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

INFORMATION TECHNOLOGY LABORATORY

User Context in Phishing Susceptibility and Implications for Practitioners

Kristen Greene
Michelle Steves
Mary Theofanos

Federal Computer Security Managers' Forum

May 2019
NIST

Today, we will cover…

1. Who we are
2. Our focus in this talk
3. Our research findings
4. Actionable implications

Who we are and what we do

Visualization and Usability Group	**Research to develop user-centered measurement and evaluation methods, guidelines, and standards**
Multi-disciplinary • Computer science • Cognitive psychology • Industrial engineering • Mathematics	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
domains
antivirus
databases
training
trojan
PII
botnet
phishing
breaches
software
firewalls
security
devices
VPNs
backups
cloud
malware
ransomware
reporting
exploits
servers
information
compliance
attacks
virus

PHISHING GAZETTE

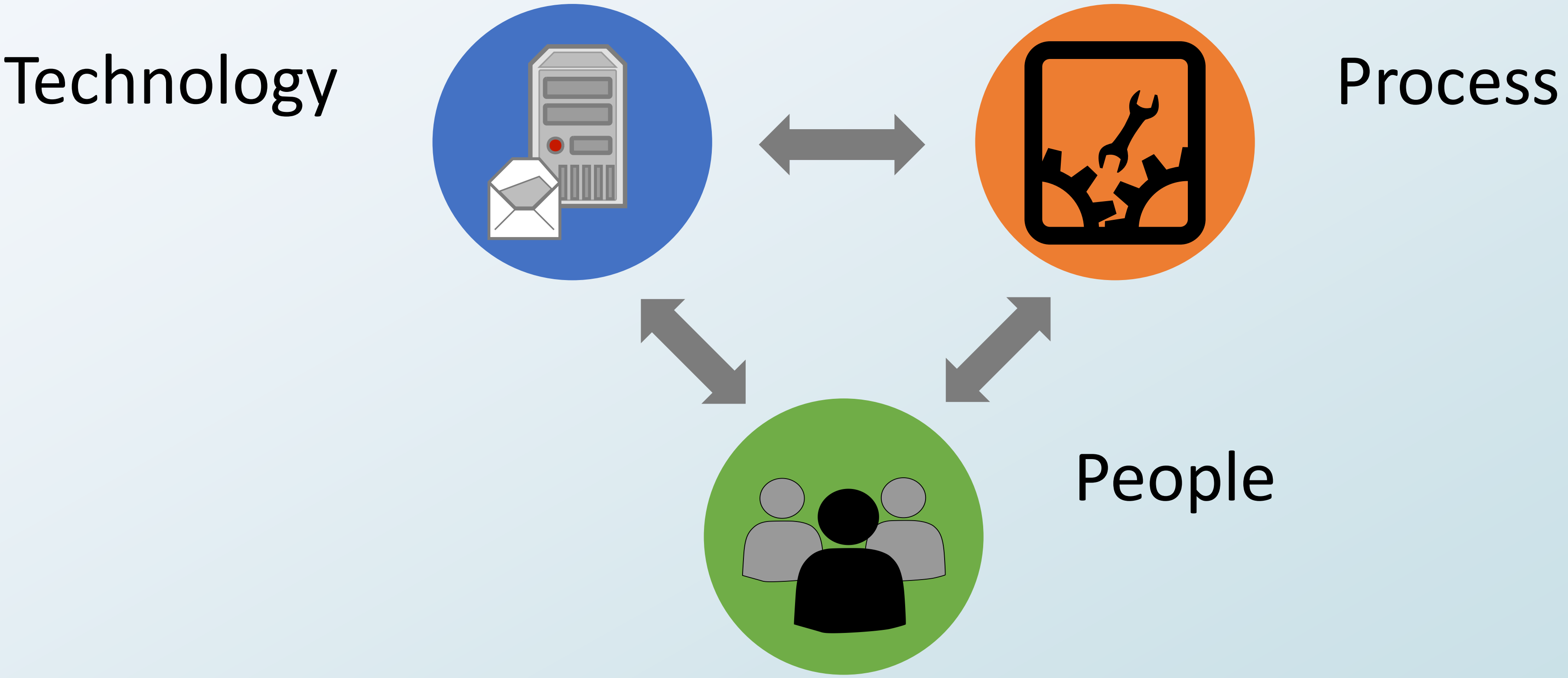
no.203.078 THE LATEST IN PHISHING NEWS

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

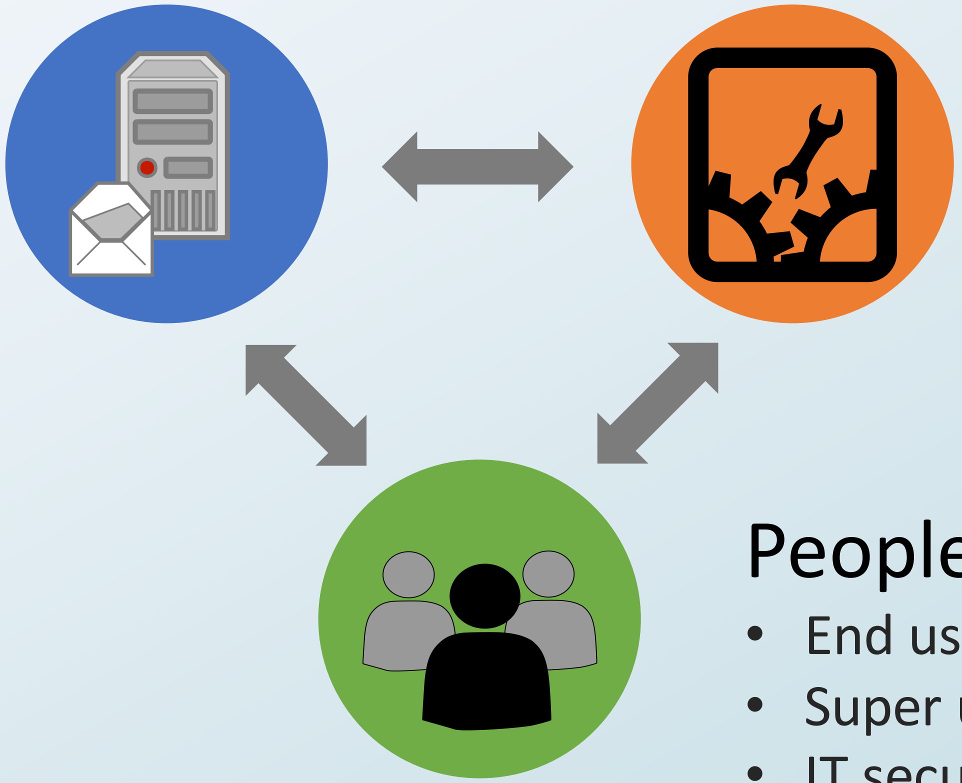


Technology

Process

People

Phishing defense must be multi-pronged



Technology

- Filtering
- DMARC, DKIM
- AI & ML

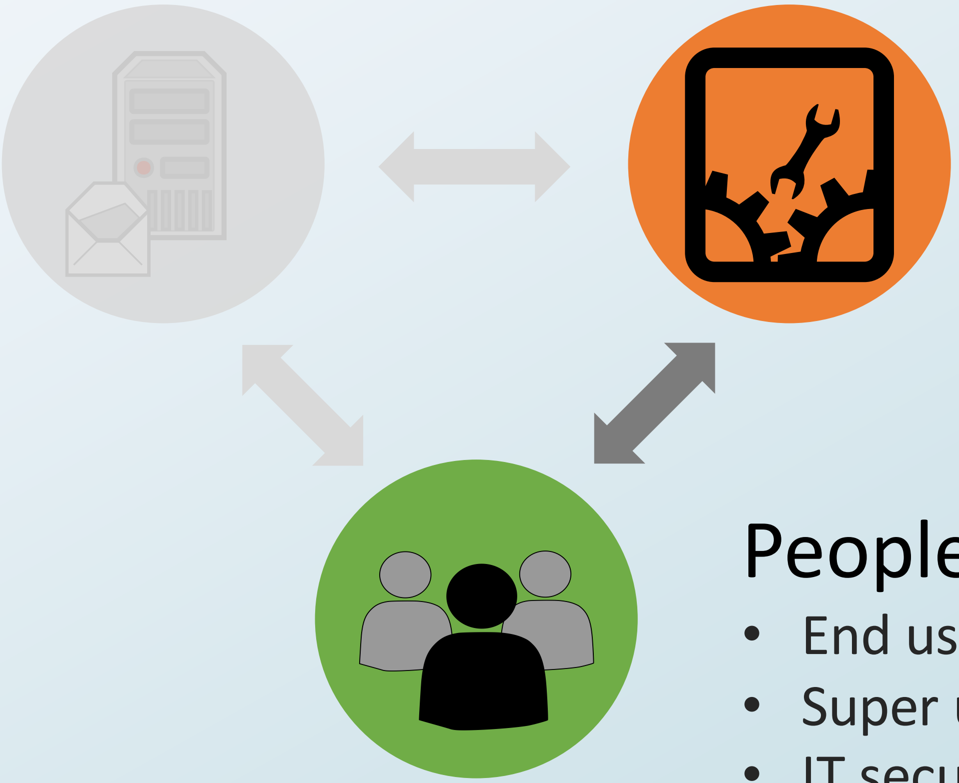
Process

- 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

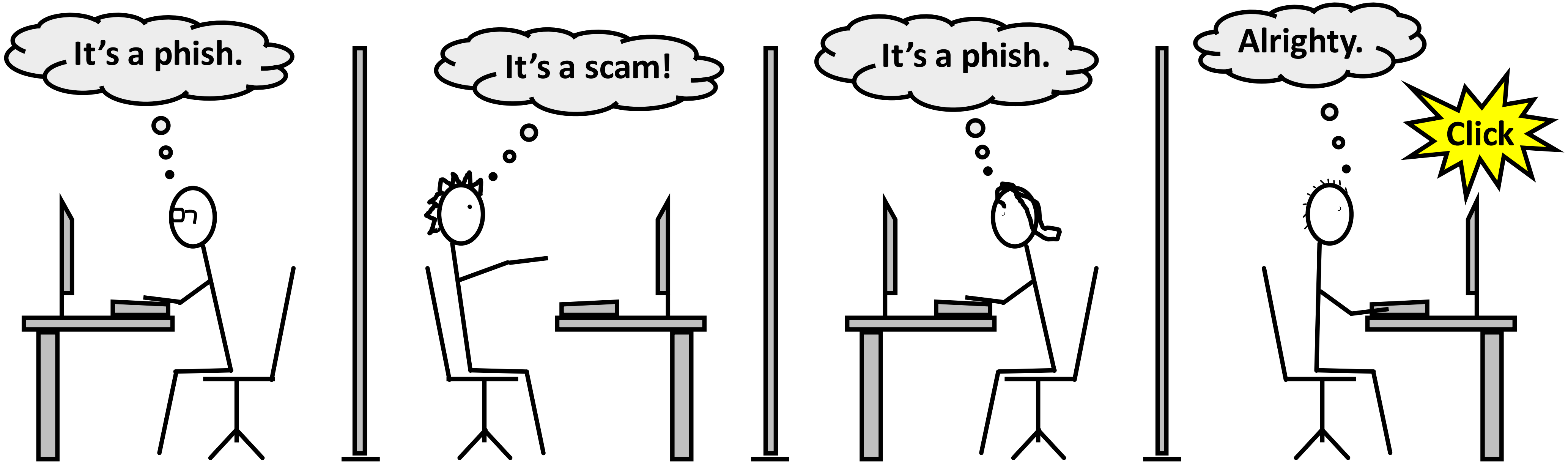
- Identify vulnerabilities
- Awareness training
- Reporting & early warning
- Meaningful metrics

People

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

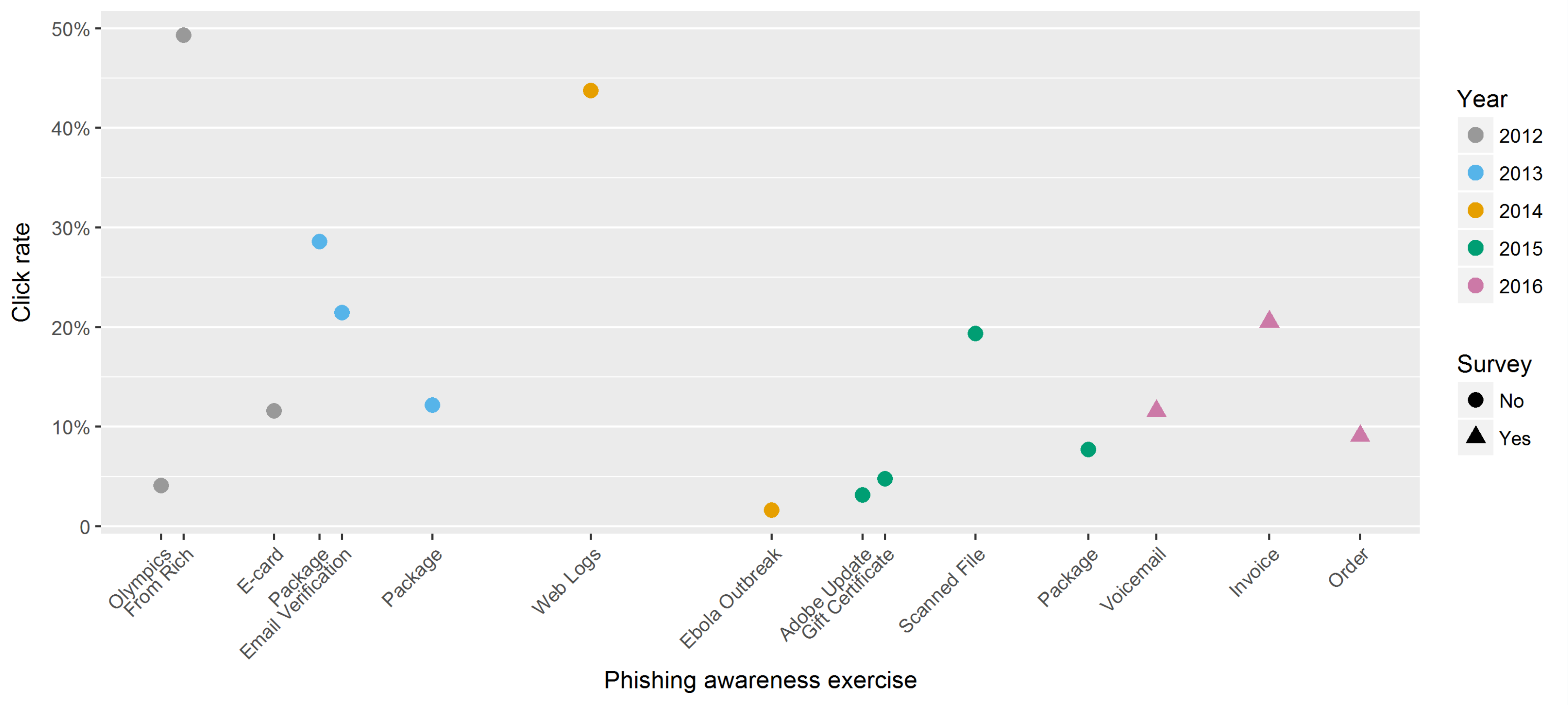
Our focus today…

Phishing scams continue…



Some users click, some don't. Why?

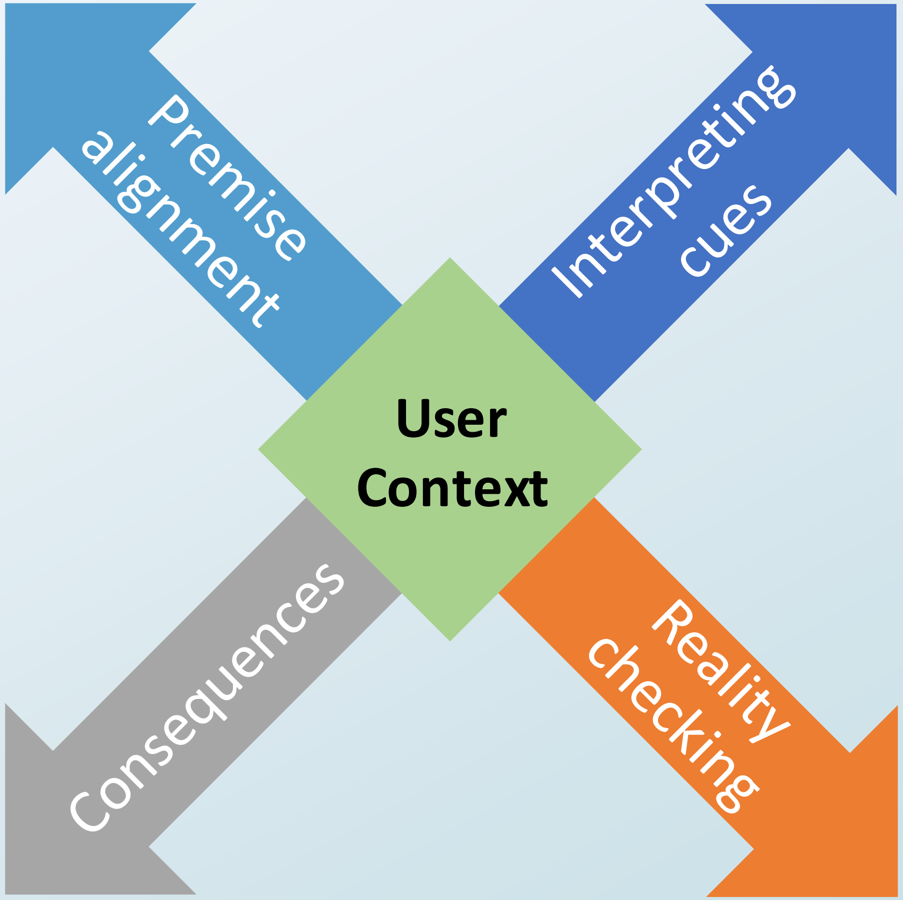
NIST exercise click rates



User context is key!

Alignment vs. misalignment with expectations and external events

Compelling vs. suspicious cues



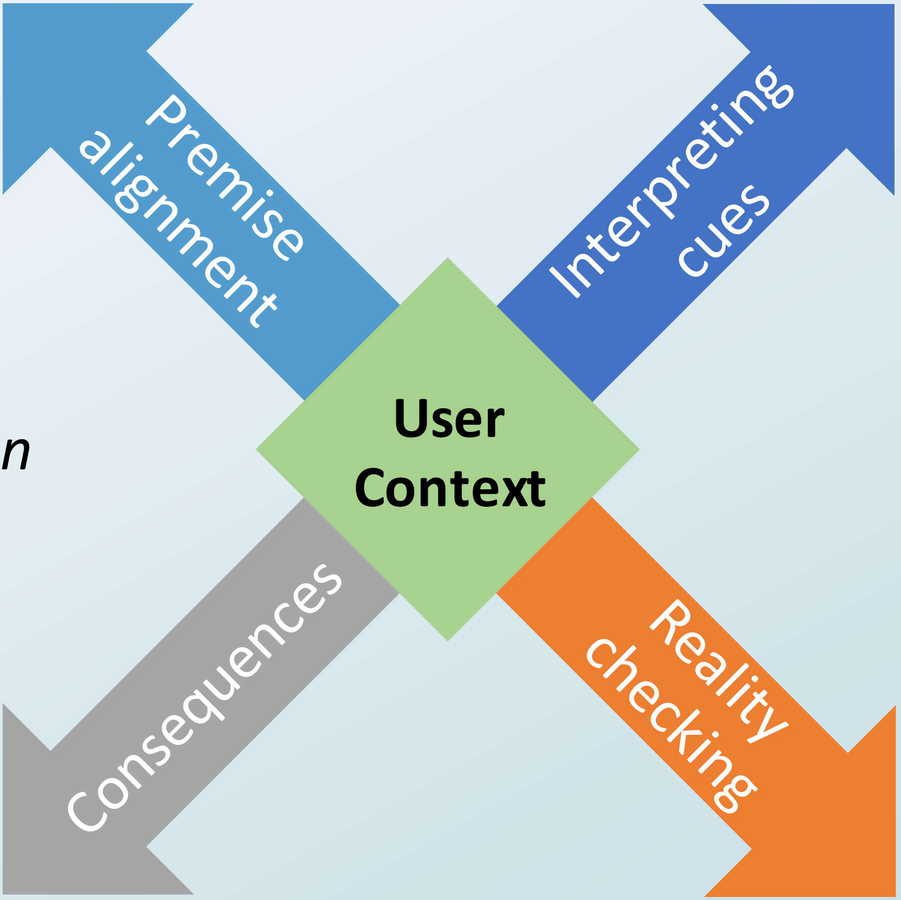
Concern over consequences

Reality-checking strategies

Participants said…

Clicker

The unfamiliar email is common at work, and generally not a problem. Did not trigger anything in my brain that would indicate that it was harmful.



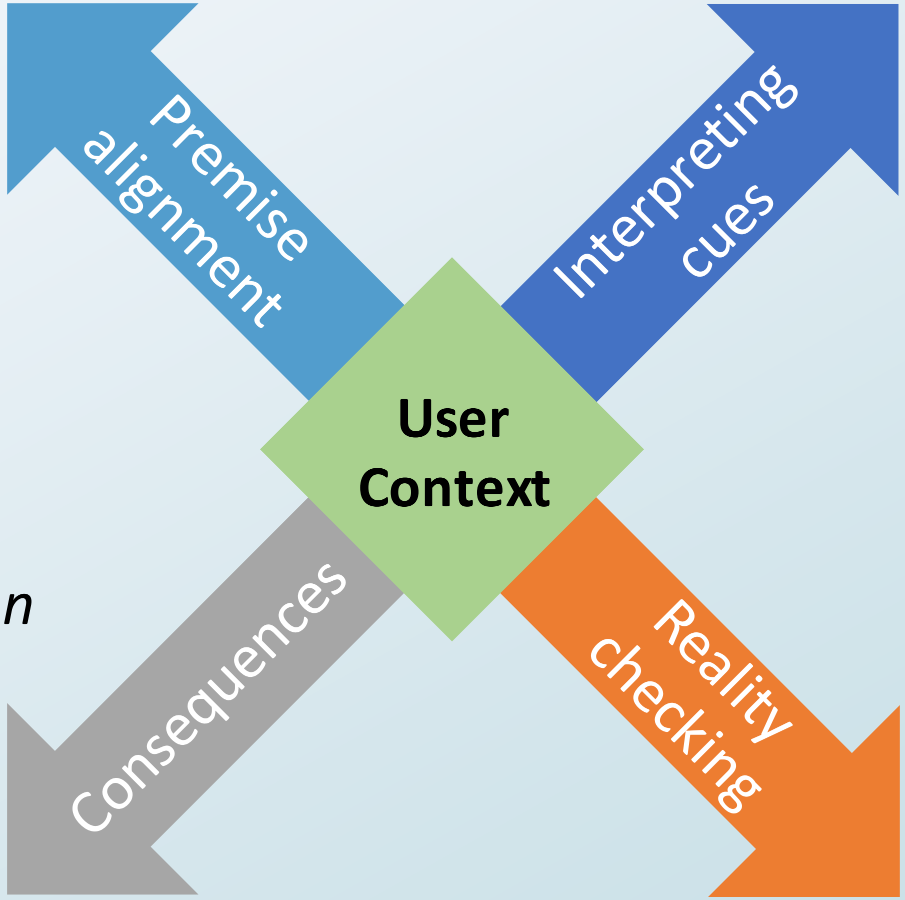
Non-clicker

…upon re-reading the email I became very suspicious. The email references a .doc attachment, but the attachment was a .zip file. After noticing that, I checked the NIST directory and saw that there was not a Jill Preston (Fed) at NIST. I immediately forwarded to my ITSO.

Participants said…

Clicker

I am always interested in ensuring that I get any messages and act on them. It could have been my supervisor or other person requiring an action on my part.



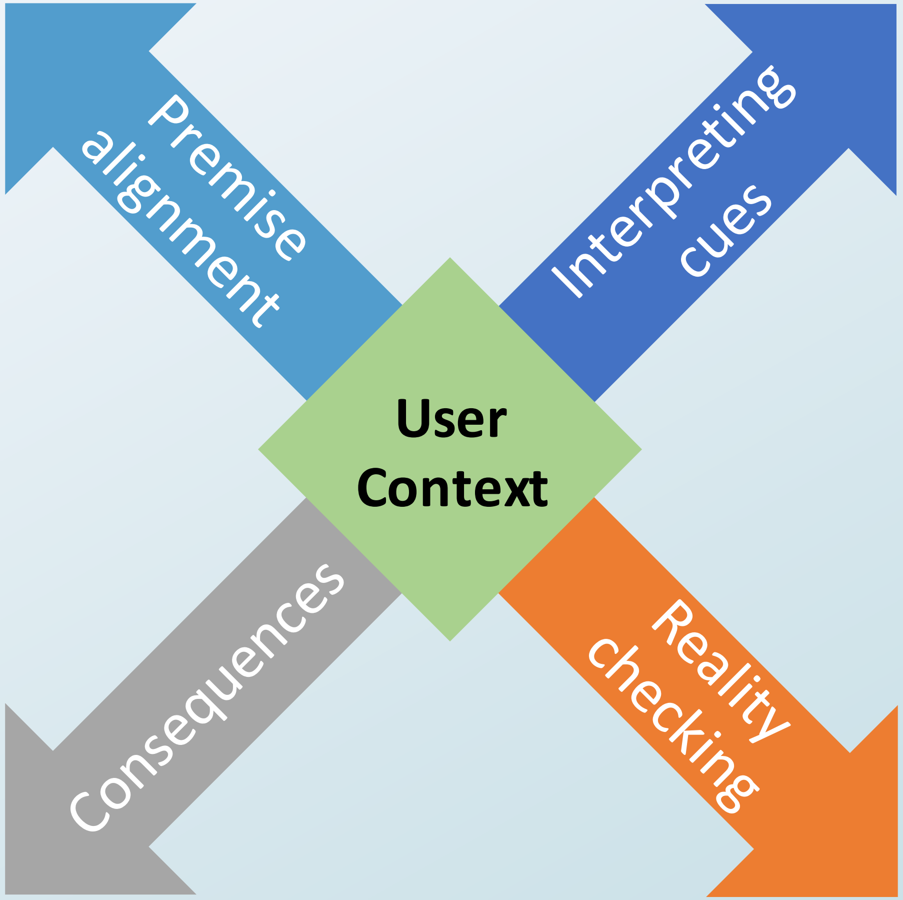
Non-clicker

I was concerned something might be downloaded onto my computer or I could get a virus.

Participants said…

Clicker

I thought the NIST firewall would block it.



Non-clicker

…some phishing emails will get through no matter how good the security measures are.

I know I'm a target.

Take-aways!

Operational data

Importance of operational data with ecological validity

Context is key

Depth of processing
Predicting susceptibility

Click rates

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

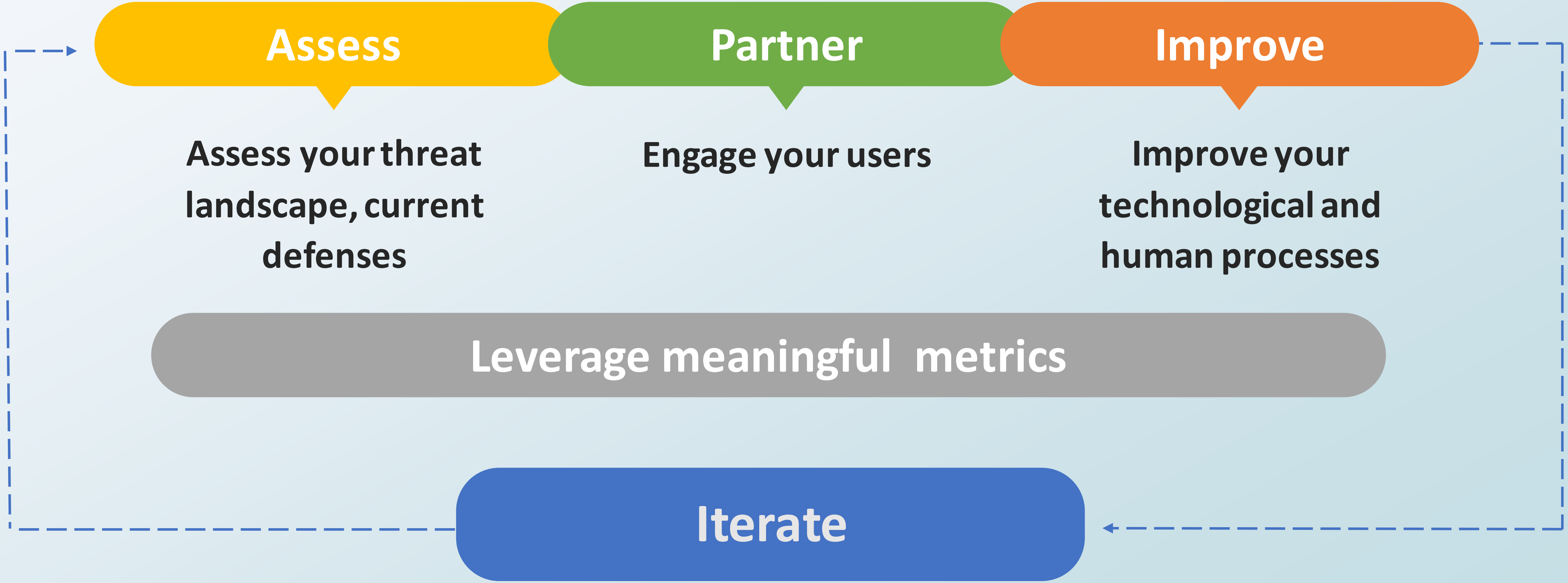
No silver bullet

Awareness training is not the silver bullet in phishing defense

What’s an organization to do?

- Use a multi-pronged approach
- Attend to the changing nature of phishing
- Ensure staff are not overly-confident in institutional security
- Don’t expect zero click rates
- Build resilience

Improving phishing resilience



Assess

Assess your threat landscape, current defenses

Partner

Engage your users

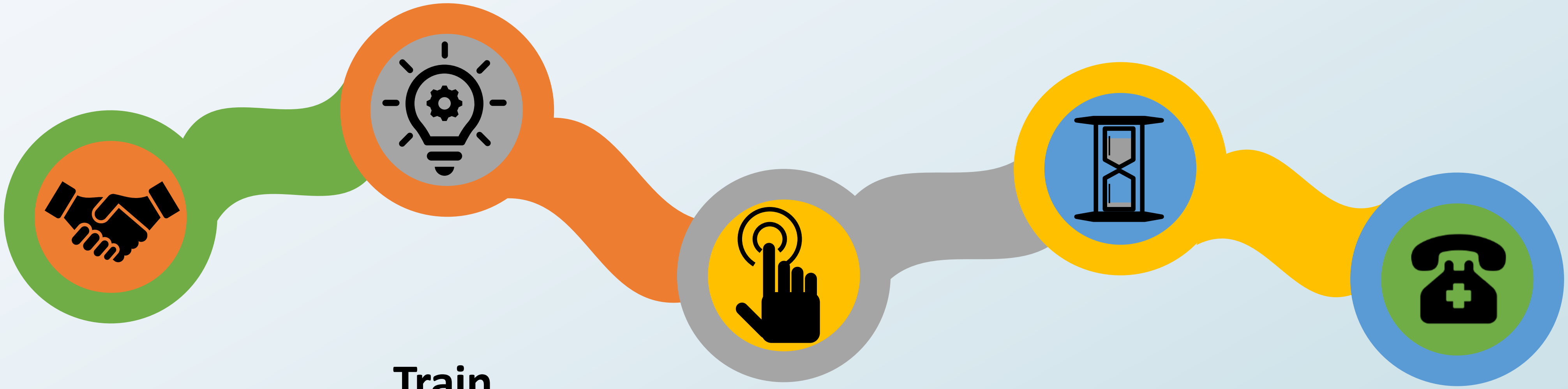
Improve

Improve your technological and human processes

Leverage meaningful metrics

Iterate

Users: Your early warning system



Partner

Engage users and help them understand their important role

Train

Educate users what to look for and how to report

Easy

Make reporting easy and give feedback

Early

Encourage early reporting

Mitigate

Mitigate damage based on user reports

Make the numbers work for you!

Discern your vulnerabilities

Track phishing patterns

Test technological defenses

Click rates

Don't over-focus on click rates in isolation

Premise alignment

Contextualize click rates with premise alignment categorization

Reporting rates

Promote increasing reporting rates

Time to first report

Early reporting is key

Phishing resilience yields big rewards

Additional information

- K.K. Greene, M.P. Steves, M.F. Theofanos, J. Kostick, "User Context: An Explanatory Variable in Phishing Susceptibility". Workshop on Usable Security (USEC) 2018, 18 February 2018, San Diego, CA, DOI: https://dx.doi.org/10.14722/usec.2018.23016
  - Contains the validated survey instrument for re-use
- K.K. Greene, M.P. Steves, M.F. Theofanos, "No Phishing beyond this Point," in IEEE Computer, vol. 51, no. 6, pp. 86-89, 2018.
  DOI: http://doi.ieeecomputersociety.org/10.1109/MC.2018.2701632
- M.P. Steves, K.K. Greene, M.F. Theofanos, A Phish Scale: Rating Human Phishing Message Detection Difficulty. USEC NDSS 2019. Usable Security Workshop at the Network and Distributed Systems Security Symposium. February 24, 2019. San Diego, CA. DOI: https://dx.doi.org/10.14722/usec.2019.23028
- NIST phishing video and press release: https://www.nist.gov/news-events/news/2018/06/youve-been-phished
- NIST Computer Security Resource Center, https://csrc.nist.gov/
  - https://cms.csrc.nist.gov/projects/usable-cybersecurity
  - Trustworthy Email, SP 800-177 Rev. 1

NIST phishing video

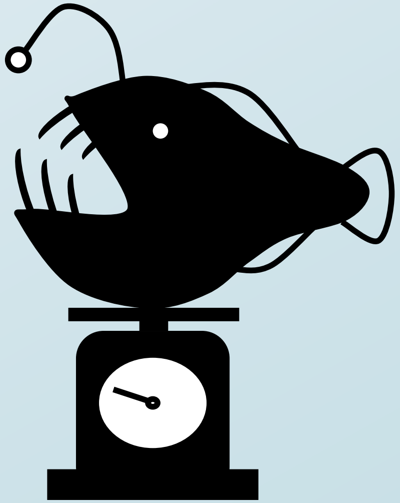
https://www.nist.gov/video/youve-been-phished

Questions?

Kristen.greene@nist.gov

Michelle.steves@nist.gov

Mary.theofanos@nist.gov



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.