MetaCompliance®

How To Run A Successful **Phishing Simulation** Campaign

Phishing simulation campaigns are an effective way to teach employees to spot deceptive messages and help combat phishing. Making these campaigns successful requires planning, communication, and analysis.

Email phishing is the main cause of stolen login credentials and is a successful method used to infect IT networks with ransomware. In Q2 of 2021, phishing was one of the top two most popular and effective techniques used by cybercriminals to hack into corporate networks.

Phishing is successful because cybercriminals can hide malicious content to avoid detection by security tools. It is also successful because it deceives and manipulates employees, making them inadvertent insiders.

Here are some guidelines to ensure your phishing simulation campaign works.

Steps for a successful phishing simulation campaign

Simulated phishing campaigns are designed to automate security training and deliver learning experiences directly to employees. These simulated phishing training packages deliver realistic-looking phishing emails, that track real-world phishing campaigns.

However, to get the most out of a phishing simulation campaign you must plan, be aware of the phishing threat landscape, communicate with employees, and understand how your business goals map to your cyber security needs.

To get the most out of a campaign you should follow these steps listed.

Plan your phishing simulation campaign strategy

All good campaigns are based on solid preparation work. Preparation should cover the following areas:

1. Research current phishing email trends to deliver more realistic simulated phishing messages: Ask your team or advisors what type of emails are being used to target your industry or sector? Are specific apps and brands, for example, Microsoft 365, popular as spoof targets in phishing campaigns? Collate this data for use during the 'build' part of your campaign.
2. How often will the simulated phishing emails be delivered? This may be weekly, monthly, quarterly, etc. The frequency of campaigns should be in line with your overall cyber security risk strategy.
3. Communicate with employees. Develop a set of clear instructions for employees on how to report any identified phishing emails, and/or associated social engineering attacks. This should include details on how to capture the details of the threat.
4. Decide how to further train employees who fail to spot phishing emails. This should explore the use of 'point-of-need' education to focus on enhanced training.
5. Be prepared to adjust your strategy and associated preparation work as the phishing landscape changes.

Build your phishing campaign

An automation platform for phishing simulation campaigns allows you to generate the elements needed to deliver the campaign; this includes the creation of phishing templates. A simulated phishing automation platform will offer templates that are based on current known phishing threats using the most common spoofed brands. Because certain sectors have specific threats, these templates should be modifiable to reflect those specifics.

The important thing to note is that templates should be easy to adjust and configure by the campaign administrator using a centralised management console.

Create learning experiences that make the training stick

The goal of phishing simulation campaigns is to educate employees on how to spot a phishing email and to change the 'urge to click' behaviour that fraudsters rely on. To ensure a memorable and effective learning experience, a phishing simulation platform should provide a 'point-of-need' learning experience.

Typical elements of this type of interactive learning are the presentation of a warning notice, relevant infographic, survey to capture metrics for further tailoring of training, etc., to any employee who fails to spot a phishing email.

This point-of-need will explain what has happened and the dangers associated with a phishing email. Some advanced systems will take this one step further and educate the employee on avoidance strategies to help prevent future phishing attempts.

Collect and analyse metrics

As the simulated phishing campaign progresses, employees should be encouraged to report observed phishing emails. The set of instructions that you develop during your planning stage are the basis for employee reporting of phishing attempts.

Some automated phishing simulation platforms offer a metrics dashboard that uses captured simulated phishing campaign data to analyse the success rate of the campaign.

These metrics are an important part of ensuring that the training is optimised. Metrics also give you the ammunition needed to show the C-level and board that Security Awareness Training is effective.

Some simulation platforms provide data on the percentage of users that are vulnerable to attack and the type of device used to access the phishing email. A greater level of granularity of metric data facilitates more tailored campaigns. These metrics also allow you to continuously improve the effectiveness of a simulated phishing campaign to focus on increasingly sophisticated phishing email content.

Rinse and repeat the simulated phishing campaign

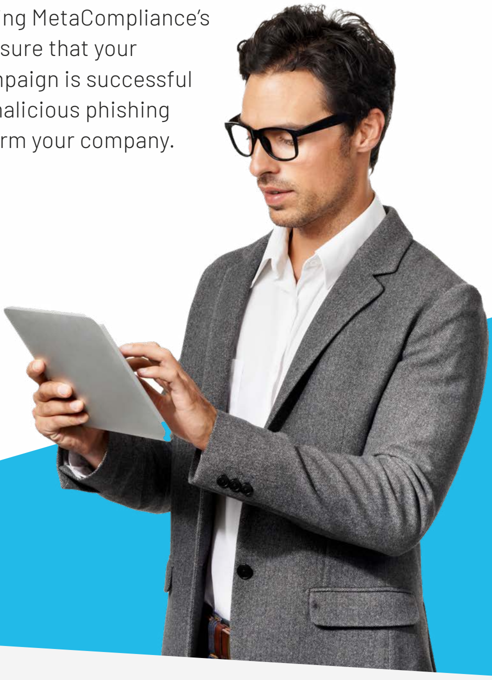
The phishing landscape is always changing as fraudsters work to evade detection. To map to this change, simulated phishing campaigns must also update in line with these changes. This means that your phishing simulation campaign will likely change to reflect the phishing landscape, regularly and over time.

How often you do this is determined by your overall security risk analysis. Recommendations on the periods between campaigns vary, but every 4-6 weeks is a good rule of thumb. However, campaign delivery timings should also be adjusted if significant changes in the phishing landscape appear, as was the case during the Covid-19 pandemic.

Time to phish

A literature review by researchers at Swedish Defence Research Agency found that 24% of phishing email recipients will click on a link and 21% go on to enter their passwords in spoof sites. This alarming figure shows the vital importance of using relevant and focused phishing education for employees.

But making this education effective requires a plan of action. By following MetaCompliance's suggestions, you can ensure that your phishing simulation campaign is successful and stops the real and malicious phishing attempts before they harm your company.



About the author

James MacKay is the COO of MetaCompliance and a recognised Security Awareness Training expert. James has a deep understanding of delivering effective training and is committed to helping organisations keep their staff safe online, secure their digital assets and protect their corporate reputation.

Third Floor, Old City Factory,
100 Patrick Street, Londonderry BT48 7EL
t: +44 (0)28 7135 9777 e: info@metacompliance.com
www.metacompliance.com

MetaCompliance®