ISSA
Information Systems Security Association

Thought Leadership Web
CONFERENCE

State of the Phish

April 8, 2020

State of the Phish

ISSA
Information Systems Security Association International

Today’s web conference is generously sponsored by:

proofpoint®

https://www.proofpoint.com/

Moderator

Rob Martin, CISSP

Robert Martin is a Certified Information Systems Security Professional with over thirteen years of experience in information security. He holds a Master of Science in Network Technology with a concentration in Information Security. He also holds a Cyber Security Masters Certification. He is a Sr. Security Engineer for Cisco Systems, Inc. in RTP, NC. Robert specializes in areas such as risk management, regulatory compliance, security solutions architecture, security audits, vulnerability assessments, and penetration testing. From 2012-2015, Robert served as President of the Raleigh Chapter of ISSA. During that time, the chapter membership grew at a rate of 125%. Currently, Robert serves on the Raleigh ISSA Board as the Sponsorships Director. Robert is committed to serving the community through outreach by expanding the chapter's mission to students and military. He has held several other IT Security Advisory Board positions over the years with a focus to bring about awareness of information security threats in an ever-changing global IT Security economy.

State of the Phish

Speaker

Gretel Egan
Security Awareness and Training Stategist
proofpoint

Gretel Egan is the Security Awareness and Training Strategist for proofpoint. A graduate of Carnegie Mellon University, she has extensive experience in researching and developing cybersecurity education content and was named one of “10 Security Bloggers to Follow” by IDG Enterprise. Gretel has written and provided commentary for national, industry, and trade publications, and has previously presented at events hosted by SecureWorld, Infosecurity Europe, ISACA, SC Media, and others.

ISSA

Information Systems Security Association International

www.issa.org

2020 State of the Phish Report

Using phishing data to inform decision-making
for your organization

Critical, Actionable Insights

- Sixth annual report, more data-rich than ever
- Multiple sources of data

A survey of more than

3,500

working adults across seven countries

(the United States, Australia, France, Germany, Japan, Spain and the United Kingdom)

A survey of more than

600

IT security professionals across the same seven countries

Nearly

50M

simulated phishing attacks sent by our customers over a 12-month period

More than

9M

suspicious emails reported by our customers' end users

In the Mind of the End User

Global Awareness Levels of Working Adults

Conquering the Cybersecurity Language Barrier

What is **PHISHING?** ✓ Correct **61%**

What is **MALWARE?** ✓ Correct **66%**

What is **RANSOMWARE?** ✓ Correct **31%**

What is **SMISHING?** ✓ Correct **30%**

What is **VISHING?** ✓ Correct **25%**

How Lack of End-User Awareness Leads to Risk

26%

believe they can **safely connect to public Wi-Fi networks in trusted locations**

32%

don’t know **what a virtual private network (VPN) is**

51%

think **IT teams are automatically notified** when viruses and/or malware are accidentally downloaded

66%

believe up-to-date anti-virus software **prevents attackers from accessing devices**

Phishing Impacts and Insights

What infosec pros are experiencing

What Phishing Looked Like for Infosec Teams in 2019

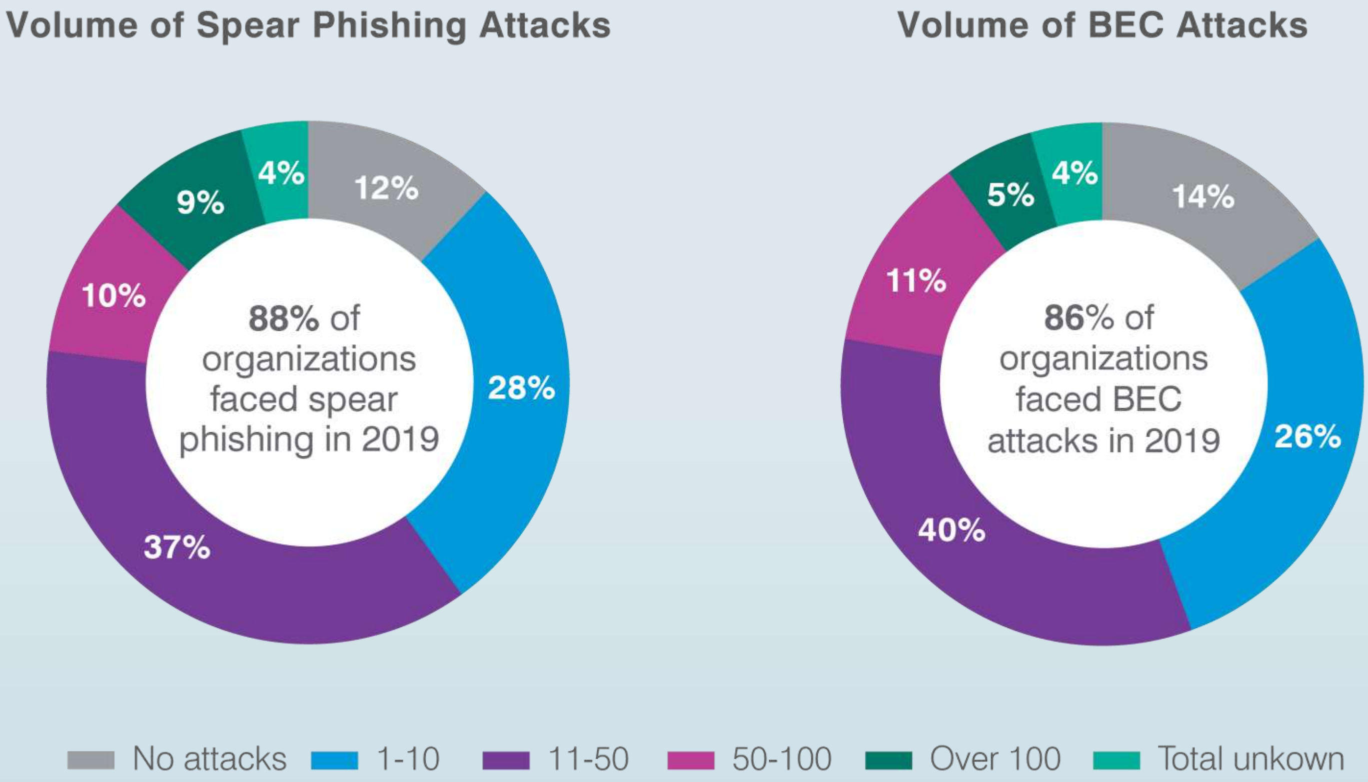
~60%

said the rate of **phishing attacks stayed the same or decreased** compared to 2018

55%

of organizations **experienced at least one successful phishing attack** in 2019

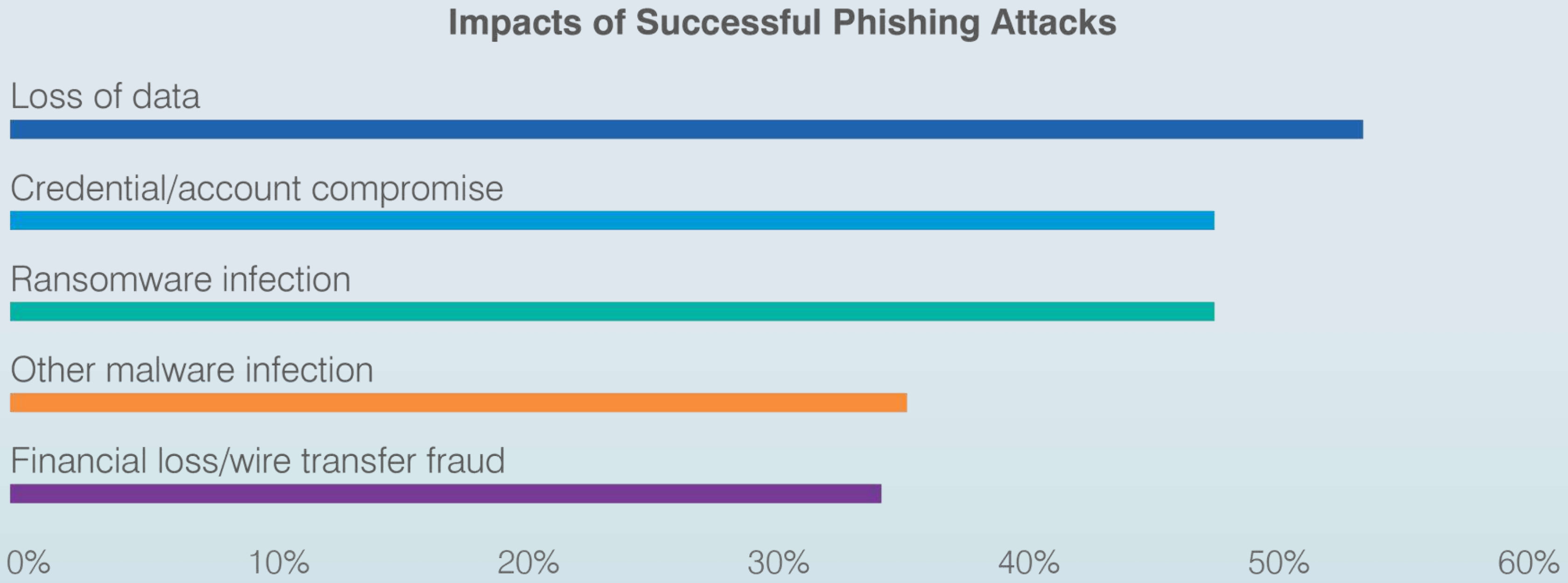
Targeted Attacks Seen by Most Organizations



88% of organizations faced spear phishing in 2019

86% of organizations faced BEC attacks in 2019

How Organizations Were Affected by Phishing

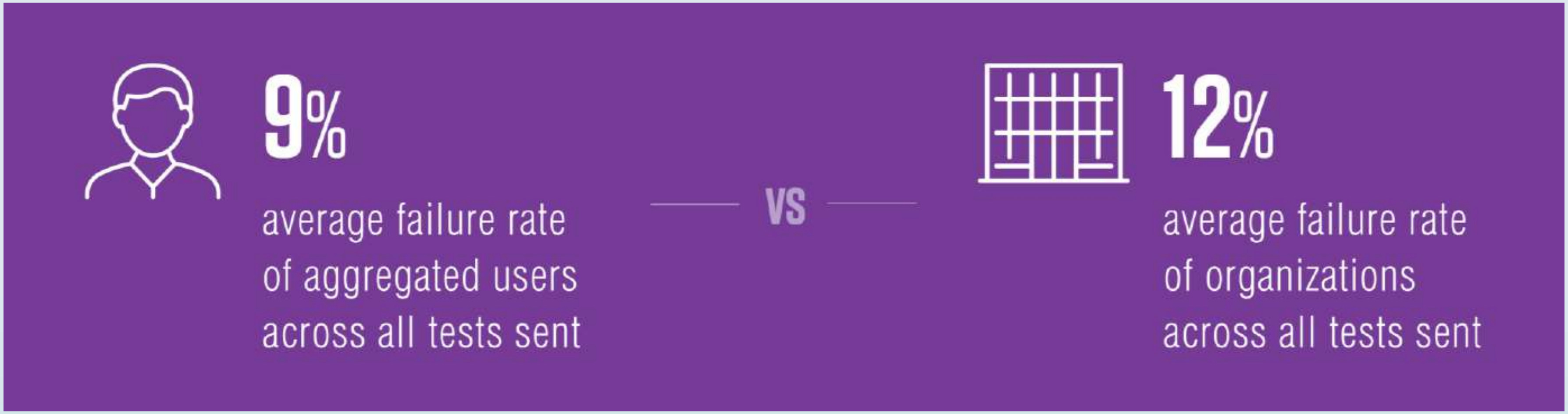


ISSA
Information Systems Security Association International

Putting Data to Work for You

Using benchmarks and organizational data to your advantage

Failure Rates: A Fresh Look for 2020



9%

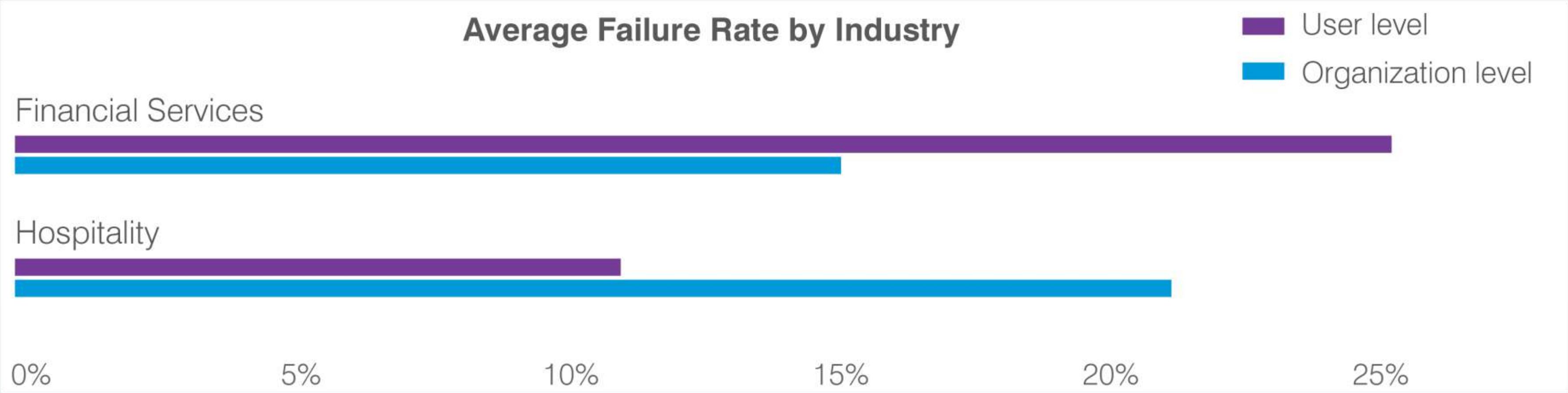
average failure rate of aggregated users across all tests sent

VS

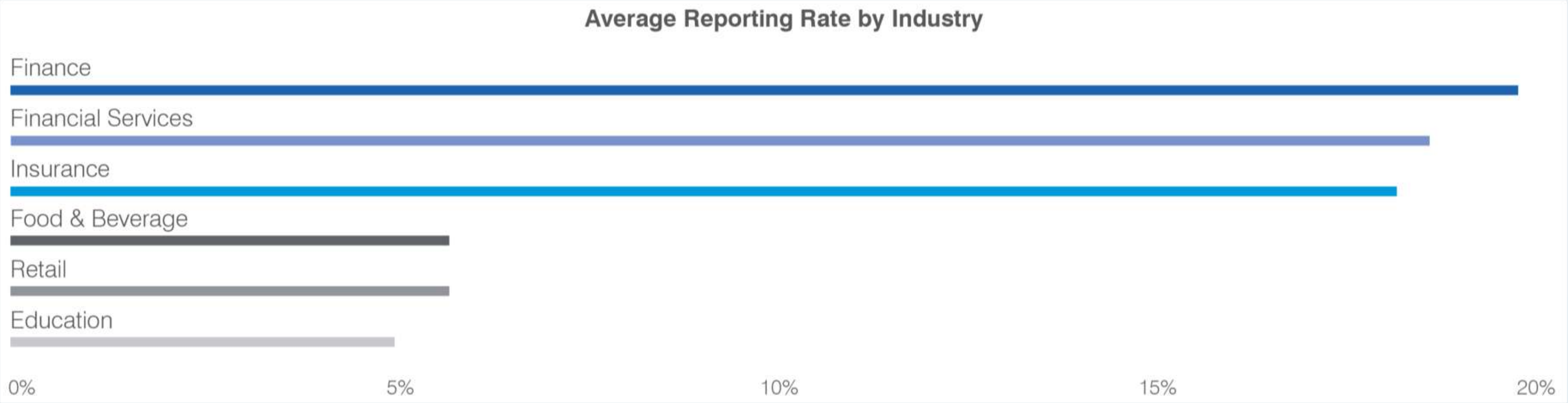
12%

average failure rate of organizations across all tests sent

Industry Failure Rates: Better Benchmarking for 2020



Email Reporting Metrics: Key for Gauging Success



Deep Data Dive: Get to Know Your VAPs

Regularly review your Very Attacked People™ so you can:

- Identify who is being attacked and how attackers are attempting to compromise them
- Address threats with greater certainty
- Identify potential attack trends
- Make more informed decisions about your training approach
- Deliver the right training to the right people at the right time

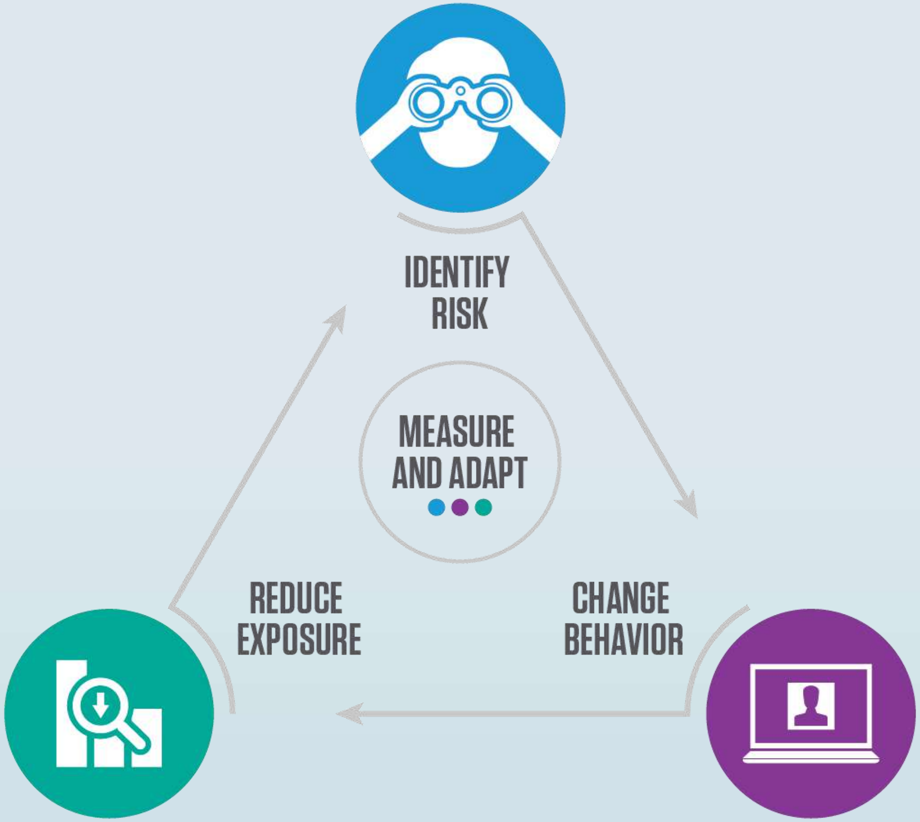
Key Takeaway: Focus on Actionable Data

Use our report to guide you

The Goal: Putting It All Together

Combination of four key activities:

- ➢ Identifying risk
- ➢ Changing behavior
- ➢ Reducing exposure
- ➢ Measuring and adjusting



State of the Phish

Speaker

Steve Sanders
Vice President of Internal Audit

Steve is an experienced cybersecurity and audit expert who specializes in helping board members and senior management excel in risk oversight. He as an educational background in computer security and data protection, and he possesses more than 15 years of audit experience with a focus on information security, privacy, and cybersecurity. Steve has extensive experience with corporate governance and regulatory oversight. He holds the following certifications: Certified Information Security Auditor (CISA), Certified in Risk and Information Systems Control (CRISC), and Certification in Risk Management Assurance (CRMA)

@SteveSanders7

ISSA

Information Systems Security Association International

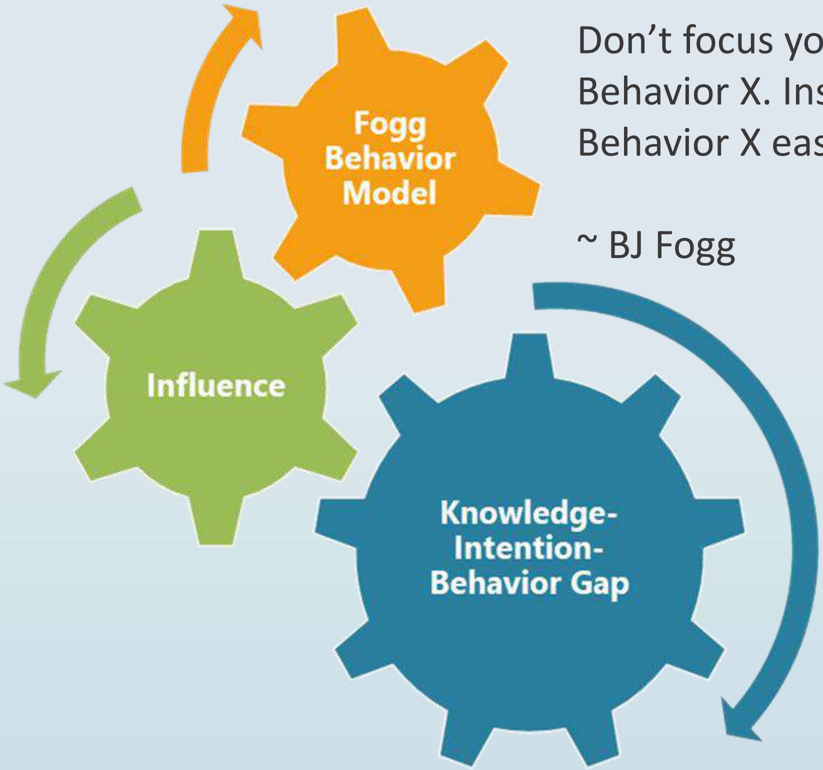
www.issa.org

Phishing Psychology

The CHALLENGE

That's a fool's game to think that every situation will yield to the same tactic or strategy. We have to assess every situation in terms of what's truly available for us there.

~ Robert Cialdini



Don't focus your motivation on doing Behavior X. Instead, focus on making Behavior X easier to do.

~ BJ Fogg

Three realities of security awareness:

1) Just because I'm aware doesn't mean that I care.
2) If you try to work against human nature, you will fail.
3) What your employees do is way more important than what they know.

~ Perry Carpenter

KNOWLEDGE-INTENTION-BEHAVIOR GAP

When it comes to the human side of security, you must treat the knowledge-intention-behavior gap as a fundamental law of reality that affects any behavior your hope to encourage or discourage.

~ Perry Carpenter, 'Transformational Security Awareness'

Knowledge

The mental understanding of what needs to be done and why it needs to be done.

Intention

The desire to do the right thing – or the wrong thing!

Behavior

The ultimate outcome: your actions.

INFLUENCE & PERSUASION

- "All the weapons of influence […] work better under some conditions than others. If we are to defend ourselves adequately against any such weapon, it is vital that we know its optimal operating conditions in order to recognize when we are most vulnerable to its influence."
- ~ Robert Cialdini, 'Influence'.

Reciprocity

People feel an obligation to give back when someone first gives to them (Quid Pro Quo).

Scarcity

People want what they cannot have.

Authority

People follow the lead of 'experts', whether real or imagined.

Consistency

People want to honor their commitments.

Liking

People want to say yes more to those people they like.

Consensus

People want their actions to be in line with the actions of others.

Speaker

Paige Yeater

Director of Information Security Program Management

Mainstay Technologies

Paige is the Director of Information Security Program Management at Mainstay Technologies. In this role, she works with clients across many industries, of many sizes, supporting their Information Security Programs.

With an MBA from The Citadel, and close to 20 years of experience in training, client operations and program management, she works to align business operations with Security and Compliance requirements. Most of her time is spent working with clients to educate them on their security risk and compliance requirements, and to align their business processes with a strong security posture. Her love of a well written policy has proven to be beneficial in this role!

Paige leverages her time in the training field to work with clients on their training and awareness programs, to ensure that their staff is well educated, aware and alert, and can help protect the organization from Security threats.

Information Systems Security Association International

www.issa.org

Corporate Culture & Phishing

Where to start

- ➢ Awareness – What to Know
  - ❑ Understanding the threat
  - ❑ Where it might come from
  - ❑ The impact it may have
  - ❑ Ongoing Discussion

- ➢ Training – What to do
  - ❑ How to Identify a phishing email
  - ❑ What to do if you get one
  - ❑ How to report them
  - ❑ Test, Retest, Support

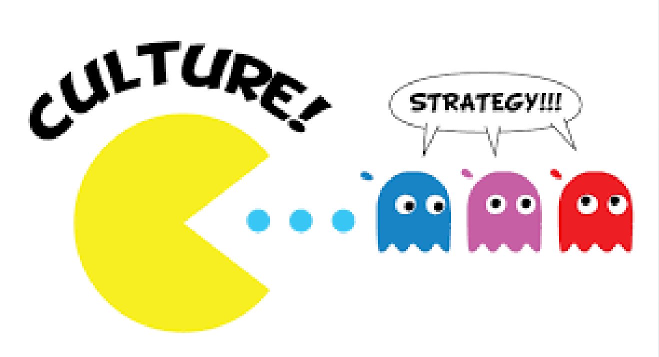
Meet Joe

Misspellings, Phishy Links, Request for information, odd delivery times, spoofed addresses, odd requests, sense of urgency … are all signs of a potential phishing email

https://www.shutterstock.com/search/happy+employee+cartoon

Things to Consider

- What is your email Culture?
- Is there a belief that IT will prevent Phishing?
- Are there formal procedures for key processes?
- “Can you do me a quick favor?”
- Are there guardrails in place?
- Does your culture offer a “Safe Space”?



Next Steps

- ➢Assess your culture and its possible impacts
- ➢Align it with your training and awareness programs
- ➢Stay Safe out there friends!

ISSA

Information Systems Security Association International

www.issa.org

QUESTIONS?