



 **Digital Alliances**
continue collaboration

CISO Alliances – UK&I
17th June 2021

In Partnership with :

proofpoint®

Alliance - 'A union
formed for mutual
benefit'



Food For Thought/Topics Discussed

Digital Alliances
continue collaboration

CISO Alliances

"Security Awareness is Stale. How do we change it?"

UK&I

Thursday 17th June 3pm (GMT)
www.alliances.global
james@alliances.global

Session Leaders:
Andrew Rose Resident CISO , EMEA
Proofpoint

Eddie Whittingham
Director, Security Awareness
Content Development
Proofpoint

In Partnership with :
proofpoint



Session Leaders:

Andrew Rose – Resident CISO – EMEA – Proofpoint
Eddie Whittingham – Director, Security Awareness Content Development – Proofpoint



Session Title:

Security awareness is stale. How can we change it?



Session Synopsis:

Security Awareness has been a focus for security leaders for several years now, but the improvements made by picking the 'lowest hanging fruit' appear to have dried up, and external attackers are still successfully focusing their attacks almost entirely on our employees via email, SMS and even voicemail. When the average click rate is around 12%, and one third of these people will hand over credentials, it's clear that there is still much work to do. But how do we make our next security awareness course, more effective than the last one, when staff are overloaded with both workload and competing education? Join our discussion where we will analyse and debate:

- Why do people still click despite the training they've had?
- What teaching strategies could we consider going forward, and what are the pros and cons of these?
- How do you measure progress?



Digital Alliances
continue collaboration

Food For Thought/Topics Discussed



Agenda

- Intro
- Why people click, and why that's important (AR)
- Teaching strategies analyzed (EW)
- Metrics & measurements (AR/EW)
- Open discussion

proofpoint.

© 2021 Proofpoint. All rights reserved

 **Digital Alliances**

continue collaboration



Food For Thought/Topics Discussed

proofpoint

I – Why People Click, & Why That's Important

We Live in an Anywhere, Everywhere World

OLD WORLD

TODAY'S WORLD

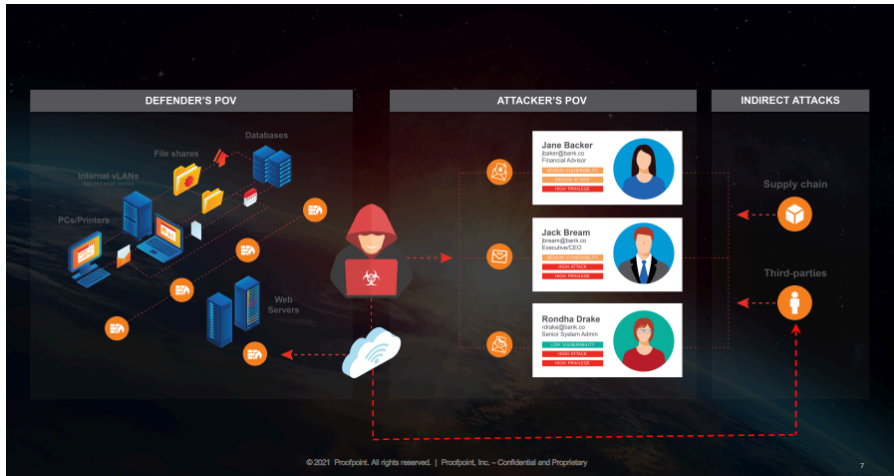


- Some executives still think its their technology that is under attack. This isn't the reason anymore.
- Since digital transformation, the end user has been placed at the center of the organization.
- This plays into the hand of the attacker, as this is where their focus is on.

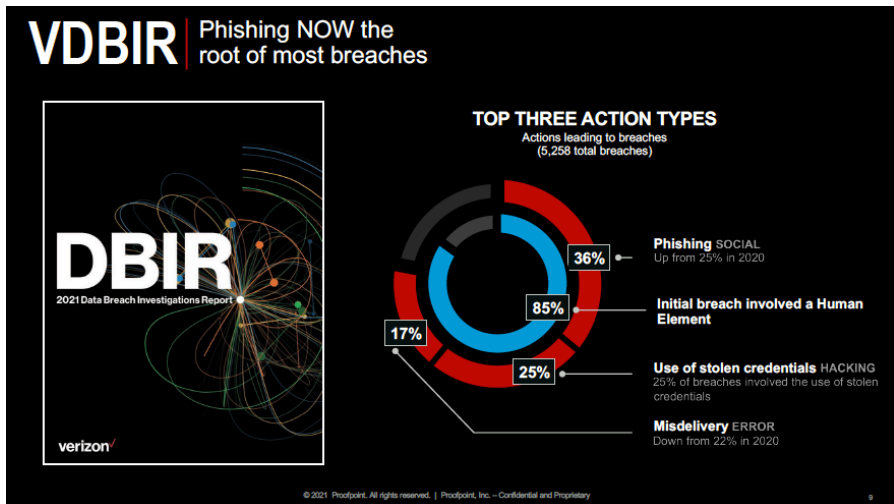
Digital Alliances

continue collaboration

Food For Thought/Topics Discussed



- From a defense point of view, organisations look at completely different things compared to what the attacker will look at.

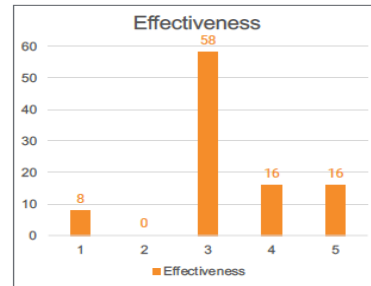
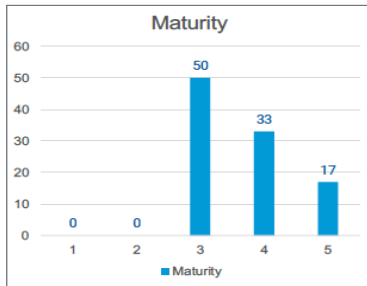


Digital Alliances

continue collaboration

Food For Thought/Topics Discussed

Pre-Session Poll Analysis



proofpoint.

© 2020 Proofpoint. All rights reserved | Proofpoint, Inc. - Confidential and Proprietary

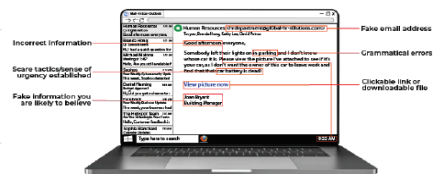
11

- The attending community have an average to mature security awareness within their organisations, however the effectiveness of this is spread across the board.



Terminology: Prognosis Negative

What is PHISHING?	Correct 63%	Incorrect 22%	I Don't Know 15%
What is RANSOMWARE?	Correct 33%	Incorrect 36%	I Don't Know 31%
What is MALWARE?	Correct 65%	Incorrect 21%	I Don't Know 14%



proofpoint.

© 2019 Proofpoint. All rights reserved

12

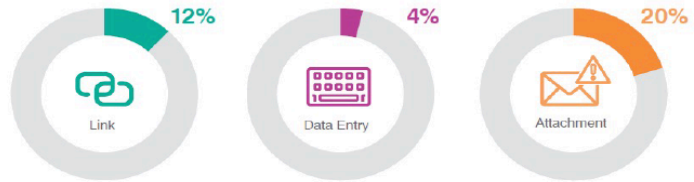
Digital Alliances

continue collaboration

Food For Thought/Topics Discussed

Click Rates: Prognosis Negative

Phishing Template Types: Average Failure Rates



proofpoint. © 2019 Proofpoint. All rights reserved.

How Attackers Exploit People



FATIGUE



TRUST



EMOTIONS

proofpoint.

15

- Attackers will target the emotional part of a person's brain as this is the most vulnerable. This is to stop a person's rational side kicking in, to do this they will attack your emotions especially when fatigued to gain trust.

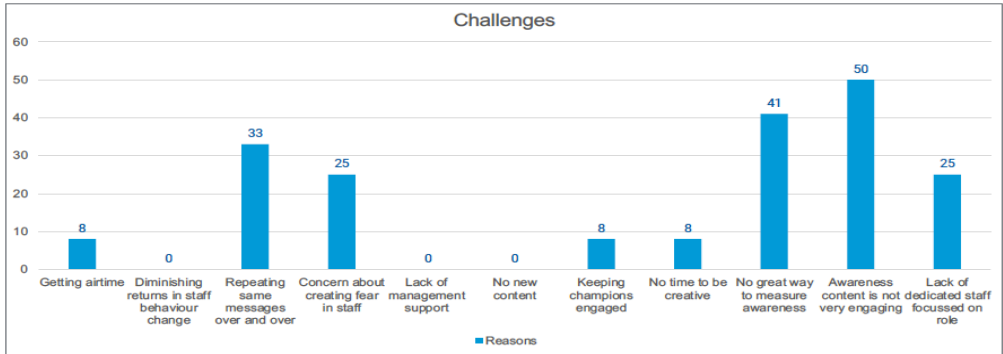
Digital Alliances

continue collaboration

proofpoint.

II – Teaching Strategies

Pre-Session Poll Analysis

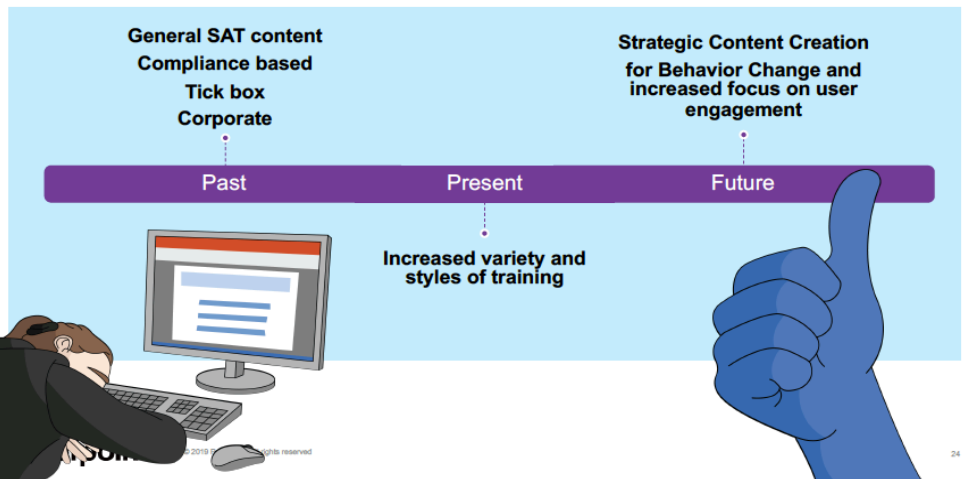


proofpoint.

© 2020 Proofpoint, Inc. All rights reserved | Proofpoint, Inc. - Confidential and Proprietary

23

The Evolution of SAT



24

Digital Alliances

continue collaboration



Food For Thought/Topics Discussed

Mapping the learning



MEASURE AND EDUCATE ACROSS ALL CONTROLS

Control Domains	
Email & Social Engineering	Cloud & Internet Security
Data Handling & Protection	Insider Threats
Mobile Devices	Identity & Authentication
Physical Security & Remote Working	Compliance
Security Operations	Security for Developers

CISO: Content to address threats, risks and compliance needs
Admin: Easier content choices and reporting
Learner: Fresh content to help them want to be part of a security culture

proofpoint. © 2021 Proofpoint. All rights reserved | Proofpoint, Inc. - Confidential and Proprietary

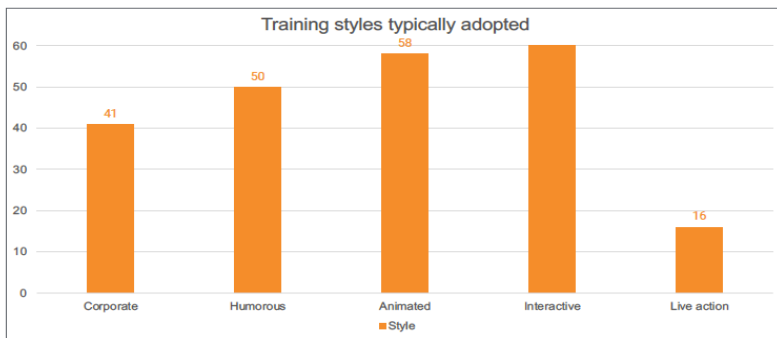
What's available?

- Micro-learning
- Monthly
- Animated
- Interactive
- Humorous
- Live-action
- Industry specific
- Role specific



proofpoint. © 2021 Proofpoint. All rights reserved

Pre-Session Poll Analysis



proofpoint.

© 2020 Proofpoint. All rights reserved | Proofpoint, Inc. - Confidential and Proprietary

Digital Alliances

continue collaboration

Food For Thought/Topics Discussed

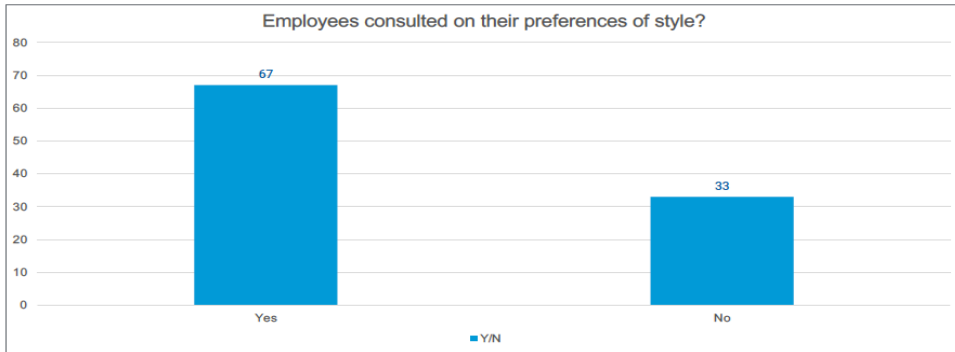
End user focus

- How can we get employees to engage?
- Reprogramming their mindset to want to care:
 - Teach them the why
 - Teach them what's in it for them



proofpoint. © 2011 Proofpoint. All rights reserved

Pre-Session Poll Analysis



proofpoint. © 2010 Proofpoint. All rights reserved | Proofpoint, Inc. - Confidential and Proprietary

31



Extra links to training videos ;

- Here's a comedy sketch based example for phishing: <https://www.youtube.com/watch?v=wcXw3q91L7M>
- A further link was shared but only for community view.

Digital Alliances

continue collaboration

1- The Power of Scrutiny

Using metrics to address the 'long tail'

- An organization had a click rate of 10% and despite continued training, it refused to budge
- The CEO stated that 10% was still too much of a risk
- A strategy was created that had two aspects
 - Increased diversity of training
 - Increased metrics
- One year later the click rate was around 1.5%



proofpoint.

© 2020 Proofpoint. All rights reserved | Proofpoint, Inc. - Confidential and Proprietary

1- The Power of Scrutiny (2)

Visibility drove accountability which drove improvement

- Three metric changes were behind this transformation:
 - Click rates were reported by department, not by the organization as a whole
 - Reporting rates were prioritized and highlighted as a better indicator of security culture
 - A controversial '9 strikes and out' rule was adopted
- The reports went to the CEO on a bi-monthly basis
- The alignment to department drove clear accountability are markedly increased the leadership focus on improvement, driving competition and even aspects of gamification
- The '9 strikes' rule ensured that staff recognized the gravity of the demands, and reacted appropriately

proofpoint.

© 2020 Proofpoint. All rights reserved | Proofpoint, Inc. - Confidential and Proprietary

Digital Alliances

continue collaboration

Food For Thought/Topics Discussed

2 – Using competition as a catalyst for change

Department level leaderboards drove accountability and engagement

- Construction industry
- Largely uninterested workforce

Introduction of department level leaderboards and micro learning

- Shared results throughout the organization to incentivise staff
- Drove engagement from 26% on yearly training to 87% on month to month training

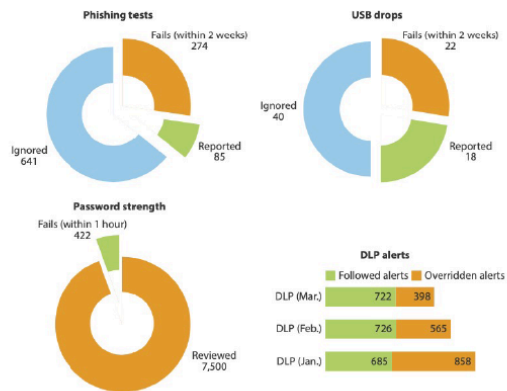
Other organisations have created rewards based systems – e.g. X completion results in an hour off, etc or highest performing team wins free lunch.

proofpoint.

© 2020 Proofpoint. All rights reserved | Proofpoint, Inc. - Confidential and Proprietary

3 – How do you Measure A Security Culture?

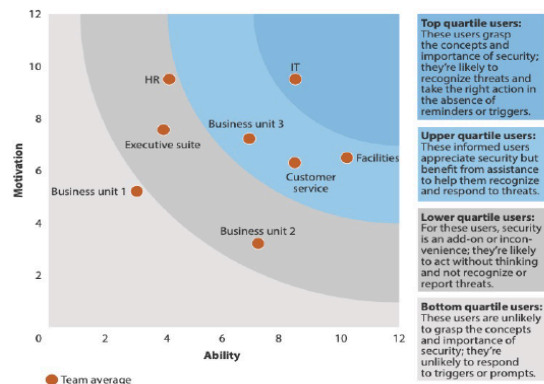
- Org had 'standard' people-centric metrics, but wanted to measure culture, not just when an incident or problem occurred



proofpoint.

3 – How do you Measure A Security Culture?

- Broke desired security culture down into component parts
- Cyber questions embedded into wider annual survey provided scores
- Scored were analysed by department and charted



proofpoint.

Digital Alliances

continue collaboration

Food For Thought/Topics Discussed

4 - Moving Forward

MEASURE AND EDUCATE ACROSS ALL CONTROLS

DESIGN FOR BEHAVIORAL CHANGE

BENCHMARK AND DRIVE OUTCOMES

Tailored Learning Experiences That Engage and Drive Results

proofpoint. © 2021 Proofpoint. All rights reserved | Proofpoint, Inc. - Confidential and Proprietary

Conclusions

Actively work to help staff recognize and avoid emotional reactions to emails.



- Attackers actively target our staff to trigger emotional reactions, bypassing the rational and learned behaviour we have invested time and energy into nurturing
- Recognize that 'more awareness' isn't a solution
- Consider what new styles can you implement to keep your SAT programme fresh?
- The future of SAT will be give you more clarity on specific areas of improvement / deeper insights
- Metrics and scrutiny enable security professionals to be more targeted and focused in communication to address key risk areas and individuals.



proofpoint.

© 2020 Proofpoint. All rights reserved | Proofpoint, Inc. - Confidential and Proprietary

45

Supportive Links :

'State of the Phish' Report

<https://www.proofpoint.com/uk/resources/threat-reports/state-of-phish>

Blog

<https://www.proofpoint.com/uk/blog/email-and-cloud-threats/phishing-prevention-top-concern-todays-cisos>

Global report

<https://www.proofpoint.com/uk/resources/white-papers/voice-of-the-ciso-report>



Digital Alliances

continue collaboration

Community Questions/Comments

- Debate around is it the content of awareness programs is this problem, the content can be fairly consistent. The method and how it is delivered is more important and the issue. Feedback needs to be better, using PR and marketing teams to help write the content.
- When we say awareness, what are we actually trying to achieve? Do we challenge ourselves in terms of the outcomes, stopping people clicking on emails, do we want them to report it to the security team.
- Awareness on its own, doesn't achieve anything, it needs to be linked to an outcome. Understanding those outcomes is the main point.
- The word 'Awareness' focusses your view point on a certain amount of what you want to achieve, but not the whole thing. Smoking is a prime example, there is 100% awareness but people still smoke. Awareness does not change behavior. Culture and behavior are the key points we need to be hitting.
- Getting engagement is helped by putting an at 'home' spin on things instead of work spin.
- With organisations that are world wide cause more of a challenge as dealing with different cultures throws up different challenges.
- With including comedy on videos you need to be careful as there is so many different humors, this is culture wise as well as individual. Using American actors or humor in a UK organization doesn't really work.
- The organisations sector also plays a part, le . Automotive industry, was mentioned that they need to be hit with a point straight away as lack of concentration.
- There needs to be multiple channels of delivery, there isn't a one size fits all.
- This is where focus groups are needed, to understand what is going to work for each organisations.
- Instead of having 200 modules, a better approach could be to have 10 different modules but delivered 20 different ways.
- Short and sweet messages to employees, PDA's and mobiles could also be an effective route.
- Q – Do you find there is a size threshold of staff members where internal training is no longer beneficial, whereby bringing in external teams has a better message as it comes from outside the organization?
- A – This will depend on the delivery method being used, gamification for example takes up so much time that having external organisations becomes more beneficial due to time. External credibility does help, hearing a different voice does help.



Digital Alliances

continue collaboration