Can you spot a phish?

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

Shanée Dawkins, Ph.D.
Jody Jacobs, M.S.

October 2022

Disclaimer

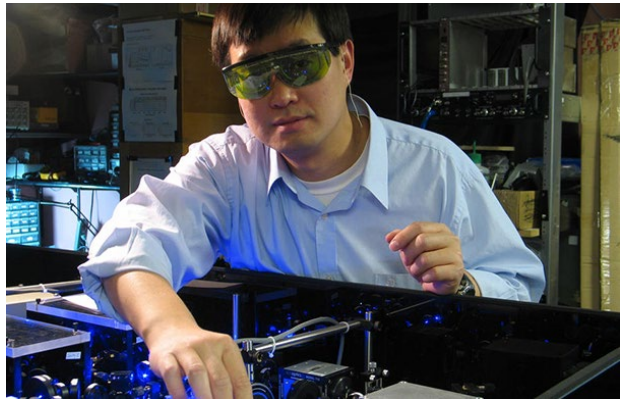
Throughout the presentation, certain commercial companies or products may be identified to foster understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the companies or products identified are necessarily the best available for the purpose.

Presentation Overview

- Who we are
- Phishing threat landscape
- Our research
- How to spot a phish

Our Mission

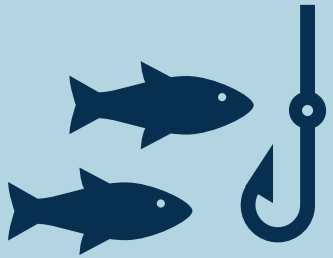
- **NIST**: To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life
- **Information Technology Lab**: To cultivate trust in IT and metrology.



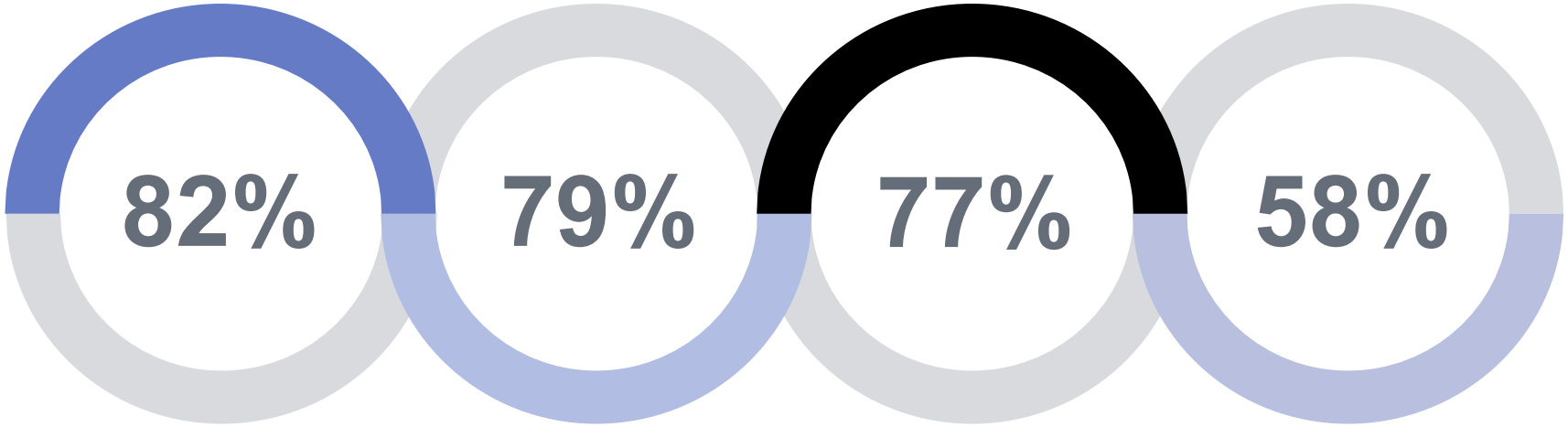
Championing the Human in I.T.

Phishing Threat Landscape

Phishing Overview

Phishing Social engineering attempt, often via email		**Spear Phishing** Direct and targeted email attacks	

Phishing Threat Landscape



Breaches

Involved the human element in 2021[1]

Spear Phish

of organizations reported targeted phishing attacks[2]

Cyber attacks

of organizations are most concerned about phishing attacks[3]

Training

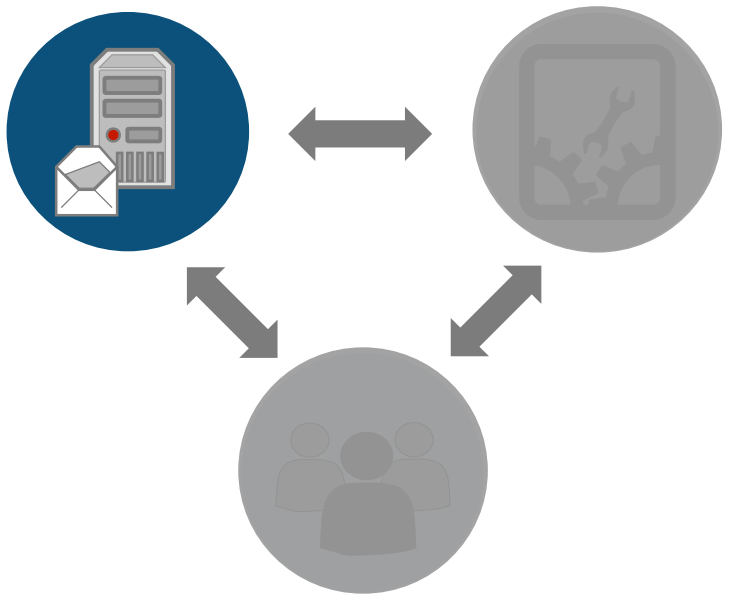
Of people were better at recognizing phishing messages after training[4]

[1]Verizon, 2022 Data Breach Investigations Report
[2]Proofpoint, 2022 State of the Phish Report
[3]SonicWall, How to deal with BEC, 2022
[4] Oh, Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2022

Phishing Defense

Technology

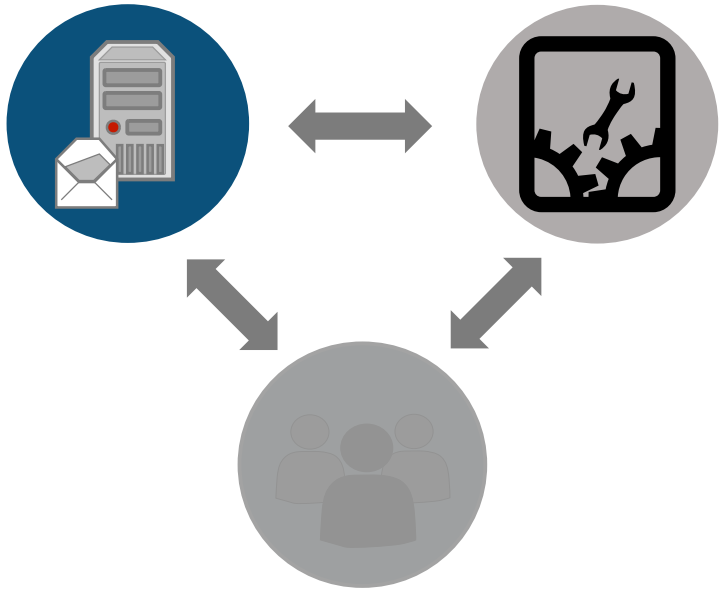
- Filtering
- DMARC, DKIM
- AI & ML



Phishing Defense

Technology

- Filtering
- DMARC, DKIM
- AI & ML



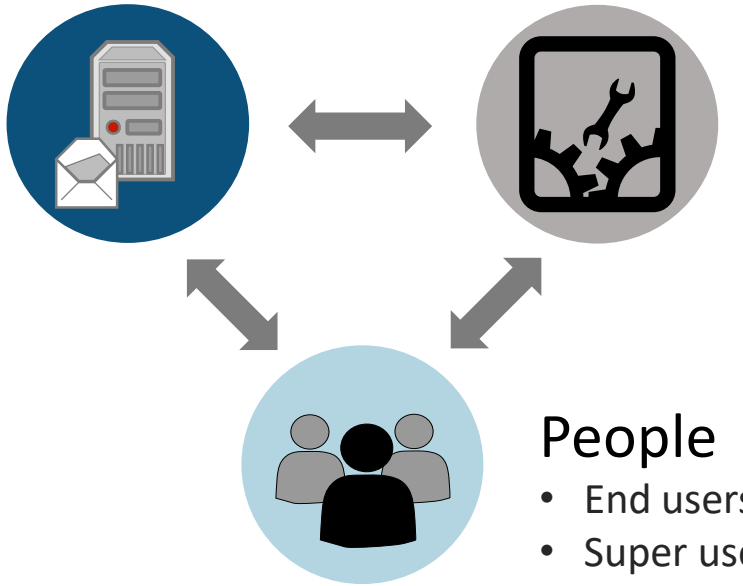
Process

- Identify vulnerabilities
- Awareness training
- Reporting & early warning
- Meaningful metrics

Phishing Defense

Technology

- Filtering
- DMARC, DKIM
- AI & ML



Process

- Identify vulnerabilities
- Awareness training
- Reporting & early warning
- Meaningful metrics

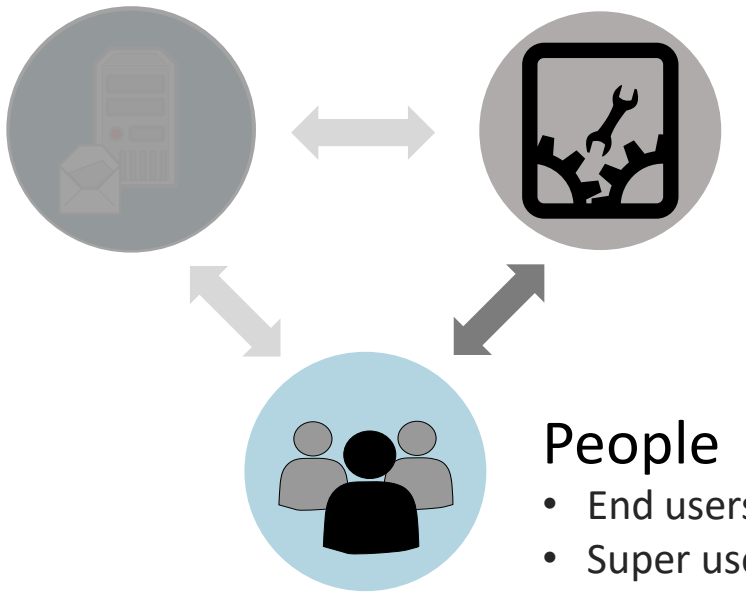
People

- End users
- Super users
- IT security staff
- Leadership

Phishing Defense

Technology

- Filtering
- DMARC, DKIM
- AI & ML



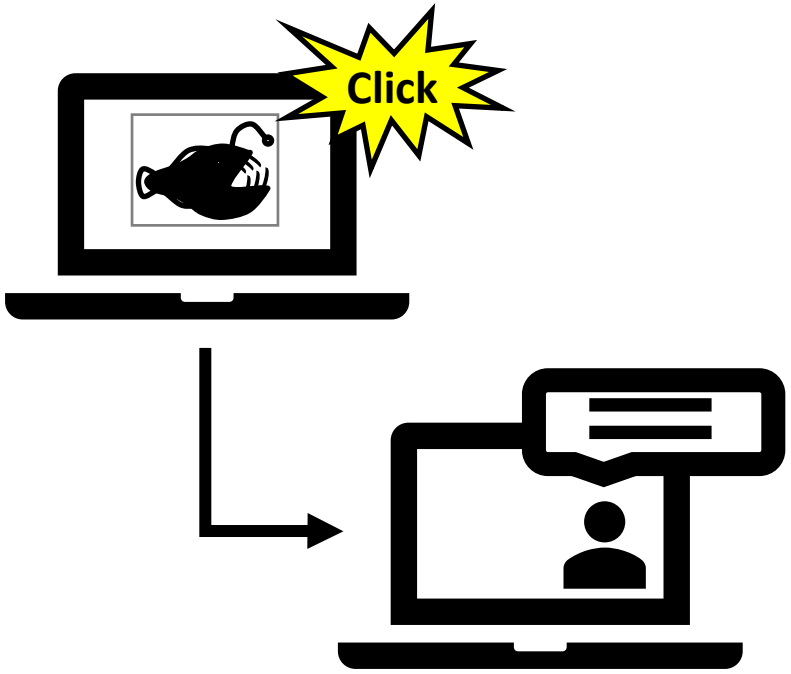
Process

- Identify vulnerabilities
- Awareness training
- Reporting & early warning
- Meaningful metrics

People

- End users
- Super users
- IT security staff
- Leadership

Phishing Awareness Training

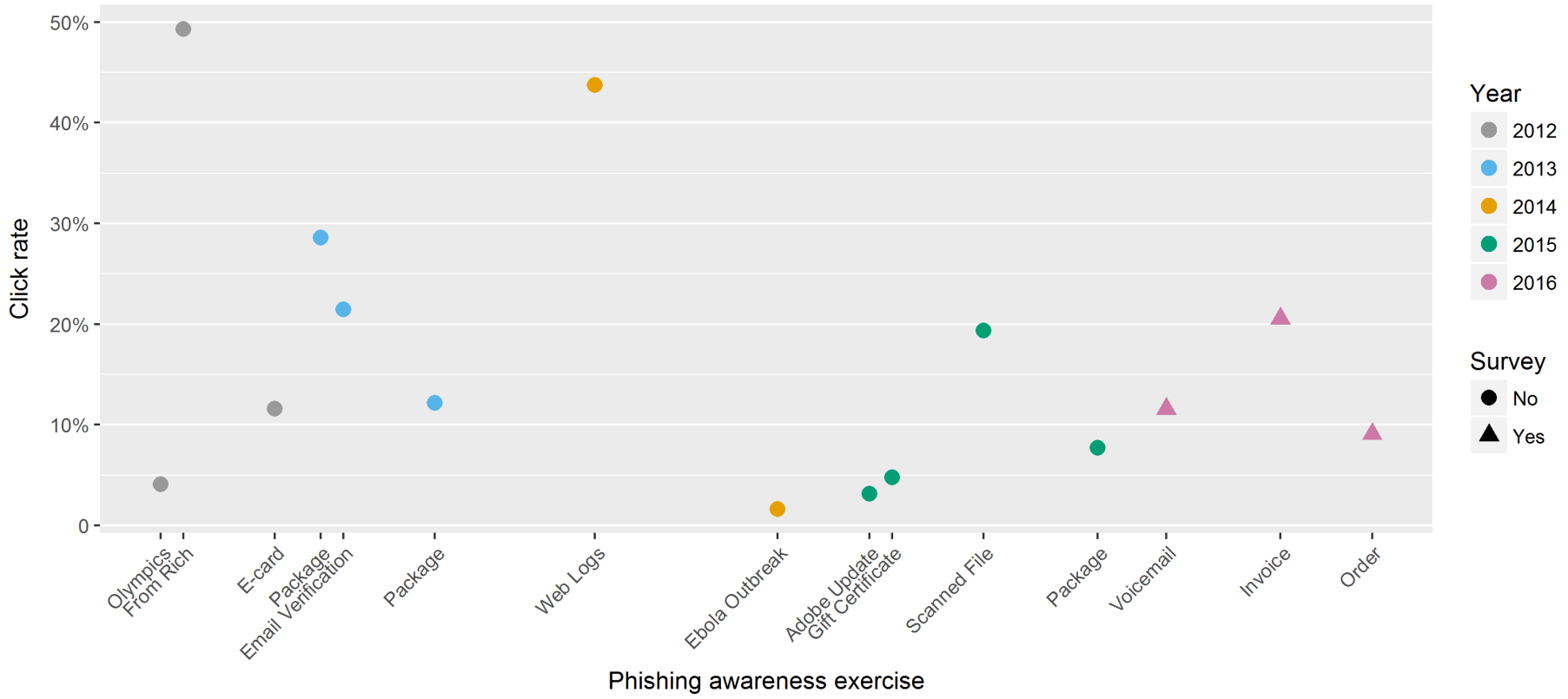


- Simulated phishing emails that mimic real-world attacks
- Click rates, reporting rates, reporting times
- NIST, and many other government agencies do this

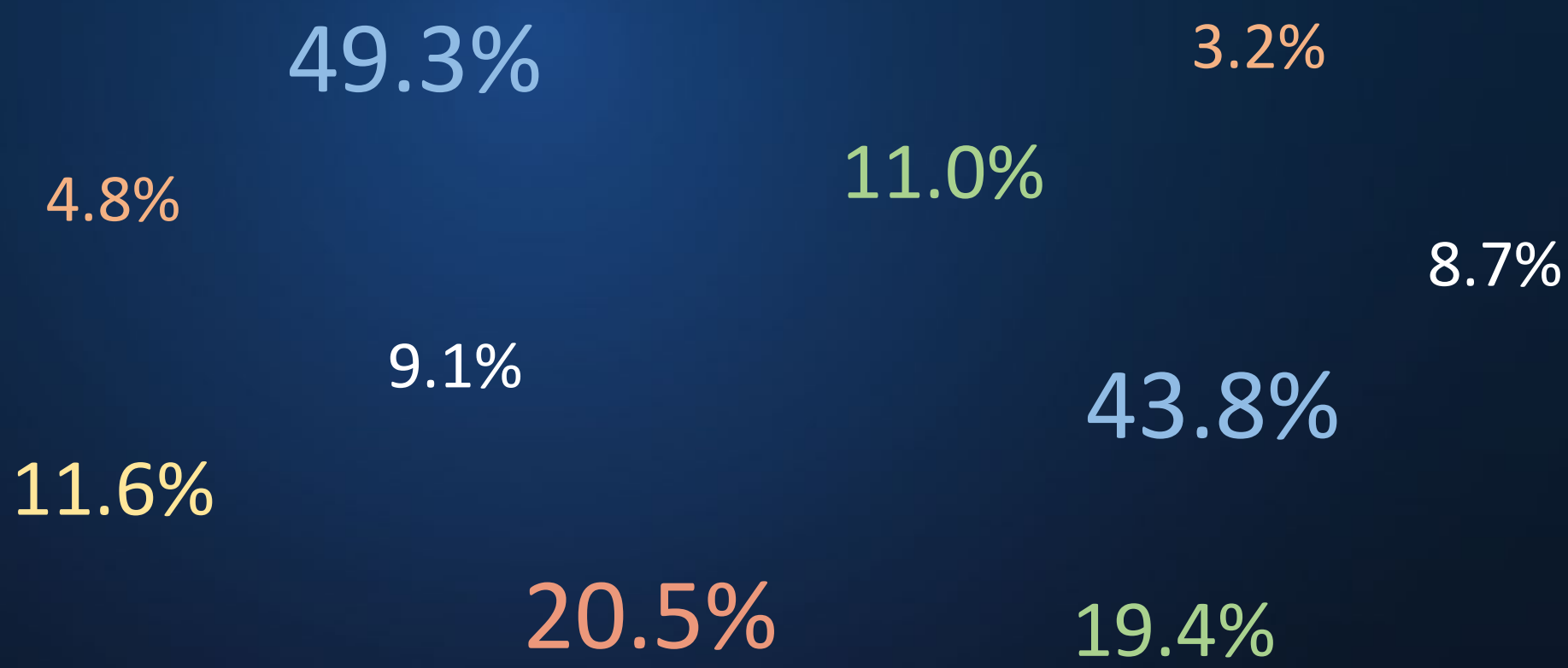
Our Research

Our Research – Phishing Awareness Study

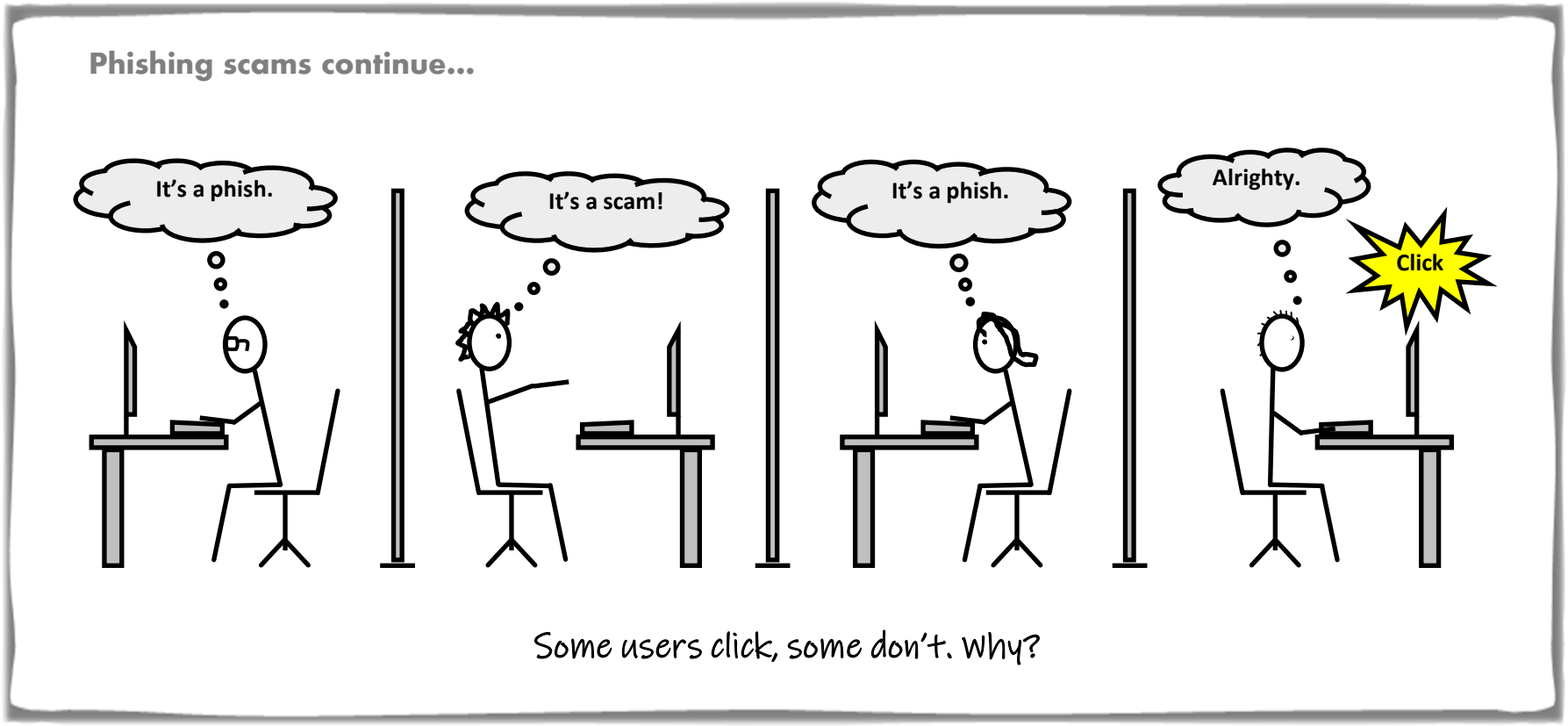
- 15 training exercises over 4.5 years



Our Research – Phishing Awareness Study

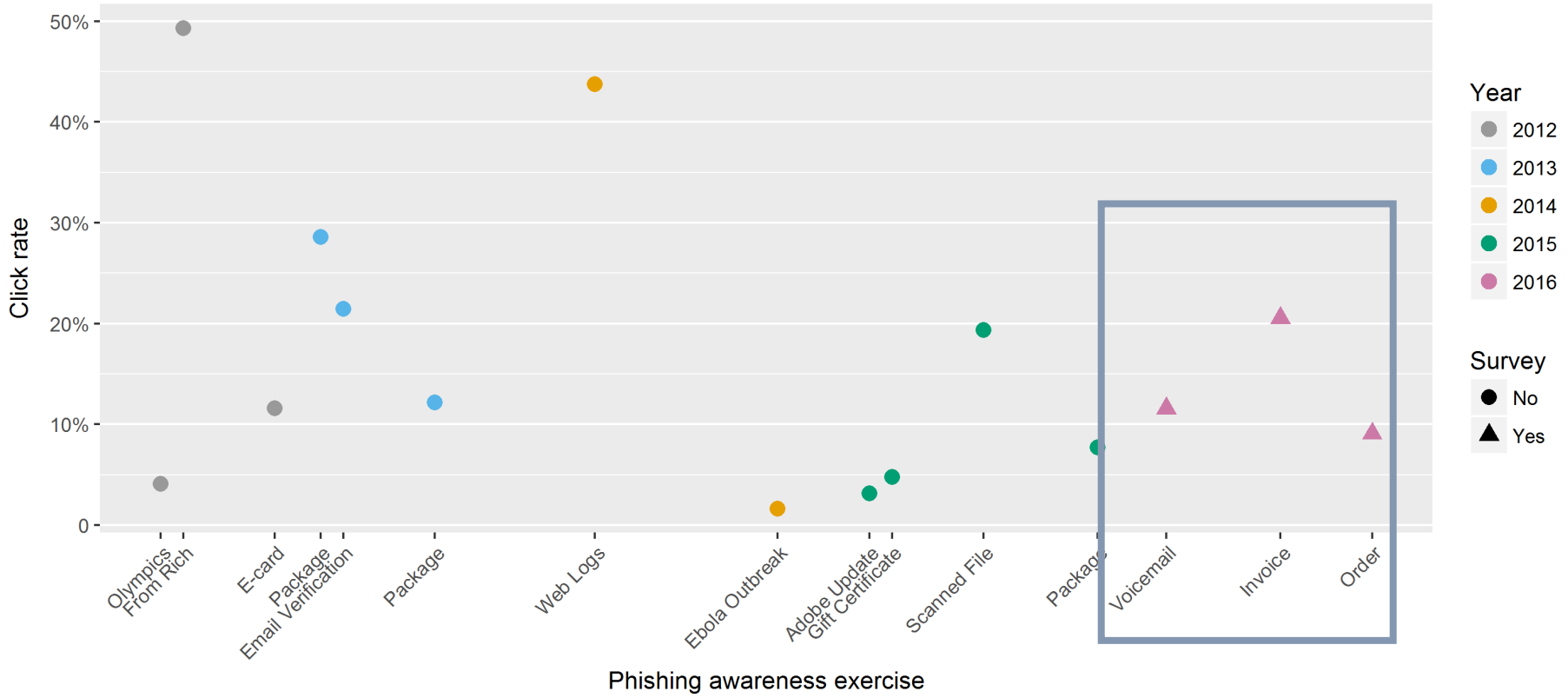


Our Research – Phishing Awareness Study



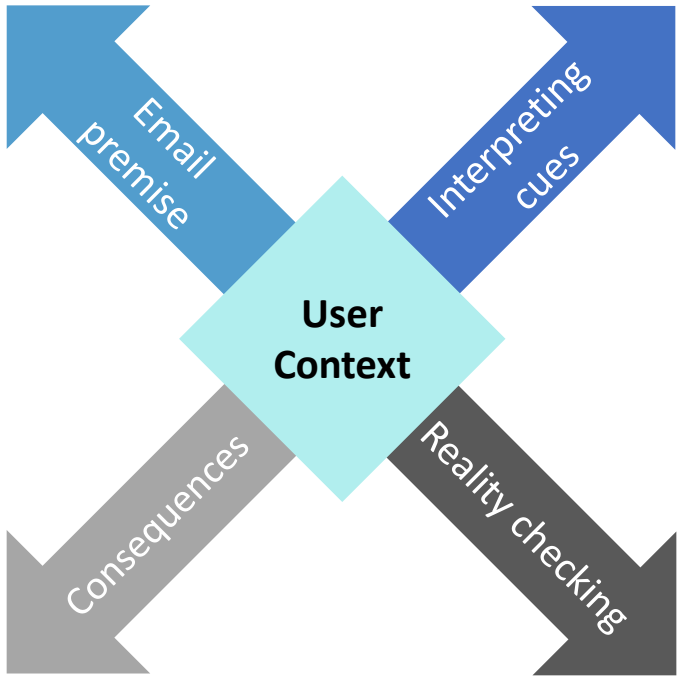
Our Research – Phishing Awareness Study

- 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



Compelling vs. suspicious cues

Concern over consequences

Reality-checking strategies

Our Research – NIST Phish Scale

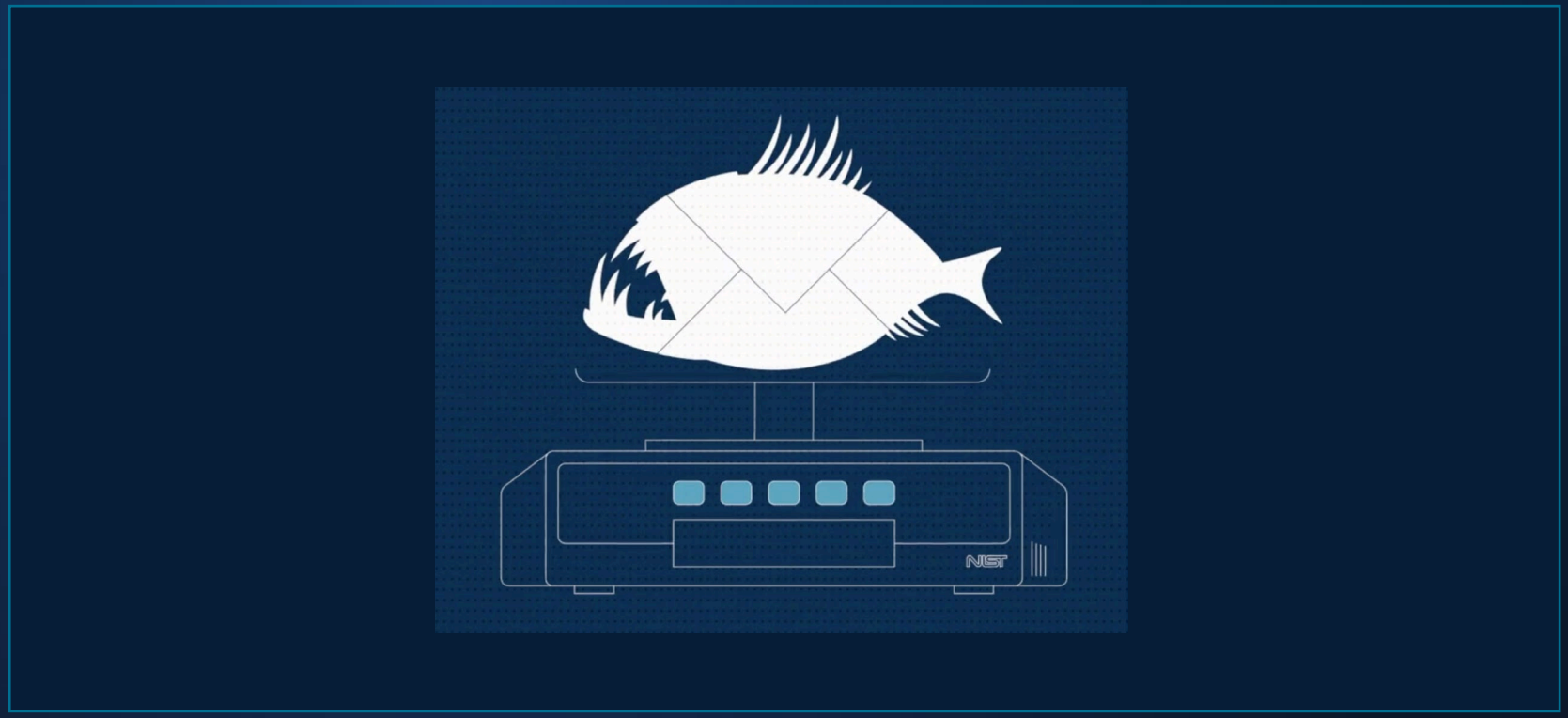


Image credit: NIST

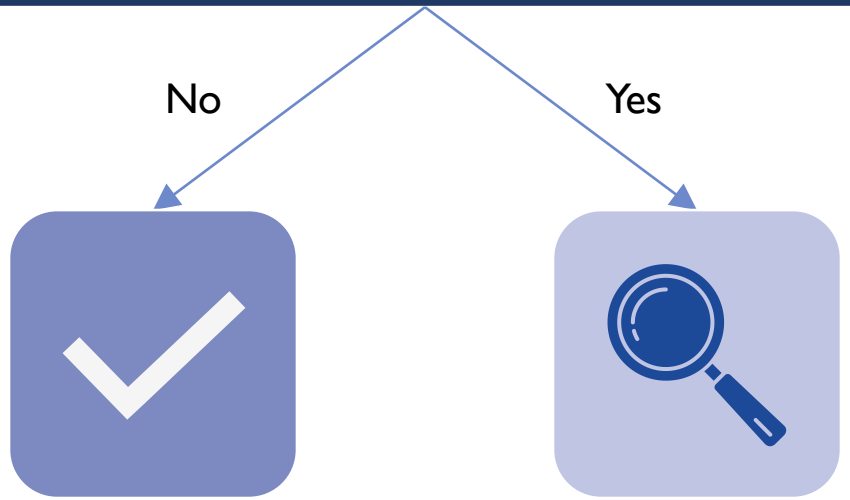
https://www.nist.gov/video/introducing-phish-scale

How to Spot a Phish

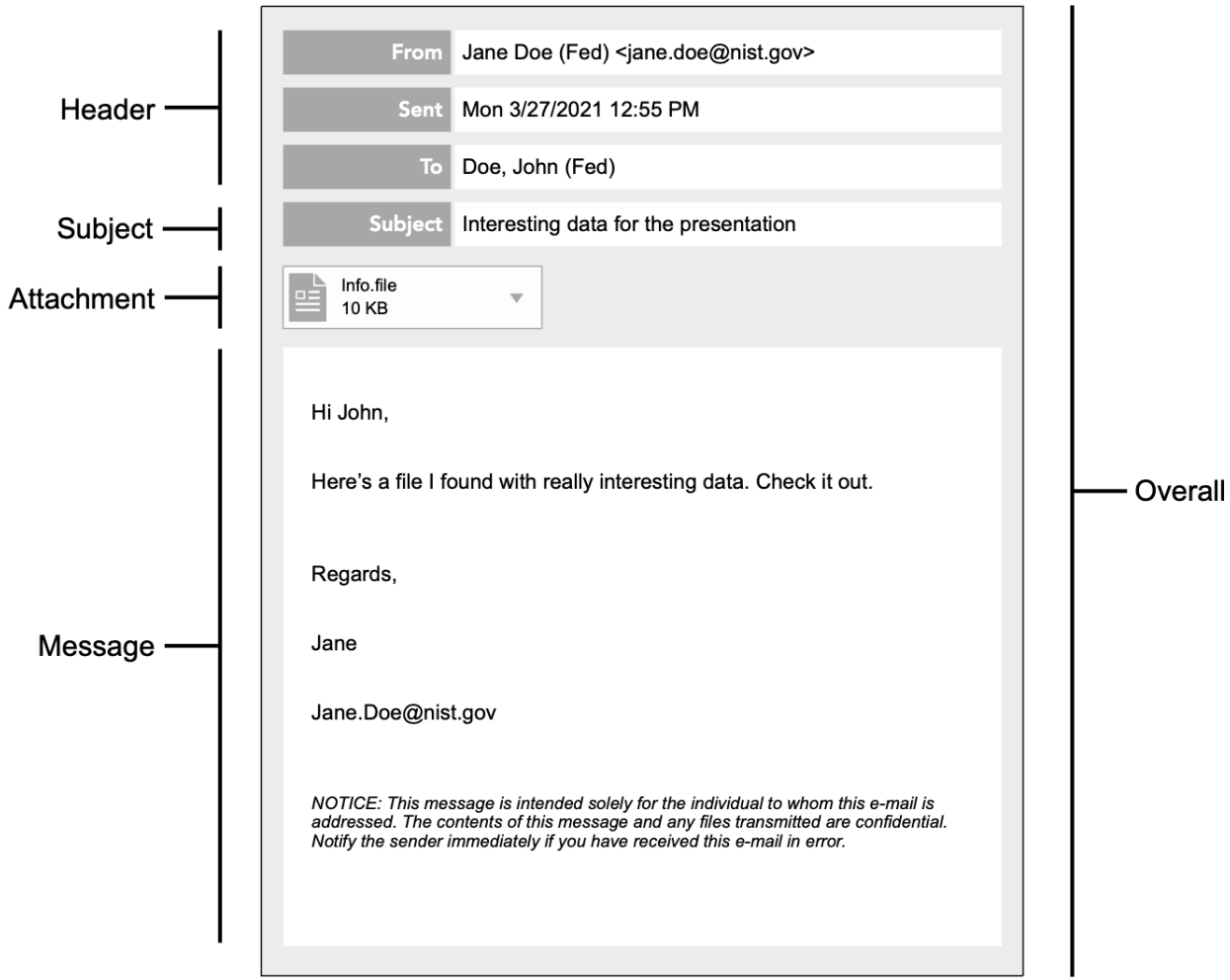
How to Spot a Phish – Investigate Email

Check if the email is a threat:

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



How to Spot a Phish – Where to Find Cues



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

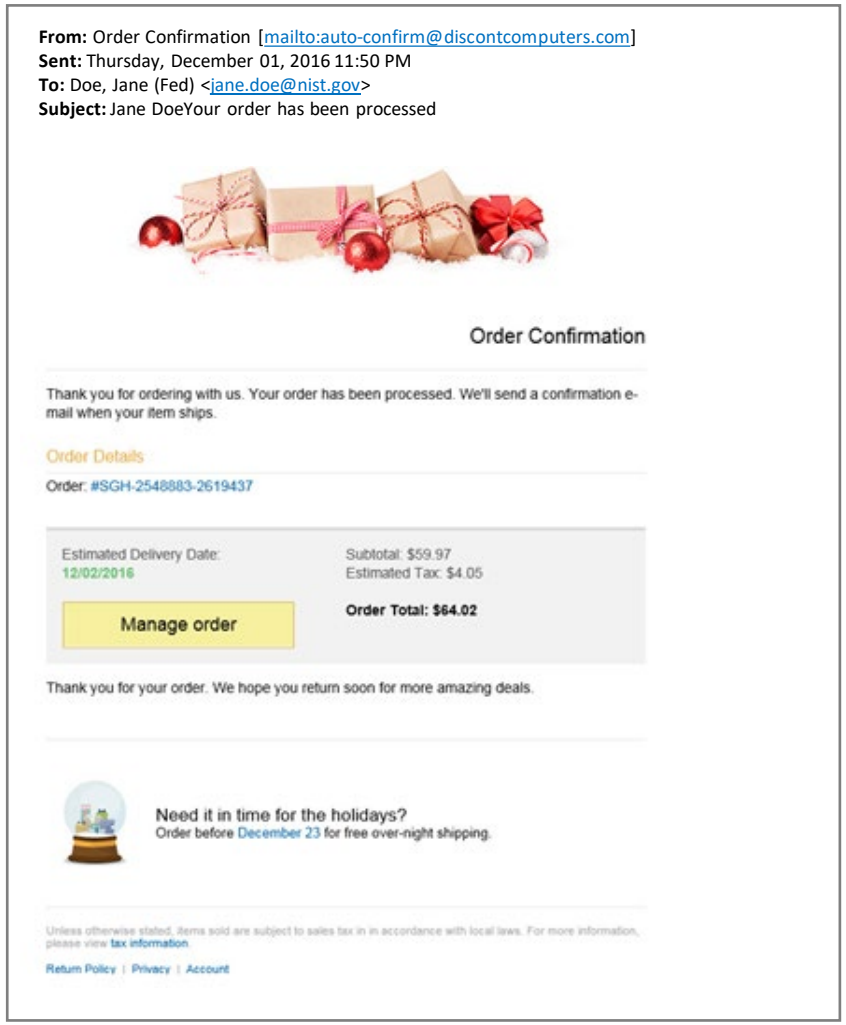
How to Spot a Phish – What Cues to Look for

- 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

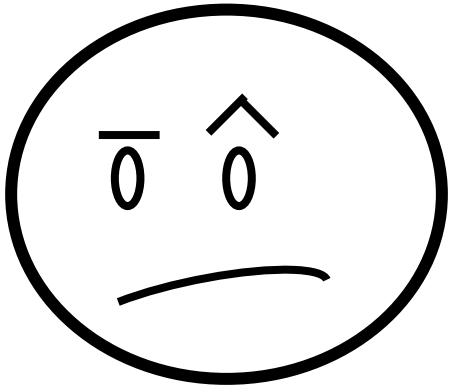
How to Spot a Phish – What Cues to Look for

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

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

How to Spot a Phish – What Can You Do?

- Be wary of common phishing tactics:
  - Contains a scare tactic
  - Sense of urgency or threat
  - Poses as friend, colleague, supervisor
  - Promise of money
  - You're special or limited offer
  - Wants information
  - Mimics a work process
  - Your context that could be scraped from browsing history



How to Spot a Phish – What Can You Do?

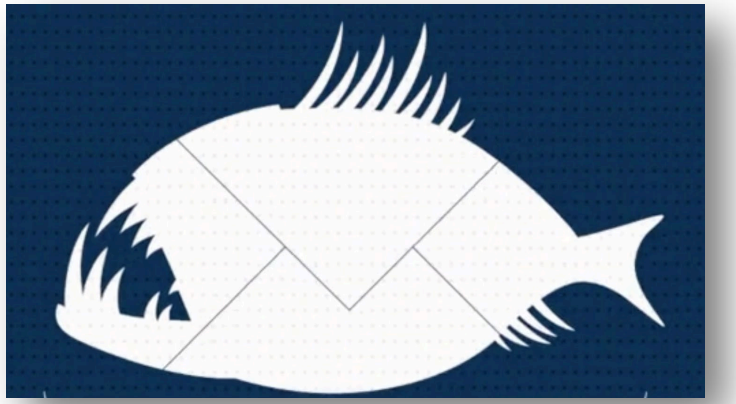
- Be vigilant
  - Consider your context. Does it make you vulnerable?
    - Are there links, attachments, or requests for information?
    - Look for cues
    - Inspect carefully
  - Use bookmarked links/favorites instead of clicking
  - Use a search engine, don’t click on ads
  - Consider calling the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

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