PhishNet

How to Prevent Cybersecurity Breaches Caused by Human Error

In this eBook we outline 4 simple tips to help protect your organisation and people against cyber threats.

How to Minimise Human Error

The first step in minimising human error in your organisation is to measure your company's cybersecurity awareness proficiency.

Cybersecurity has become a critical competitive differentiator for businesses, and as such, its degree of adoption needs to be tracked. But internal security control audits alone paint an incomplete picture of cyber resilience; even the most sophisticated controls fail to prevent a data breach facilitated by human error.

A more accurate method of evaluating an organisation's cybersecurity culture is by measuring its level of cybersecurity awareness.

What is Cybersecurity Awareness?

Cybersecurity awareness refers to the amount of cyber threat knowledge possessed by an individual. At an organisational level, it's a measure of how well employees can recognise and avoid cyber threats, particularly across the most commonly targeted region of a business's attack surface - email.

Cybersecurity awareness and human error have an inversely proportional relationship - the greater the degree of cyber awareness, the smaller the chances of data breaches facilitated by human errors.

How to Increase Cybersecurity Awareness?

The best way to increase cybersecurity awareness is through education. Cybersecurity awareness training is specifically designed to identify an organisation's initial level of cyber threat awareness and lift that standard to a level that's resilient to most phishing attack attempts.

Government Initiatives and Tax Incentives

There's never been a better (and more crucial) time for organisations to transform their employee's cybersecurity awareness.

Now, businesses can save a bonus 20% on cybersecurity awareness training thanks to a new government initiative.

As part of the 2022-2023 budget, the Australian government has announced the Small Business Technology Investment and Small Business Skills and Training Boost. The plan details that small businesses with an annual turnover of less than $50 million can now claim 120% of the cost of employee training and new technology as a tax deduction.

This lucrative incentive impacts an estimated 3.6 million small businesses and is aimed at encouraging small businesses to invest in new technologies that will enable them to grow without incurring significant financial burden.

For instance, if a small business invests $1,000 in a cybersecurity awareness training, they can claim $1,200 as a tax deduction.

How to Choose the Right Cybersecurity Awareness Training for Your Organisation

When choosing a cybersecurity awareness program, there are five essential requirements to consider.

1. Understand the scope of your security training needs

The first step while assessing a program is understanding its scope, cost, and implementation. Consider the following questions:

- What cyber threats will the program cover?
- Will phishing attacks be the primary focus?
- Is it customisable?
- Is support available?
- Does the program cater to a remote workforce?

These questions will help you determine your needs and any discrepancies between a prospective program and the knowledge gaps you're seeking to fill.

Though courses should cover a broad range of cyber threats, the primary focus should be phishing attacks. If a prospective program doesn't teach students how to avoid falling victim to the most common type of cyberattack, it should instantly be disregarded. According to CISCO's 2021 Cybersecurity Threat Trends report, about 90% of data breaches occur due to phishing.

2. Make sure the lessons are engaging

The problem with traditional cybersecurity programs is that they often fail to resonate with employees. Long-winded theoretical lessons delivered over several hours won't change cybersecurity habits. Your employees will just walk away bored with very little recollection of the essential security lessons they were taught. In fact, according to a study done by the MIT, videos lasting less than 6 minutes were determined to be more engaging in a training environment. Engaging content maintains attention and helps employees understand the real-life implications of their actions.

3. Consider varying levels of cybersecurity understanding

Not all of your employees will commence security awareness training on the same footing. When assessed, you'll be surprised by how many of your staff are unfamiliar with even the most basic cybersecurity knowledge.

Your ideal cybersecurity awareness training program must cater to the varying knowledge needs of all your employees. The training should aim to lift the entire company's baseline of cyber threat awareness without leaving anyone behind.

4. Test Knowledge with Simulated Cyberattacks

To further increase knowledge retention, theoretical content should always be accompanied by a practical component. In the case of phishing attack awareness training, phishing simulation attacks should follow theoretical lessons to allow students to put their improved email security habits into practice. Periodic testing will keep your employees aware of the ongoing potential of phishing attacks and prevent regression to previous poor security habits.

5. Ensure Training Modules are Continuously Updated

Cybercriminals are constantly evolving towards more sophisticated cyberattack methods. An ideal awareness program must remain at the cusp of the threat landscape by continuously updating its learning modules. When considering an awareness solution, ask the provider about their efforts to ensure the program maintains its relevance.

PhishNet: Delivering Best-In-Class Cybersecurity Awareness Training

The best way to protect against cyber attacks is to prevent them in the first place. This is most easily accomplished by cybersecurity awareness training. Staff who receive effective cybersecurity awareness training are better prepared to recognise and take the necessary steps to avoid malicious email-based cyber threats.

When it comes to protecting your employees, clients, and business assets, it's important to work with a partner you can trust, who understands the unique challenges faced by your industry.

Our cybersecurity awareness training program is designed with prevention in mind while simultaneously positioning companies to respond more effectively when faced with cyber issues. Our program empowers you to:

- Proactively monitor and report on staff awareness of phishing attacks
- Continuously address the human risk element of a security incident
- Use our toolkit for meaningful conversations at board level

PhishNet delivers highly effective, engaging, and affordable cybersecurity awareness training to help businesses mitigate the risks of human error data breaches.

Talk to PhishNet today to learn more.

PhishNet

Contact Us

https://phishnet.global

1300 165 046

info@phishnet.global