

AN OFFERING IN THE BLUE CYBER SERIES

Can you spot a Phish?

By Jody Jacobs

National Institute of Standards and Technology



26 September 2023

BLUE CYBER EDUCATION SERIES



Can you spot a phish?

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
- How to spot a phish

Championing the Human in I.T.



PHISHING THREAT LANDSCAPE

Phishing Landscape

↑ 5x

Phishing attacks have quintupled since 2020.¹

\$10.2B

Victim losses in 2022.²

82%

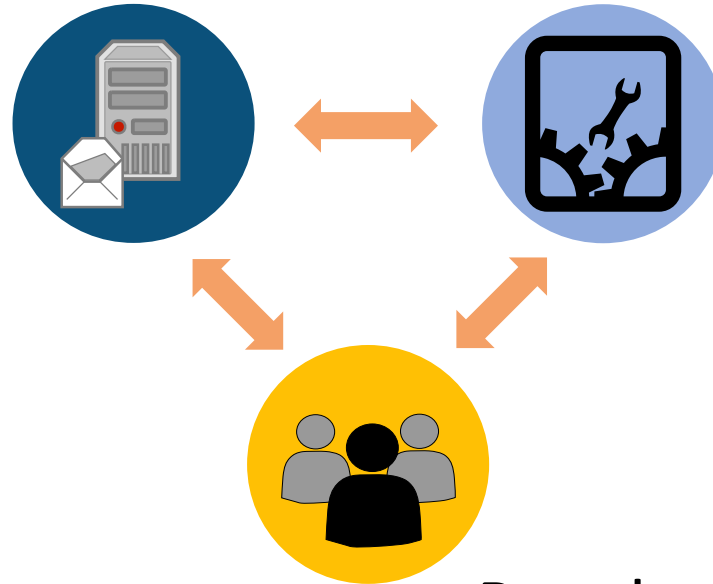
Breaches involved the human element in 2021.³

74%

Reported spear phishing attacks in 2022.⁴

Technology

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



Process

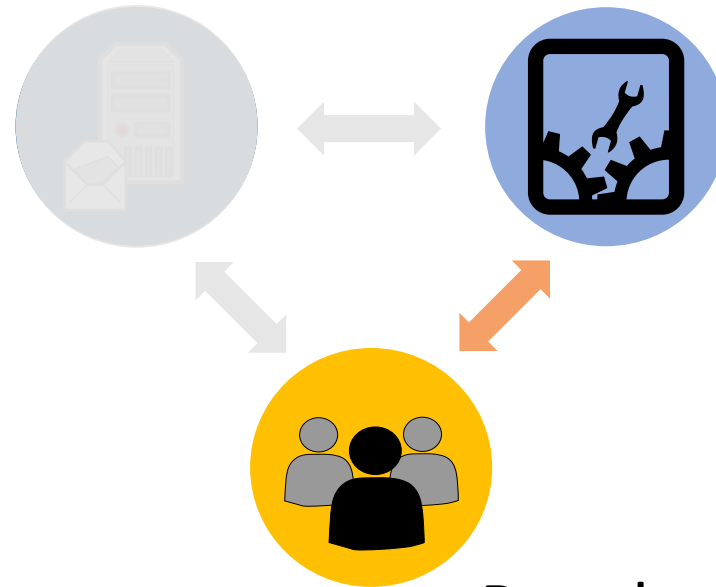
- Identify vulnerabilities
- Limiting publicly available information
- Awareness training
- Easy and clear reporting mechanism
- Meaningful metrics

People

- End users
- IT security staff
- Leadership

Technology

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

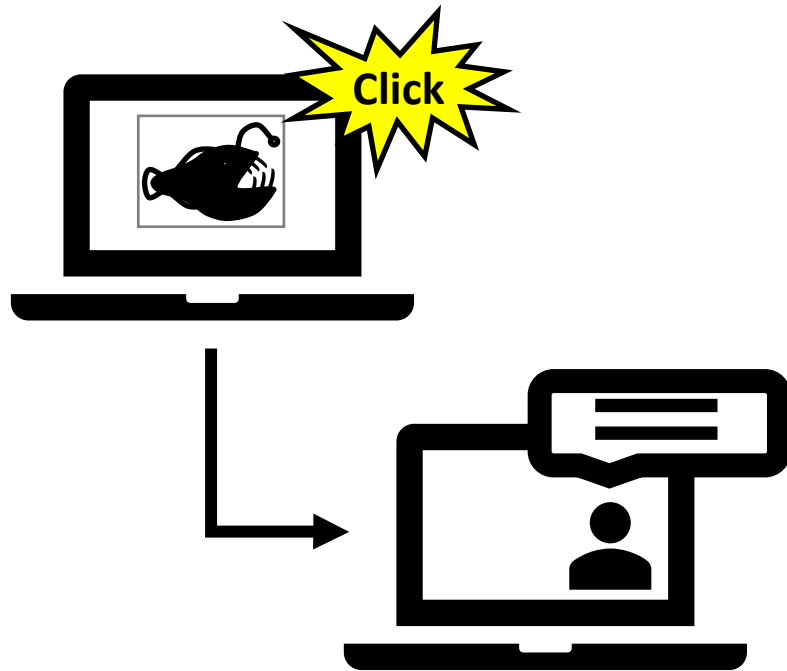


Process

- 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

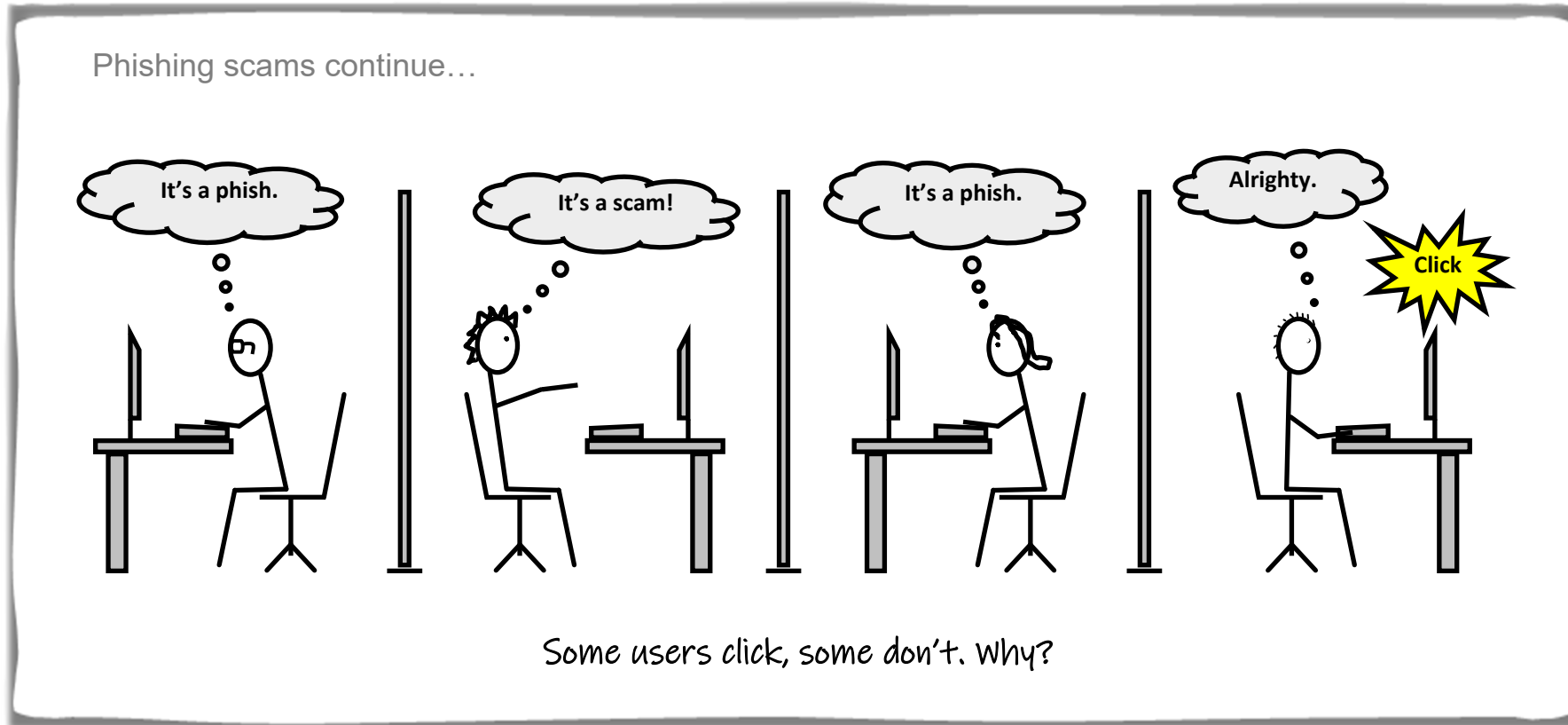
- Simulated phishing emails
- Gamify phishing
 - e.g., phish hunting badges, shark awards
- Staff Profiles

Common Metrics and Behaviors

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

OUR RESEARCH

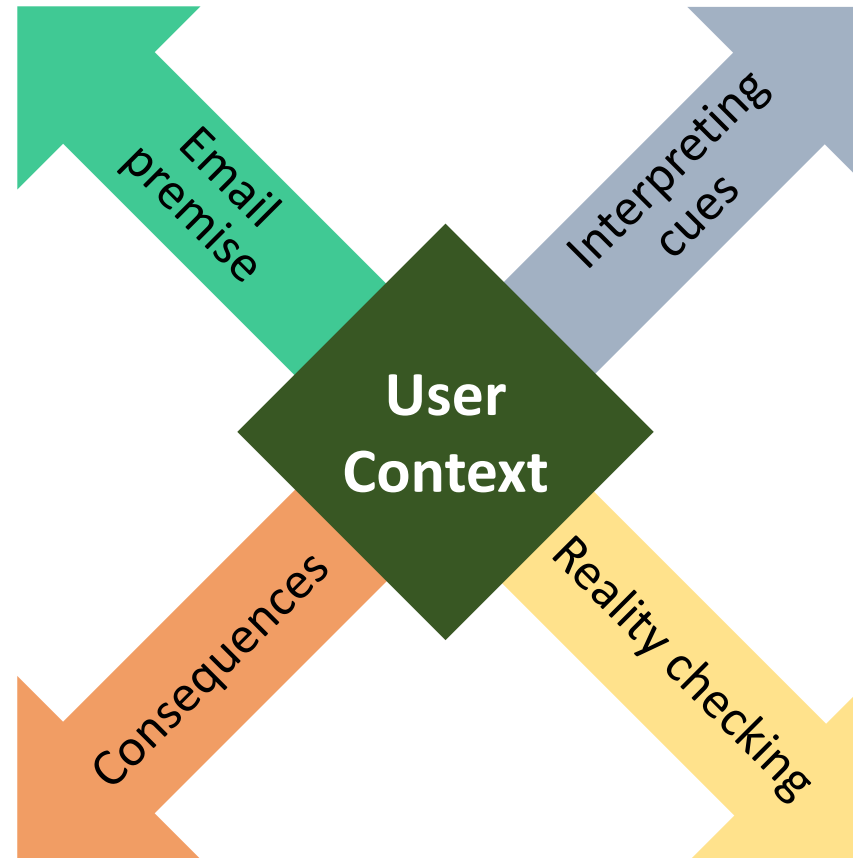
Our Research – Phishing Awareness Study



Our Research – Phishing Awareness Study

Alignment vs.
misalignment with
expectations and
external events

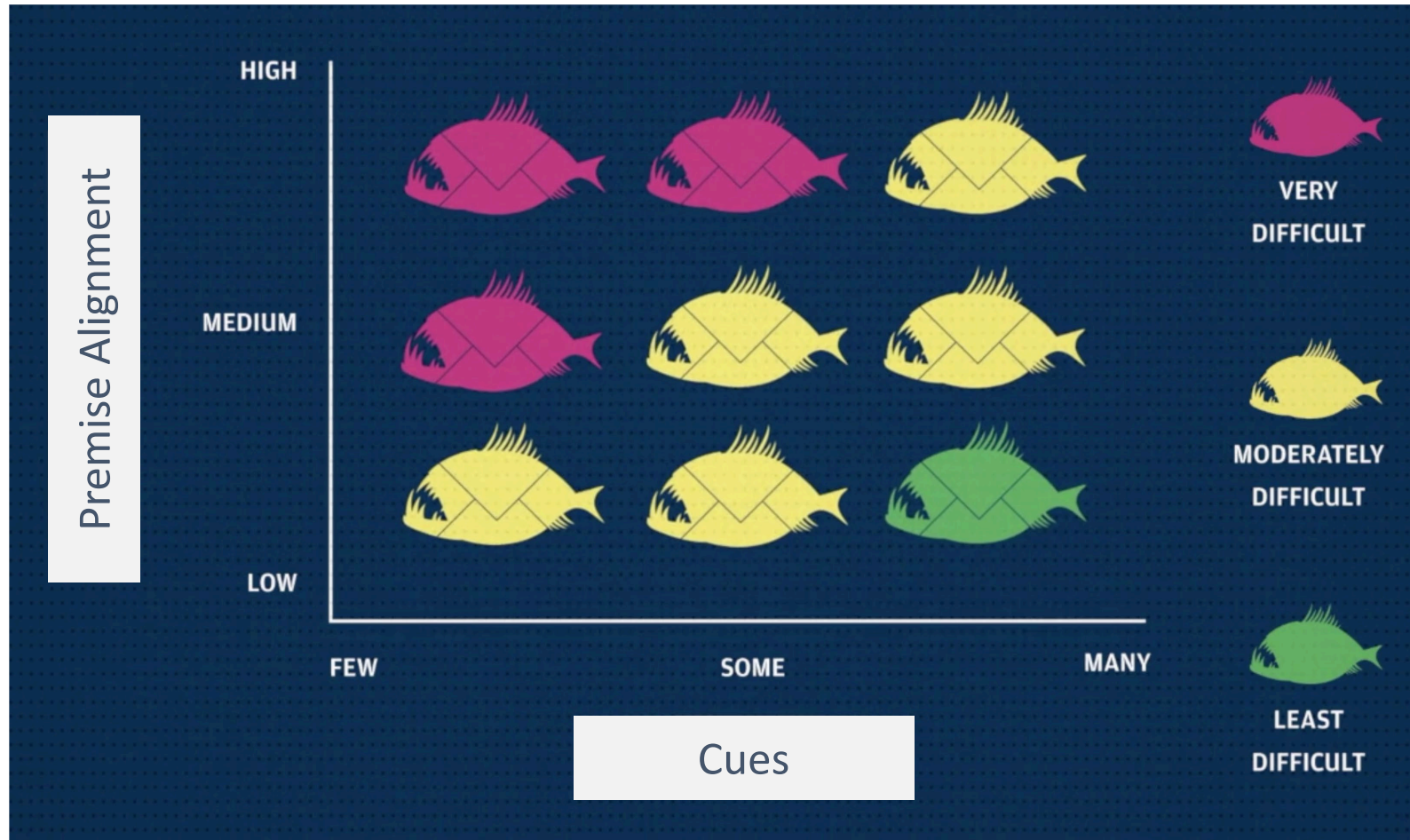
Concern over
consequences



Compelling vs.
suspicious cues

Reality-checking
strategies

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?

No



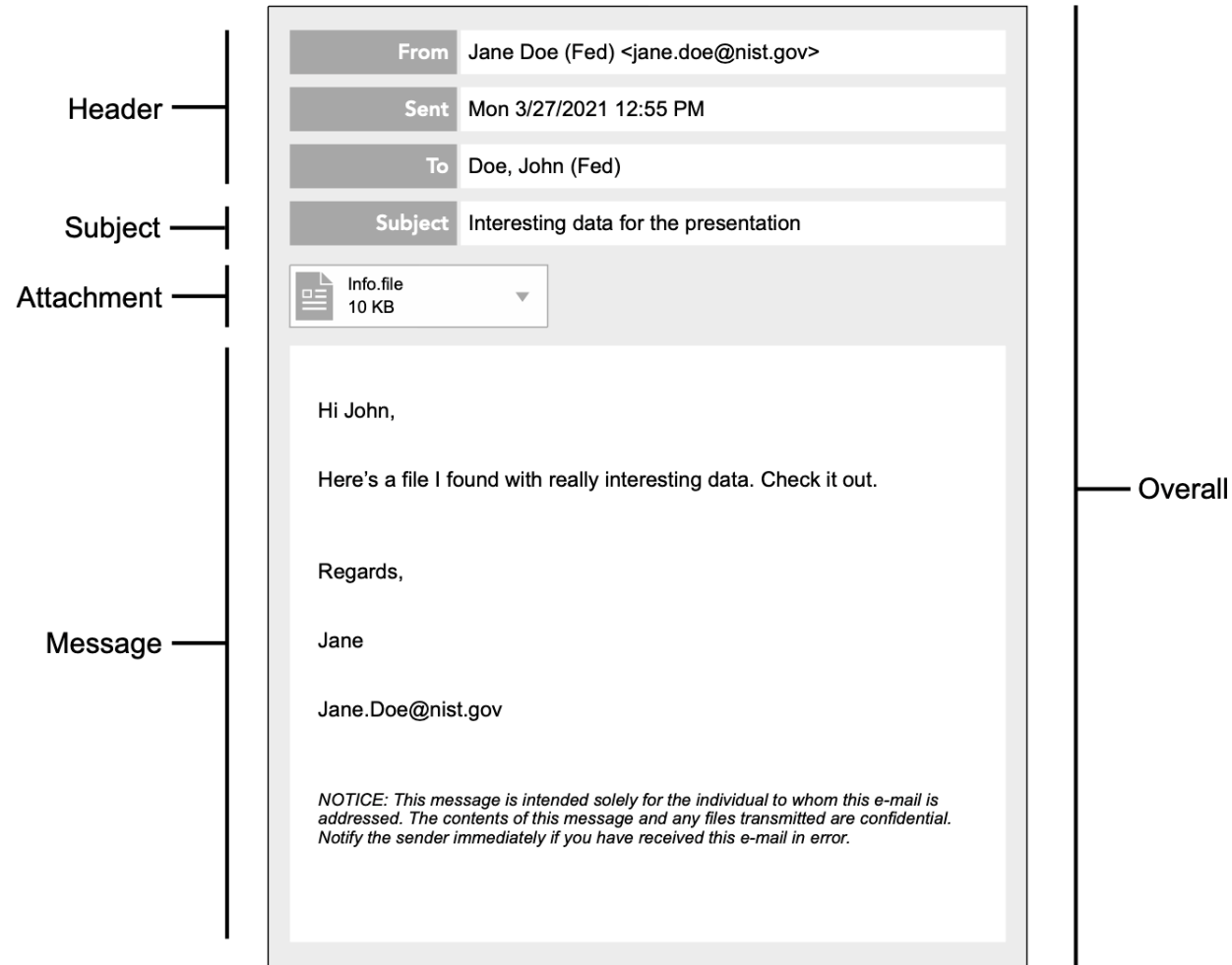
Yes



Phish Scale – Cues



How to Spot a Phish – Where to Find Cues



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

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

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

How to Spot a Phish – What Cues to Look for

- 5 Types of Cues

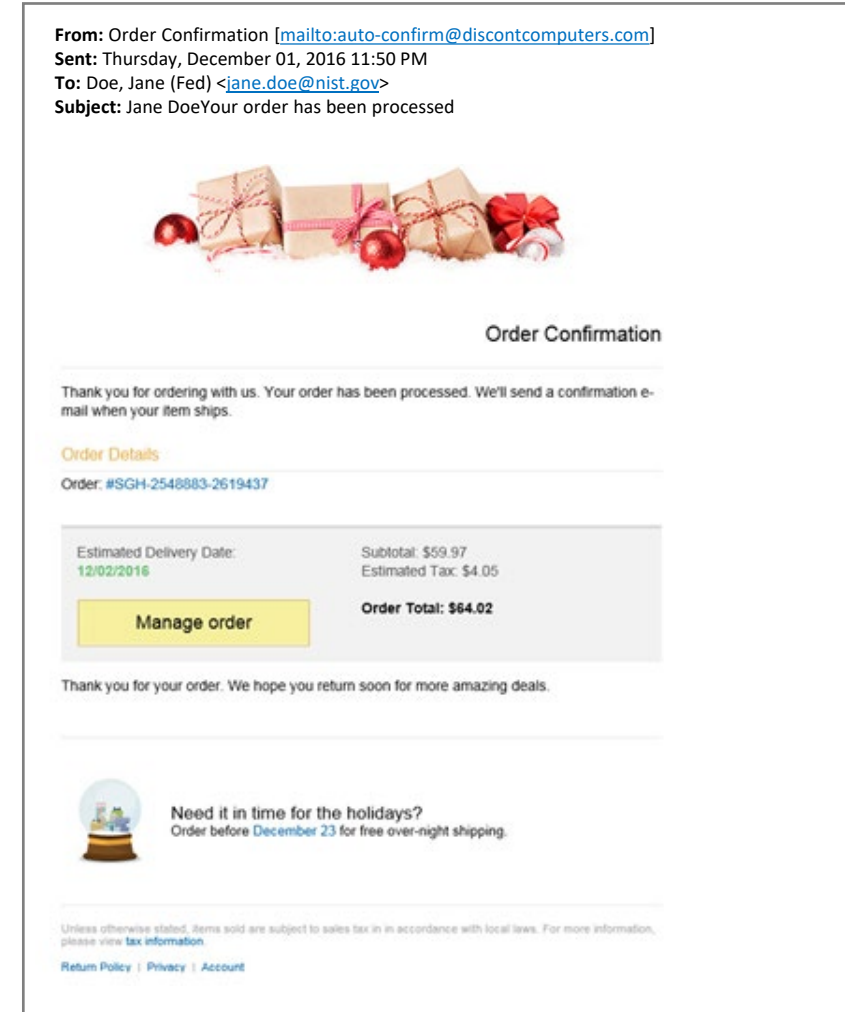
- Errors
- Technical indicators
- Visual presentation indicators
- Language and content
- Common tactics

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

How to Spot a Phish – What Cues to Look for

- 5 Types of Cues

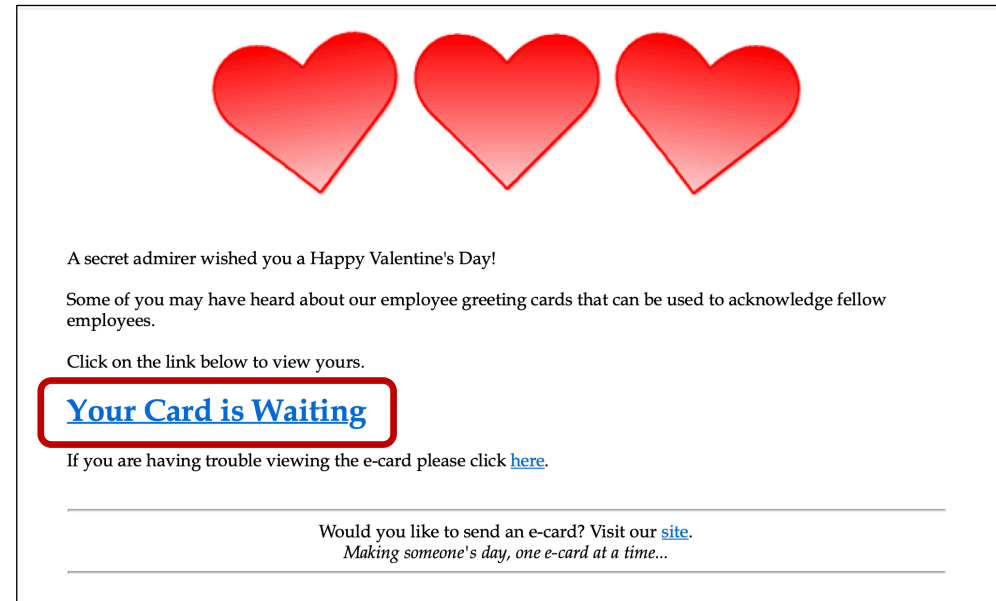
- Errors
- Technical indicators
- Visual presentation indicators
- Language and content
- Common tactics



How to Spot a Phish – 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 – What Cues to Look for

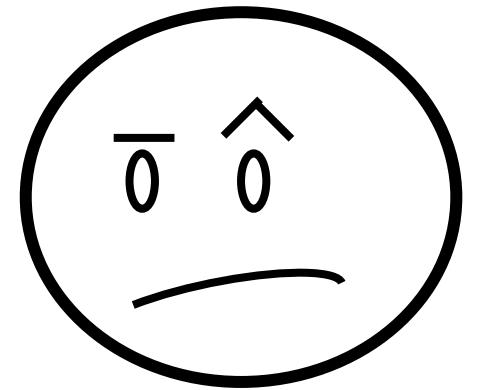
- 5 Types of Cues

- 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

How to Spot a Phish – What Can You Do?

- Be vigilant
- Consider your context. Does it make you vulnerable?
- Look for cues
 - Are there links, attachments, or requests for information?
 - Inspect carefully
- Use bookmarked links/favorites instead of clicking
- Use a search engine, don't click on ads
- Consider calling the sender
- Clicking is the last resort!

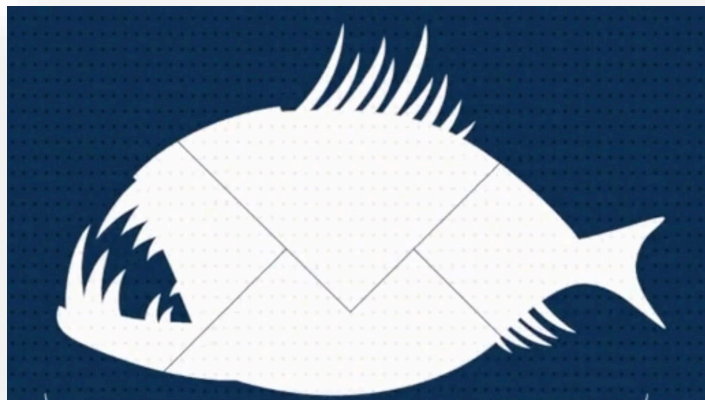


How to Spot a Phish – What Can You Do?

- You are the last line of defense against a phishing attack
- Malware can make it past firewalls and filters
- Phone, postal mail, and in-person social engineering attempts can't be detected with tools
- You are the Detective and Judge
- Every questionable email should be considered guilty until proven innocent

How to Spot a Phish – What Can You Do?

- What if you see a potential phish?

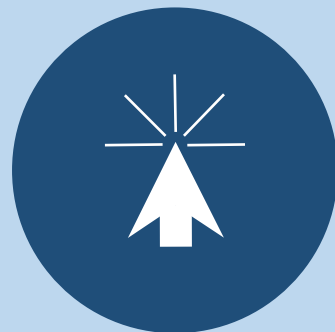


- Don't:
 - Click on links
 - Download attachments
 - Provide any requested information
- Do:
 - Follow agency guidance for reporting suspicious emails
 - Contact sender through an alternative route



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**

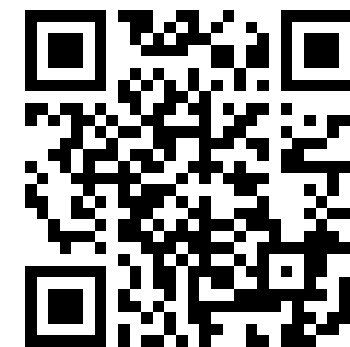


No silver bullet

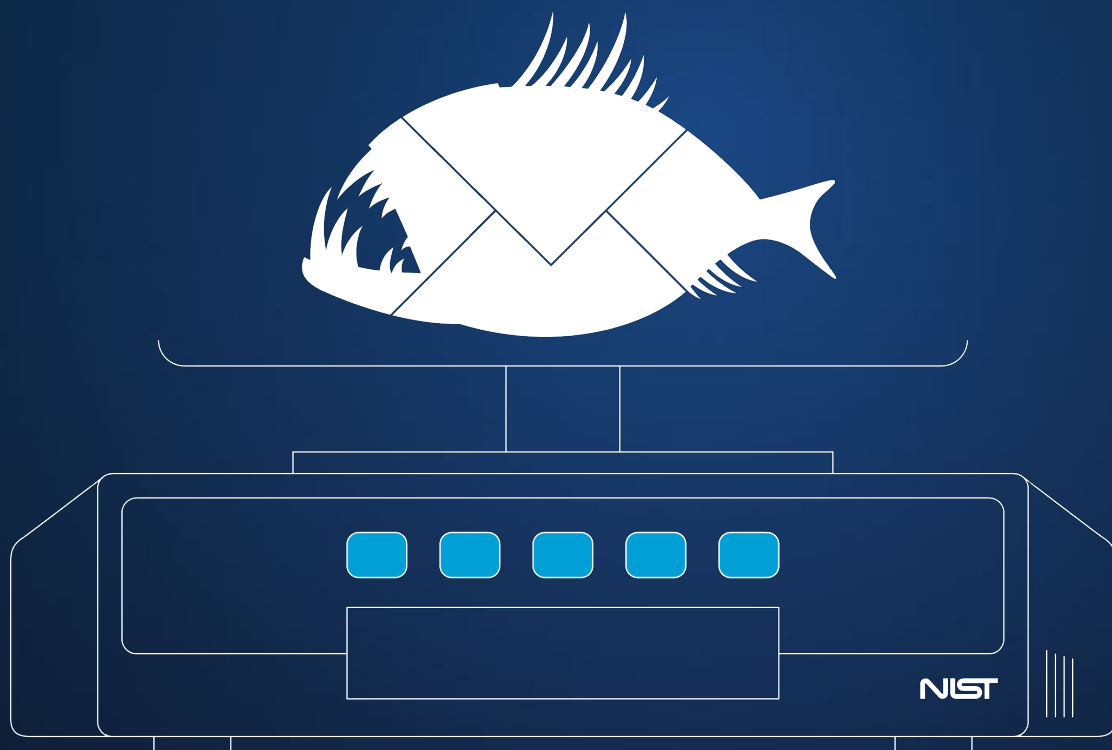
**Awareness training
is not the silver
bullet in phishing
defense**



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