is not the silver
bullet in phishing
defense**

Additional Resources



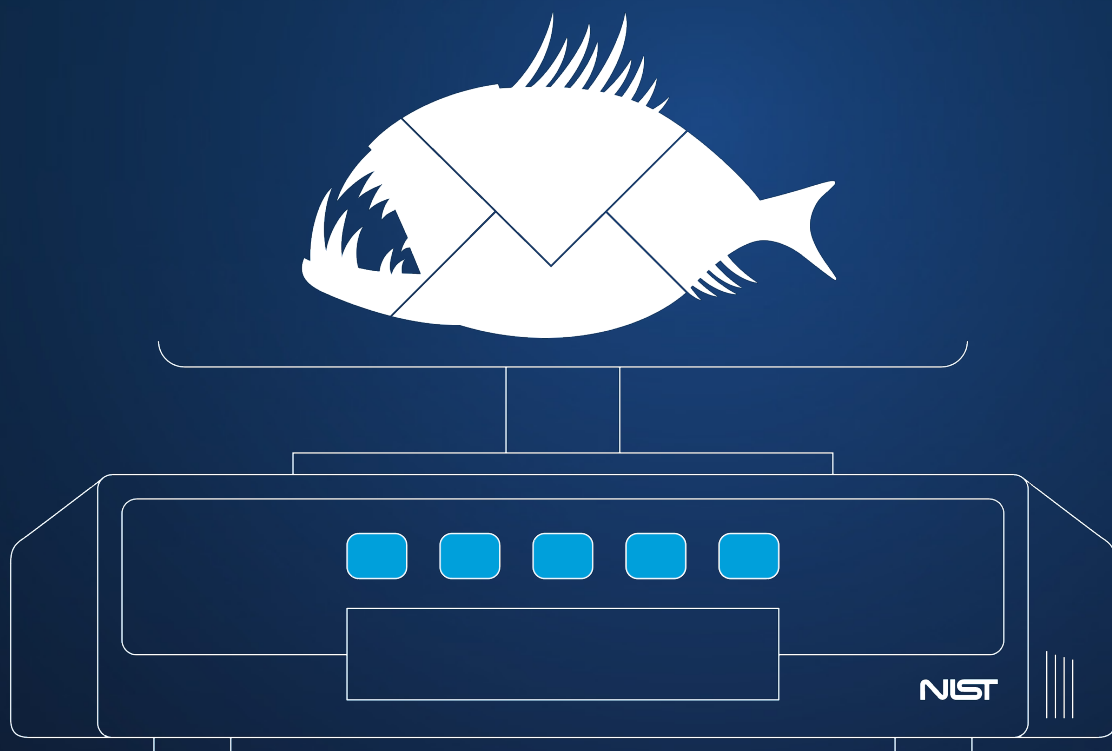
- Shanée Dawkins, dawkins@nist.gov
- Jody Jacobs, jody.jacobs@nist.gov



- <https://csrc.nist.gov/projects/usable-cybersecurity>
- <https://csrc.nist.gov/usable-cybersecurity/phishing>



NIST Phishing Research



Q&A

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)
5. 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)

- 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 HCI 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)