How to run an effective simulated phishing test on your users

COPEAR
GLOBAL COMMUNICATIONS

Phishing your employees

Target the weakest areas

It’s all well and good telling your employees that phishing is a big issue for companies. But, how they approach the situation when one appears in their inbox is what matters.

Phishing simulations bring reality to your employees and create a mindset that scrutinises phishing emails before taking actions.

Simulations help your employees to understand their weakest areas, but they also will provide you with a clear insight into how vulnerable your organisation actually is, and where the knowledge gaps are.

Getting started

There are 6 very simple steps to follow in order to ensure your phishing simulation achieves its full effectiveness, as well as improving your employee's cyber security knowledge and behaviour long term.

Step #1

Finding a partner

First things first, you need to find a phishing test tool that suits your needs. Depending on your budget and experience there are a number of phishing tools available.

A partner that is experienced in this area will be able make sure you get the maximum value from your experience.

71%

of targeted attacks involved the use of spear phishing emails

Email Phishing rate is 1 in every 1,846

Step #2

Create your programme

One thing to consider is that your simulated phishing programme should sit alongside your security awareness program and tie into compliance/auditory and regulatory compliance purposes.

An ideal simulated phishing program should allow you to:

- Track your employees progress
- Present a format which is better for auditory and compliance purposes.
- Provide you with better management data
- Increase user acceptance
- Make your business more secure

Step #3

Inform your employees

The whole purpose of a phishing test is to educate your end users, so they can spot and avoid phishing emails in the future.

Informing your employees that a phishing simulation is going to be conducted can divide opinion under "best practices". If you choose to not inform them, then you run the risk that they will feel they are trying to be caught out. Which is not the objective.

Business email compromise is becoming one of the most successful methods of phishing.

$2.3 Billion

The amount of money stolen from CEOs and finance teams during phishing attacks last year.

$1.6 Million

The average cost for a medium size business to bounce back after a phishing attack.

Step #4

Mix it up

When running phishing simulations the biggest challenge you may face is ensuring the validity of the results. If an employee spots the simulated phishing email and decides to inform their colleagues this can have a knock-on effect on the results.

Here are a few ways you can mix up your phishing simulations:

- Spread out the simulations with logical times between each one.
- Target smaller representatives samples of your business
- Mix up the type of simulation, use different phishing templates and spear phishing approaches

Step #5

Record Results

When results are recorded this allows you to analyse them over time, and understand where your risks areas are and spot any trends. Over time, you should notice an increase of reporting the emails and a decrease of interaction with the phishing emails.

Check at least the following statistics after a phishing simulation:

- Users that provided any confidential information
- The number of users who reported the email
- The number of users who did nothing

4000

Ransomware attacks occur everyday.

59%

The percentage of employees that steal proprietary corporate data when they quit or are fired.

PCworld 2018

Step #6

Communication

It's good to encourage open communication when employees discover phishing emails. If they're worried that it may affect other employees, they should post a warning using company communication tools, such as email and slack.

It is also wise to communicate to your employees why the phishing simulation was run and what they should have been expected to notice.

Awareness

After the simulation

Once the simulation has finished it is important to educate any employees that clicked on the email or compromised any valuable information. It's good practice to send reminders to all employee's with tips on what to do and what not to do.

Implementing soft reminders with the use of guides, posters and quizzes is a great way to maintain awareness of your business.

Phishing is over 20 years old.

The average cost of a data breach will exceed $150 million by 2020.

Juniper Research

Hacktivism is the main motivation that drives cyber attacks.

Tel: +44203 4753272
Web: https://www.copear.com
Email: accounts@copear.com