CYBEREADY

The Phishing Simulations Playbook

10 BEST PRACTICES FOR AN EFFECTIVE PHISHING SIMULATION PROGRAM

Wondering how to effectively protect your organization against phishing attempts?
Follow these best practices to transform your employees' behavior and build organizational resilience.

You are well aware of the risks you face as a security professional—after all, they're numerous, constantly evolving and ever present. And much of the results you're able to achieve depend upon people who spend little time thinking about security at all.

If only security was a top of mind issue for all of your staff. As it likely isn't, it is crucial that you are able to plan, operate and evaluate a cyber awareness training program that truly transforms employee behavior. In order for this effort to be successful, however, it will involve much more than simply sending out emails to employees.

To attain optimal long-term results, companies should follow a scientific methodology that implements the following best practices:

1. Total workforce training

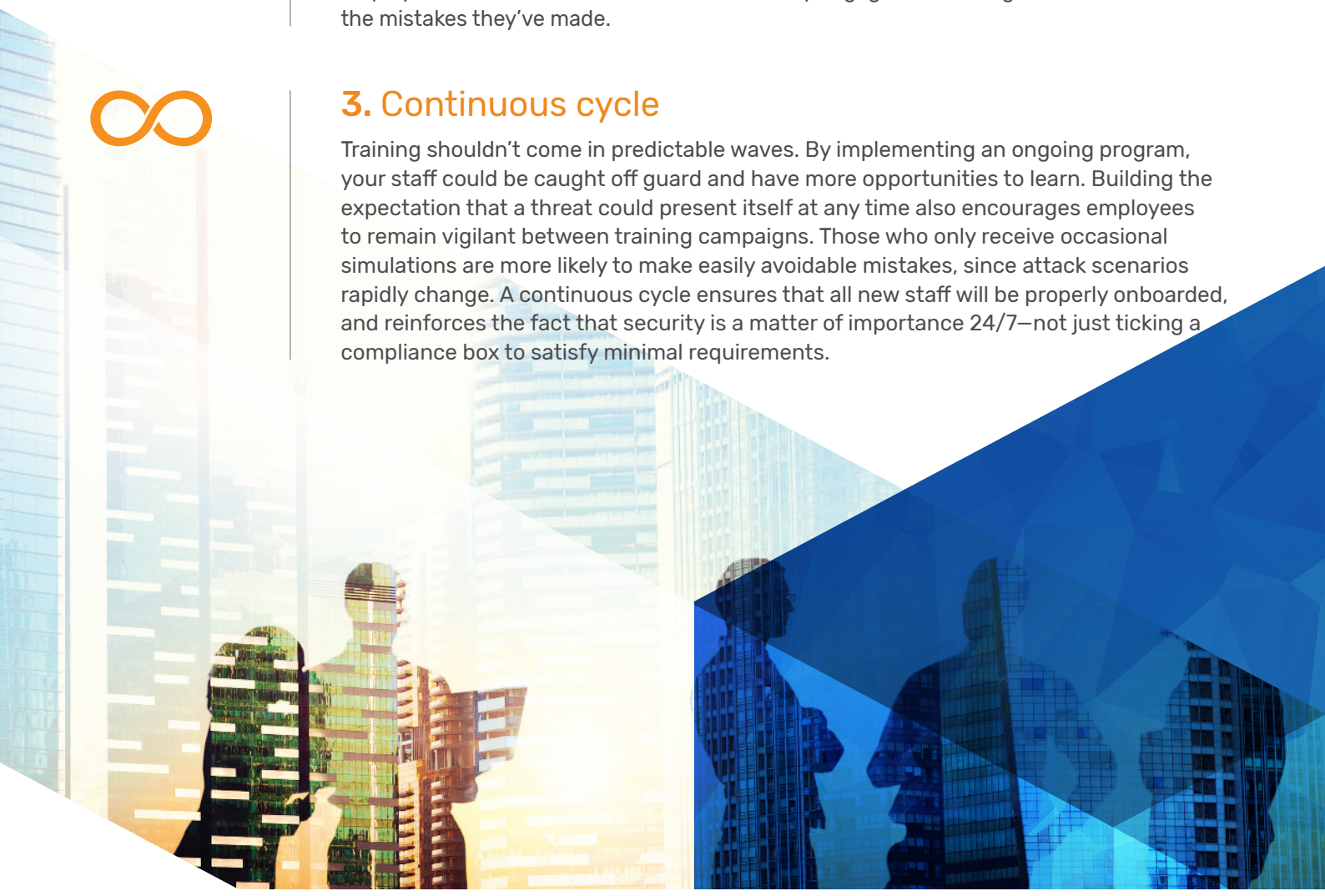
Research shows that ad hoc, scattershot attempts at training staff subgroups is largely ineffective. To bolster internal defenses against sophisticated phishing threats, you must train 100% of your employee population every single month. This becomes more complicated as teams grow and are spread across various locations. Yet opting for anything less than total workforce training leads to piecemeal results, leaving security 'holes' in the form of gullible employees. The worst part: incomplete workforce coverage means not knowing some employees' current awareness of threats, potentially missing the weakest links that put the organization at greatest risk. By the time hackers exploit them, you'll be running internal and external emergency triage with company leadership, HR, and PR staff.

2. Just-in-time learning

There's a limited window of time in which lessons derived from training will have the strongest long-term impact on employees. This is the 'golden moment'—the instance in which providing timely, engaging, and effective content can make a lasting impression, versus having to enforce follow-up training sessions that are often perceived as random, irrelevant, and less memorable—let alone harder to enforce. Associating risks with specific employee behaviors is key. Staff who experience just-in-time learning are more likely to retain critical knowledge and awareness of risk factors, and better able to respond accordingly in future attack scenarios. In essence, companies must ensure that any employees who fall for a simulation immediately engage in a training session that covers the mistakes they've made.

3. Continuous cycle

Training shouldn't come in predictable waves. By implementing an ongoing program, your staff could be caught off guard and have more opportunities to learn. Building the expectation that a threat could present itself at any time also encourages employees to remain vigilant between training campaigns. Those who only receive occasional simulations are more likely to make easily avoidable mistakes, since attack scenarios rapidly change. A continuous cycle ensures that all new staff will be properly onboarded, and reinforces the fact that security is a matter of importance 24/7—not just ticking a compliance box to satisfy minimal requirements.



4. Adjusted difficulty level

At some point, everyone masters the basics of identifying threats. Since malicious actors won't stop there, however, your training shouldn't, either. It's important to start with a low difficulty level and continually make your way up - adjust simulations' difficulty levels and contexts in order to support more robust learning for employees. That said, forecasting actual difficulty is a complex process; it requires daily monitoring of campaign performance to ensure any assumptions regarding specific groups were accurate. It's also recommended that your security team stays abreast of evolving global phishing trends, as various attacker styles and scenarios will become more popular in some geographies or languages than in others.

5. Timely training intervals

While the element of surprise matters, conducting totally random or sporadic security training is counterproductive. The most secure companies ensure that phishing campaigns occur in timed intervals. These may overlap with one another, but can be set as once or twice monthly, bimonthly or more. A set schedule enables CISOs and their teams to establish a solid general baseline for overall employee performance. The understanding gained from quantitative data regarding staff members' 'starting point,' or typical threat response, allows you to identify your biggest problem areas and determine how to mitigate them. Note: individual employee performance comes into play only after you've established intervals and a baseline.

6. In-depth BI reports

All roads lead to your training data. But reports shouldn't just indicate your company's current security health or pinpoint weaknesses; they should measure and display real-time KPIs and business intelligence that drill down to country, department, team or other levels—all without breaching individual employees' privacy. Reports should contain clear, concise graphs and summary information that convey substantive changes. Ensuring that your key stakeholders receive weekly reports, campaign summaries, and Quarterly Board Reviews with actionable data will keep them apprised of ongoing progress and offer visibility into your training program's long-term impact. You'll also eliminate unnecessary administrative work to demonstrate the efficacy of your efforts; instead, your team can attend to more urgent security matters.

7. Data-driven training

Security professionals know that employees respond differently to a variety of attack vectors. For those known as 'serial clickers,' a knee-jerk reaction to download, click, or open an attachment can often land them (and their organizations) in danger. Identifying and maintaining an updated list of serial clickers requires consistent monitoring of all employees' performance. But they aren't the only group you should examine; new hires, executive leadership and veteran employees respond differently to potential threats, so you may want to analyze data to better understand how these groups behave. Next, your team needs to be able to build specially designed campaigns that shift these different or potentially problematic groups toward a more discerning approach to email management.
The 'treatment plan' you create should include an adjusted frequency, timely reminders, custom simulations and training content that helps to reform particularly susceptible groups. Doing all this is crucial, yet it has to be done with the utmost respect to employees' privacy.

8. Adaptive content

Once you've placed employees into segmented groups, it's time for training to become adaptive. The scenario difficulty level is, of course, just one parameter. Determining future attack campaigns based on individual behavior is critical, as is adapting content to specifically address the challenges of a given scenario. These could involve password or data requests, messages from seemingly legitimate senders or sources, or realistic content tailored to an employee's department or role. Material that adapts to both individual employees' responses as well as certain attack vectors serves to further fine-tune employees' defenses, turning the human element into an edge for your company.

9. Adjustable frequency

Your savviest users likely won't fall for the same simulations twice. But those serial clickers are a different story. Therefore, the cadence of your campaigns should be dynamic and personal, reflecting a calculated level of risk for employees across the learning curve based on the data you've collected. Ideally, you'll need to create campaign frequencies that are tailored to employee clusters until they've adjusted to a given training scenario threshold. This may mean that those in a higher risk group will initially receive two targeted training emails per campaign, for example, which will further familiarize them with training content and encourage a modified response.

10. Globalized context

If you're part of a global company with English as its corporate language, you should consider using multilingual content that includes your employees' native tongues, as this will dramatically enhance their learning retention. Especially for multinational business environments, it's important to adapt security training material to the cultures in which your employees live. Depending upon your company locations, there are various legal implications regarding email compliance standards. And by citing local references in training simulations like national holidays, prominent news outlets, popular social media platforms and seasonal sales, you'll increase the odds that your email simulations will be believable, while strengthening employees' awareness of stealthy and highly realistic attacks.

Planning, managing and analyzing a security campaign that incorporates the above best practices will provide companies with concrete results. Few organizations operating off-the-shelf solutions are able to achieve that. The challenge lies in doing so manually, as staff time is often at a premium, and the appropriate expertise across all of these categories is typically lacking in most corporate security teams.

Whether due to internal resource or tech limitations, the outcome is the same: inadequately trained employees who become frustrated with the elementary scenarios they routinely encounter. Expecting project managers or other team members with no training in the cognitive sciences to make decisions and take actions that properly execute such campaigns is unrealistic, and it's fraught with complications—especially in the context of large, multinational enterprises.

A platform powered by machine learning like CybeReady can achieve these effectively. The solution offers security teams an array of data-driven suggestions and BI reports using industry best practices. This comes at a fraction of the cost of in-house simulation creation and analysis, as attempting to offer such content manually requires a significant time investment.

Employee satisfaction with security training also increases as simulations and their resulting training content are considered to be relevant and worthwhile instead of haphazard, out of context or poorly designed. And by introducing more challenging attacks based on employees' previous performance, you'll prevent complex hacker attempts from tricking your staff—further reinforcing your security program's enduring relevance. Most importantly, the right platform can support companies in transforming employees' behavior toward potential email attacks for the long-term, which represents a significant competitive advantage in any industry that relies heavily on digital communication.