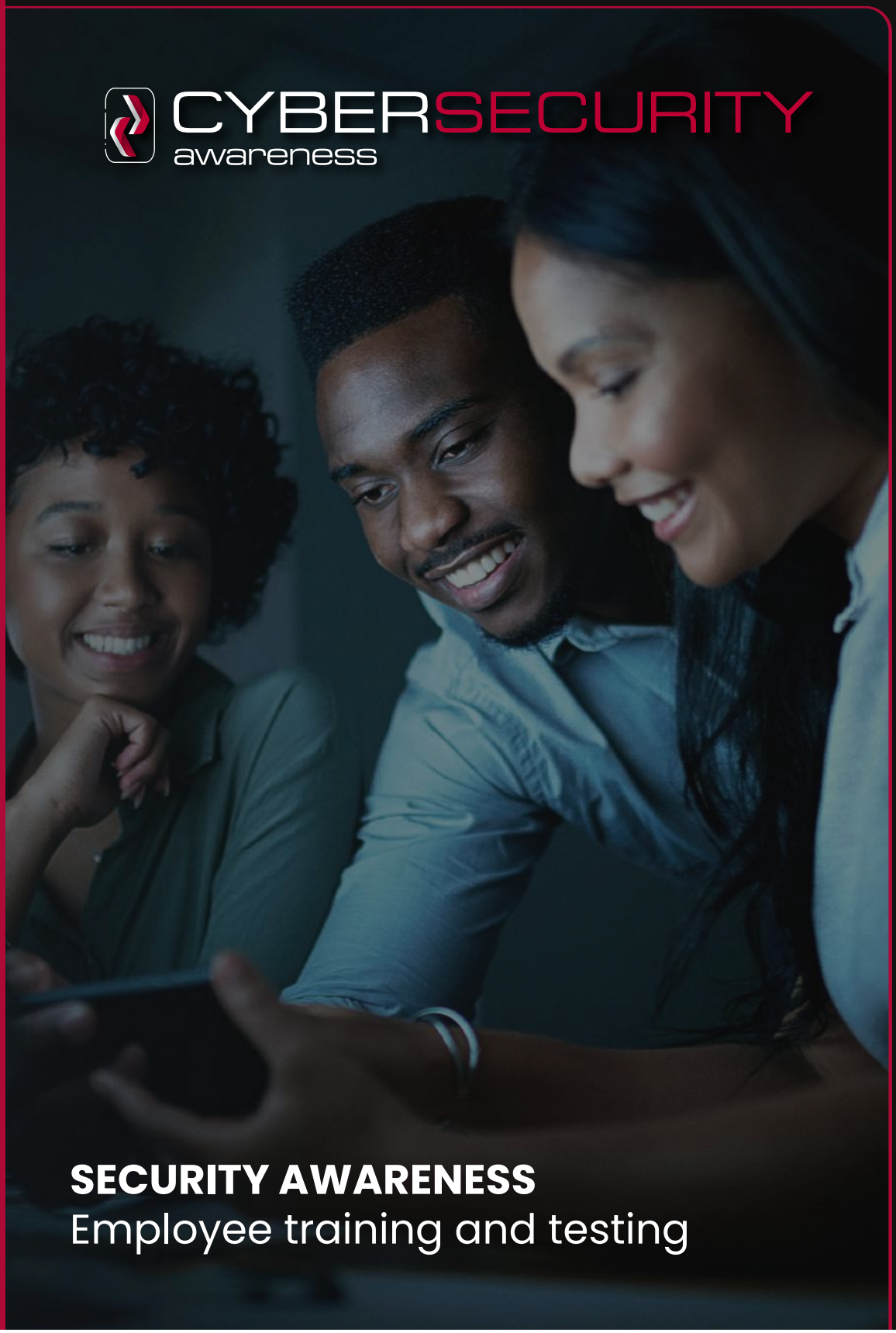
CYBERSECURITY
awareness



SECURITY AWARENESS
Employee training and testing

Security Awareness Training and Testing that makes a difference.

Stop your employees causing security incidents without the hefty price tags and without adding to your workloads.

Over 90% of successful cyber attacks could be stopped by a trained and vigilant workforce

Employees are still responsible for the vast majority of security incidents. Regardless of the security technology an organisation has in place, attacks still land in front of staff, leaving your organisation to rely on the know-how of your workforce to keep you protected against targeted cybercrime.

The solution is to regularly train your staff on today's cyber threats and keep them vigilant, though nearly all organisations lack the time, resource and expertise to manage an effective security awareness training and testing program.

Our **fully managed** Security Awareness Training and Testing (SATT) service is outcomes driven, guarantees results and will make a meaningful difference by changing staff behaviour when it comes to identifying cyber security threats, all without taking up any of your time or resources.

Key features and benefits

Outcomes driven with guaranteed results
Our mission is to make a lasting difference with every organisation we work with. We're all about providing a true return on investment, so our approach is dynamic to ensure that every customer receives a service that works for them.

Fully managed and bespoke service
Phishing testing and security awareness training solutions can be time-consuming and difficult to manage. Let our team manage your programme for you, freeing up your time and resources so you can focus on what matters most.

UK provider with global coverage
As a UK provider, our course content is voiced by British actors and supports over 26 languages. We work with businesses all across Europe and the globe with their cyber security awareness requirements.

Interactive cyber security training
Engaging e-learning courses with integrated quiz questions to provide a unique learning experience that ensures staff understand cyber security risks and methods to stop cybercrime.

Targeted phishing testing
You shouldn't settle for anything less than simulated phishing attacks that are true to life, as if a cybercriminals is targeting your organisation, which is what our expert engineers do for every customer.

Detailed reporting and portals
Board-level reports for training and phishing campaigns that help you gain compliance and cyber insurance, with a user-friendly reporting portal for a real-time view of your service progress.

How it works

Our three step process is trusted by thousands of organisations and has helped over 600,000 employees improve their cyber security awareness.

Other security awareness solutions prove to be a wasted investment, resulting in staff still being a cyber security risk. Our simple process will stop employees from causing security incidents.

The cost of keeping staff trained and vigilant is always significantly less than the cost of just one security incident.

Stage 1 - Baseline

Understand your risk level
Get started with a baseline phishing test to understand your staff susceptibility to targeted cyber attacks.

This is a realistic spear phishing attack that's created bespoke for your organisation.

Typically 40 to 70% of your employees will engage in the attack and be identified as a cyber security risk.

Stage 2 - Training

Interactive e-learning
Teach your staff the skills required to identify and prevent modern cyber attacks with interactive, online training.

Our cyber security training videos are created by experts and cover a range of security topics, providing your workforce with a well-rounded understanding of the cyber threat landscape.

Stage 3 - Monthly phishing

Maintain vigilance with ongoing phishing testing
We'll work closely with your organisation to ensure vigilance towards cyber threats is maintained with regular phishing testing, remedial training, reports and additional support.

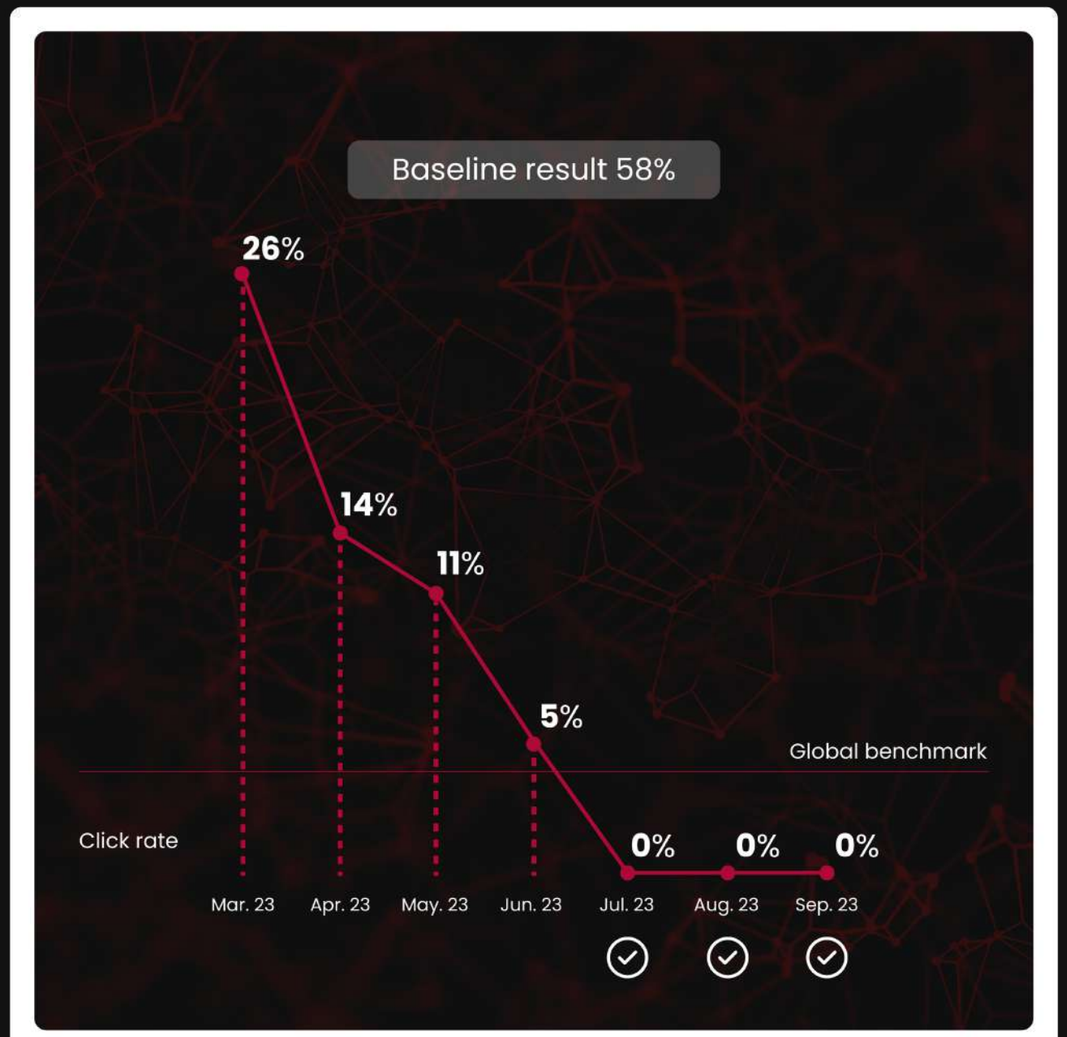
Staff who continue to click phishing emails and put security at risk will be provided with the extra support they need to ensure they don't make the same mistake again.

Our mission that you maintain a 0% click rate on a monthly basis.

The key to stopping security incidents

Training alone is not enough to rely on staff to prevent security incidents on an ongoing basis. Training is usually taken annually and only has a short term effect.

After a couple of weeks, staff are likely to fall back into old habits because the skills they've learnt are not being reinforced. It is only with our **monthly phishing emails** and **refresher training** that you can maintain regular staff vigilance and see a positive reduction in risk, as demonstrated below.



Why you need SATT

IT Departments know they need to implement security awareness training, but many face internal roadblocks.

To help you, here are the common objections we often hear and the reasons why every organisation needs to invest today in outcomes-driven security awareness training and ongoing testing for all employees, from the top down.

The SATT service is the best (small) investment you can make.

It will have the biggest impact in ensuring your reputation, customers, finances, data and IT assets stay secure.

Let’s start with the financials

Although you know that employee security awareness training is required, there is no specific budget available.

And your organisation thinks cybercriminals will wait to attack you until after the start of your next financial year…

Before training, our baseline phishing tests show that 40% to 70% of employees are a security risk. This is not a problem to ignore. Ask us for a quote and we guarantee you will be pleasantly surprised at the low investment (in time and money) and the immediate measurable returns.

You’ll quickly see the benefits of the training and testing, over the course of the SATT service, as employees become more vigilant and aware of cyber security risks.

Do you have budget to cover the cost of just one ransomware attack or data breach?

Our customers are rapidly making budget available for the SATT service, as the total cost to train all staff and keep them vigilant is far less than just one security incident.

It is far better to invest a small amount now and be in the best possible situation to prevent future attacks. Taking immediate action is far more effective and cheaper than the clean-up costs and reputation impacts of a security incident.

Does training actually stop end users causing security incidents?

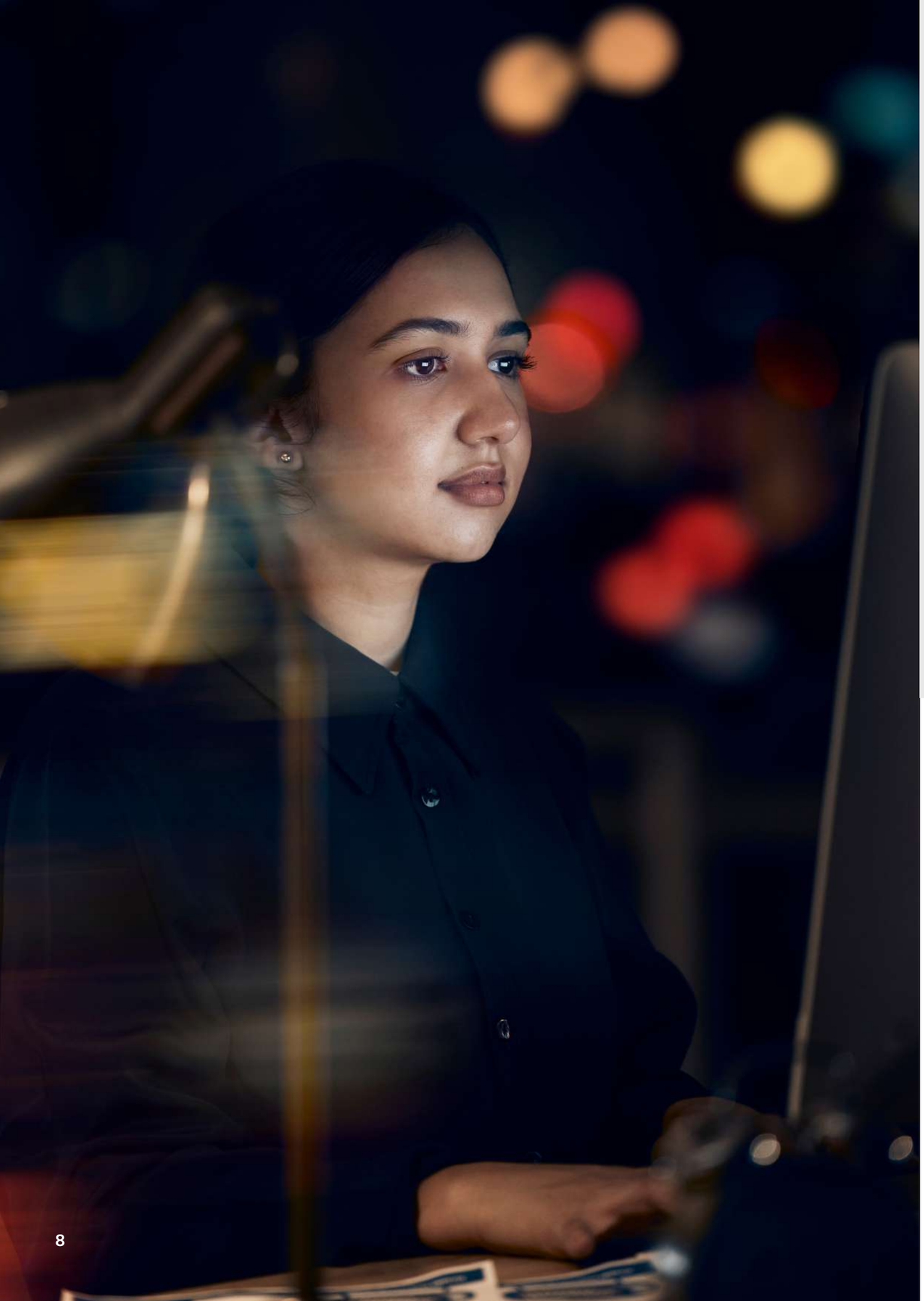
We have found that security awareness training makes an immediate difference to staff behaviour. However, what normally happens after completing any training, without continuous reinforcement, is that the message is gradually forgotten within a few weeks of returning to day to day activities.

This is where our fully managed training and testing managed service is unique. Our service actually stops your end users causing security incidents.

It is only by combining workplace security awareness training with ongoing, random test phishing emails, supplemented by additional targeted training for those who are (still) vulnerable, that you build a human firewall. A firewall of vigilant, knowledgeable and empowered employees ready to protect themselves and your organisation.

A human firewall ready to identify potential security incidents.

Only our integrated training and testing service will help you build a relevant, robust security culture that stands the test of time.



Our organisation is not a target

Organisations often think that their specific data will not be targeted by cybercriminals, or that they are too small to be on the radar.

Unfortunately, the facts are simple. Cybercriminals don't care about your business size or sector. All data is valuable data in today's world, plus it's also the links you have to other valuable assets through your supply chain that is attractive to threat actors. They are also motivated to gain financially and damage brand reputation.

If you become a victim of ransomware and the attackers are demanding Bitcoin to let you have your data back, it suddenly becomes extremely important.

You, your employees, customers, suppliers and the organisation as an entity, all have bank accounts and IT equipment, which means you are already a target and need to take immediate action to prevent financial, data and/or reputation loss.

Our staff know better

Like most organisations we expect your staff are good at identifying obvious phishing emails (banking etc.), but threats are constantly evolving and criminals are using new and advanced methods (targeted spear phishing and social engineering) to breach organisations.

With our training and ongoing testing, your employees will be able to spot and stay safe against these ever evolving and sophisticated threats.

Our employees don't have time for phishing training

The training only takes 15 minutes. We have developed the best available security awareness training videos (drawing on our cyber security expertise) to ensure every employee is trained on the latest cyber security threats.

We are covered with our existing email and web security

You are not!

Regardless of your current IT security systems and any advanced threat protection methods that you are currently using, your staff members will always pose the biggest risk.

Modern cybercriminals are breaching organisations with new and advanced methods. Often there is nothing malicious in either the emails or the pages they direct to, or they are seemingly legitimate emails requesting payments are made. New websites are created, categorised as legitimate sites and then become infected with payloads within hours.

At some point (regardless of your IT security measures) your employees will be faced with something malicious. The only way to not fall victim is to provide staff with the correct skills and ensure they remain vigilant.

I don’t have time for this at the moment

SATT is a fully managed service. There are no demands on your time or resources.

We do everything for you, all you do is provide us with a list of all your staff email addresses.

The SATT managed service includes:

- Researching, creating and sending targeted test phishing emails
- Ongoing reporting on the % of users who are a security risk and training status
- Enrolling your staff in the training
- Chasing employees to ensure completion of training
- Further training enrolment where needed

Plus, the training covers a great deal more than just email phishing threats:

Topic	Modules
Email security	Phishing Overview Generic Phishing Spear Phishing CEO Fraud
Web Security	Pop-ups Toolbars Phishing Websites HTTP and HTTPS Suspicious URLs Links
Physical	Removable Media Shoulder Surfing Leaving Technology Unattended Social Engineering ID Badges
Mobile and Wi-Fi	Smishing Applications Vishing BYOD Wi-Fi
Handling Sensitive Information	Handling Paper Based Information Handling Electronic Based Information
Best Practice	Secure Passwords Keeping Technology Up To Date Email Web Physical Mobile

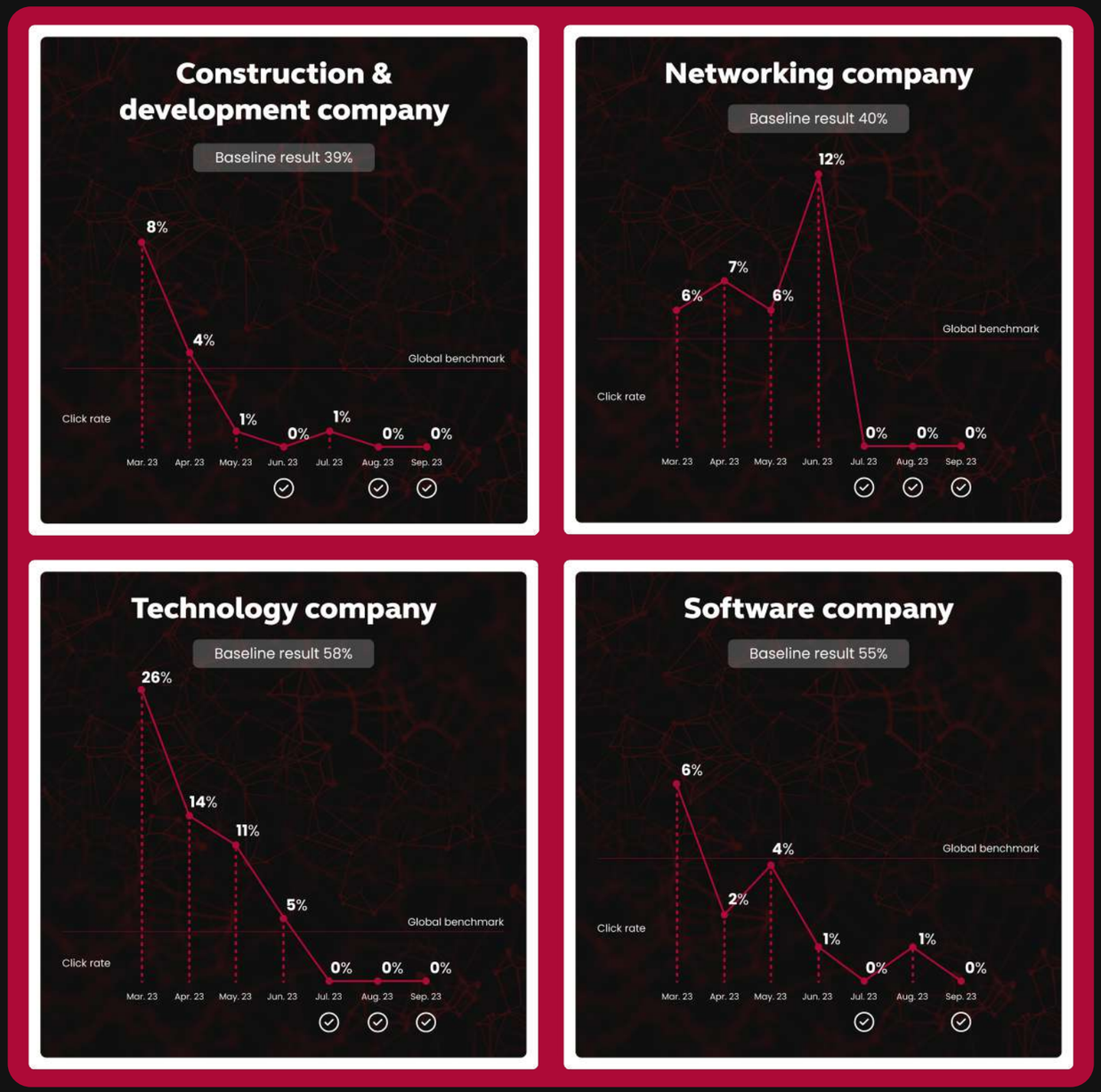
All training videos are delivered at your employee’s desks, to be watched at their convenience and can be paused and returned to at any time.

15 Minutes of training to protect your organisation’s reputation, client confidentiality and finances, is all that your workforce needs to take.

Experts at solving human risk

Every customer is different and the journey to reaching 0% is not a fixed, linear process. We work with your organisation closely to ensure staff are responding well to refresher training and not putting your security at risk in monthly phishing tests.

As shown below, almost all customers start with a high Baseline result. As we roll out training and begin monthly phishing, the risk level is reduced down to 0% of staff clicking phishing emails.



Don’t just take our word for it

We’ve helped over 3,000 organisations and 600,000 employees stop security incidents with Security Awareness Training and Testing.

Customers include organisations of all sizes and in all sectors, and all grade the service as ‘meets or exceeds expectations’ as per our quarterly satisfaction survey.

“With our multiple office locations and busy workloads, the ability to access flexible, on-demand training at the desktop was a key consideration. Once we found out the SATT service could provide an integrated program of training and simulated phishing tests, we knew this was the right solution for us.”

“Our employees all liked the training videos as they were packed full of UK-content, and could be watched at their own pace and convenience. They are now applying this knowledge in their day to day jobs.”

“We’re a business full of highly educated people, who often think that they won’t be caught out by phishing emails. Running the initial baseline test, where 40% of staff clicked, confirmed the need for the training and I’m pleased to say that the SATT service has already made us all more aware and vigilant.”

“The simulated phishing attacks were very effective and we were somewhat alarmed by the number of employees that clicked on the email link prior to training. This information was presented back to the staff in a statistical format, not naming names and significantly increased the buy-in to the training, and the overall awareness and vigilance of the staff.”

“We’ve recently renewed the SATT service for another year – as we now have over 700 extra people on our security team!”

“Many companies offer Security Awareness Training, however the SATT service is certainly the best. With unique UK content, the training is both relevant and engaging. Plus, the combination of training and simulated cyber- attacks, with additional focused training as needed, keeps us all on our toes.”

Get in touch

sales@cybersecurityawareness.co.uk

01256 379977

cybersecurityawareness.co.uk