AREA 1

SECURITY AWARENESS TRAINING

CAN PEOPLE BE PATCHED?

Security Awareness Training: Can People be Patched?

Some things just go together: Bacon and eggs, peanut butter and jelly, Batman and Robin, anti-phishing tech controls and security awareness training.

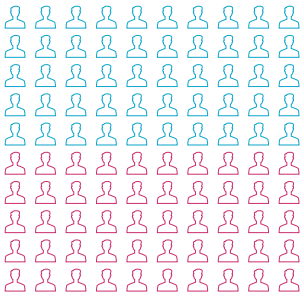
Phishing attacks continue to be the root cause of 95 percent of cyber breaches. **That's why Gartner advises CISOs to make anti-phishing (and particularly Business Email Compromise) a top security project for 2019.** Specifically, they recommend CISOs combine advanced anti-phishing technical controls and security awareness training to best reduce risk and protect from breaches. For organizations that are experiencing successful phishing attacks against their employees, Gartner suggests deploying anti-phishing technical controls as the primary strategy to block as many attacks as possible and integrating security awareness training as a supplement to those controls.

WHY BOTH TECHNICAL CONTROLS AND TRAINING?

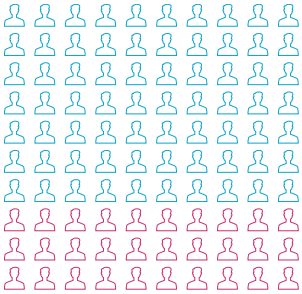
On its own, security awareness training isn't sufficient to defend against phishing attacks. The good news is that awareness training helps reduce phishing risk. Security awareness vendors report that after their customers execute a training program, employee susceptibility to interacting with phishing emails is reduced from approximately fifty percent before training, to about fifteen percent after training.

That's good progress, but it takes only one successful phishing email to breach your organization. Let's look at the math:

Before Training:
20,000 employees x 50% susceptible to phishing
= 10,000 subsceptible employees



After Training:
20,000 employees x 15% susceptible to phishing
= 3,000 subsceptible employees



If a company employs 20,000 people, and 50 percent of employees are susceptible before training, that's **10,000** people likely to fall for a phishing email. If after training, 15 percent of employees are susceptible, that's still **3,000** employees likely to interact with a phishing email.

So even after training, there's still a risk that 3,000 employees are susceptible to phishing, and that's 3,000 too many, since it only takes one click for a phishing attack to succeed and breach your network. ***The odds are in favor of threat actors*** when security awareness alone is relied on to protect against attacks.

AREA 1

Security Awareness Alone Can't Stop Phishing Breaches

Organizations are often required to deploy security awareness training to meet regulatory, legal, or industry requirements, but even when organizations are required to implement training, recent cybersecurity incidents demonstrate that phishing attacks still succeed. For example, the Health Insurance Portability & Accountability Act (HIPAA) §164.308.(a).(5).(i) requires that healthcare organizations implement a security awareness and training program for all members of their workforce. Despite this, we've still seen multiple successful phishing attacks in the healthcare industry over the past year.

HERE ARE A FEW RECENT HEADLINES:

- **1.4 MILLION PATIENT RECORDS BREACHED IN UNITYPOINT HEALTH PHISHING ATTACK.** UnityPoint Health notified 1.4 million patients that their records may have been breached when its business system was compromised by a phishing attack.
- **THOUSANDS OF PATIENTS' DATA STOLEN AFTER CHILDREN'S MERCY EMPLOYEES FALL FOR SCAM.** A phishing attack targeting employees at Missouri-based Children's Mercy Hospital may have compromised PHI on more than 60,000 individuals.
- **PHISHING ATTACK BREACHES 38,000 PATIENT RECORDS AT LEGACY HEALTH.** The hackers went undetected for several weeks at this Portland, Oregon-based health system.

The financial industry is also subject to meeting regulatory requirements for security training. The Gramm-Leach-Bliley Act (GLBA) specifies information security training requirements via its GLBA Safeguards Rule, 16 CFR 314.4., and yet we've seen multiple successful attacks against this industry in the past:

- **HACKERS BREACHED VIRGINIA BANK TWICE IN EIGHT MONTHS, STOLE $2.4M.** Hackers used phishing emails to break into a Virginia bank in two separate cyber intrusions over an eight-month period, making off with more than $2.4 million.
- **FROST BANK SAYS DATA BREACH EXPOSED CHECK IMAGES.** Frost Bank, a subsidiary of Cullen/Frost Bankers, Inc., announced that it discovered the unauthorized access to images of checks stored electronically.The information that was accessed as part of the incident could be used to forge checks, the company says.

So, while security awareness training helps organizations meet their regulatory and legal requirements to educate employees, it's clear from these incidents at organizations subject to security awareness training requirements that training doesn't stop phishing breaches.

Further, not only do phishing breaches still occur after security awareness training is implemented, the cost of training can be significant. Also, managing training programs can take resources away from critical business initiatives. Plus, employees often view security training, and the responsibility of taking the time to analyze and evaluate whether an email or a link seems authentic, as a hindrance to productivity. Training can also leave a false sense of security because copyright laws put security training solutions at a disadvantage. Unlike simulation tools which cannot use corporate logos in their emails, hackers frequently copy branding, text and images right from legitimate corporate emails. So employees are trained on more obvious malicious samples than the realistic phish they will see in the wild. Lastly, business today is mainly online. Security awareness training can make employees fearful of online interactions and can be counter-productive to getting work done.

Gartner Recommends Organizations Deploy Advanced BEC Anti-phishing Technical Controls

To best protect from BEC and other phishing attacks, Gartner recommends organizations deploy advanced technical controls to block as many phishing attacks as possible, supplementing any user training or awareness programs that are already in use.

Specifically, organizations should look towards next-generation technical controls to block phishing attacks at the outset and close the current gaps that exist. Area 1 Security is honored to have been mentioned by Gartner at their 2019 Security Summit as a "state-of-the-art technology" that helps stop BEC phishing.

Gartner highlighted how Area 1 is like a Google, preemptively crawling the world's websites and using big data and machine learning to identify phishing sites as they're constructed, and then proactively blocking attacks before they impact customer end users.

GET AHEAD OF PHISHING ATTACKS

If your organization is struggling to get ahead of phishing attacks and overly reliant on legacy defenses or user training, Area 1 Security can help immediately close that gap, in a comprehensive and accountable way. To learn more, watch the webinar.

About Area 1 Security

Area 1 Security has the industry's most comprehensive anti-phishing solution: Area 1 Horizon™ stops phishing campaigns during the earliest stages of an attack cycle, before a phishing attack on an organization can occur – the root cause of 9 out of 10 breaches.

Area 1 Security works with some of the most sophisticated organizations in the world, including Fortune 500 banks, insurance companies, and healthcare providers to preempt and stop targeted phishing attacks at the outset, improve their cybersecurity posture and change outcomes. Learn more at **www.area1security.com**, join the conversation at **@area1security** or follow the **blog** for the latest industry news and insights on how to deal with phishing.

▸ **Learn more and get in touch with us for a free trial:** INFO@AREA1SECURITY.COM