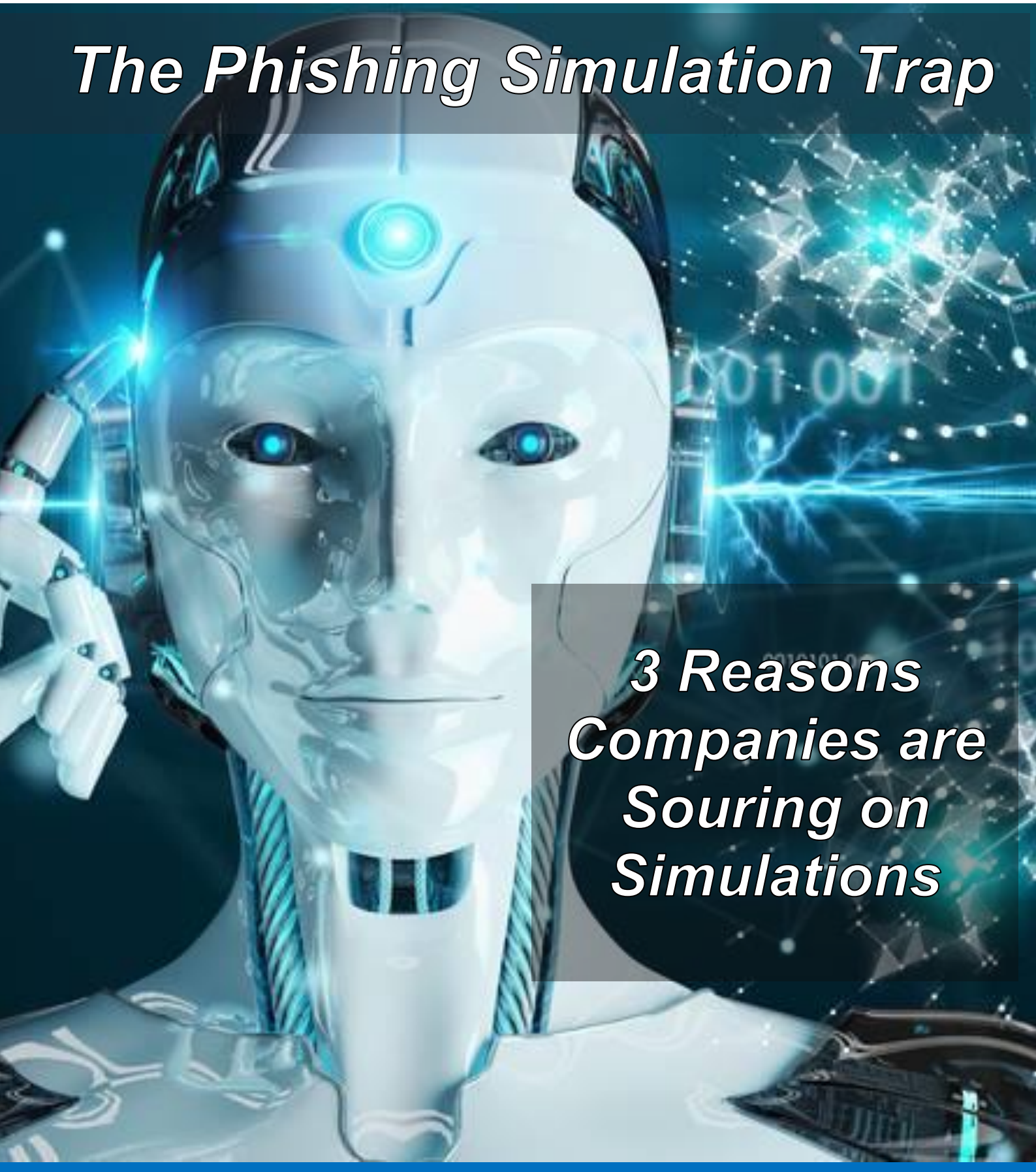
PHISHCLOUD
Empower People. Fortify IT.

The Phishing Simulation Trap



3 Reasons Companies are Souring on Simulations

Let's face it: regardless of how robust your security architecture is, it is the employees in your organization that are the weakest link. IT Security work inside the info security "bubble" every day where the common vernacular is security buzzwords and acronyms. But the employees that they support have little to no understanding of even the basic terminology, particularly when it comes to the many types of phishing.

As evidenced in Proofpoint's State of the Phish Report 2020, only 61% of employees understood the term phishing. Only 31% were familiar with ransomware. The numbers continue to go down when you ask about more modern threats like smishing and vishing. And the numbers decrease in the younger generation as those under 40 are less informed about basic security threats.

Phishing simulations have become a very popular component of the corporate security awareness training program. They are intended to teach employees how to detect and avoid phishing attacks in a safe environment. But is this approach working? The numbers above suggest that there is an overwhelming lack awareness AND knowledge with it comes to basic cyber security. Is it because employees lack concern? Are the training methods ineffective? Are there trust issues between employees and IT that are impacting employee security?

Regardless, 74% of known phishing attacks in the US last year were successful. Phishing attacks have increased 47% in Q1 of 2021 and are now the primary attack vector in 80% of security incidents, resulting in an average breach cost of $4m. It is clear that the current approach of simulations and training are not working, and that change is needed.

Let's look at three reasons companies are beginning to sour on phishing simulations.

Simulations May Create Awareness, But **NOT** Knowledge

Email continues to be the number one attack vector of phishing attacks, a substantial concern as the majority of corporate employees use email as their primary communications tool. A phishing simulation email is designed to "test" the employee on their ability to spot a phishing attack. A test, however, is only as good as the training that has taken place to prepare the student for the test. Cybercriminals constantly adapt their tactics based on

their knowledge of how simulations and protection tools work so training mush also constantly adapt for testing to be effective. Unfortunately, the ineffective nature of simulation create a gap in most companies security architecture.

Despite the awareness training and simulations that companies employ, 97% of users are unable to recognize a phishing email, especially as those attacks become more sophisticated. 20% of employees will click on phishing links and two thirds of those will enter credentials and other data into fraudulent web sites. This is a direct result of the fact that only 10% of companies spend more than 3 hours in cyber security training per year, and that training is typically high level.

According to the World Economic Forum, $5.2tn in global value will be at risk from cyber attacks. With only 3 hours per year in training, the front lines, your employees, are ill-prepared. And only 60% of companies provide formal education. The remainder rely on newsletters, bulletins, videos and user reporting to make their employees "aware." Unfortunately, this awareness does NOT arm employees with the ability to spot and avoid phishing attacks.

Simulations Negatively Impact Employee Morale

Training employees to be able to spot phishing emails is more important now than ever. Training is increasingly a legal requirement as many regulatory frameworks require phishing training for employees. Though well intentioned, these simulations can often have a negative effect on employee morale, especially when not paired with effective, reality-based training.

Many companies today are using the "name and shame" approach to force compliance in their user base. The Consequence Training Model is gaining traction as companies look to punish users who regularly fall for phishing attacks. Consequences can range from additional in-person training to monetary penalties to termination. These measures, however, can be counterproductive.

Companies who play the "gotcha" game with employees can create friction in the company, particularly between IT and the employee base. According to John LaCour, founder and CTO of PhishLabs, "It (simulations) really demotivates people, and it doesn't really teach

them anything about how to be more diligent about phishing attacks. He further explained, "each phishing simulation program needs to be accompanied by a robust training program, where you teach employees what to do when they see something phishy. Otherwise, it just creates resentment among employees."

Rohyt Belani, CEO of Cofense, echoed this same sentiment by saying, "anti-phishing education campaigns that employ strongly negative consequences for employees who repeatedly fall for phishing tests usually create tension and distrust between employees and the company's security team. It can create an environment of animosity for the security team because they suddenly become viewed as working for Human Resources instead of trying to improve security. Threatening people usually backfires, and they end up becoming more defiant and uncooperative."

Additionally, when there is a punitive result, employees are less likely to report having encountered or clicked on a phishing link.

Simulations Do Nothing to Prevent REAL Phishing Attacks

And here's the real rub with simulations: they do nothing to prevent real phishing attacks. Companies today are spending hundreds of thousands, even millions of dollars on email filtering, but emails are still getting through. Over 50 million bad emails get through filtering systems every day, and up to 15 percent of those are opened and actioned by employees. The sophistication of these attacks continues to evolve making even harder for filtering to succeed and for employees to spot malicious emails when they are received.

Additionally, email, while still a sizeable threat vector, is no longer the only vector used by phishing attacks. Social Media now represents 25% of all phishing attacks, up 11.8% from last year. There are now 75 times more phishing web sites than there are malware sites – a staggering statistic. Search engines and web browsers are consistently used to attract users to malicious sites. Even corporate messaging applications are now used for phishing attacks. Companies who focus only on email phishing are leaving a rather large gap in their overall security architecture.

Couple all of this with the lack of robust training in how to recognize and avoid phishing attacks across all digital platforms, and you have the perfect storm: untrained users,

unprotected systems, and an IT Security team with no visibility into what links their users are clicking on across the various digital platforms.

There must be a better way!

PhishCloud: Disrupting the Status Quo

The only way to address these issues is to take a different approach – a human approach. You need a solution that clearly identifies malicious, suspicious, or safe content, in email, web browser, social media and messaging apps, so you can block a threat before it's clicked. You need a solution that gives you real time visibility into malicious content that is being viewed or activated so you can respond in real time and focus on only the most critical events. And you need a solution that delivers real-time training based on what malicious content is being viewed by your users, making sure they are properly trained to spot the threats before they sink you.

What if employee visibility were a simple as a traffic light - green for safe, yellow for suspicious, and red for malicious content – so that your users could be a step ahead to make the right decisions and avoid malicious content?

What if you had complete visibility into suspicious or malicious activity so that you could automatically block bad links from being clicked, and full attribution of phishing clicks within minutes, so you know who, what machine, when, etc.?

And what if you could deliver reality-based training to your users based on the type of malicious activity, they see so that training is specific and real time?

Now you can empower both your employees and your IT and Security teams to:

- Avoid risky clicks with intelligent, traffic-light-style visual indicators that clearly identify safe, suspicious, or malicious content in email, web browsers, social media and messaging apps.
- Automatically block malicious content before it can do damage.
- Significantly reduce the time to risk prediction, incident prediction, and incident response with real-time attribution reporting
- Take advantage of machine learning and AI technology that protects your users from threats seen across the globe

- Integrate data streams with your existing tools and workflows, including SIEM platforms.
- Reduce risk across multiple email, browser, social media and messaging app platforms.
- Deliver targeted, reality-based training to employees, in real-time, based on malicious content seen, so that they are trained to spot malicious content.

PhishCloud provides the most comprehensive phishing protection and reality-based training available in the market today, all in one, easy-to-manage platform. Learn more at www.phishcloud.com.

About PhishCloud

PhishCloud, an IT Security Services company, makes people a key ingredient of your security architecture, not the weakest link, giving IT both visibility and confidence in how their people work every day. PhishCloud provides tools that empower people to make intelligent decisions on digital phishing threats, fortifies IT visibility so they can quickly respond to that threat, and delivers targeted education to reduce the risk of phishing attacks.

Founded in 2018 and headquartered in Seattle, WA, PhishCloud delivers comprehensive visibility into phishing attacks across all digital threat vectors, including email, web, social media, and messaging apps – not just email – so that IT can respond to and block phishing threats that people see in real time. PhishCloud then delivers training based on what your people see so that training is targeted, meaningful and teaches your people their role in your security architecture.

PhishCloud. Empowering People. Fortifying IT.

For more information, visit **http://www.phishcloud.com/**.