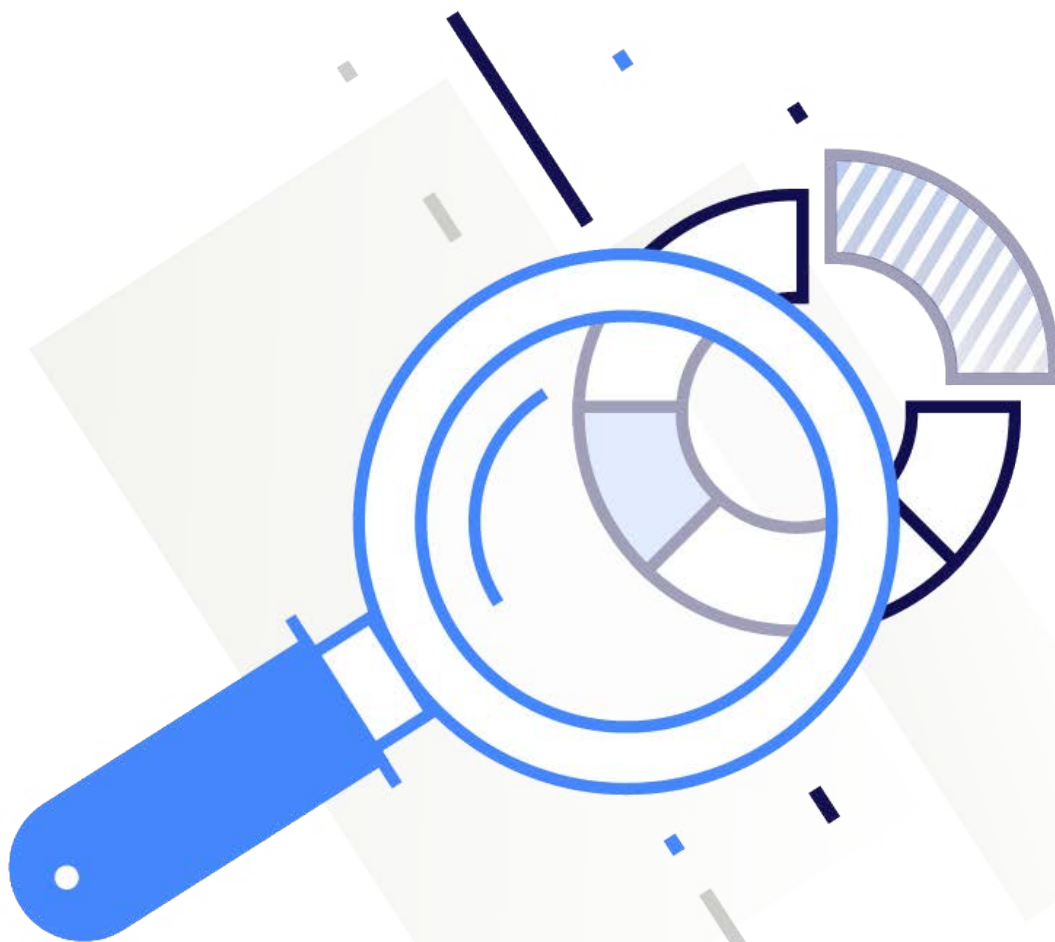


WHITEPAPER

Phishing Simulation Best Practices

Protect your practice against email attacks



Falling for a phishing attack is one of the most common cybersecurity errors employees make, and can have significant impacts on healthcare organizations. Best practices call for a phishing simulation program to monitor and train employees to avoid these attacks.

Phishing is the most common type of significant security incident for healthcare organizations, with attacks in 57% of all organizations surveyed.¹

One of the most common security errors employees make is falling victim to a phishing attack in which they click on or respond to an email that looks legitimate but is actually sent by a hacker. These emails can look like they come from an executive from within the organization, for instance, requesting sensitive information such as account numbers or passwords. In other common cases, the phishing email links to a website where the recipient completes an action that downloads malware or keystroke loggers onto their computer, or where they are convinced enough of its legitimacy that they provide sensitive data such as logins and passwords.

Phishing gives hackers access to provider databases and patient personal health information (PHI). In a growing number of cases, ransomware is downloaded and spread across the provider's network, and organizations are then forced to pay exorbitant ransoms to regain access to vital patient and clinic data and systems. These attacks have a significant impact to healthcare providers and the patients they treat.

- 94% of malware is delivered by email ²
- Phishing is a top access point for data breaches at > 20% ³
- > 25% of U.S. employees admitted struggling to identify a phishing email ⁴

Since phishing is still a significant, initial point of compromise, additional work needs to be done to further lower the click rate. This can be done through more frequent security awareness training, phishing simulation, and better monitoring of metrics pertaining to phishing (including whether there are any particular repeat offenders).

According to the HIMSS report, healthcare organizations are improving their security awareness, but states that "...since phishing is still a significant, initial point of compromise, additional work needs to be done to further lower the click rate. This can be done through more frequent security awareness training, phishing simulation, and better monitoring of metrics pertaining to phishing (including whether there are any particular repeat offenders)."¹

By following security best practices for phishing simulation, monitoring, and training, provider organizations can help employees spot and avoid these attacks.

WHAT IS A PHISHING SIMULATION PROGRAM?

A phishing simulation program is an important way for organizations to see how vulnerable their employees are to this social engineering attack and train them to do the right thing when real phishing attacks occur. The goal of a phishing simulation program is to provide employees with a safe, simulated environment where they can learn about what real phishing attempts look like in the wild. It shouldn't feel like a "gotcha" moment, or an attempt to make your employees feel stupid. The point is to make them feel like you're all working together toward keeping your organization's digital infrastructure and sensitive data safe.

Of course, the threat landscape is ever-changing, so training and email campaigns must be tailored accordingly, using best practices to change email templates and techniques for optimal end-user testing. It is critical to test employees using the latest techniques that threat actors are using to expose any security vulnerabilities.

PROGRAM REQUIREMENTS

A comprehensive simulated phishing program includes a baseline phishing test, a communications plan for employees, ongoing program campaigns that are integrated into a larger security training and awareness initiative, and regular reviews and analytics to guide your activities.

The goal of a phishing simulation program is to provide employees with a safe, simulated environment where they can learn about what real phishing attempts look like in the wild.

1. Establish a baseline

Before you launch a full program, establish a baseline response by sending a simulated phishing email without telling the company. Only your IT help desk should know.

Why all this secrecy? Keeping this first campaign under wraps is the best way to gauge your employees' everyday susceptibility to phishing emails. They won't be expecting a test, meaning they'll be just as vigilant (or not) as they usually are. This first simulated phishing email shouldn't be too simplistic or complex. Consider something like a phony package shipping confirmation or a new voicemail announcement, with a link that leads to a simple 404 page. The click-through rate for this first email becomes the baseline against which you'll measure ongoing progress and show how your phishing and training initiative improves over time.

Once this initial campaign has been completed, review the results to help your executive team and departmental leadership understand the importance of phishing simulation and how the phishing program will work. Once leadership is aware of the program, it's time to introduce the simulated phishing plan to the organization.

Keeping this first campaign under wraps is the
best way to gauge your employees' everyday
susceptibility to phishing emails.

2. Develop a communication plan

After a phishing baseline has been established, you're ready to launch by formally announcing the phishing program to all employees. As part of the communication, convey the fact that the program is not designed to trick anyone, but rather is an educational program and part of the organization's ongoing security training and awareness efforts.

This announcement should include some key elements:

- An explanation of how the simulated phishing program is part of the company's ongoing security training and awareness initiative
- How to report phishing emails (ideally, the program will include an Outlook add-on for easy reporting)
- Where employees can find additional company resources on phishing

3. Schedule the campaigns

Each quarter, set up and configure a new set of email templates and target audiences and create a campaign. Email templates should use social data such as names of executives, nearby restaurants, etc. that can be used to create credible phishing emails. Campaigns then proceed, sending emails to each employee throughout the quarter, at random times and using randomized templates. Typically, a campaign will be one phishing email per month, however this can be adjusted based on the initial test results and the previous quarterly reporting analytics.

When an employee has been lured into a phishing scenario and clicks on content or falls for the scheme, they should be presented with educational content to provide a learning opportunity. The completion of the training activity should be reported and available for review.

When an employee has been lured into a phishing scenario and clicks on content or falls for the scheme, they should be presented with educational content to provide a learning opportunity.

4. Review results and analytics

The shared goal is to reduce the click rate over time in order to help protect your organization from the risk of cyber-attacks. Advanced analytics that measure security awareness within your organization will help you understand your risks. Testing results by person will also help identify repeat offenders who can benefit from additional training and support. Review these analytics on a quarterly basis (or more often, if required) and tailor future training and phishing campaign needs for the upcoming quarter.

Another important metric is the employee report rate, which helps demonstrate your ultimate goal: engagement and therefore a reduced click rate. You want people to tell you if they think they received a phishing email, simulated or not. The more they report, the more engaged your employees are. Long story short: click rates are useful, but report rates are vital.

Phishing campaigns need detailed coordination between security, IT, and leadership teams. On a quarterly or monthly basis as necessary, these teams should meet to review results, answer questions, and plan future requirements and campaigns. Use the initial baseline metric throughout the phishing service as a starting point against which to measure improvement. This metric also helps identify how much training is needed, and areas or groups of individuals who may require more attention.

1 https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf

2 [CSO Online](#)

3 [2020 Verizon Data Breach Investigations Report](#)

4 [2020 State of Privacy and Security Awareness Report](#)

Learn more about Med Tech Solutions
comprehensive phishing simulation program.
Email us at info@medtechsolutions.com



Med Tech Solutions

medtechsolutions.com | 877.687.1222

Med Tech Solutions (MTS) creates technology systems that work the way healthcare practices work. Our Practice-Centered Care services use dedicated IT Care Teams to ensure that technology systems support essential clinical workflows. Provider organizations and networks get a secure, reliable IT infrastructure, optimized clinical and business applications, and full end-user support so they can focus on patient care. MTS was founded in 2006 and is headquartered in Valencia, California. The company has been recognized as an Inc. 5000 Fastest-Growing Company and a Channel Futures MSP 501 provider, and has achieved HITRUST Common Security Framework (CSF) certification for its cloud platform. Learn more at medtechsolutions.com.