

The NIST Phish Scale: A method for rating human phishing detection difficulty



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

Shanée Dawkins, Ph.D.

Jody Jacobs, M.S.

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 defense
- Our research
- NIST Phish Scale

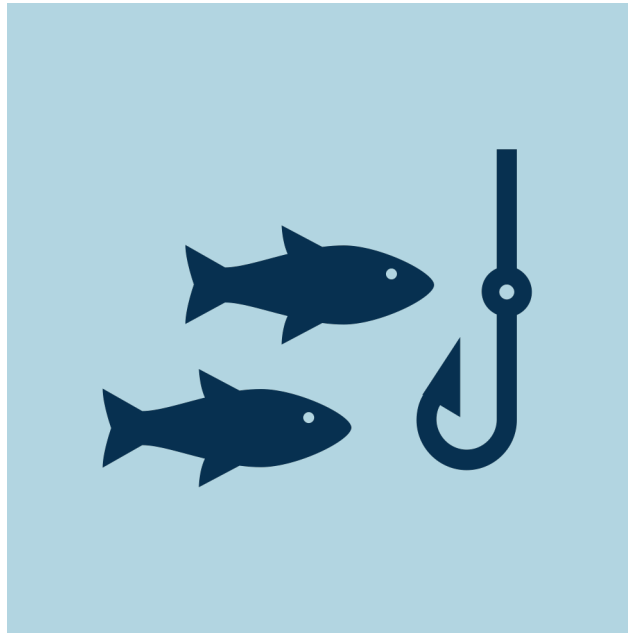
Championing the Human in I.T.



DEFENDING AGAINST PHISHING

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



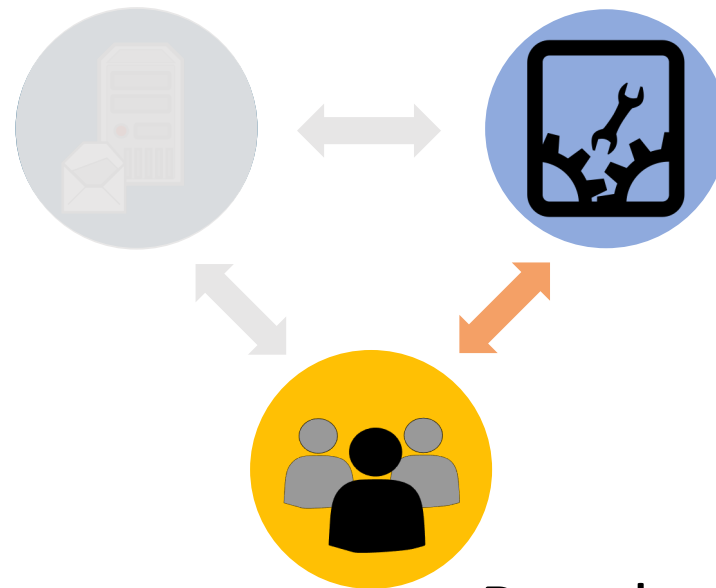
People

- End users
- IT security staff
- Leadership

Phishing defense must be multi-pronged

Technology

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

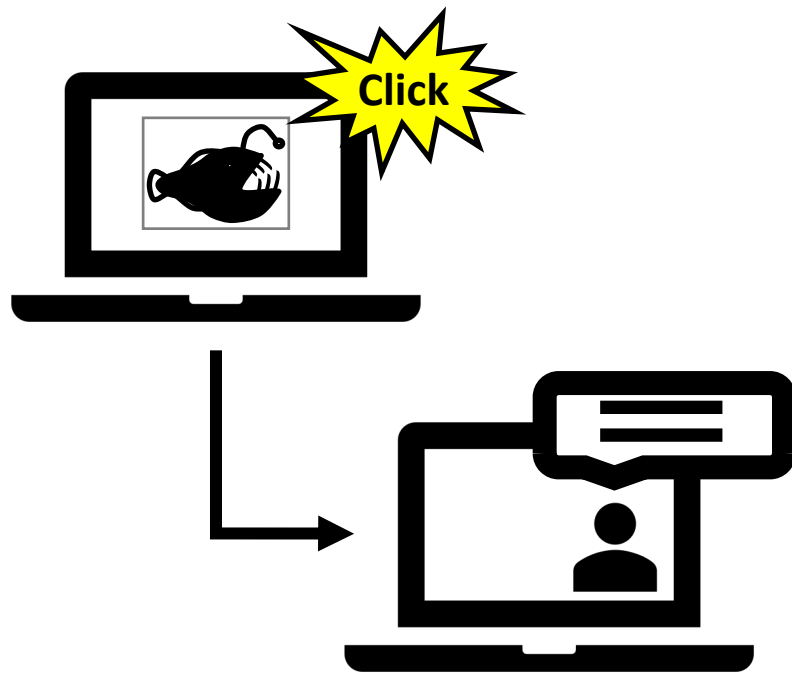


Process

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

People

- End users
- IT security staff
- Leadership



Training in Practice

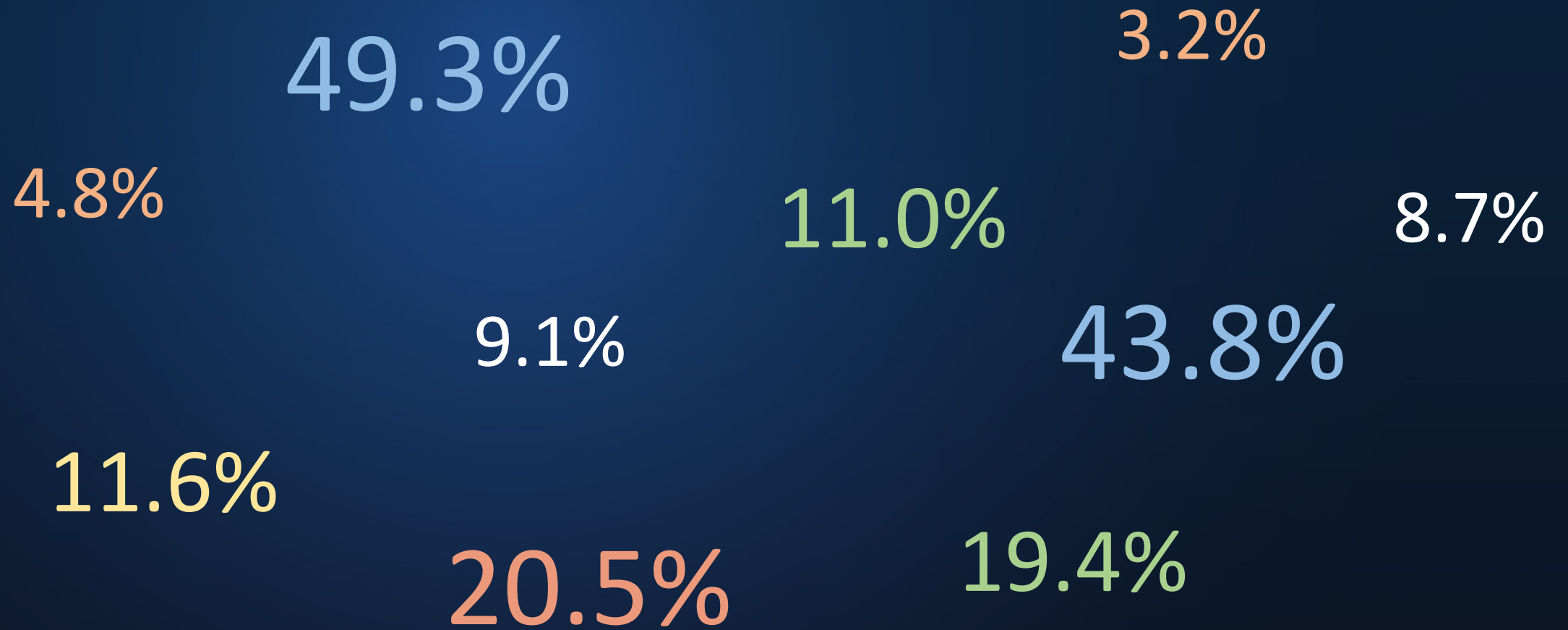
- Simulated phishing emails
- Gamify phishing
 - e.g., phish hunting badges, shark awards
- Staff Profiles

Common Metrics and Behaviors

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

Our Research

Contextualizing click rates



Phishing scams continue...

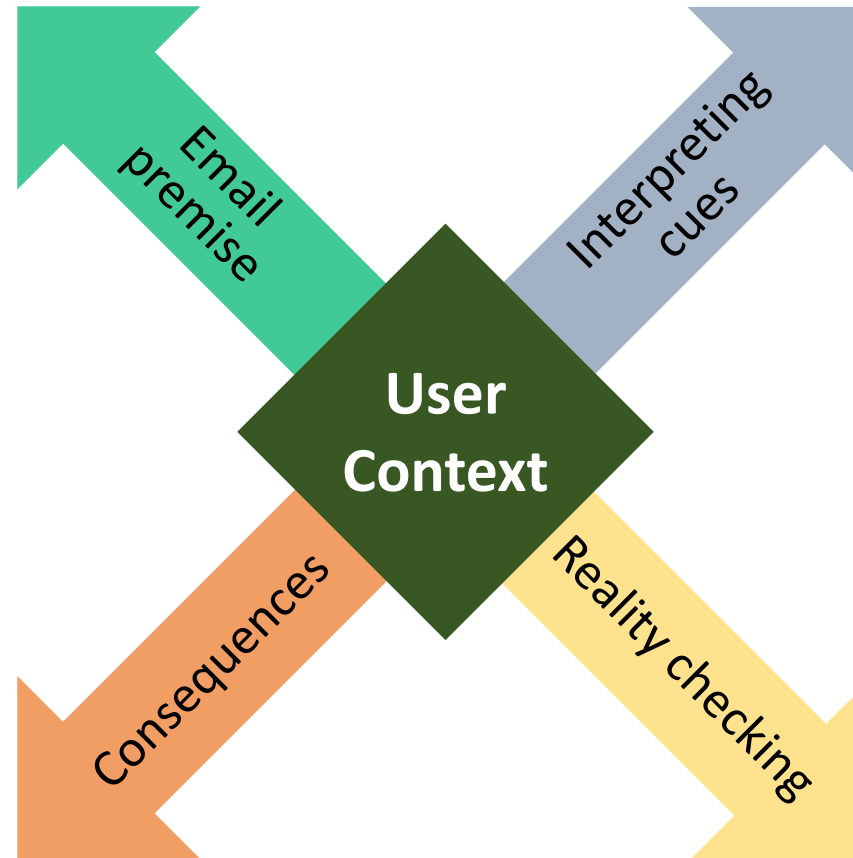


Some users click, some don't. Why?

User context is key!

Alignment vs.
misalignment with
expectations and
external events

Concern over
consequences



Compelling vs.
suspicious cues

Reality-checking
strategies

Our Research – NIST Phish Scale

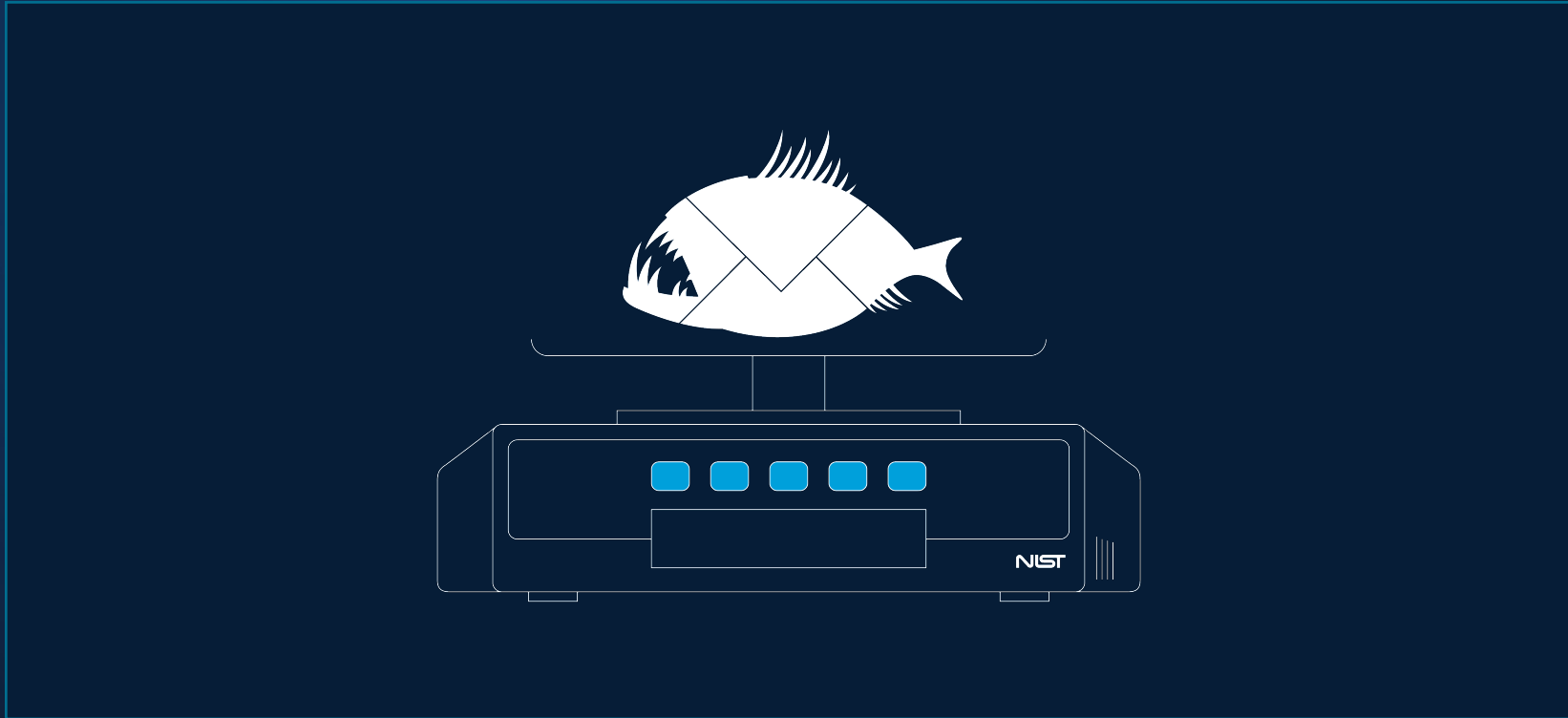
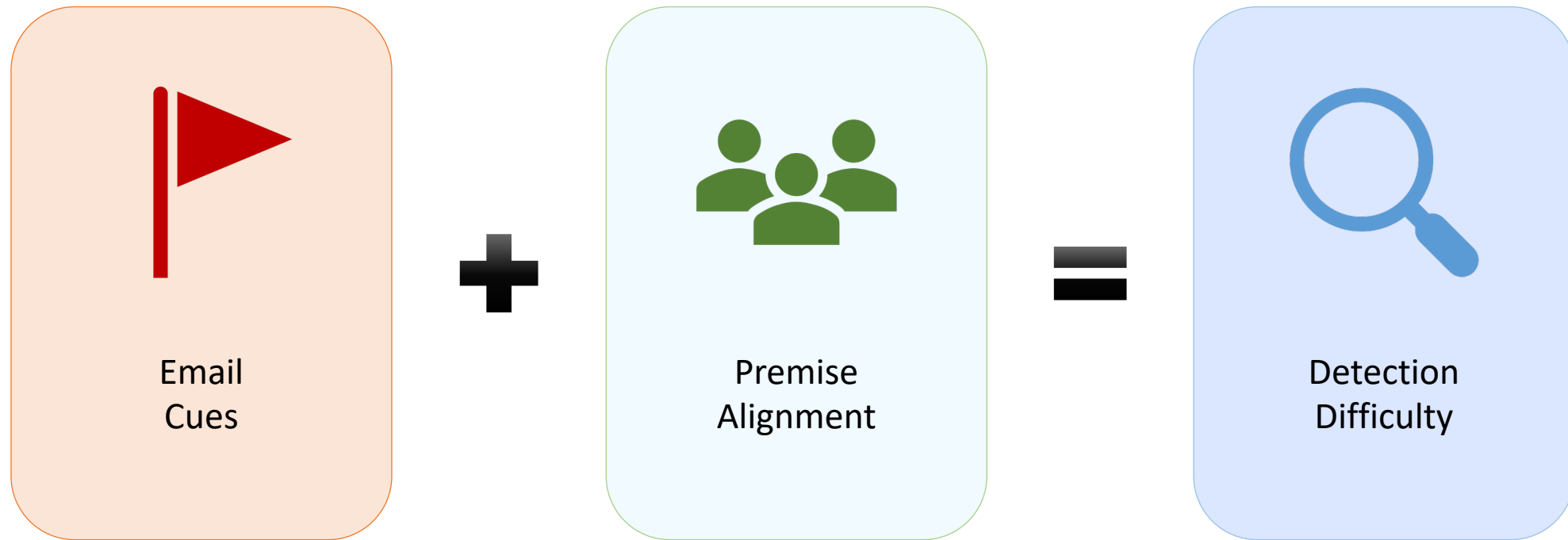
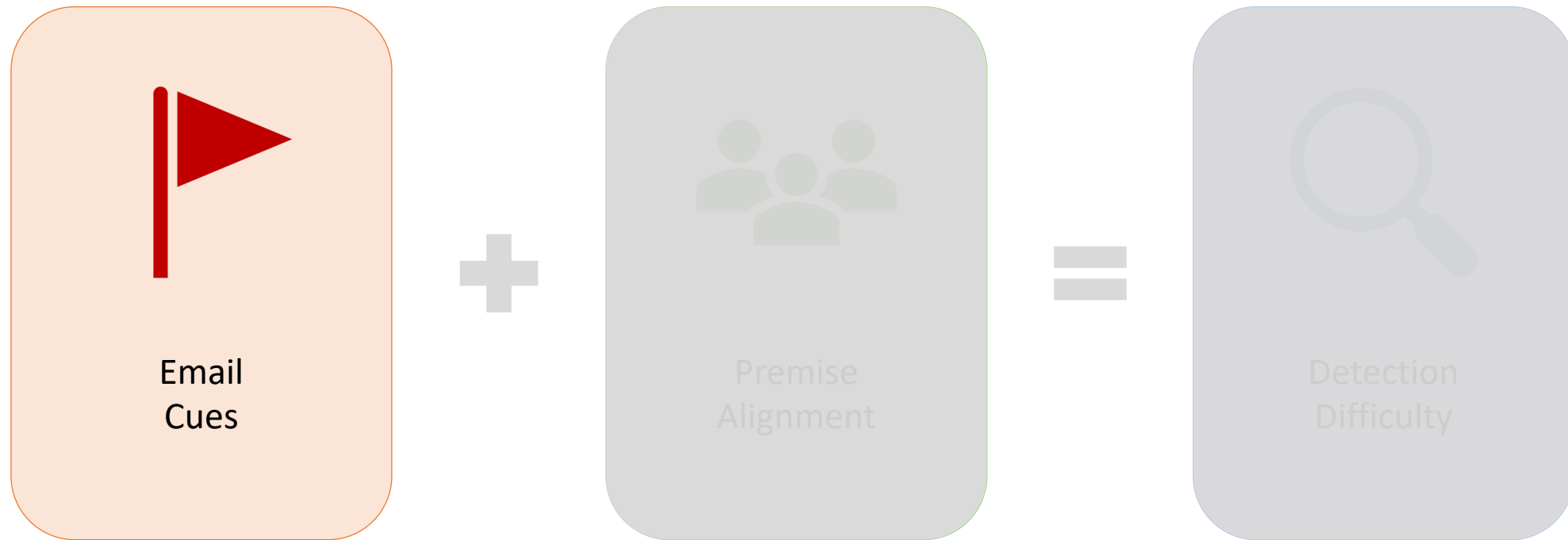


Image credit: NIST

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

NIST Phish Scale Components





NIST Phish Scale – Cues

5 Types of Cues

- Errors
- Technical indicators
- Visual presentation indicators
- Language and content
- Common tactics



5 Types of Cues

- Errors
- Technical indicators
- Visual presentation indicators
- Language and content
- Common tactics

From: Order Confirmation [<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

5 Types of Cues

- Errors
- Technical indicators
- Visual presentation indicators
- Language and content
- Common tactics

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

5 Types of Cues

- Errors
- Technical indicators
- Visual presentation indicators
- Language and content
- Common tactics

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
Manage order	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 accordance with local laws. For more information, please view [tax information](#)

[Return Policy](#) | [Privacy](#) | [Account](#)

5 Types of Cues

- Errors
- Technical indicators
- Visual presentation indicators
- Language and content
- Common tactics



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...

5 Types of Cues

- Errors
- Technical indicators
- Visual presentation indicators
- Language and content
- Common tactics

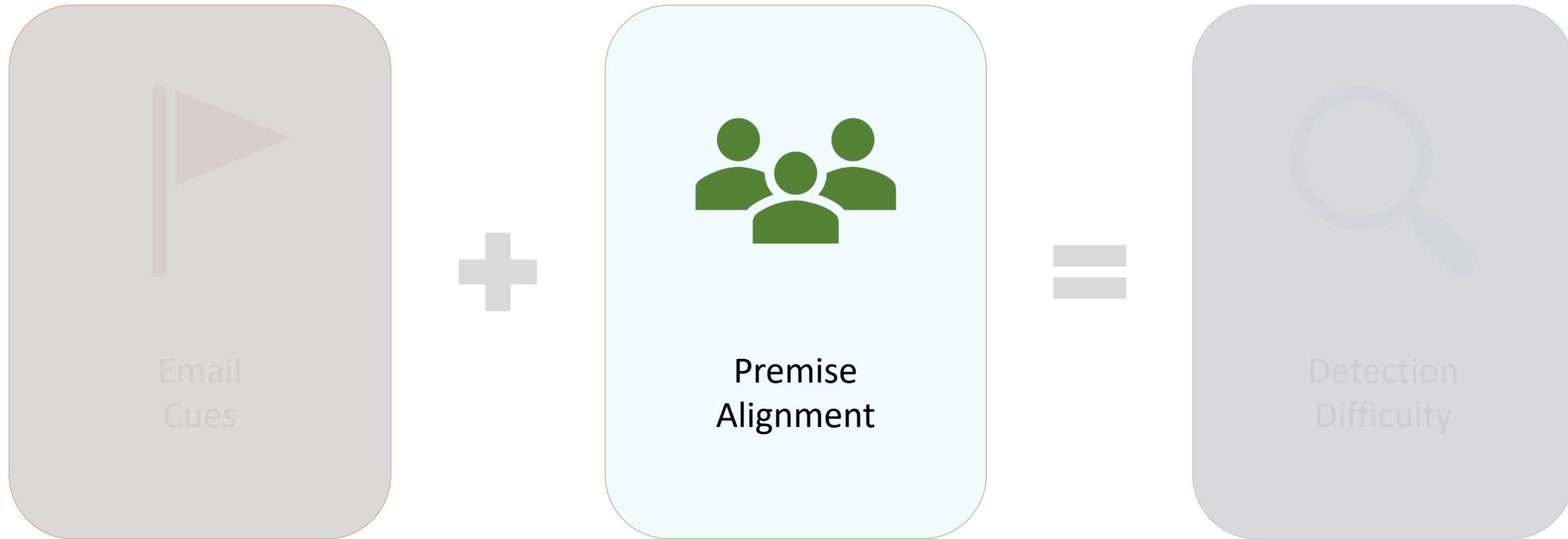
From: Jacob, Jodi [<mailto:Jodi.Jacob@gmail.com>]
Sent: Friday, August 05, 2016 12:03 PM
To: Doe, Jane (Fed) <jane.doe@nist.gov>
Subject: Unpaid invoice #4806

NIST Phish Scale – Cue Categories

- Three cue categories
 - Few – lower number of cues with **fewer** opportunities to identify phish email
 - Some – moderate number of cues
 - Many – higher number of cues with **more** opportunities to identify phish email

Total Cue Count	Cue Category
1 – 8 cues	Few (more difficult)
9 – 14 cues	Some
15 or more cues	Many (less difficult)

NIST Phish Scale Components



- Characterize relevancy of the email premise for the target audience
 - Weak, Medium, Strong
 - 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 – Premise Alignment

Assign each element a value according to the applicability scale

Applicability Scale	Applicability Score
Extreme applicability , alignment, or relevancy	8
Significant applicability , alignment, or relevancy	6
Moderate applicability , alignment, or relevancy	4
Low applicability , alignment, or relevancy	2
Not applicable , no alignment, or no relevancy	0

NIST Phish Scale – Premise Alignment

Use these criteria, along with the applicability scale, to determine the *applicability rating* for each element.

Premise Alignment Elements	Scoring Criteria
1: Mimics a workplace process or practice	Does this element attempt to capture premise alignment with workplace process or practice for the target audience?
2: Has workplace relevance	Does this element attempt to reflect pertinence of the premise for the target audience?
3: Aligns with other situations or events, including external to the workplace	Does this element align to other situations or events, even those external to the workplace lends an air of familiarity to the message?
4: Engenders concern over consequences for NOT clicking	Does this element reflect potentially harmful ramifications for not clicking raise the likelihood to clicking?
5: Has been the subject of targeted training, specific warnings, or other exposure	Does this element reflect targeted training effects that would lead to premise detection? Care must be taken to appropriately incorporate the training or warning specificity, as transfer of learning is quite difficult.

NIST Phish Scale – Premise Alignment

Assign each element a value according to the applicability scale

Element		Value
1	Mimics a workplace process or practice	4
2	Has workplace relevance	8
3	Aligns with other situations or events, including external to the workplace	6
4	Engenders concern over consequences for NOT clicking	2
5	Has been the subject of targeted training, specific warnings, or other exposure	4

NIST Phish Scale – Premise Alignment

Sum values of elements 1 through 4. Subtract element 5 from sum.

Element		Value
1	Mimics a workplace process or practice	8
2	Has workplace relevance	4
3	Aligns with other situations or events, including external to the workplace	6
4	Engenders concern over consequences for NOT clicking	2
5	Has been the subject of targeted training, specific warnings, or other exposure	4

$8 + 4 + 6 + 2 = 20$

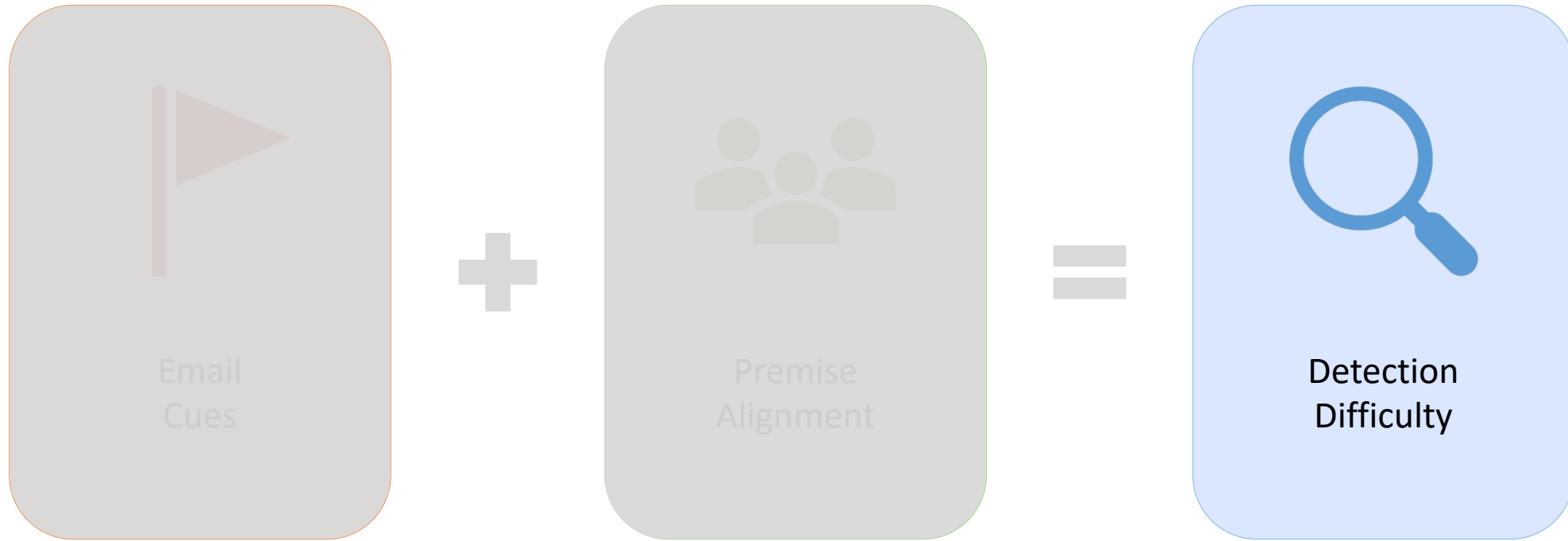
$20 - 4 = 16$

NIST Phish Scale – Premise Alignment

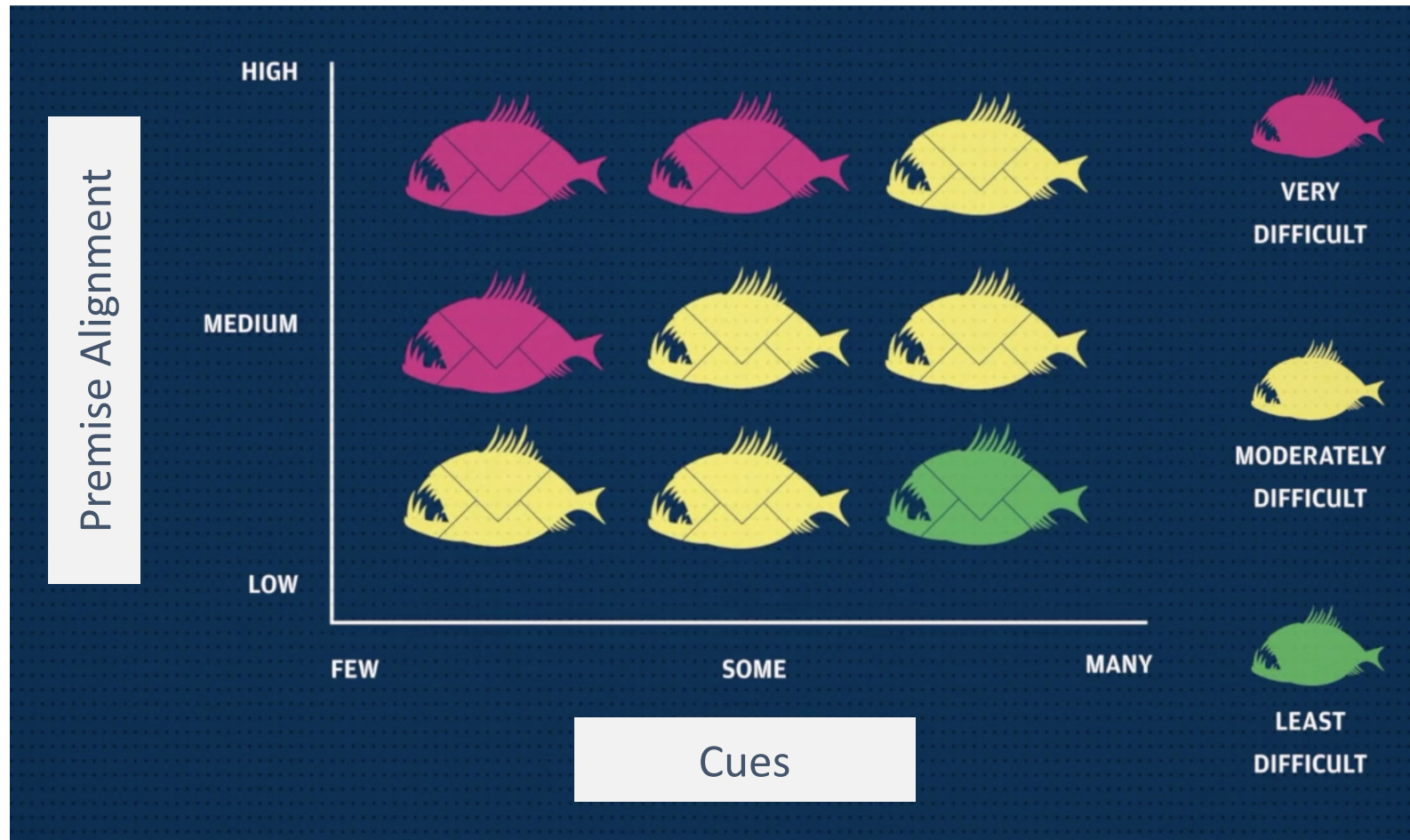
Categorize Premise Alignment

Premise Alignment Rating	Premise Alignment Category
10 and below	Weak
11 – 17	Medium
18 and higher	Strong

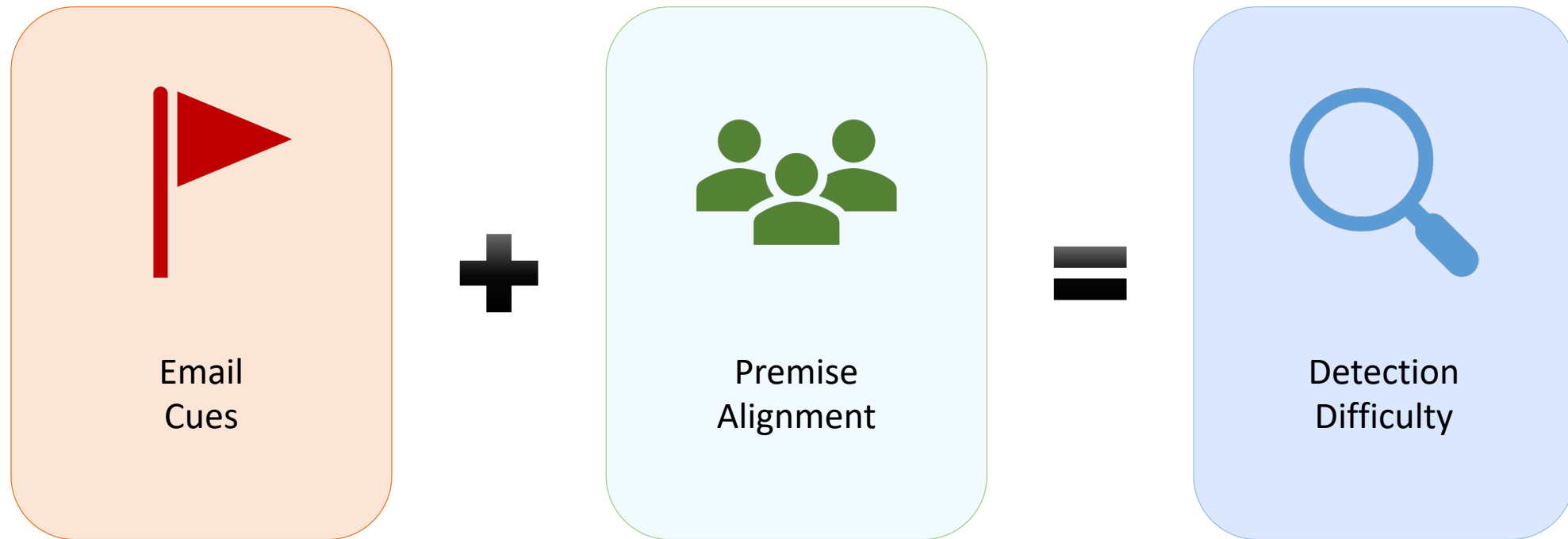
NIST Phish Scale Components



NIST Phish Scale - Detection Difficulty

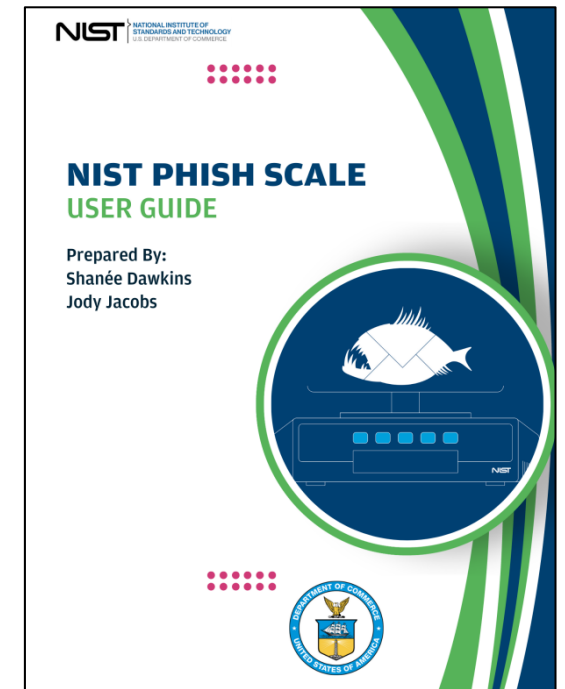


NIST Phish Scale Components



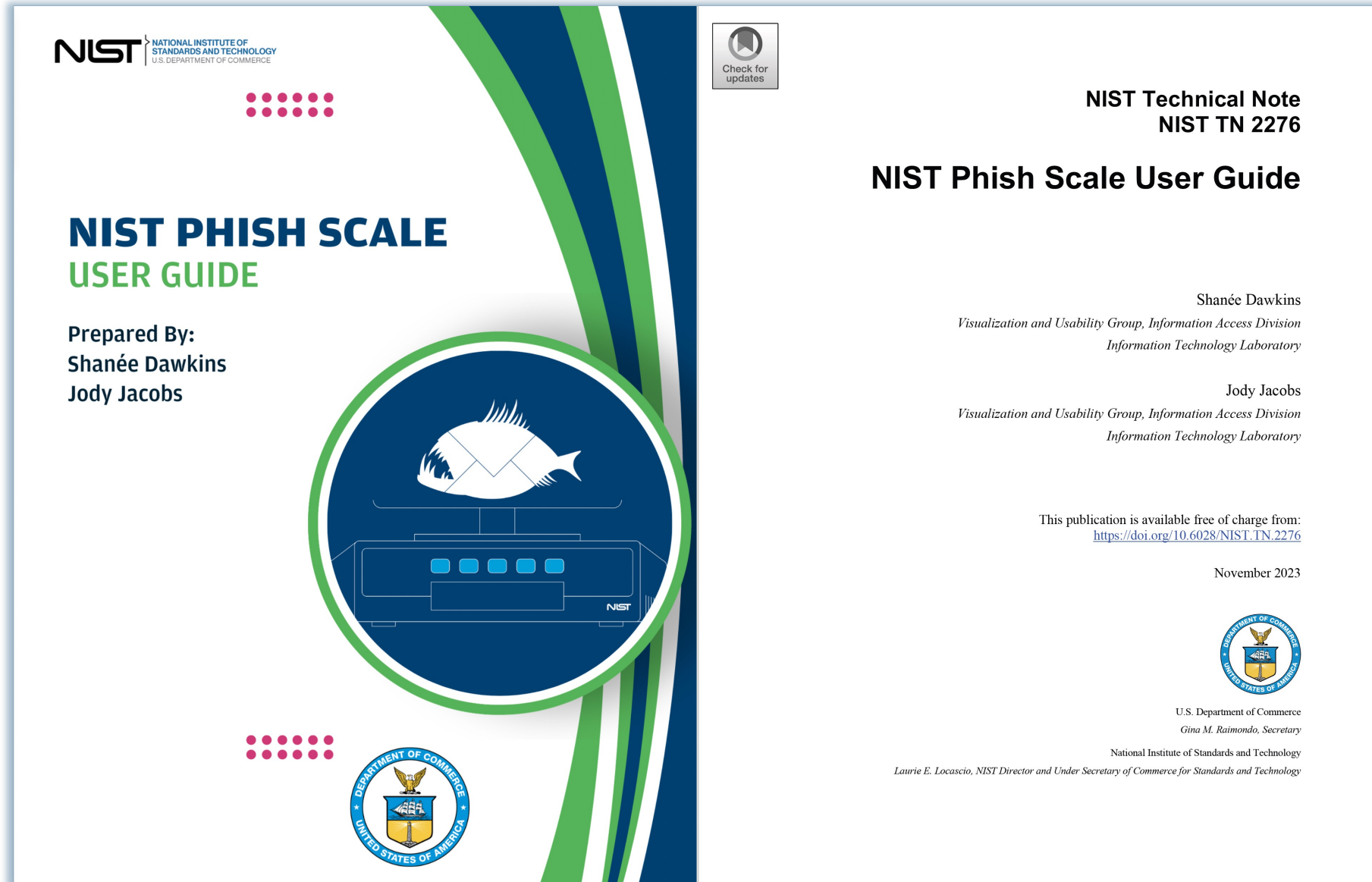
NIST Phish Scale User Guide

- 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 TN 2276

NIST Phish Scale User Guide



NIST PHISH SCALE USER GUIDE

Prepared By:
Shanée Dawkins
Jody Jacobs



NIST Technical Note NIST TN 2276 NIST Phish Scale User Guide

Shanée Dawkins
*Visualization and Usability Group, Information Access Division
Information Technology Laboratory*

Jody Jacobs
*Visualization and Usability Group, Information Access Division
Information Technology Laboratory*

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.TN.2276>

November 2023

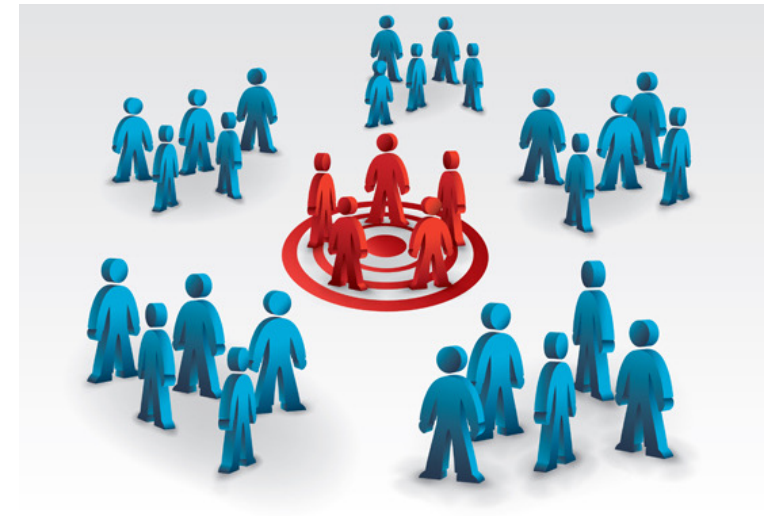


U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Applying the NIST Phish Scale Broadly

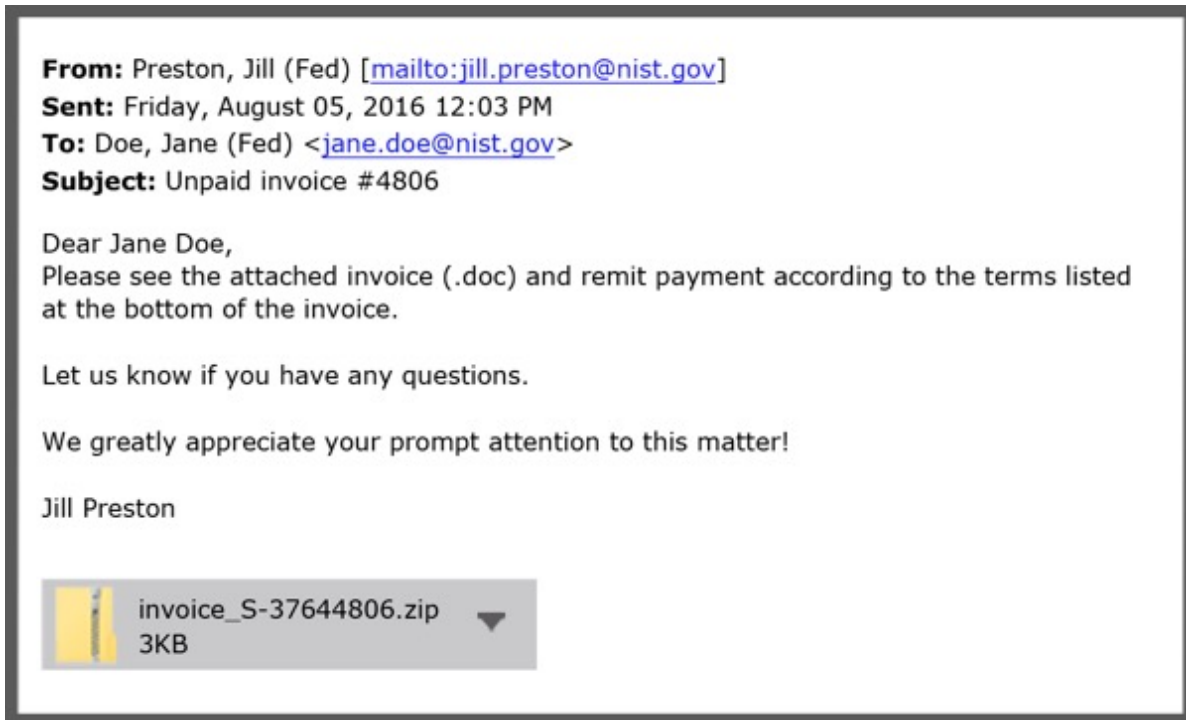
- Designed to use a target audience
- Many organizations conduct phishing training and exercises as a one-size-fits-all approach
- Question: How to apply NIST Phish Scale to whole organization accurately?



- 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



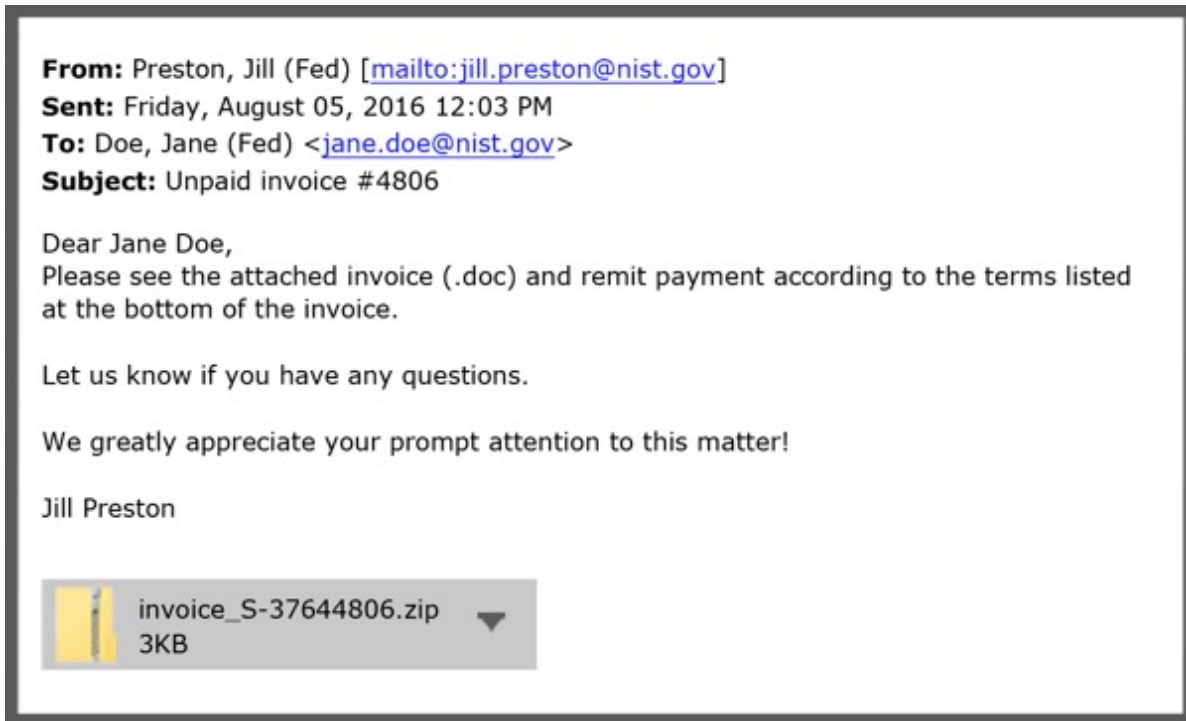
Whole Organization Application

Workplace Relevance: Low

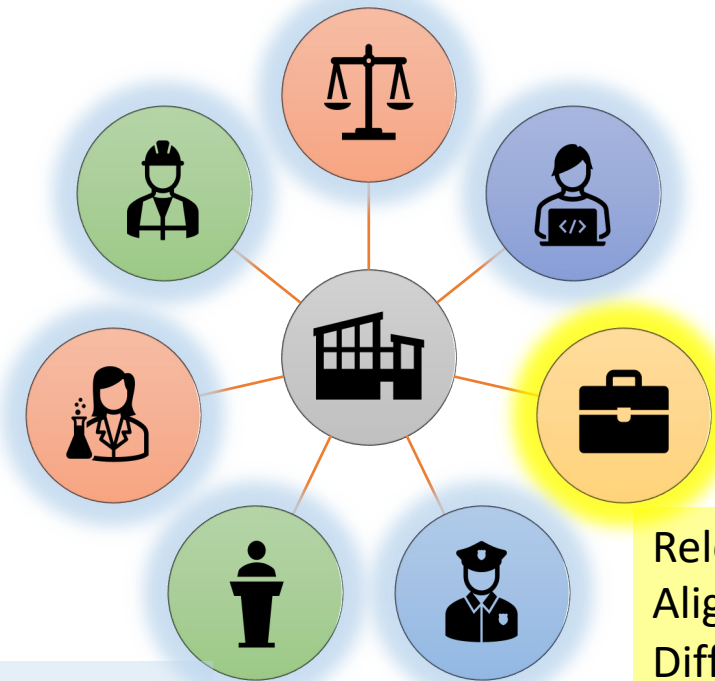
Premise Alignment: Low

Detection Difficulty: Moderate

Applying the NIST Phish Scale – Workplace Relevance



Job Family Application



Relevance: Low
Alignment: Low
Difficulty: Least

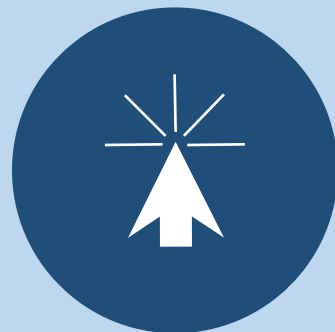
Relevance: High
Alignment: High
Difficulty: Very

Take-aways!



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**



No silver bullet

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

Additional Resources



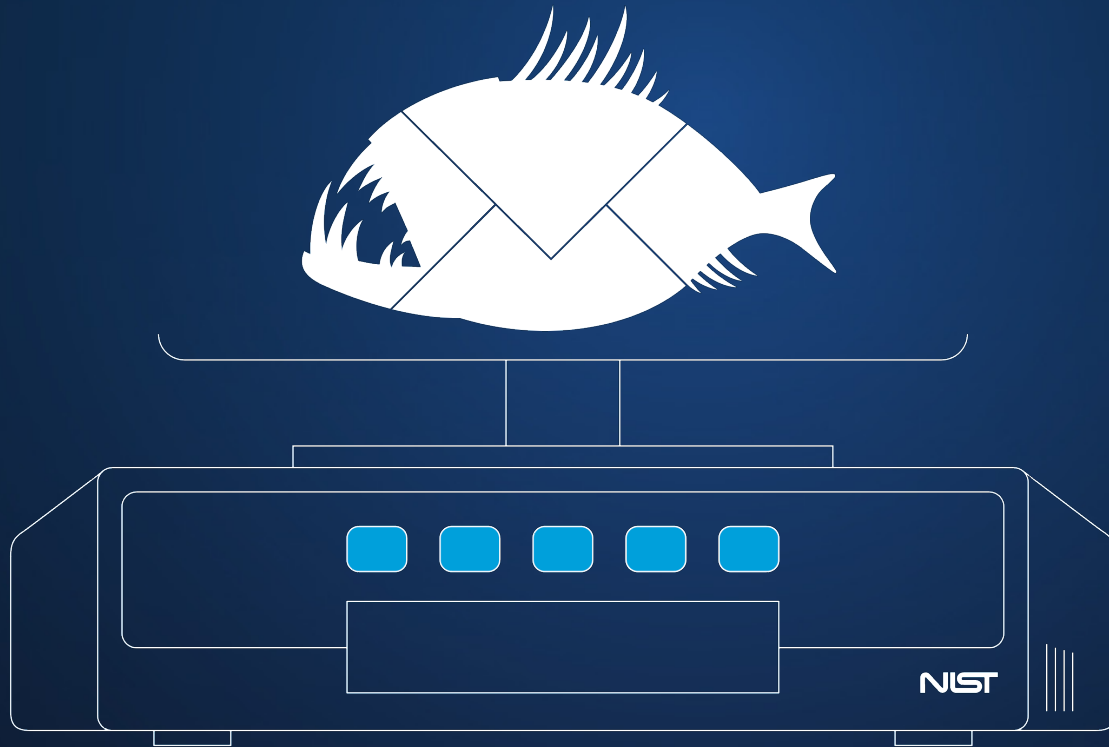
- Shanée Dawkins, dawkins@nist.gov
- Jody Jacobs, jody.jacobs.nist.gov



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



NIST Phishing Research



Q&A

- 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)