The NIST Phish Scale: Considering user context in phishing awareness programs

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

Shanée Dawkins, Ph.D.

Jody Jacobs, M.S.

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

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

Championing the Human in I.T.

The NIST Phish Scale and the Human Element

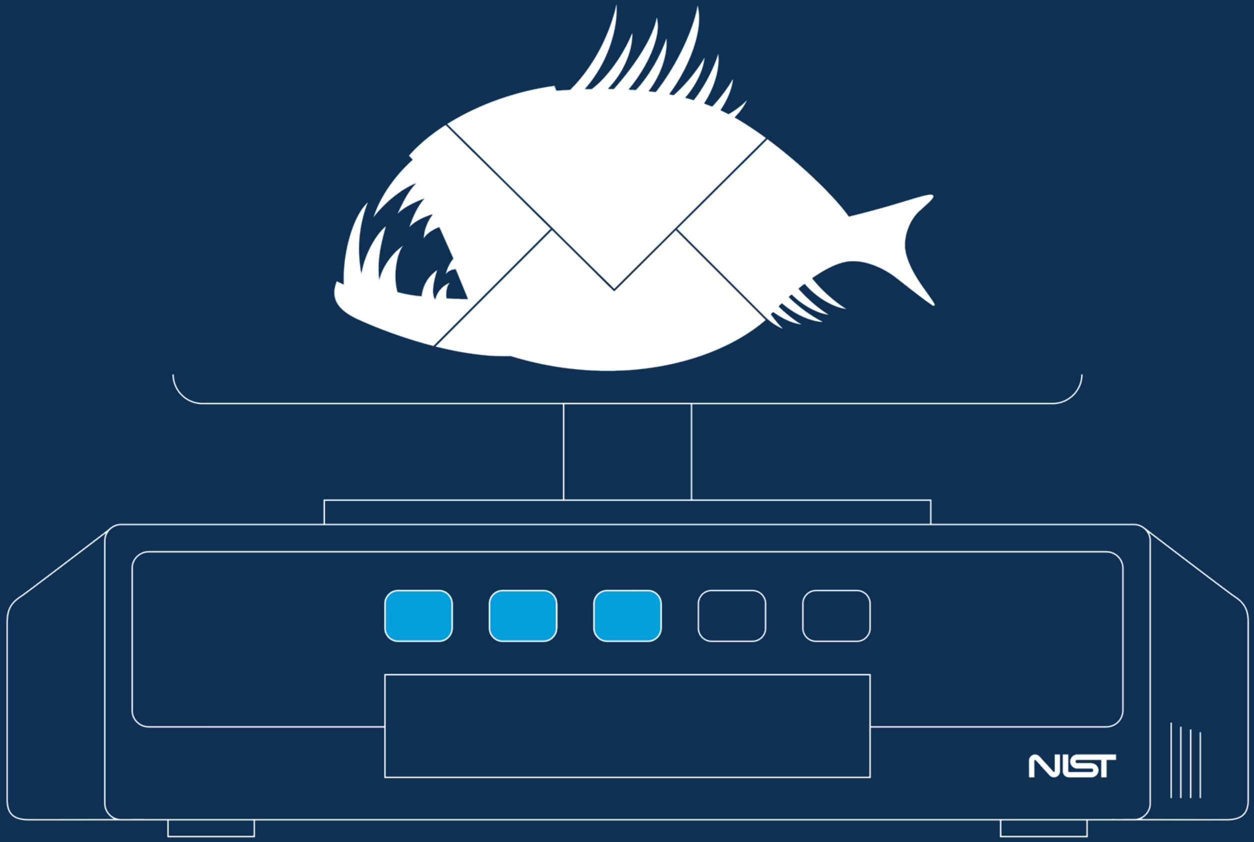


Image credit: NIST

Defending Against Phishing

Phishing Threat Landscape

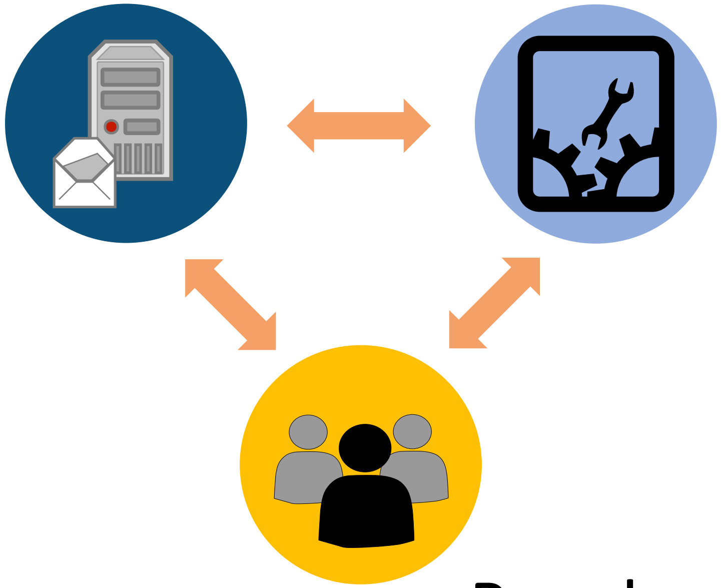
Phishing Threats

Broad cybersecurity email attacks

Spear Phishing

Direct and targeted email attacks

Phishing defense must be multi-pronged



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

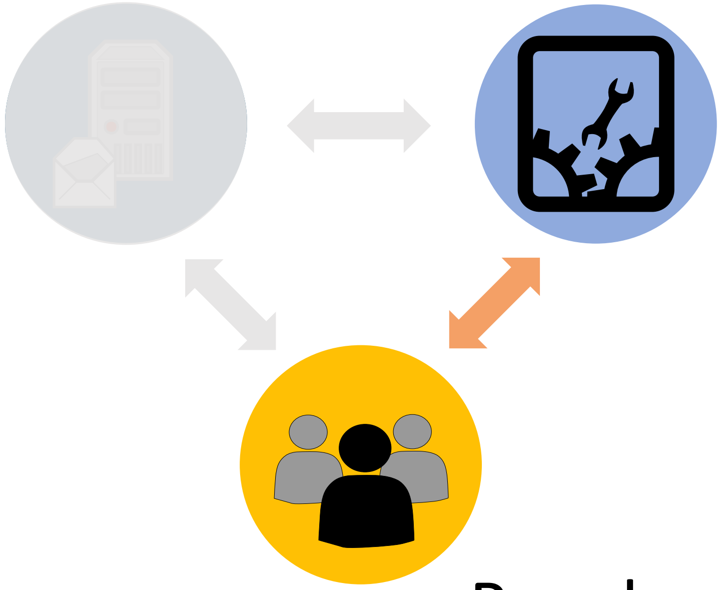
People

- End users
- IT security staff
- Leadership

Phishing defense must be multi-pronged

Technology

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



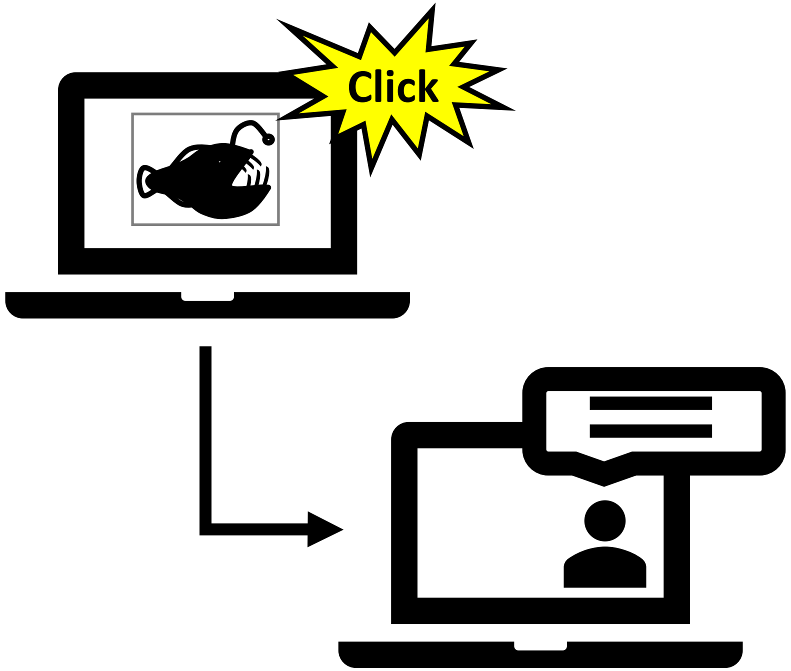
Process

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

Common Metrics and Behaviors

- Click rates
- Reporting rates
- Repeat clickers
- Protective stewards[5]

Variability in Click Rates

49.3% 3.2%

4.8% 11.0% 8.7%

9.1% 43.8%

11.6%

20.5% 19.4%

Click rates don’t tell the whole story

Phishing Study Research

Phishing Awareness Study

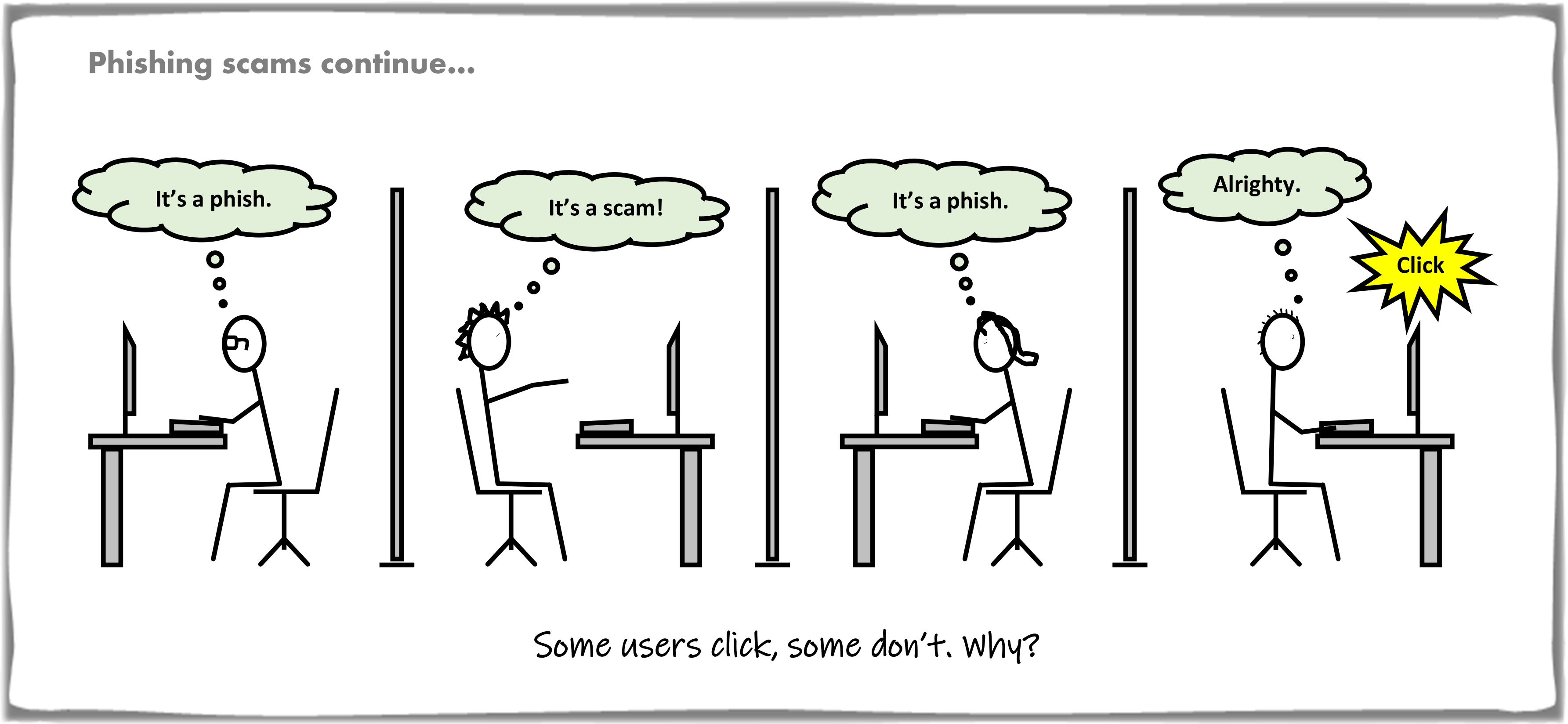
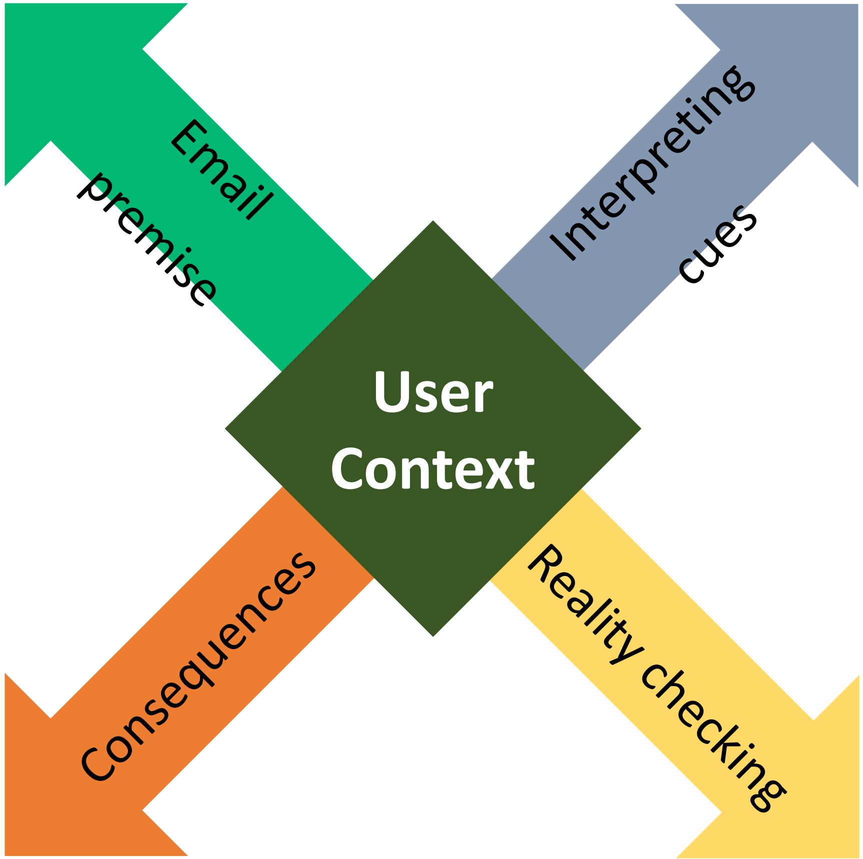


Image credit: NIST

User Context

Alignment vs. misalignment with expectations and external events

Compelling vs. suspicious cues

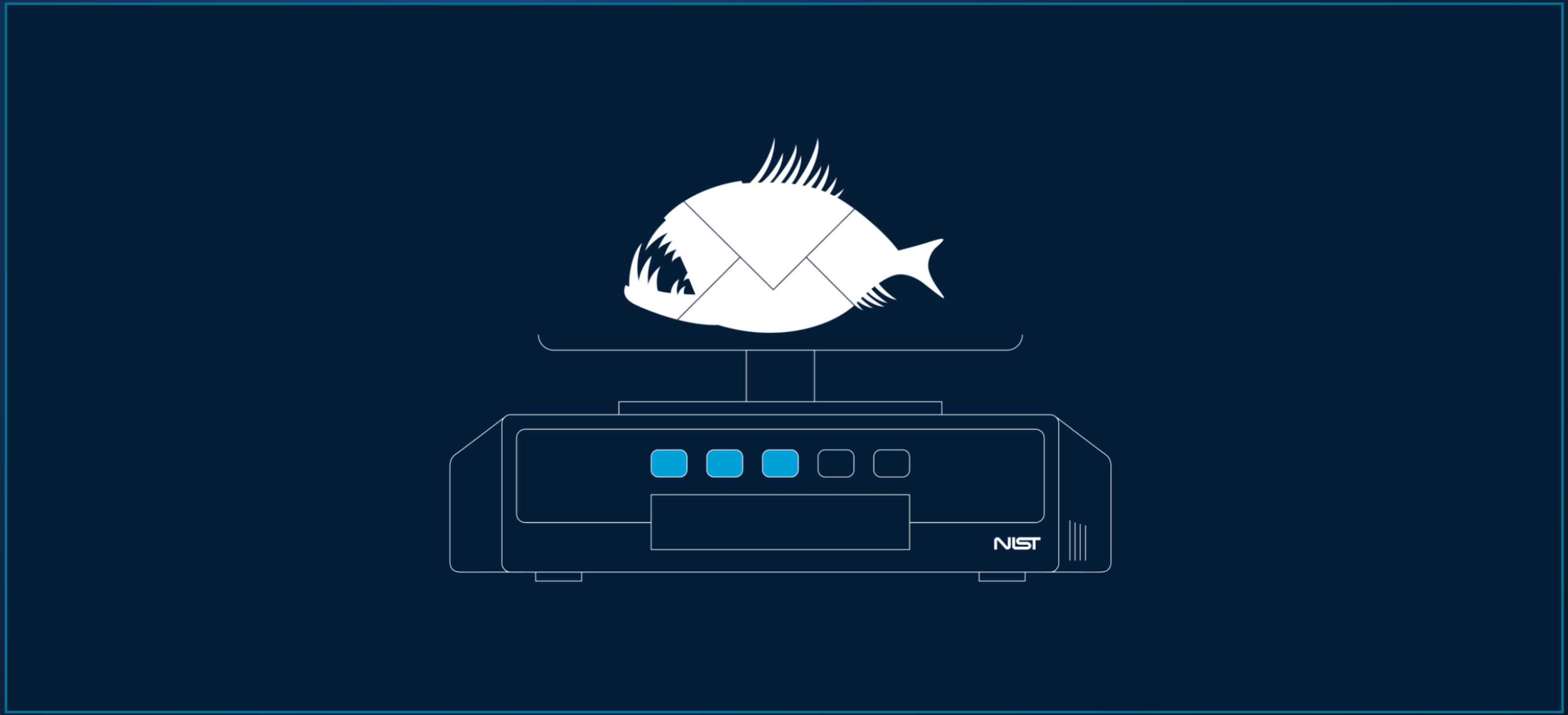


Concern over consequences

Reality-checking strategies

NIST Phish Scale

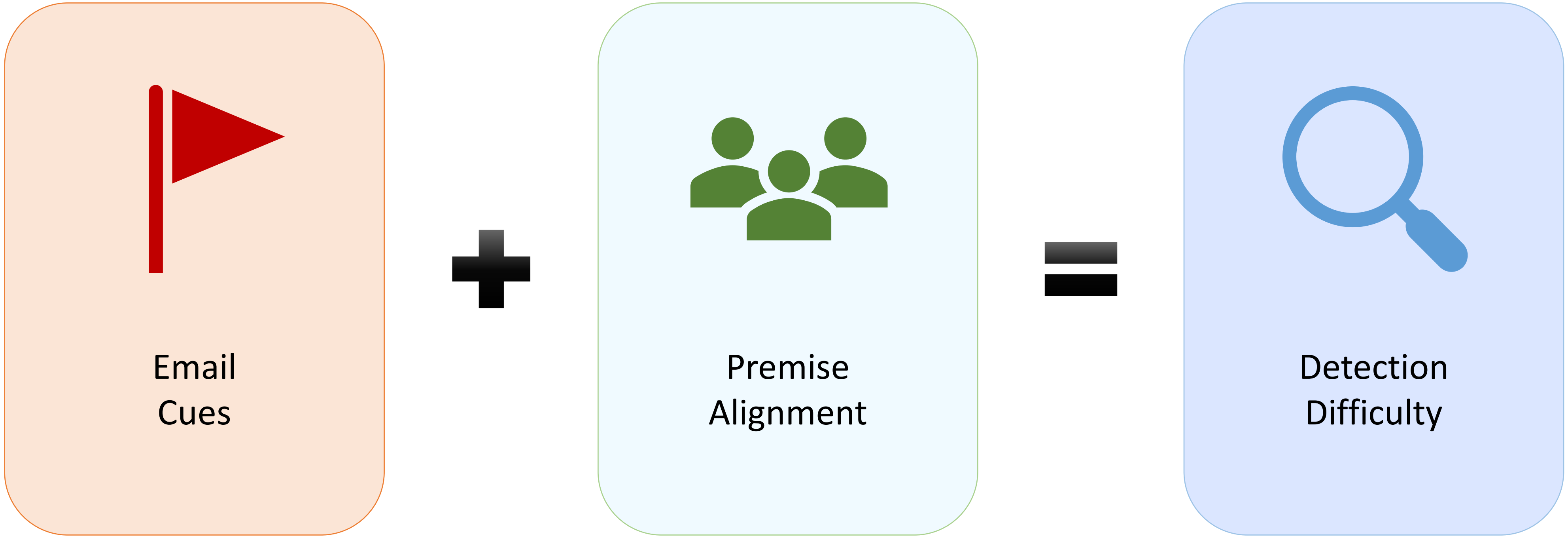
NIST Phish Scale



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

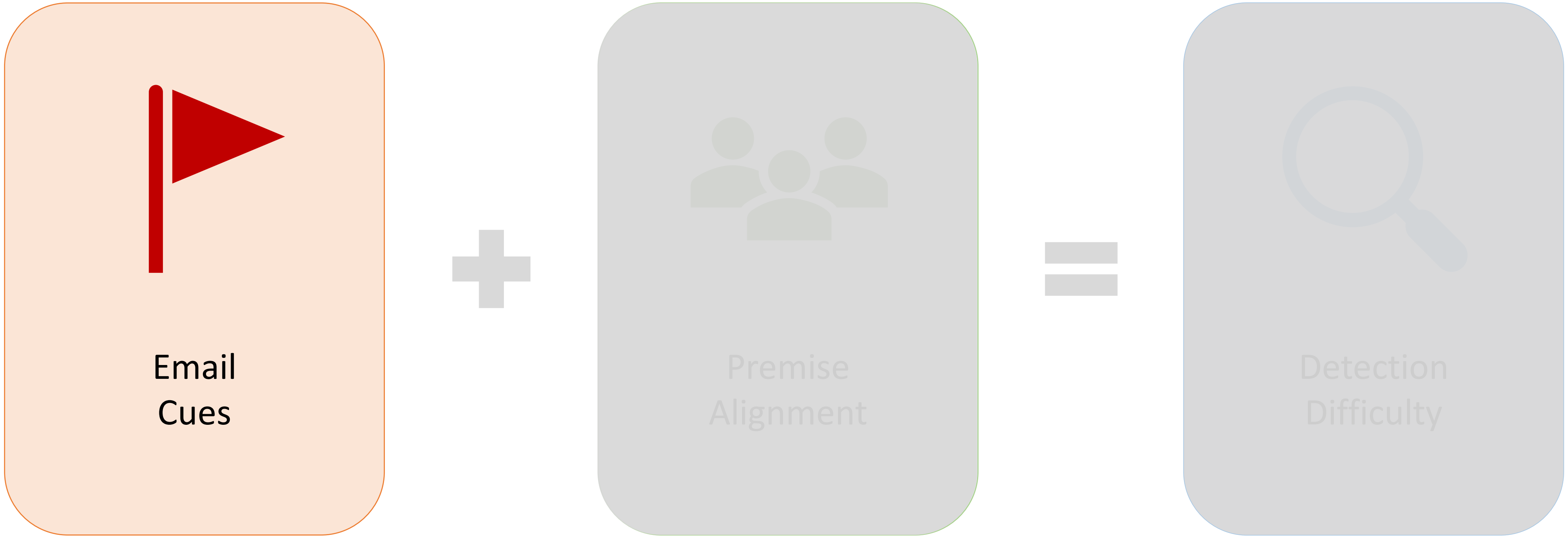
Image credit: NIST

NIST Phish Scale Components



Email Cues + Premise Alignment = Detection Difficulty

NIST Phish Scale Components



Email Cues

+

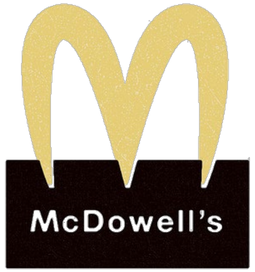
Premise Alignment

=

Detection Difficulty

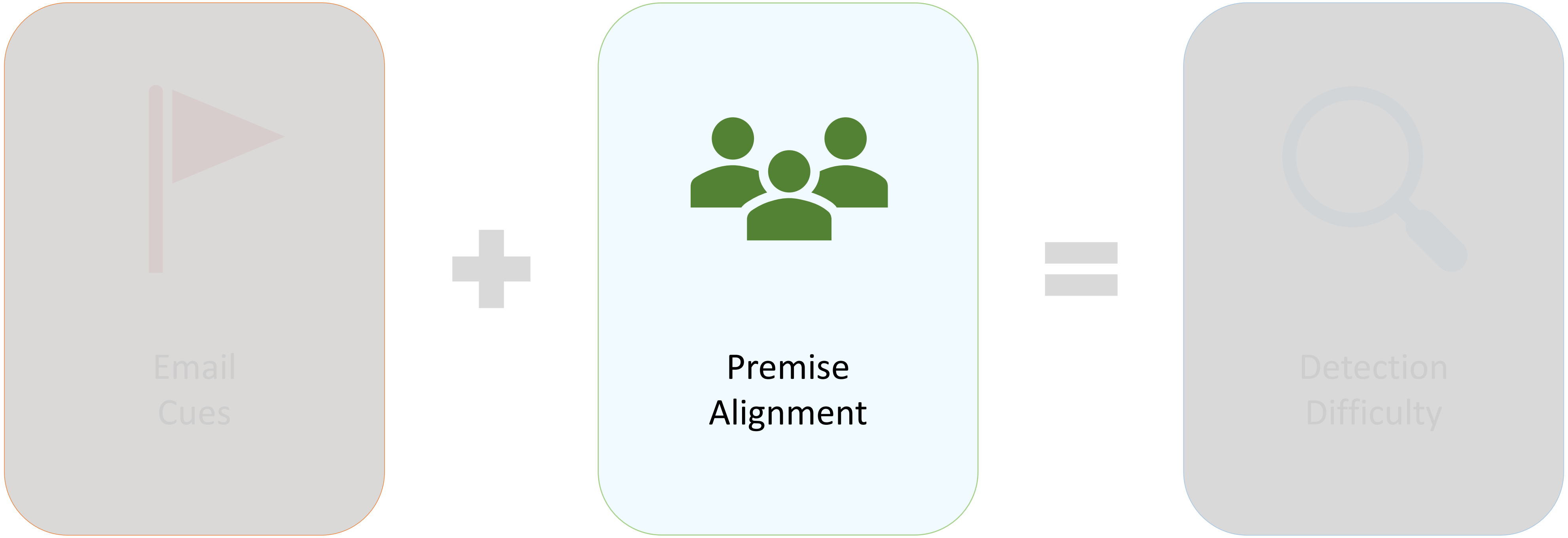
NIST Phish Scale – Cues

WINNER!
CONGRATULATIONS
YOU ARE WON!!!



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

NIST Phish Scale Components



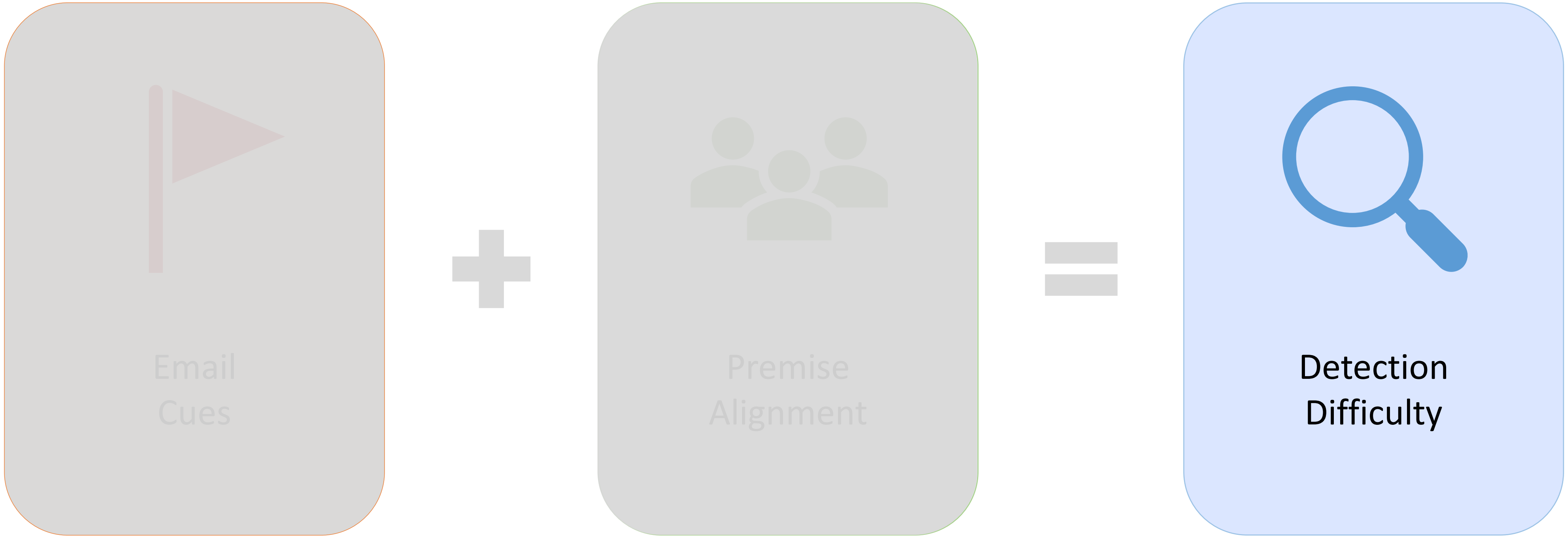
NIST Phish Scale – Premise Alignment

- 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



Email Cues

+

Premise Alignment

=

Detection Difficulty

The NIST Phish Scale – Detection Difficulty

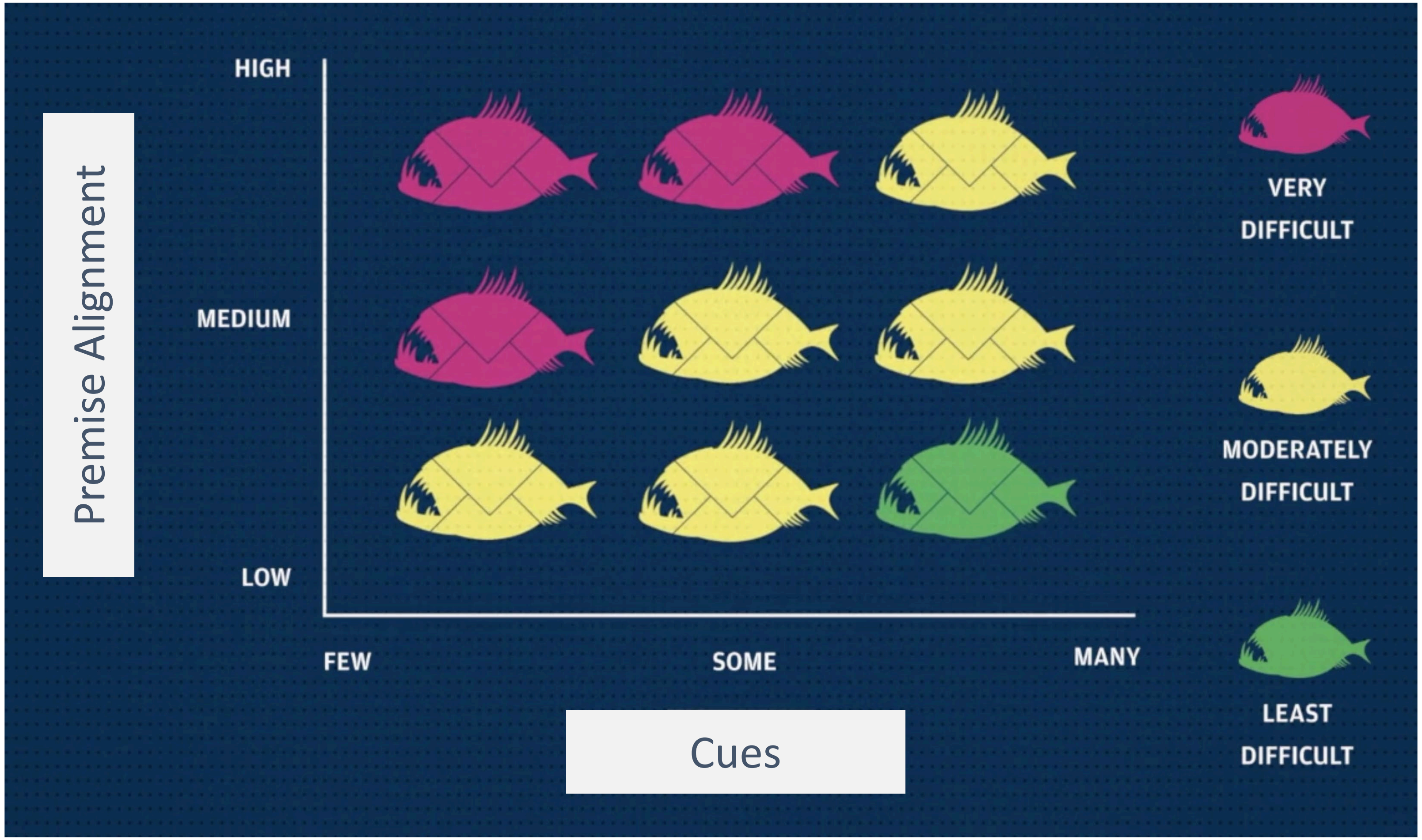
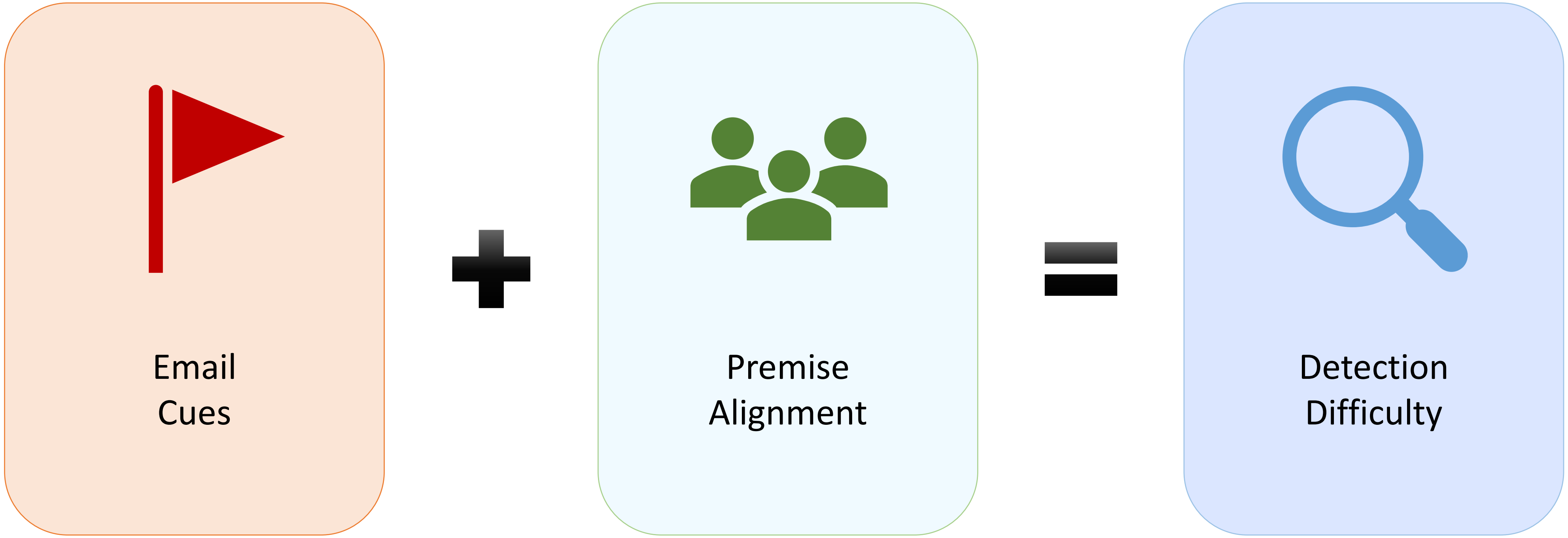


Image credit: NIST

NIST Phish Scale Components



Email Cues

+

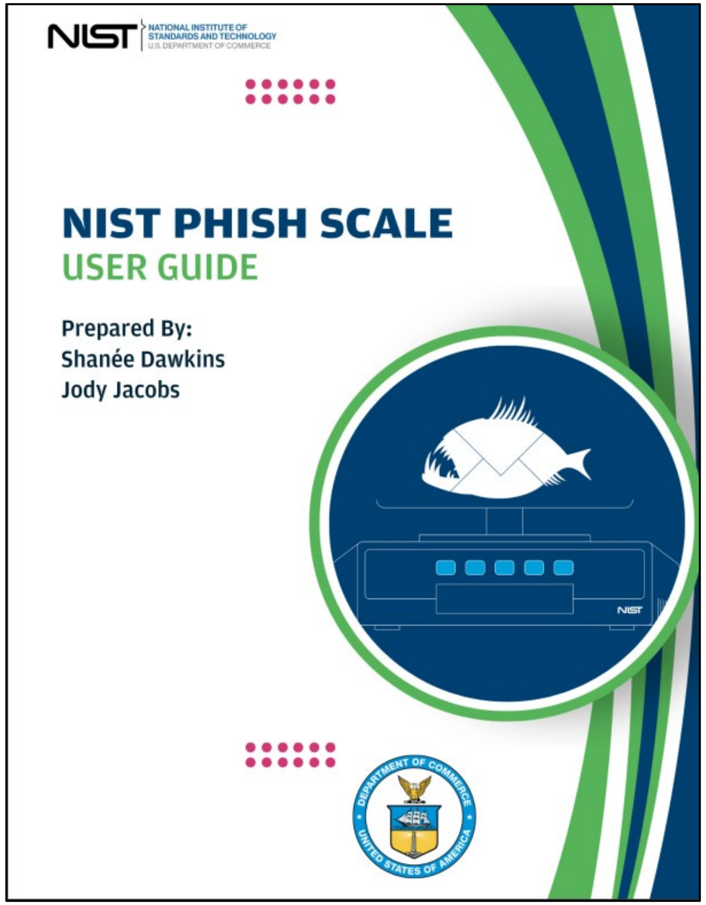
Premise Alignment

=

Detection Difficulty

NIST Phish Scale User Guide

- Released November 2023
- Provides an overview of the Phish Scale
- Walks step-by-step how an organization can implement and tailor the Phish Scale to fit their organization
- Worksheets to assist training implementers in applying the Phish Scale
- Detailed information regarding email properties and associated research in the literature



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

NIST PHISH SCALE
USER GUIDE

Prepared By:
Shanée Dawkins
Jody Jacobs

NIST TN 2276

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?

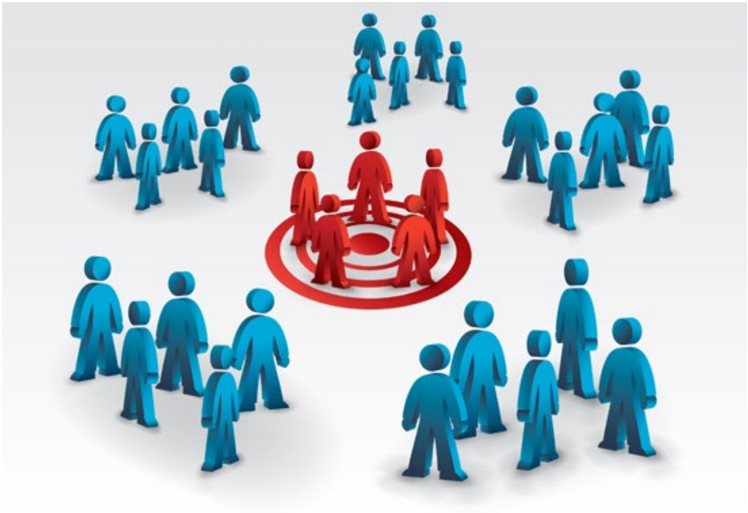
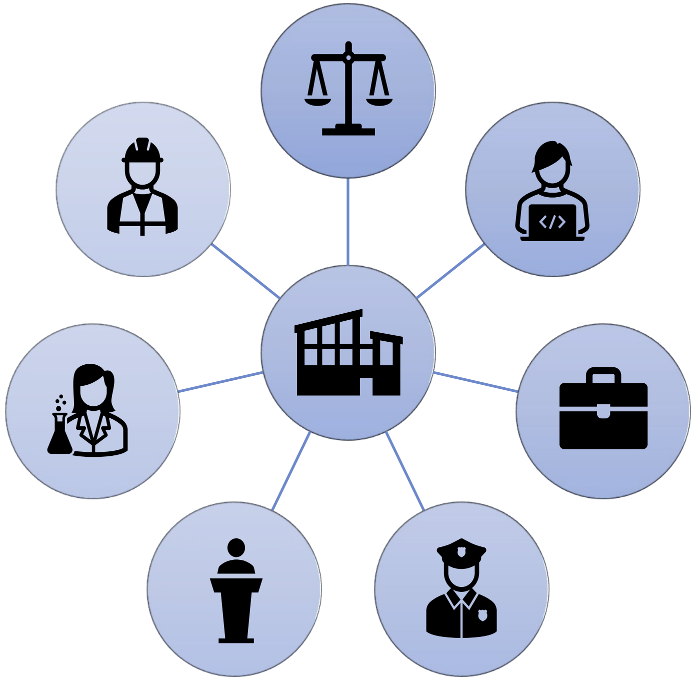


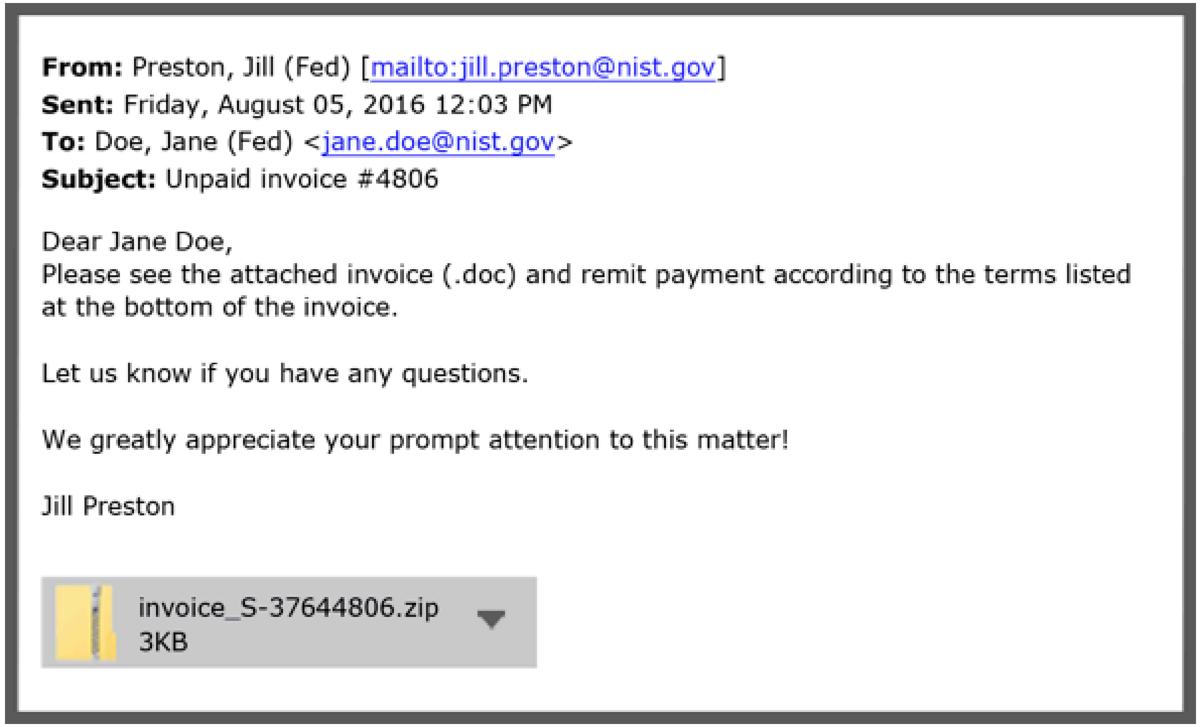
Image credit: Shutterstock

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!

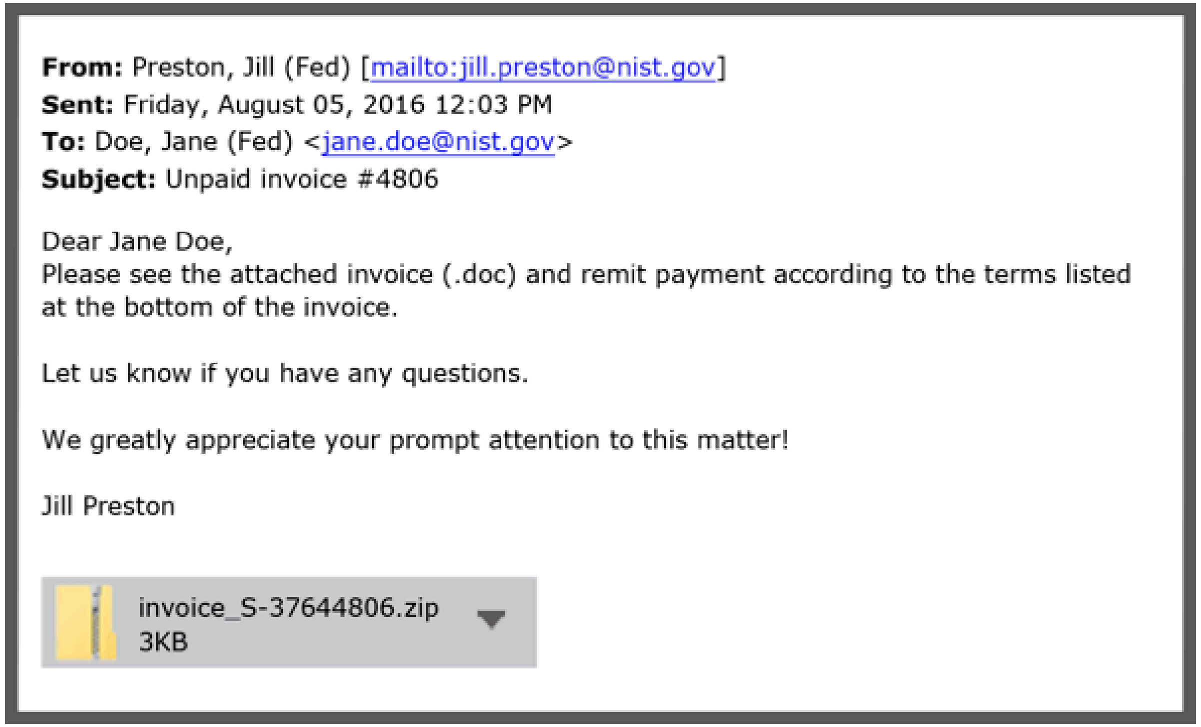
Jill Preston

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.

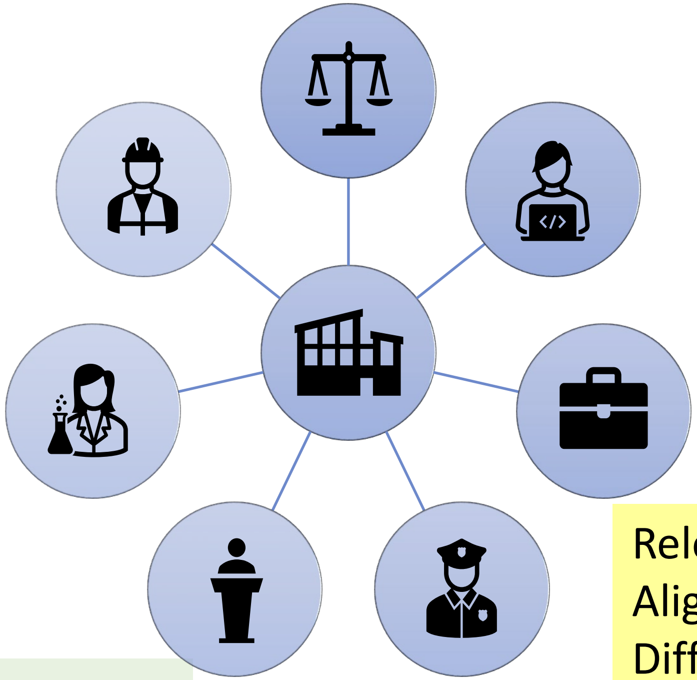
Let us know if you have any questions.

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

Final Parting Thoughts

Considering the Human

- Provides context to click rates
- Customized and targeted training
- Mitigate phishing attacks
- Understand depth of processing between clickers and non-clickers
- Better understanding of relationship between work context and phishing susceptibility

Summary

NIST

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!

Big Takeaway

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

Contacts and Additional Resources

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

https://csrc.nist.gov/Projects/human-centered-cybersecurity/research-areas/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 2024 **State of the Phish report** https://www.proofpoint.com/us/resources/threat-reports/state-of-phish (Accessed March 20, 2024)

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)