Emploware
Cybersecurity & Awareness

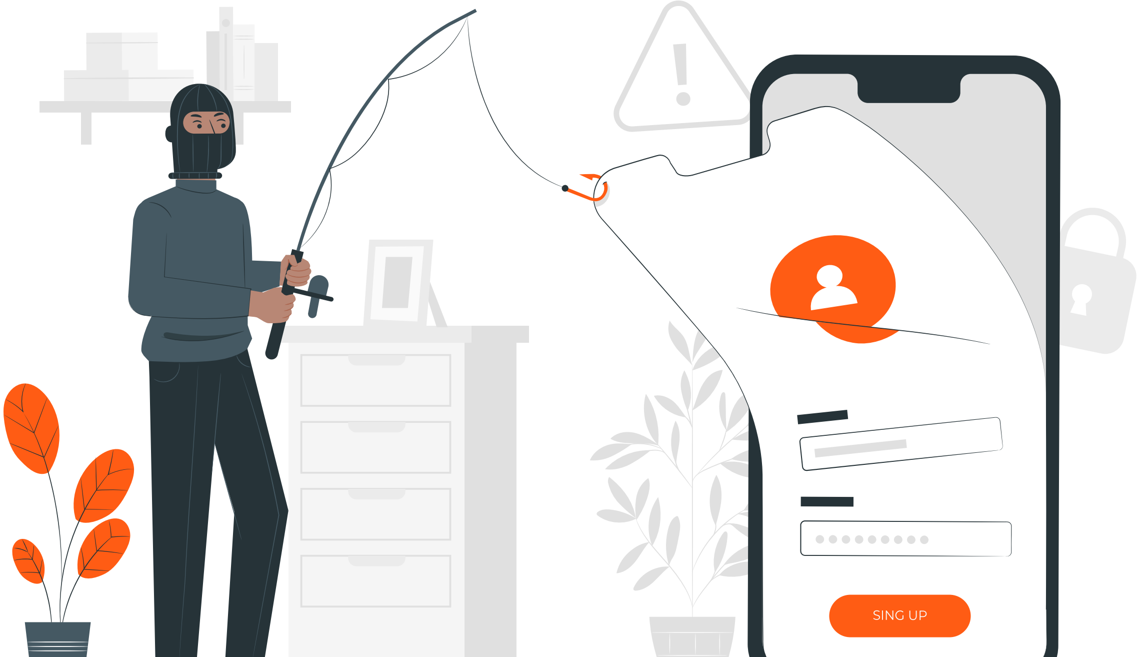
Cybersecurity Awareness Training

Introduction

Where cybercrime used to be something that only affected large companies, today that has completely changed. Smaller companies are also regularly attacked. According to Cyberint, 43% of all attacks take place against small and medium-sized companies. Anyone with valuable information is a potential target for hackers.

While you may have implemented every possible technical safeguard in your business, you are only as strong as your weakest link. It is a cliché, but unfortunately true. In the field of cyber security, that weak link is often the human factor.

No matter how good your defences are, if an employee clicks on a phishing link and enters sensitive data, this action can cause a lot of damage within your company. Offering employees the right training to create awareness has therefore become essential. Over 90% of all breaches are the result of human error. Technical security alone is no longer sufficient.



01 What is **Cybersecurity Awareness**?

What is cyber security awareness? In short, cybersecurity awareness is the extent to which end users are aware of:

- the threats that their networks face,
- as well as the risks they introduce, and
- the best way to mitigate these risks.

In other words, cyber security awareness is all about training people to be aware of threats and how to react to them. The focus here is not only on knowledge, but also on behaviour and attitude.

Whereas a hacker might launch a successful attack with just a single opening, an organisation should have complete security. Every employee, and every device connected to your network, is a potential leak.

TIP: Do you have a 'Bring Your Own Device' (BYOD) policy, where employees bring their own devices and connect them to the company network? If so, it's best to set up a separate network for this, such as a guest network, without these devices connecting to the company network. Otherwise these devices can infect the company network with malware, which they may have gotten from another environment.

02 The importance of **Security Awareness**

Are you still doubting the importance of security awareness? Cybersecurity can no longer be ignored and certainly not considered a cost item. As Easyjet entrepreneur Stelios Haji-Ioannou put it for the airline industry: 'If you think safety is expensive, try having an accident!' In a way, cyber security can be compared to the aviation industry.

It is not so much a question of whether you will be confronted with an attack, but rather 'when'. And how are you prepared for that?

As if the above issues are not enough for a company to worry about, developments such as remote work, also bring new challenges. Employees usually do not have the same security at home as an organisation. In these cases, too, raising awareness is the first step towards limiting risks.

If awareness training is not yet indispensable, it certainly will be in the future. Awareness helps your organisation in the following areas:

REDUCTION OF RISK

By learning about real-life scenarios, your employees will be better able to recognise (potential) attacks. More than 90% of all breaches are the result of human error. By means of education, you reduce this risk considerably.

REDUCTION OF DAMAGES

Training your employees not only reduces risk, it can also significantly reduce damage. The average cost of a data leak is $4.24 million, according to a 2021 report from IBM. With the right knowledge, your organisation can implement sound security measures. If your employees follow the same principles, they will be able to identify deviations faster and anticipate them, thus limiting damage.

ENHANCED EMPLOYEE PERFORMANCE

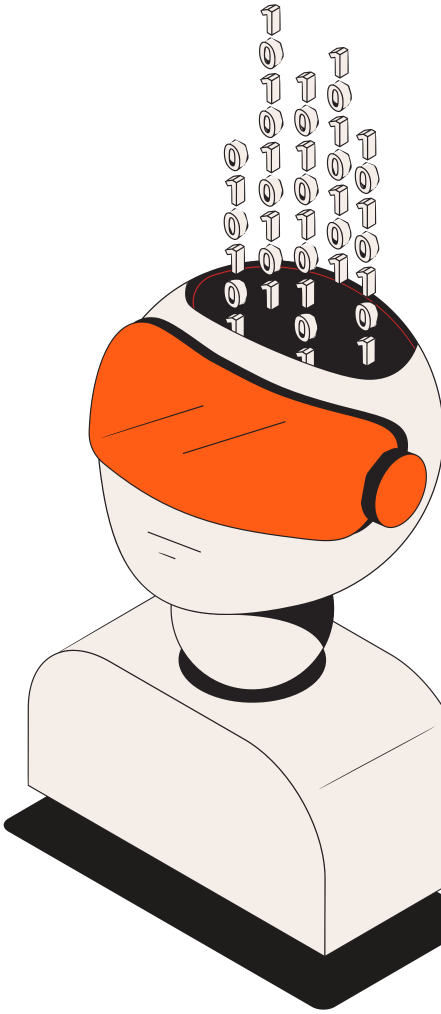
Research by *Research Scholar, Department of Business and Financial Studies, University of Kashmir* shows that training has a positive effect on the job performance of the employees. Training is a motivating factor that increases employee's knowledge of their work, which makes employees better at their jobs and able to deliver better results.[1]

EASY IMPLEMENTATION

Emploware's awareness training is entirely online. Your employees can log into their own online environment and increase their knowledge and awareness with just a few minutes a week.

[1] https://www.researchgate.net/publication/262843202_Impact_of_Training_on_Employee_Performance_A_Study_of_Retail_Banking_Sector_in_India

03 The Training



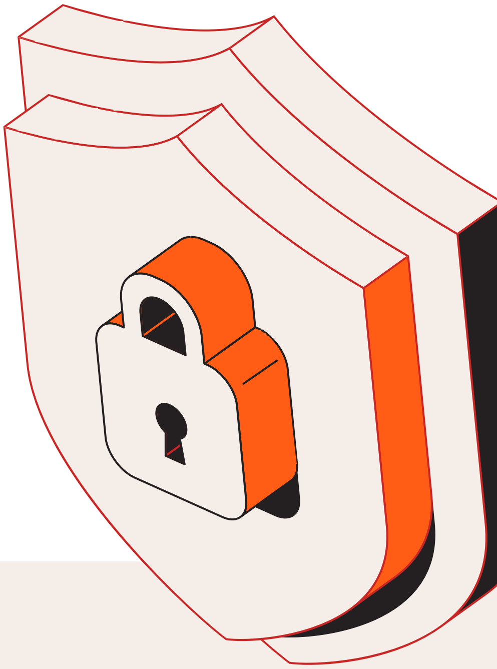
Awareness training is the foundation of any organisation, but it must be done at the pace and schedule of your employees. The training courses are therefore short, fully online, available in more than 15 languages and can be followed at your own pace. With frequent updates, we also stay current and provide new material for your employees throughout the year.

With just a few minutes spent each week, your employees will train themselves. They do this by watching real-life, short videos and answering quiz questions.

The platform

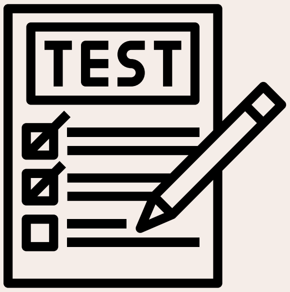
- More than 20 training programmes
- More than 15 languages
- Quiz questions
- Insight into vulnerable departments
- Training with just a few minutes per week

04 Other forms of **training**



Creating awareness through training is the first step towards a stronger organisation. However, the theory must be applied in practice. The following two training methods will allow you to see how it is implemented in practice, without harming your business.

SOCIAL ENGINEERING



The term social engineering refers to the ‘art’ of manipulating people so that they disclose confidential information. It is an umbrella term to describe various techniques. Examples of social engineering are:

- Leaving a usb stick with malware, with the aim of triggering a curious employee to put the usb stick in his computer;

- Tailgating: where the objective is to follow someone into a secured or restricted area;
- Vishing: voice phishing, or telephone phishing, in which an attempt is made to retrieve sensitive data by telephone.

If you want to test the people within your organisation, we can apply various social engineering tactics, with your approval. These can be the examples already mentioned, or variants that are relevant to your organisation.

PHISHING SIMULATION

Phishing is a specific technique that falls under the umbrella term of “social engineering”. It involves obtaining sensitive information and normally phishing is done by email. Phishing is often about login data or credit card details. Attackers achieve this by imitating well-known institutions, such as a bank, and luring people to a malicious website.

With a phishing simulation, your employees will receive harmless phishing mails, announced or unannounced. Our system allows you to see which employees open a link, click on it or perhaps even download attachments.

05 Statistics

88% of organisations worldwide experienced spear phishing attempts in 2019. (Proofpoint)

In 2020, it took an average of **207** days to identify a breach. (IBM)

In 2018, an average of **10,573** malicious mobile apps were blocked per day. (Symantec)

The average cost of a ransomware attack on businesses is **$133,000** (SafeAtLast)

Every minute **$17,700** is lost to a phishing attack. (CSO Online)

By 2023, the total number of DDoS attacks worldwide will reach **15.4M** (Cisco)

Attacks on IoT devices tripled in the first half of **2019** (CSO Online)

1 in 36 mobile devices have high-risk apps installed. (Symantec)

Home workers have caused a security breach at **20%** of organisations. (Malwarebytes)

43% of all cyber-attacks target small and medium-sized businesses (Cyberint)

94% of all malware is sent by email (CSO Online)

IoT devices: The term IoT is an abbreviation for Internet of Things and by this we mean physical objects that are connected to the Internet and can transmit data. These include cars, smart doorbells, smartwatches, etc.

DDOS attack: During a DDoS attack, a website's server is overloaded by sending a large number of requests within a specific period of time. As a result, the server can no longer process these requests and therefore no longer functions properly.