Your quick guide for driving **employee cyber security awareness**

COPEAR
GLOBAL COMMUNICATIONS

Learn where your users are at now

First thing's first, start with a baseline. You need to gain a clear insight into where your users' security understanding is at now, then, advance that knowledge over time.

Treat this as a 'gap analysis' stage, where you'll determine areas in which education is most needed, rather than deploying generic or painfully repetitive training. We recommend two ways of pre-testing your users:

> **Gap Analysis Questionnaire**

This should cover a range of key information security topics in order to determine where your users are at and what areas they need to strengthen.

> **Simulated Phishing Tests**

As a best practice, these tests are used *after* awareness training has begun (to help determine ROI). However, simulations are also an effective way of determining initial user vulnerabilities.

Gain support from your execs

There's nothing worse than launching a programme that has neither the backing nor budget from anyone else in your business.

The best way to ensure that a culture of security is driven throughout your business is to get your company execs on board. Having the backing of senior figures will not only widen your budget, it will also demonstrate to everyone the importance of information security.

This will give your organisation the ability to balance security objectives with other business-related risks.

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

Avoid the 'one size fits all' approach

To successfully raise security awareness across your entire company, you need to know your audience. From left brains to right brains, millennials to baby boomers, your audience is not singular, and neither is their security knowledge.

Your demographic is varied, so the delivery of your awareness training needs to match this, whether that be through blogs, email shots, videos or posters.

Automated security awareness programmes are also a great resource where users receive educational eLearn courses that are tailored to weakest areas, based on initial assessments.

Cover a variety of training topics

Many businesses fall into the trap of educating end-users solely on the headline-worthy types of cyber attacks - be it ransomware, phishing or physical data loss.

While covering these kinds of attacks is essential, there are an endless list of employee-focused security risks that are exploited everyday. User training needs to be comprehensive and include a variety of subjects.

Here are some of the topics we recommend as the foundation of your user training efforts:

- Phishing awareness
- Social engineering
- Social media safety
- Handling data
- Working remotely
- Password hygiene
- Using public Wi-Fi
- Physical security

12 recommended 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

Ensure continuous security awareness training

For security awareness training to work, it needs to be treated as an everyday business function, rather than the old fashioned way of clamming your employees into a one-hour classroom session, 1-2 times per year.

Short but consistent doses of security training that cover a range of topics are essential to making any sort of progress. This means more than sending a simple company-wide "here's the latest phishing email that's been doing the rounds" communication.

Security awareness eLearning platforms are a great way of delivering regular snippets of engaging educational content.

Choose the right training software

Relying on irregular and inconsistent training delivered by your IT or HR team has proven to be an ineffective and often wasteful approach to awareness training.

Choosing a training provider that specialises in modern learning, modern threats and return on investment is always our strongest recommendation.

There are many security awareness platforms out there that provide great learning material, but lack in the key areas that should be utilised in your training efforts. It's important to look for a solution that offers:

- A library of relevant security awareness topics
- Easily-accessible learner progress
- Long-term metrics (ideal for compliance purposes)
- Practical tests (i.e., phishing simulations)

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

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