Can you spot a phish?

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
- How to spot a phish

Championing the Human in I.T.

DEFENDING AGAINST PHISHING

Phishing Threat Landscape

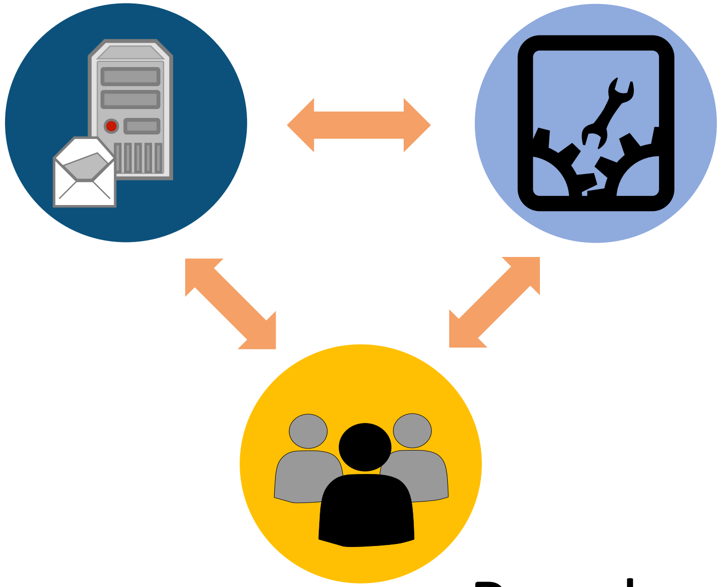
Phishing Threats

Broad cybersecurity email attacks

Spear Phishing

Direct and targeted email attacks

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

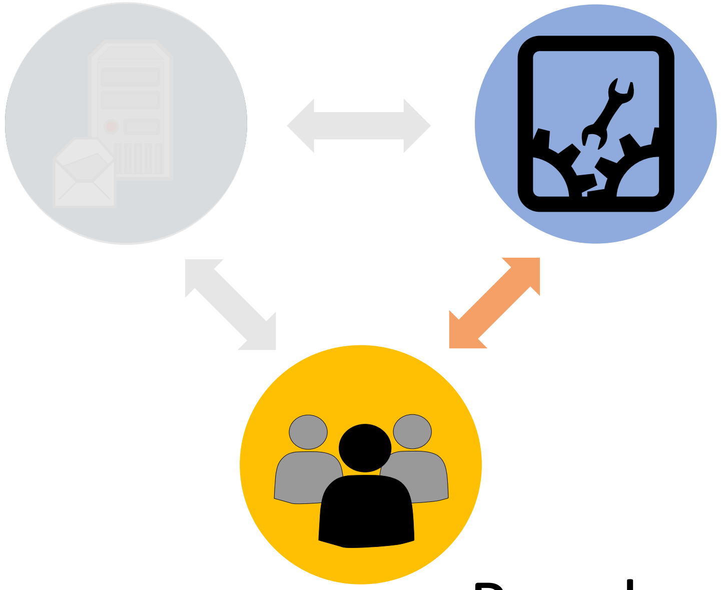
People

- End users
- IT security staff
- Leadership

Phishing Defense

Technology

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



Process

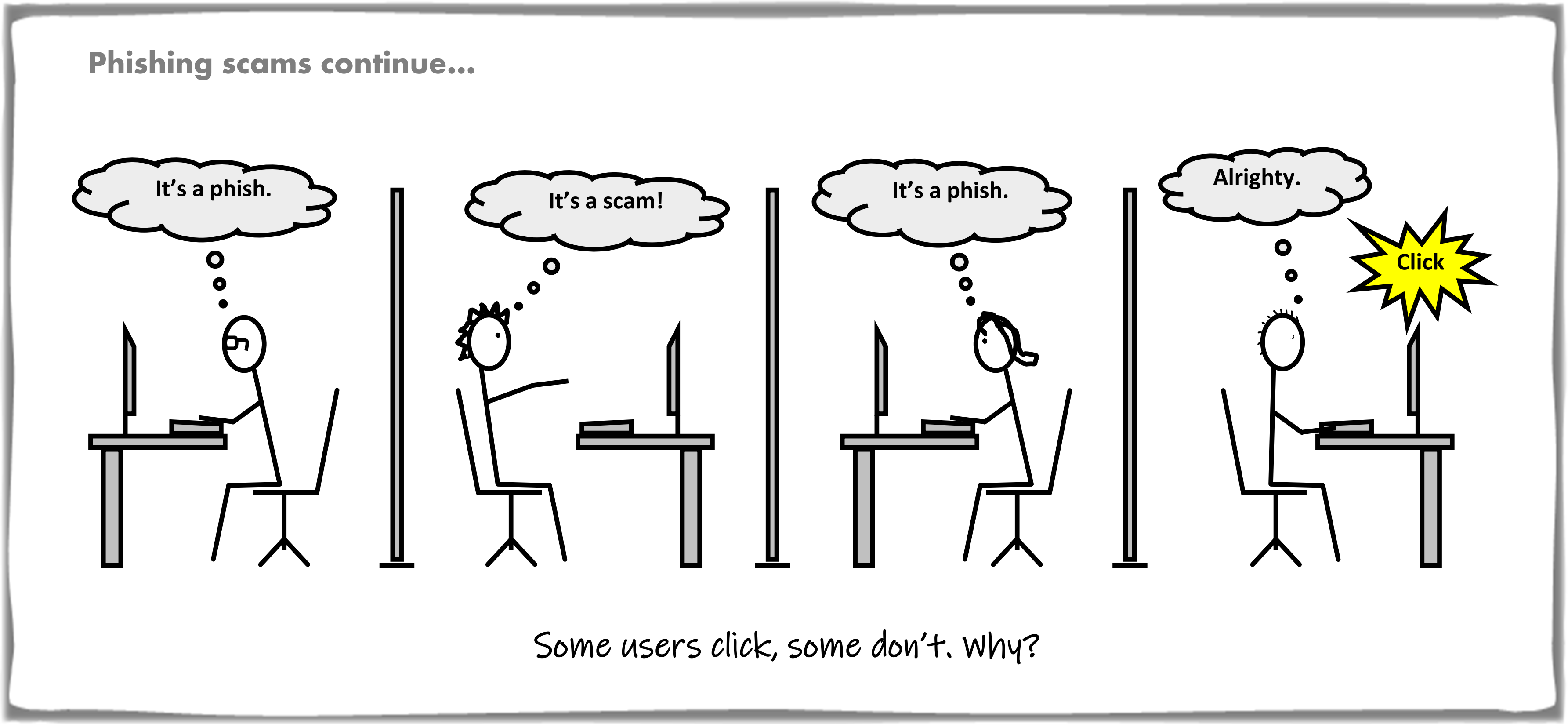
- Identify vulnerabilities
- Limiting publicly available information
- Awareness training
- Easy and clear reporting mechanism
- Meaningful metrics

People

- End users
- IT security staff
- Leadership

Our Research

Our Research – Phishing Awareness Study



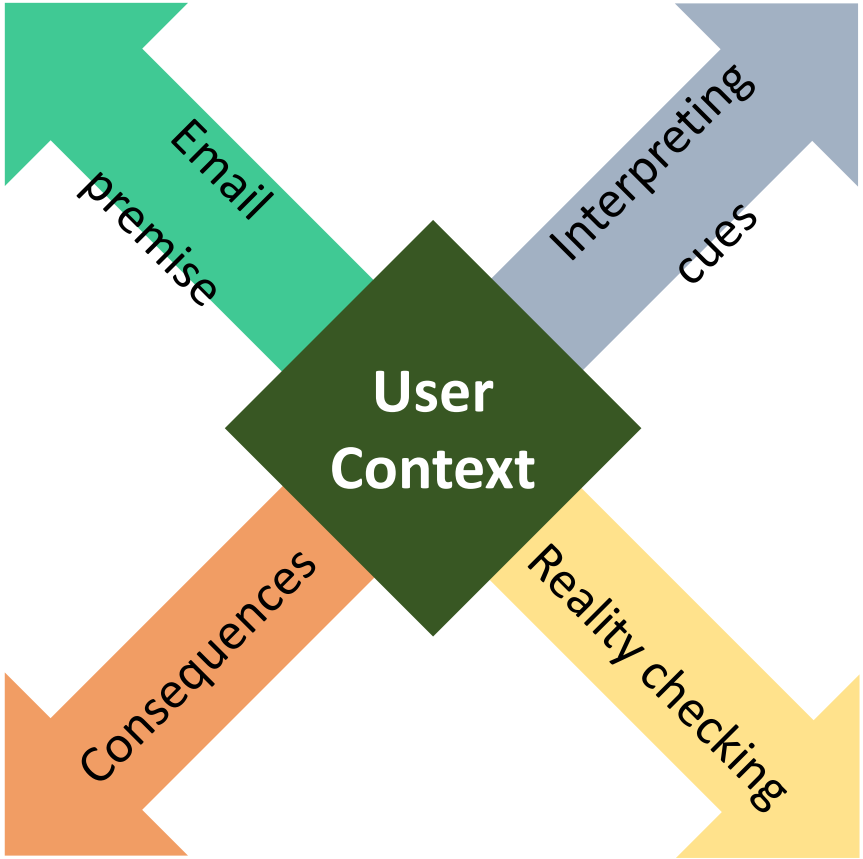
Phishing scams continue…

Some users click, some don't. Why?

Our Research – Phishing Awareness Study

Alignment vs. misalignment with expectations and external events

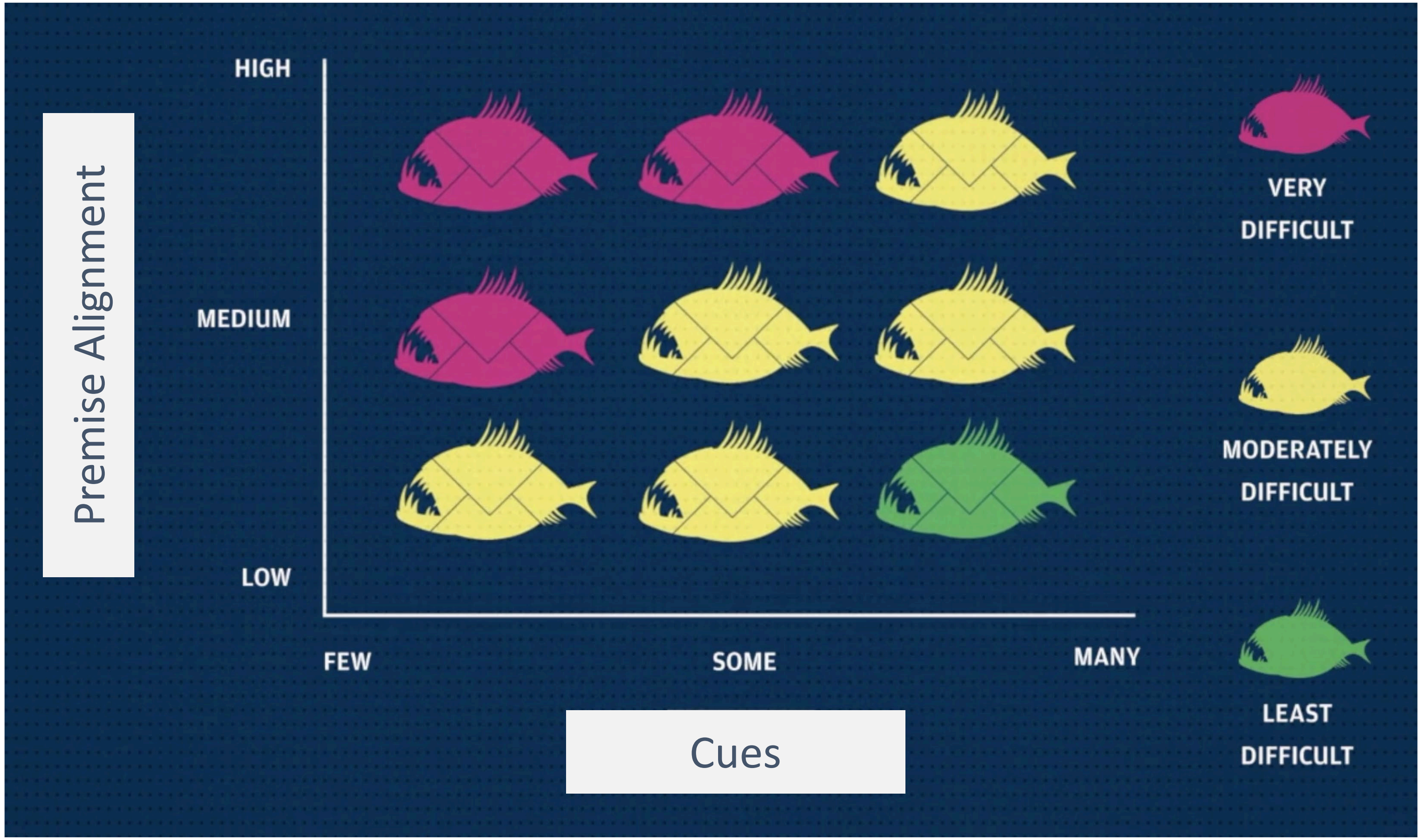
Compelling vs. suspicious cues



Concern over consequences

Reality-checking strategies

NIST Phish Scale



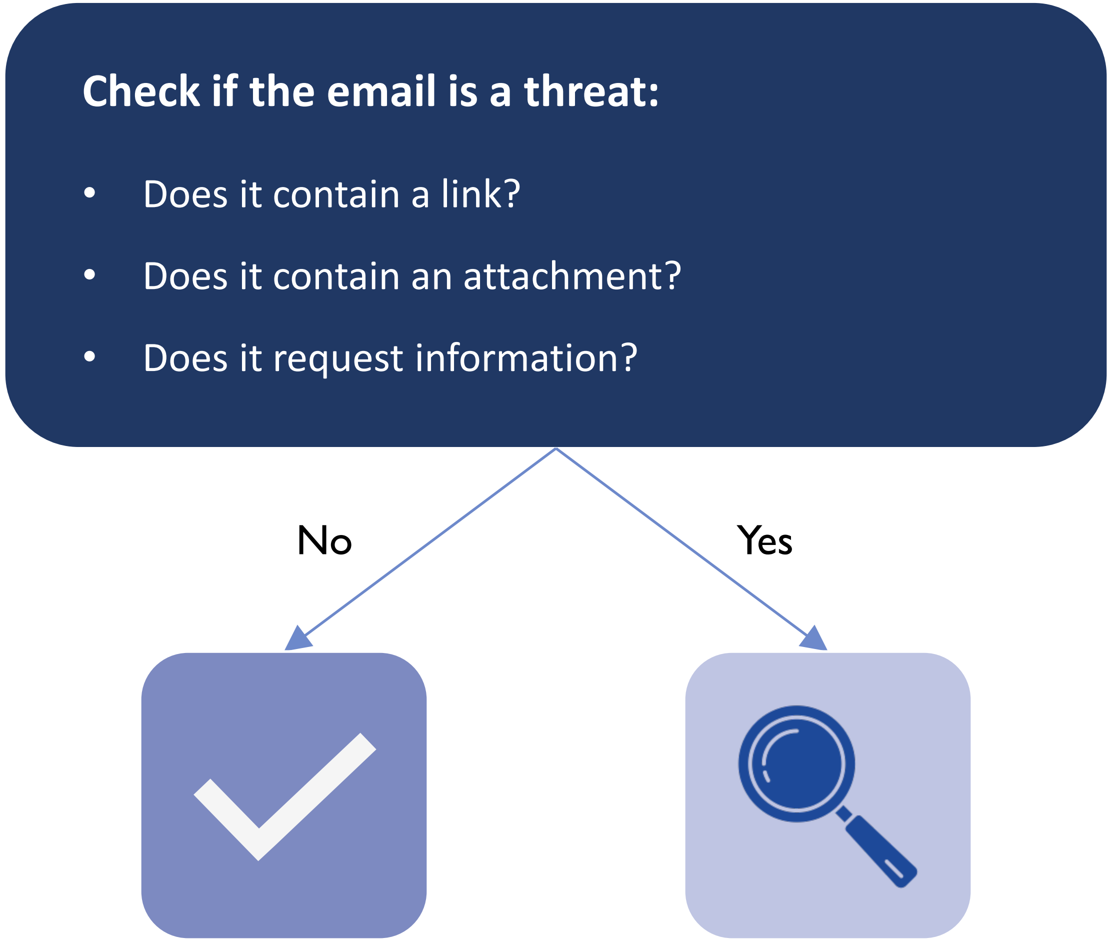
Our Research

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:

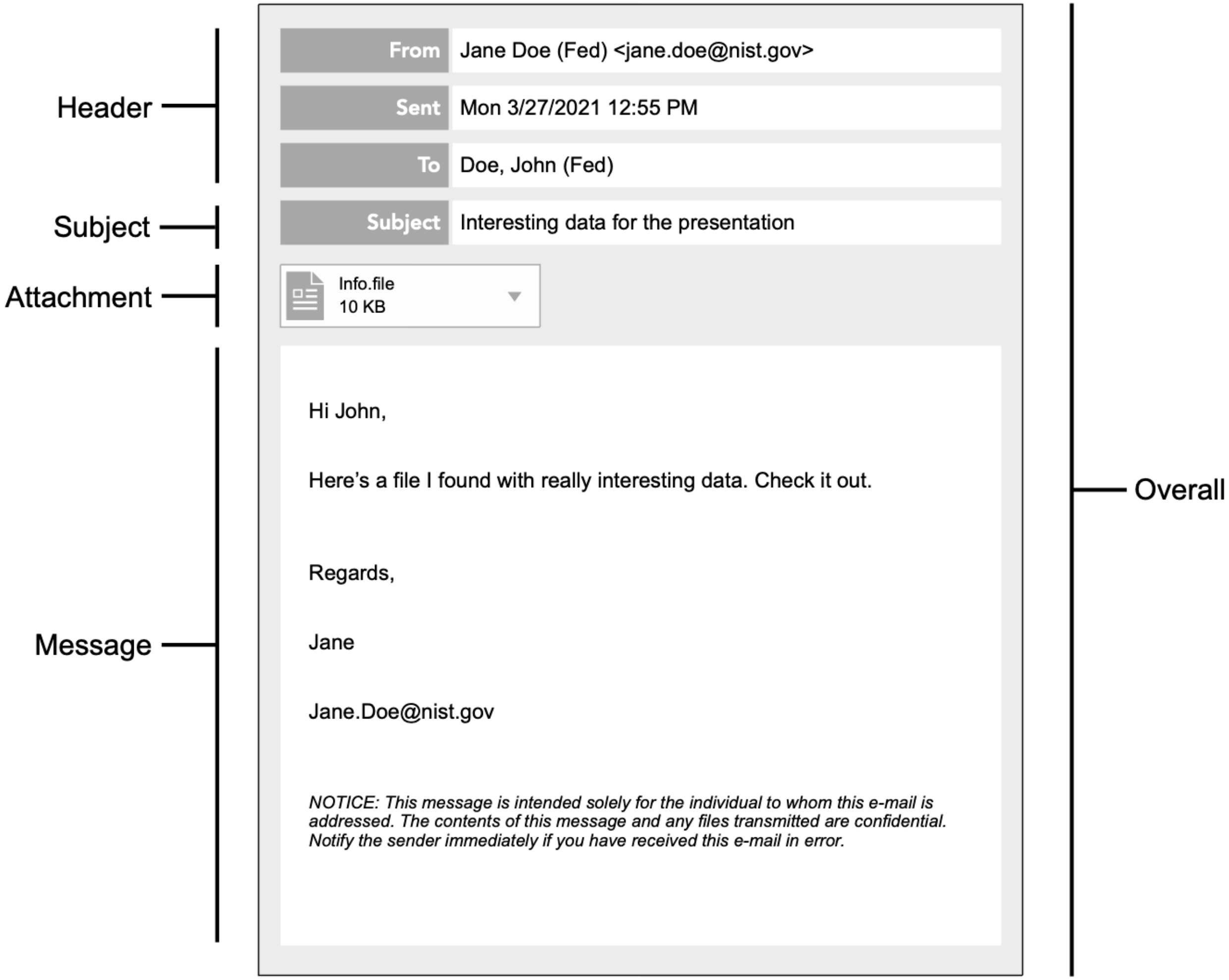
- Does it contain a link?
- Does it contain an attachment?
- Does it request information?

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*

How to Spot a Phish – Where to Find Cues



From: Jane Doe (Fed) <jane.doe@nist.gov>

Sent: Mon 3/27/2021 12:55 PM

To: Doe, John (Fed)

Subject: Interesting data for the presentation

Info.file
10 KB

Hi John,

Here's a file I found with really interesting data. Check it out.

Regards,

Jane

Jane.Doe@nist.gov

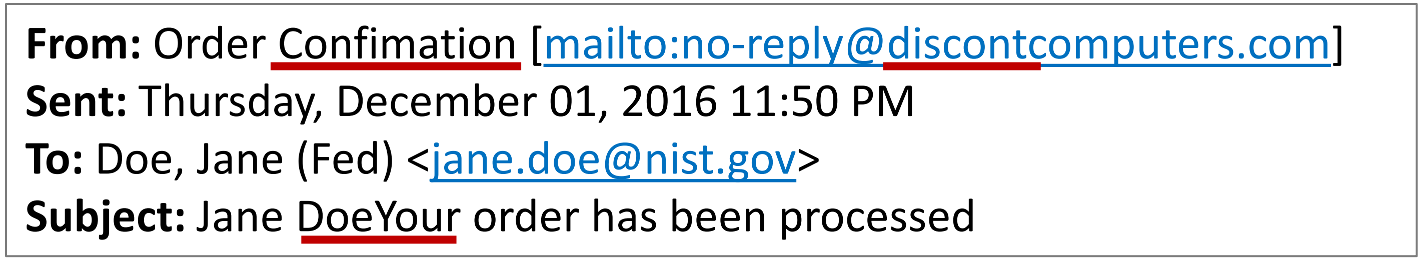
NOTICE: This message is intended solely for the individual to whom this e-mail is addressed. The contents of this message and any files transmitted are confidential. Notify the sender immediately if you have received this e-mail in error.

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

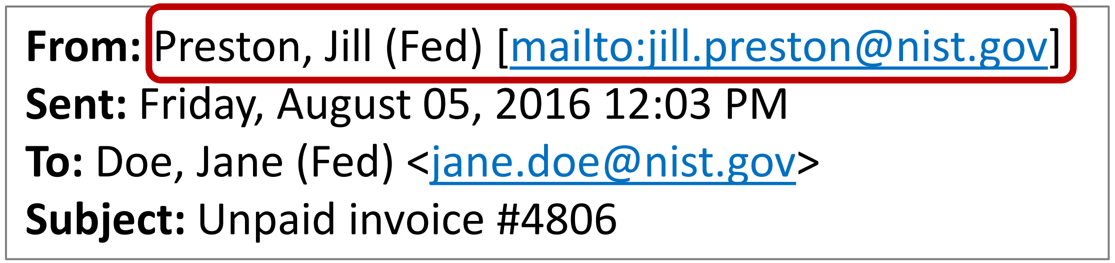
- 5 Types of Cues
  - Errors
  - Technical indicators
  - Visual presentation indicators
  - Language and content
  - Common tactics



From: Order Confimation [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

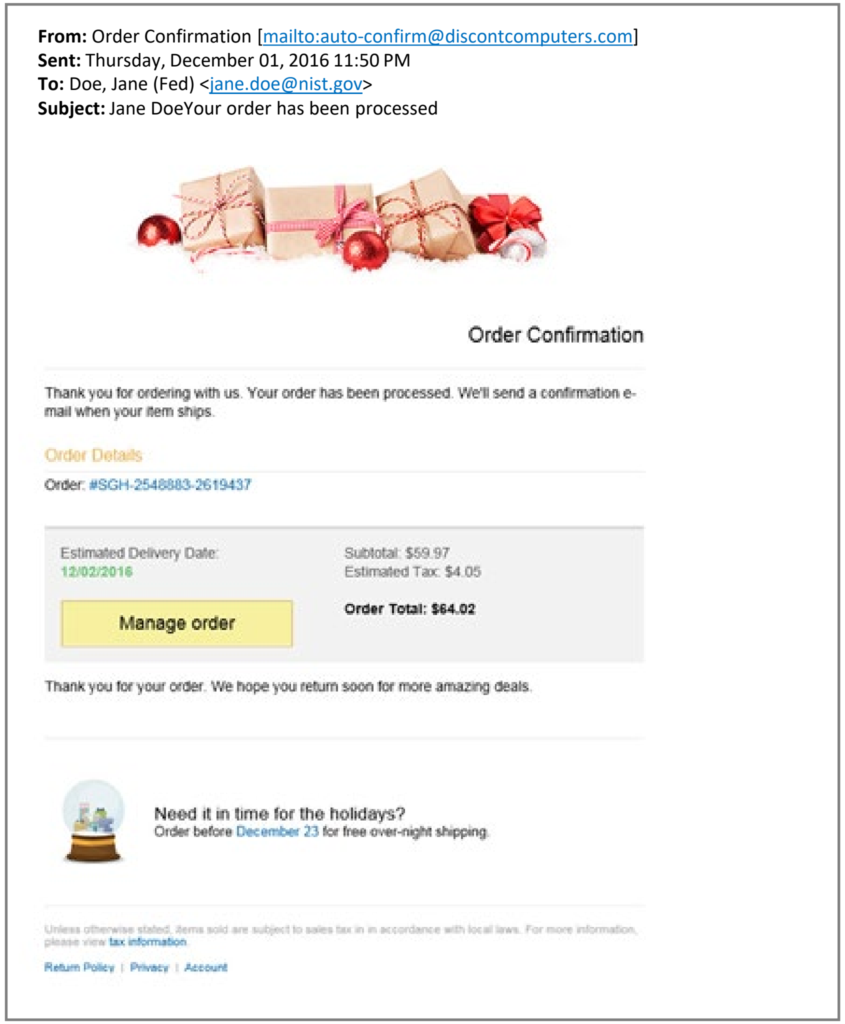
- 5 Types of Cues
  - Errors
  - Technical indicators
  - Visual presentation indicators
  - Language and content
  - Common tactics



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



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.

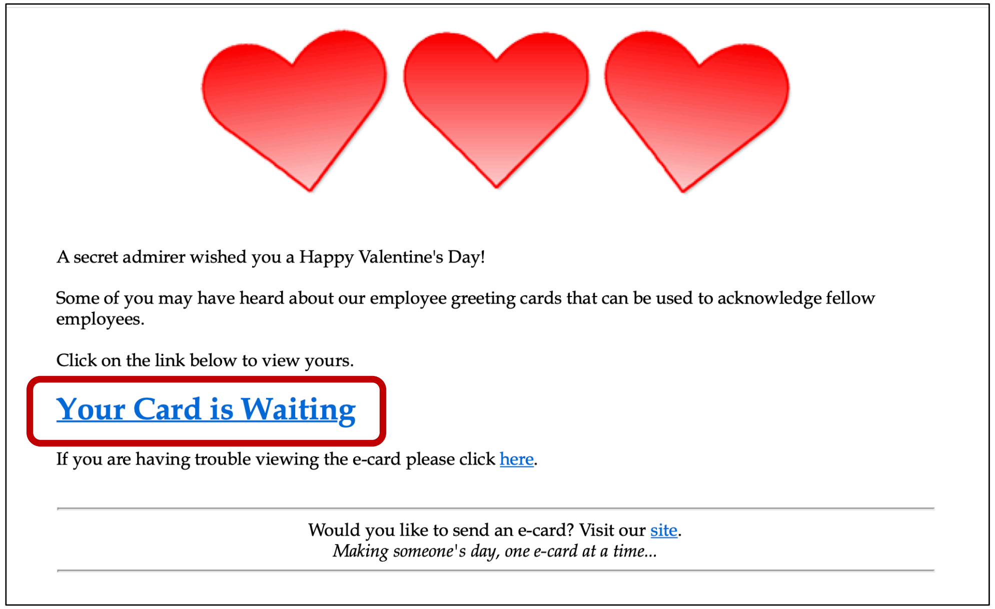
Need it in time for the holidays?
Order before December 23 for free over-night shipping.

Unless otherwise stated, items sold are subject to sales tax in in accordance with local laws. For more information, please view tax information.

Return Policy | Privacy | Account

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



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.

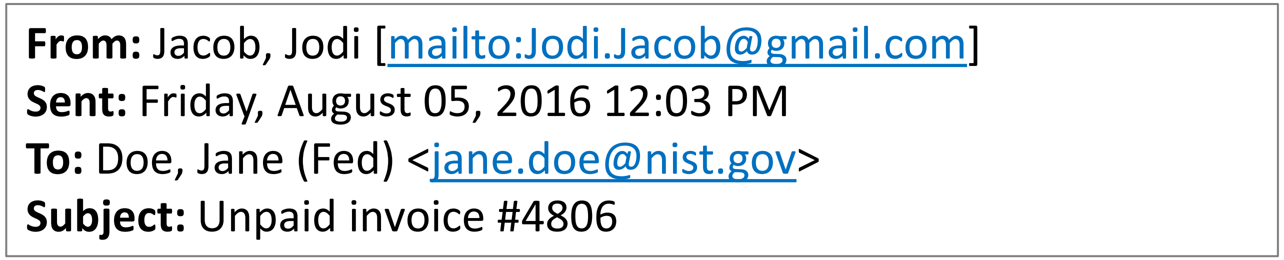
Your Card is Waiting

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...

How to Spot a Phish – What Cues to Look for

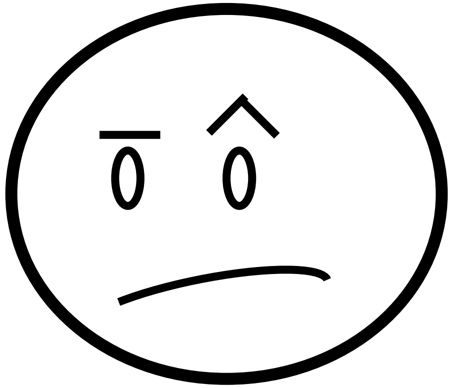
- 5 Types of Cues
  - Errors
  - Technical indicators
  - Visual presentation indicators
  - Language and content
  - Common tactics



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

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

No silver bullet

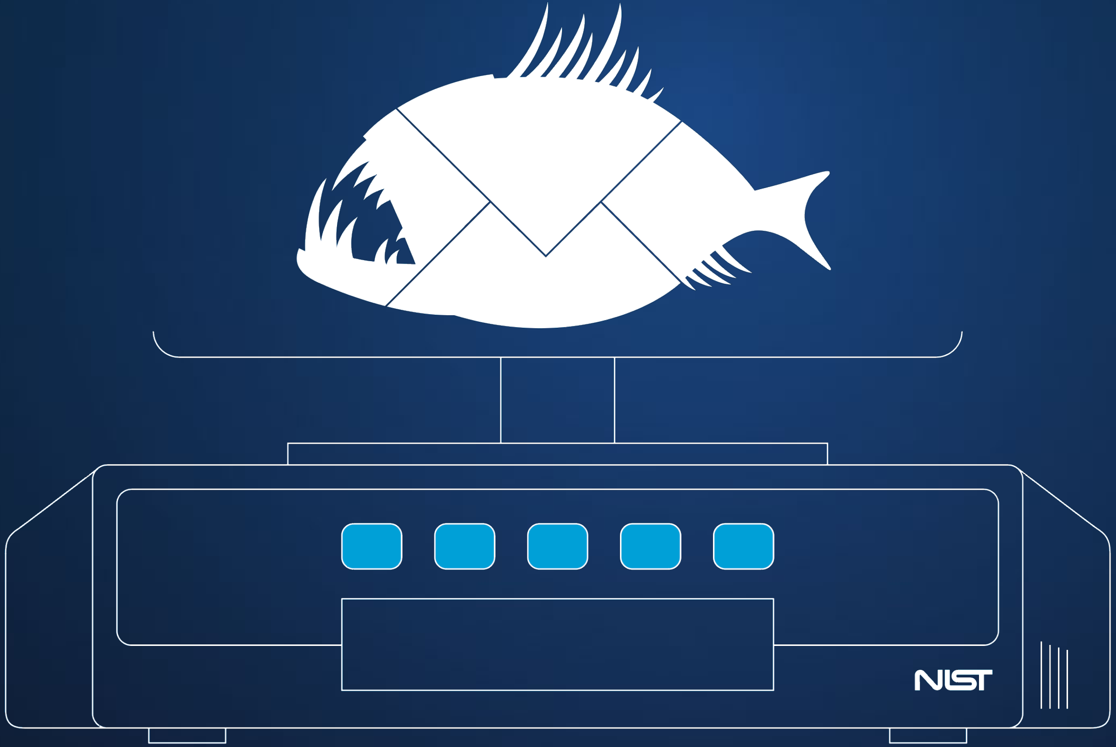
Awareness training is not the silver bullet in phishing defense

Additional Resources

- 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

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)
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/10.1177/21582440211990656 (Accessed February 9, 2023)

References

- 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 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 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)