The NIST Phish Scale: Method for rating human phishing detection difficulty

National Institute of Standards and Technology
U.S. Department of Commerce

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

This presentation will cover…

1 Who we are

2 Our research

3 NIST Phish Scale

4 Actionable Implications

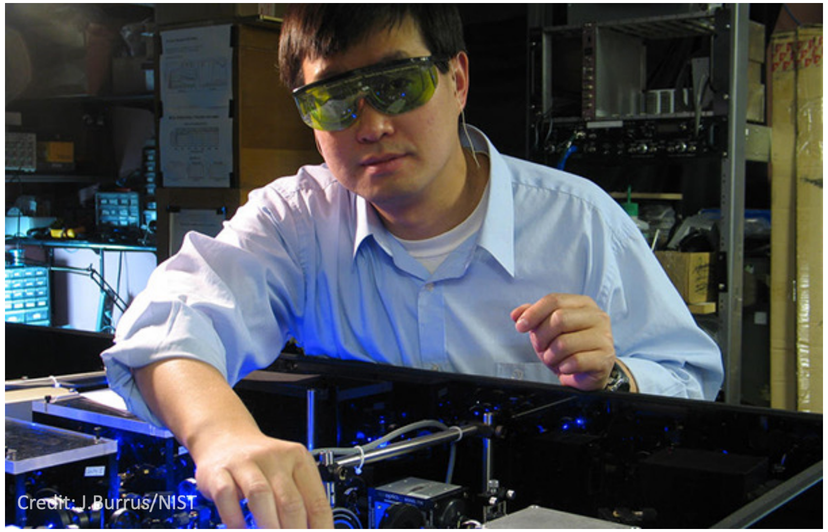
NIST Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.

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.

©Robert Rathe


Credit: J.Burrus/NIST

©Nicholas McIntosh Photography

Who we are and what we do

Visualization and Usability Group

Multi-disciplinary

- Computer science
- Cognitive psychology
- Industrial engineering
- Mathematics
- Cybersecurity

Championing the Human in Information Technology

- Performing research to develop user-centered measurement and evaluation methods, guidelines, and standards
- Improving human system interaction by applying:
  - Human factors,
  - Cognitive science,
  - User-centered design, and
  - Usability principles

Enhancing the usability of cybersecurity

Guidance

For policy makers, system engineers, cybersecurity professionals

Grounded

Based in empirical data

Solutions

Secure in practice, not just in theory

User-focused

Account for user needs and behaviors

Varied threat landscape

data
intrusions
spoofing
access
updates
IPsec
worm
deception
DDoS
hacking
unauthorized
antivirus
databases
domains
trojan
training
PII
botnet
phishing
breaches
software
security
firewalls
devices
VPNs
cloud
backups
malware
ransomware
reporting
exploits
servers
information
compliance
attacks
virus

PHISHING GAZETTE

no.203.078

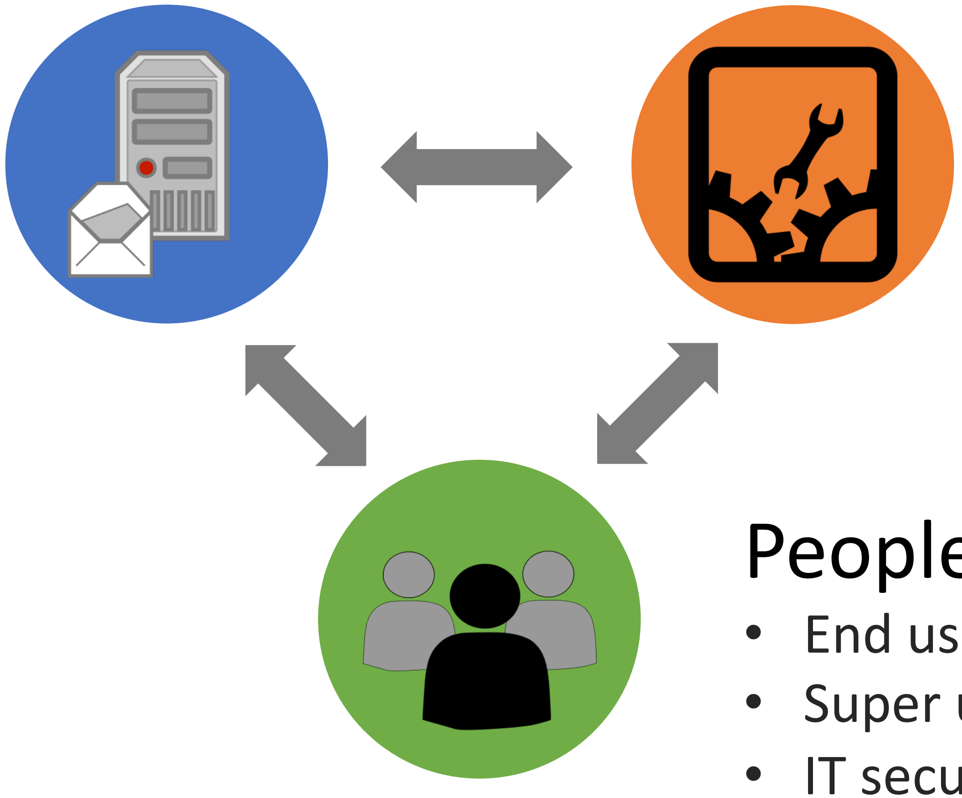
THE LATEST IN PHISHING NEWS

PHISHING AMONG TOP PUBLIC-SECTOR THREATS

Phishing, malware, ransomware among top public-sector threats, reports find. Recurring online threats of phishing, malware, and ransomware threaten governments …

Full story at https://www.govtech.com/security/Phishing-Malware-Ransomware-Among-Top-Public-Sector-Threats-Reports-Find.html

Phishing defense must be multi-pronged



Technology

- Filtering
- DMARC, DKIM
- AI & ML

Process

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

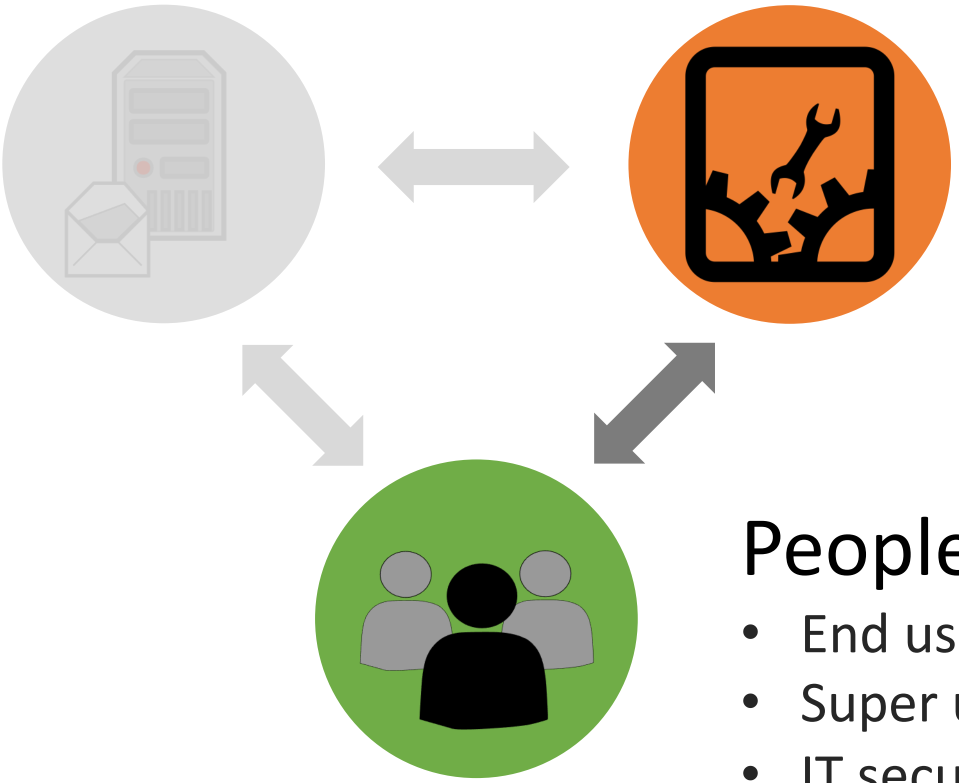
People

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

Phishing defense must be multi-pronged

Technology

- Filtering
- DMARC, DKIM
- AI & ML



Process

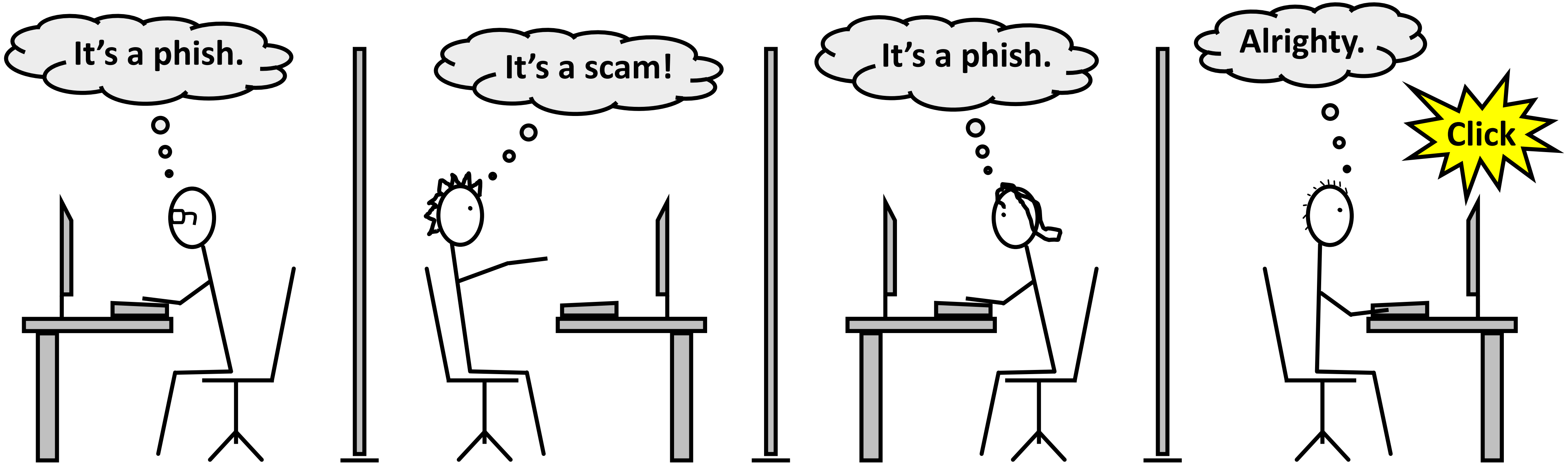
- Identify vulnerabilities
- Awareness training
- Reporting & early warning
- Meaningful metrics

People

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

Our Research

Phishing scams continue…



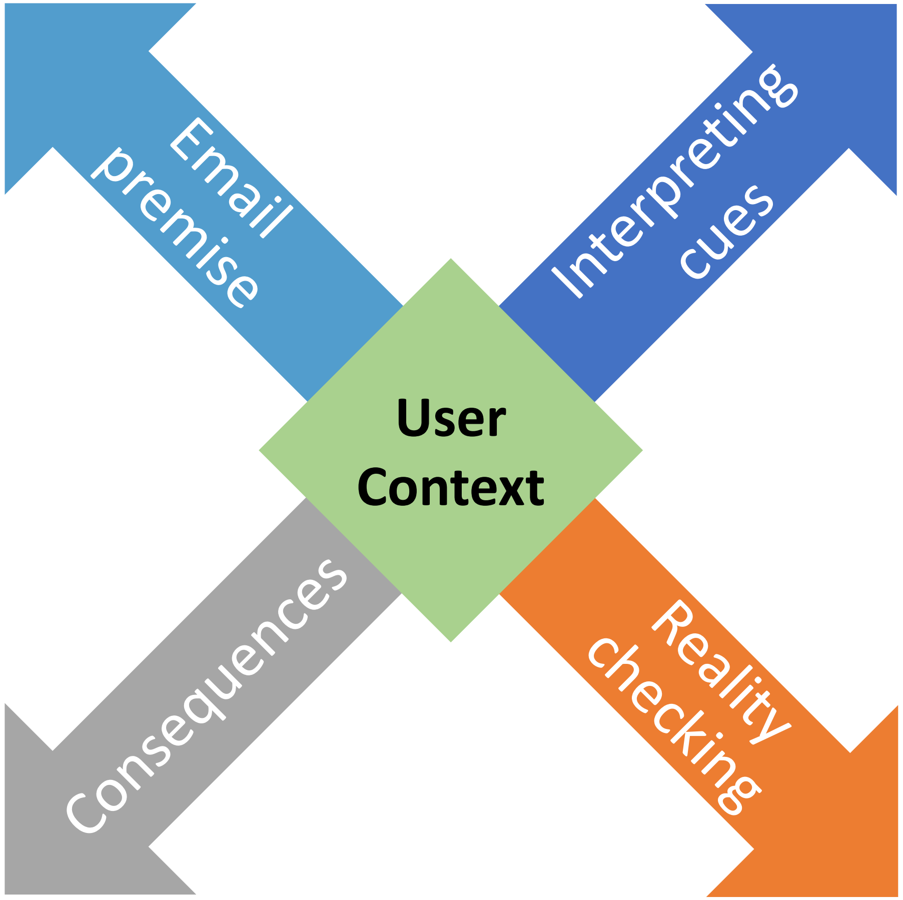
Some users click, some don’t. Why?

Image credit: NIST

User context is key!

Alignment vs. misalignment with expectations and external events

Compelling vs. suspicious cues



Concern over consequences

Reality-checking strategies

Contextualizing click rates

3.2%

49.3%

4.8%

11.0%

8.7%

9.1%

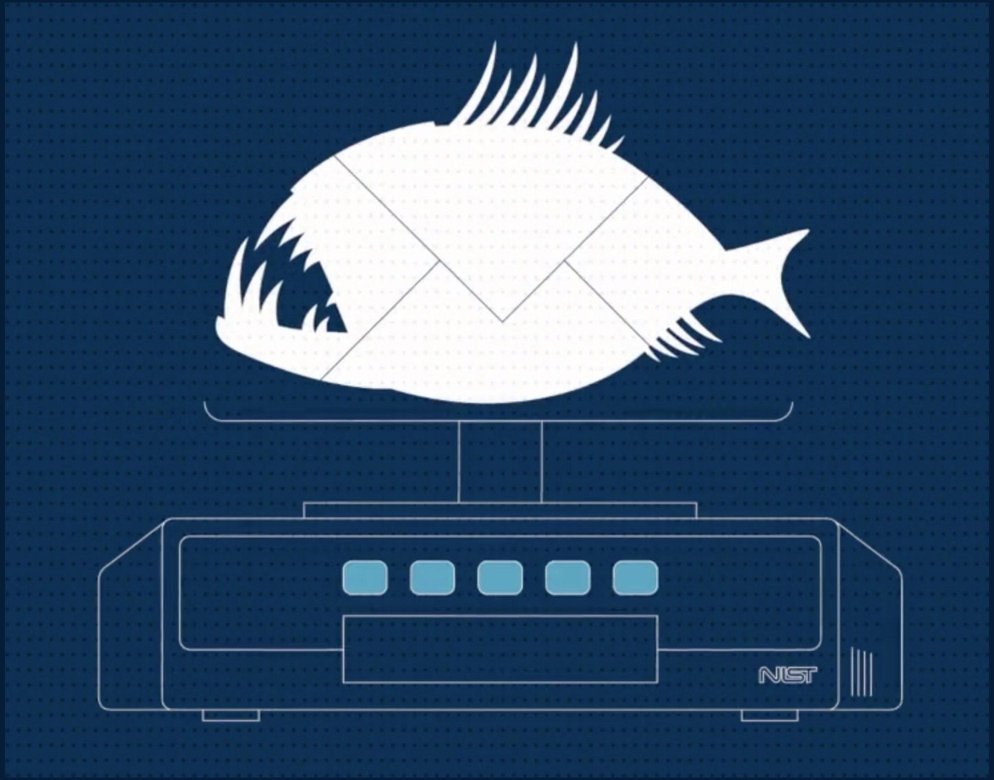
43.8%

11.6%

19.4%

20.5%

NIST Phish Scale



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

Image credit: NIST

The NIST Phish Scale - Overview

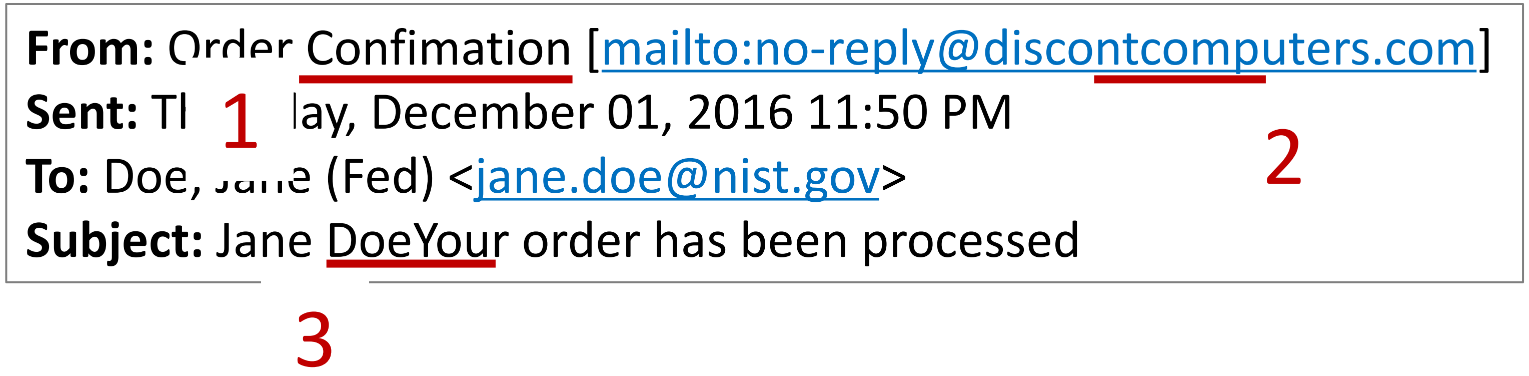
- Know the target audience
- Apply NIST Phish Scale to individual phishing emails
  - Cues
  - Premise Alignment
- Determine phishing detection difficulty

The NIST Phish Scale – Cues

- Quantify and categorize observable characteristics of the phish
  - Few, Some, Many
- 5 Types of Cues
  - Errors
  - Technical indicators
  - Visual presentation indicators
  - Language and content
  - Common tactics

The NIST Phish Scale – Cues

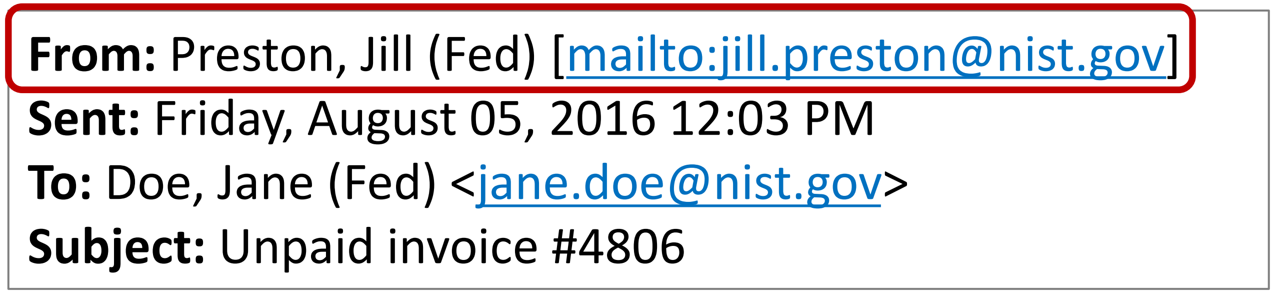
- 5 Types of Cues
  - Errors
  - Technical indicators
  - Visual presentation indicators
  - Language and content
  - Common tactics



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

The NIST Phish Scale – Cues

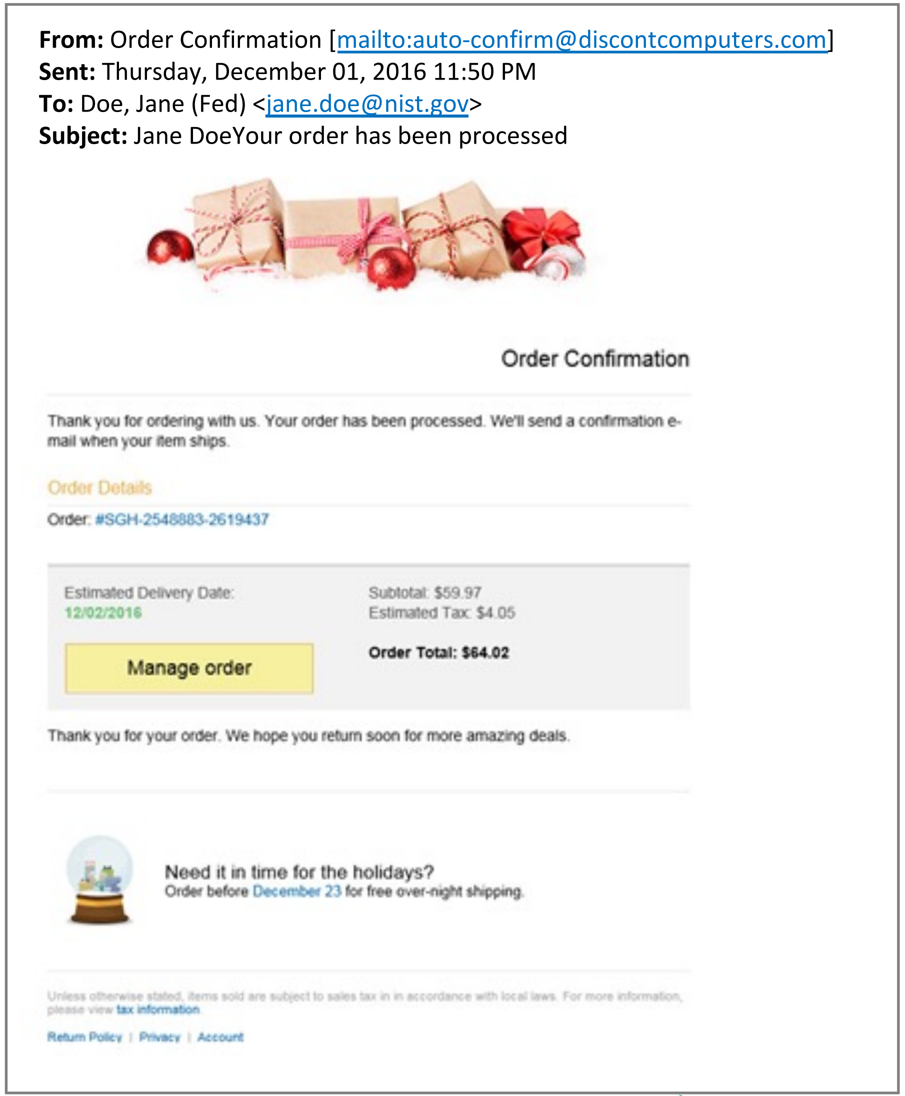
- 5 Types of Cues
  - Errors
  - Technical indicators
  - Visual presentation indicators
  - Language and content
  - Common tactics



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

The NIST Phish Scale – Cues

- 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

Order Total: $64.02

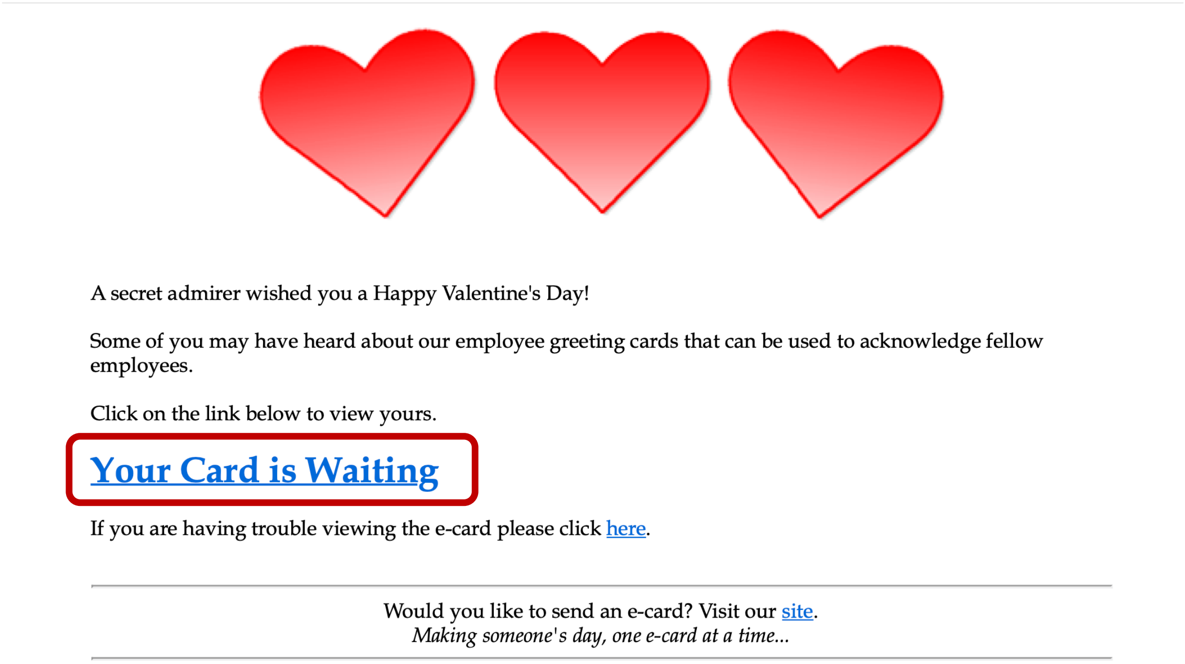
Thank you for your order. We hope you return soon for more amazing deals.

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.

The NIST Phish Scale – Cues

- 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.

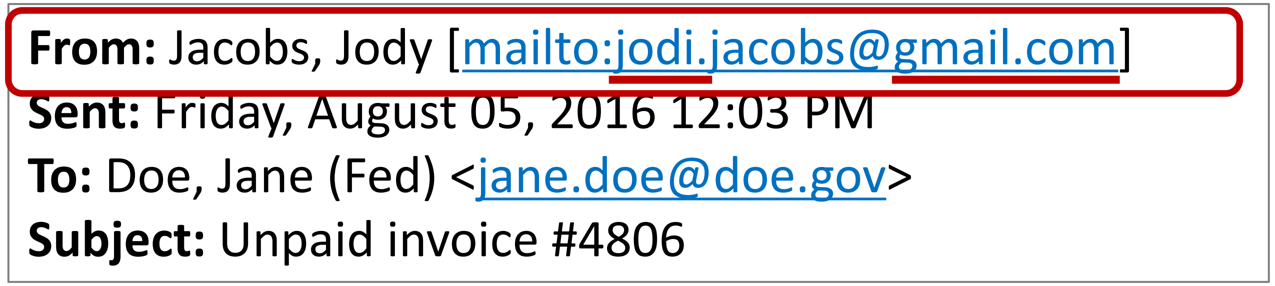
Your Card is Waiting

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...

The NIST Phish Scale – Cues

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



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

The NIST Phish Scale – Cues

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

- Categorize the number of cues

Few	1 – 8
Some	9 – 14
Many	15 +

The NIST Phish Scale – Premise Alignment

- Characterize relevancy of the email premise for the target audience
  - High, Medium, Low
  - Based on workplace responsibilities and culture, business practice plausibility, staff expectations, etc.

The 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

The NIST Phish Scale – Premise Alignment

- Assign each element a value according to the applicability scale

Applicability	Numeric Scale
Extreme	8
Significant	6
Moderate	4
Low	2
Not applicable	0

The NIST Phish Scale – Premise Alignment

- Assign each element a value according to the applicability scale

Element		Value
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	

Numeric Scale
8
6
4
2
0

The 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

20

-4

= 16

The NIST Phish Scale – Premise Alignment

- Categorize Premise Alignment

Overall Score	Premise Alignment Category
18 & up	High
11 – 17	Medium
10 & below	Low

The NIST Phish Scale - Detection Difficulty

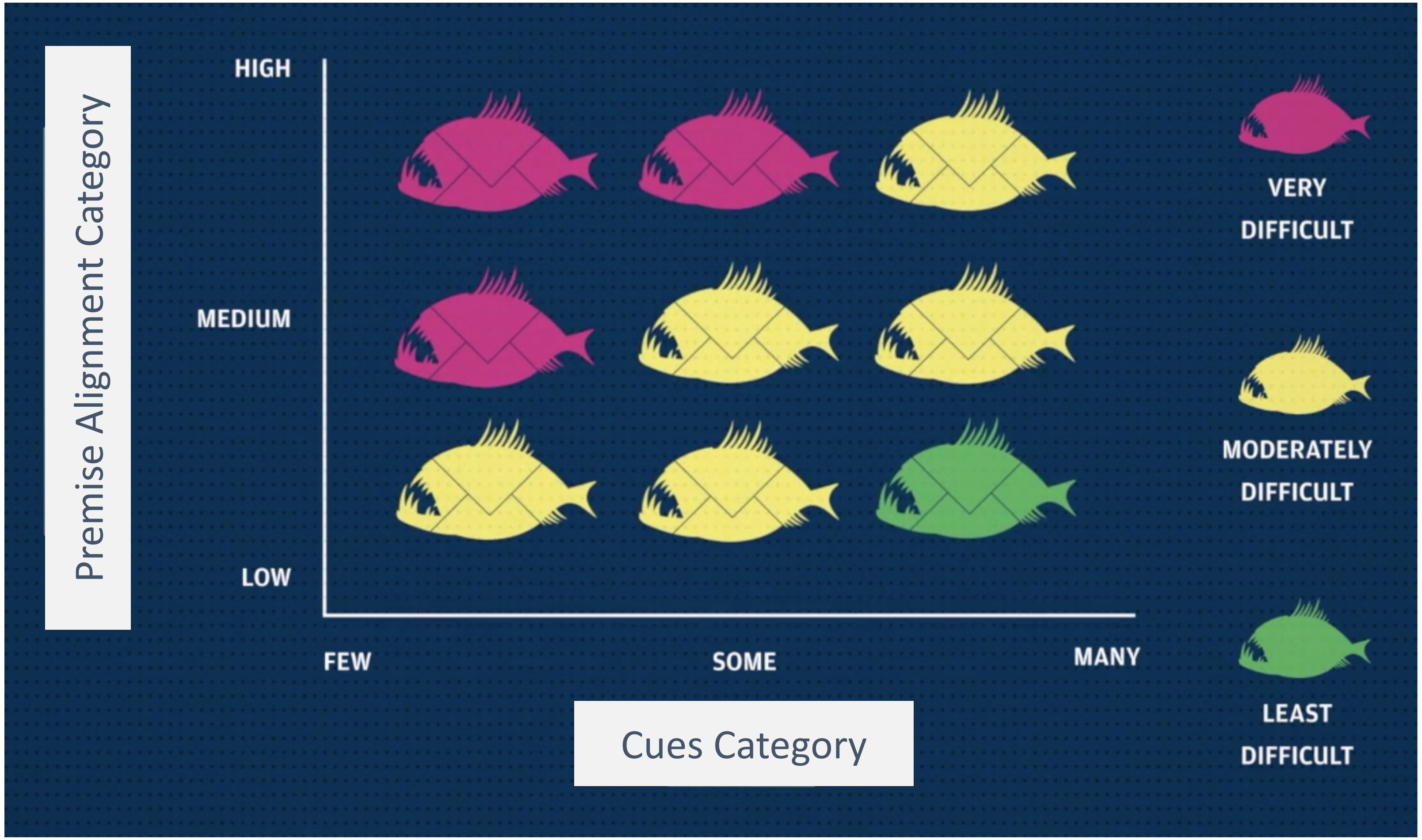


Image credit: NIST

The NIST Phish Scale

What’s next?

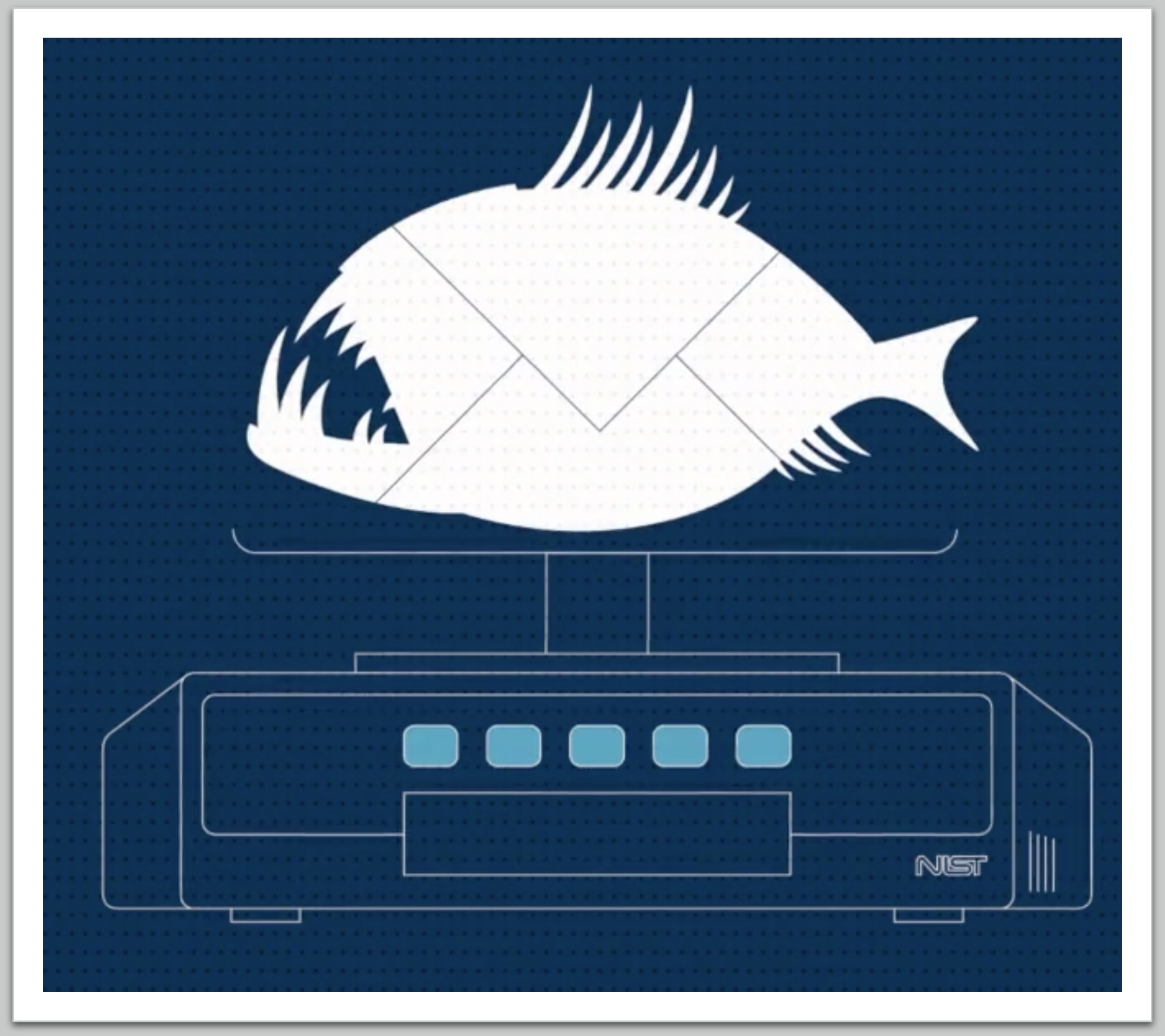


Image credit: NIST

Take-aways!

- ● Use a multi-pronged approach
- ● Attend to the changing nature of phishing
- ● Build resilience
- ● Bolster security posture of organization

Take-aways!

Click rates

Click rates will not go to zero!
(and stay there)

Operational data

Importance of operational data with ecological validity

Context is key

Understand context for click rates with the NIST Phish Scale

No silver bullet

Awareness training is not the silver bullet in phishing defense

Phishing resilience yields big rewards

Additional Resources

- Shaneé 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

Thank you