7 Essential Steps To Making Your Security Awareness Training Work

Security Awareness
Life After 'Death by PowerPoint'

Gone are the days of hauling your grudging employees in front of a one-hour security awareness PowerPoint presentation.

With human-caused data breaches at an all time high, these types of much-loathed training days are rightfully seen as a waste of time, money and sanity. Their replacement? Sophisticated eLearning awareness modules that provide a more efficient, smarter and progress-driven educational experience.

But how do you ensure that you implement this type of change in this most effective way? Well, with the right steps, you can easily dodge many headache-prone growing pains...

Training Employees
Where Do You Start?

In this guide, we'll look at the seven key elements your security awareness programme needs to execute, in order to harvest the highest ROI from your training.

We'll look at where to start, what to include, who to include, and what to avoid. Let's dig in...

No awareness?
Big problem.

97%

The percentage of people around the world unable to identify a **sophisticated** phishing email.

InspiredLearning, 2017

12%

The percentage of users who **click the link** after opening a malicious email.

Dashlane, 2018

Step #1

Gain Support From The C-Suite

If your business is serious about security awareness, then this should be a comfortable start. Gaining support from the senior team will give you plenty of future ROI - increasing the level of freedom, user adoption, and budget for your programme.

Clearly **highlight the repercussions** of not supporting a security awareness training program - and there's plenty of those to choose from, such as:

- Failure to gain compliance
- Financial loss
- Sensitive data loss
- Regulatory fines
- Long-term reputation damage

Step #2

Get Involved With Other Departments

"Cyber security? That's not my problem!". For IT and HR professionals, this statement is enough to make your stomach turn.

From finance and accounting, to customer service and marketing, **every department** has a responsibility to ensure company data is secure, so encouraging other department leaders to view awareness training as a company-wide benefit is key. As covered in step one, already having the support of the C-suite can significantly boost this effort.

Additional support in the form of funding and distribution is always welcome, as it will fortify the foundations laid by the upper management.

Growing threats, **growing budgets.**

$1tn

The approximate global **expenditure** on cyber security, expected from 2017 to 2021.

2018 Cyber Security Market report

200bn

The approximate amount of global **connected devices**, expected by 2020.

IHS Markit, 2017

Step #3
Choose The Right Training Platform

Stepping away from PowerPoint and towards e-Learning is undeniably a huge step forward for your awareness programme, but it is essential to make sure that you're **choosing the right software**.

Rather than opting for a generic eLearn platform, choose a software vendor which specialises in security awareness training, to ensure that your users are receiving the best education possible. This should include:

- Bite-sized modules
- Expertly written content
- Regular courses
- Relevant topics
- Varied difficulties
- Easily-accessible metrics

Step #4
Cover The Basics

From speaking with countless IT heads, we often see a huge focus on implementing a programme and having uses adopt it, but not so much focus on what topics their users should actually be educated on.

It is vital to cover the **most common** and **most relevant** types of attacks that your users could face. Here's some of the fundamentals:

- Phishing
- Social engineering
- Password security
- Physical Security
- Working remotely
- Social media

With the right security awareness platform, these topics should already be included in your library of modules, but is worth remembering just in case they are not.

Top 12 training topics.

1	Phishing
2	Password Security
3	Social Engineering
4	Social Media
5	Internet/ Email Use
6	Physical Security
7	Working Remotely
8	Mobile Devices
9	Cloud Security
10	Public Wi-Fi
11	Security at Home
12	Cloud Security

Step #5

Include a Training Procedure

It is important that your business differentiates between security training and security awareness programmes.

Security training enlightens your users with only a finite set of knowledge, usually including tests to aid short-term memory. Security awareness programmes endeavour to **change the behaviour** of users and enable a strong security culture.

Awareness isn't about telling users to be choose a stronger password or else bad things will happen, awareness is a continual process that requires a distinct set of knowledge, skills and abilities.

Step #6

Diversify Your Awareness Channels

Cyber attacks are more diverse than ever, so your awareness programme needs to be equally as **comprehensive**. There's no such thing as a "one size fits all", meaning that your awareness efforts should be delivered through various channels and methods, including:

- Phishing simulations
- Newsletters
- Newsfeeds
- Blogs

The thing to remember here is that not only will diversifying your awareness programme help you elevate your messaging, it will also enable your business to educate users under their preferred learning style and increase progress.

Lack of preparation, **easy target.**

38%

The number of global organisations who claim to be **prepared** for sophisticated cyber attacks.

Cybint, 2018

3M+

The amount of records stolen **everyday** as a result of data breaches, since 2013.

NuData Security, 2018

Step #7

Don't Shy Away From Metrics

Without tracking user progress, it would be impossible to determine whether they are any less susceptible to online threats, or whether your organisation is more at risk than ever.

Choosing the right eLearning platform means that these types of metrics should be easily accessible -- which can prove to be invaluable during times of compliance audits.

Phishing simulations are also a great way of testing your programme's effectiveness, which will also help to keep users alert to the real-world possibility of falling victim to cyber crime.