



THE ESSENTIAL GUIDE TO SECURITY AWARENESS TRAINING AND TESTING (SATT)



Stop End Users Causing Security Incidents

The UK's premier **Security Awareness Training and Testing (SATT) service** helps organisations build a vigilant, informed and empowered work force ready to stop malicious cyber-attacks.

The consequences of failing to do so go well beyond the bad headlines.

One security incident can lead to lost jobs, substantial legal costs, non-compliance penalties, loss of brand reputation, customer loss, and a catastrophic hit on the bottom line.

ORGANISATIONS USING SATT

Over 65,000 IT end users worldwide are enrolled on the SATT service, protecting their data, clients and reputation. Customers include organisations of all sizes and in all sectors, and all grade the service as 'meets or exceeds expectations' (quarterly satisfaction survey).

OUR CUSTOMERS SAY:

"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."



FOR CLIENT CONFIDENTIALITY, WE CANNOT PUBLISH OUR CUSTOMER LIST, BUT WOULD BE HAPPY TO SHARE WITH YOU, ON A ONE TO ONE BASIS.

THE SATT SERVICE

The purpose of the SATT managed service is to stop security incidents. It is only by providing your end users with relevant security awareness training and regular testing that you will achieve this goal.

SATT is a fully managed service that is bespoke and tailored to every individual organisation. It takes up none of your time or resources, and is guaranteed to make a difference.

SECURITY INCIDENTS ARE STOPPED BY HAVING REGULAR TARGETED EMAILS SENT TO ALL STAFF, WITH ADDITIONAL MORE IN-DEPTH TRAINING PROVIDED AT THE DESKTOP TO ANY VULNERABLE USERS - THOSE WHO STILL CLICK ON POTENTIALLY MALICIOUS LINKS OR ATTACHMENTS.

THE 3 STAGES OF SATT:

The SATT service combats the weakest cyber security link in any organisation – your end users – and is delivered in three stages over a 12-month service agreement. The service is fully managed, so there are no additional demands on your time.



STAGE 1

BASELINE ALL USERS

A bespoke, targeted email is sent to all users (it's best you don't tell them this is happening) and we report on how many users put your security at risk.

This baseline test provides a real-world reflection on how vulnerable your IT end users are, with typical results of 40% to 70%.

STAGE 2

TRAINING

All users receive the best available security awareness training. The training is delivered as a 15-minute online video that each user watches at their desk, and at their own convenience. The training covers everything that is relevant to modern cyber-crime (a lot more than just malicious emails) and how not to fall victim to these threats.

STAGE 3

MONTHLY PHISHING

(the most important stage)

At this stage, your users receive regular (one per user per month) bespoke targeted emails. Anyone who clicks is identified as a vulnerable user and receives additional more in-depth (40 min) training.

This is an essential stage: The targeted emails keep staff vigilant against cyber-crime (no-one wants to be caught out). Plus, users identified as a continuing security risk to your organisation receive the additional training they need.



THE TOTAL COST FOR THE 12 MONTH SATT SERVICE IS SIGNIFICANTLY LESS THAN THE COST OF JUST ONE SECURITY INCIDENT.

WHY YOU NEED SATT

IT Departments may know they need to implement organisation-wide IT User 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 results-driven security awareness training and ongoing testing for all employees - from the top down.



THE SATT SERVICE WILL BE THE BEST (SMALL) INVESTMENT YOU MAKE OVER THE NEXT 12 MONTHS. IT WILL MAKE 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 cyber criminals will wait to attack you until after the start of your next financial year...

Before training, our baseline tests frequently show that 40% to 70% of end users 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 end users 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 annual cost to train all end users 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 end users' 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, will you build a human firewall. A firewall of vigilant, knowledgeable and empowered end users ready to protect themselves and your organisation. A human firewall ready to thwart 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 DATA IS NOT A TARGET

Organisations often think that their specific data will not be targeted by cyber criminals. Or that they are too small to be on the cyber criminals' radar.

Unfortunately, the facts are simple:

Cyber criminals don't care what data you have. 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 users are good at not clicking on 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 users 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 end user 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 end users will always pose the biggest risk.

Modern cyber criminals 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 pop-up, are categorised as legitimate sites, and then become infected with payload all within days.

At some point (regardless of your IT security measures) your end users will be faced with something malicious. The only way to not fall victim is to provide users 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.

Once the order is placed we do everything for you, all you do is provide us with a list of all your users' email addresses.

The SATT managed service includes:

- Researching, creating and sending 12 months of targeted, test phishing emails
- Ongoing reporting on the % of users who are a security risk and training status
- Enrolling your users in the training
- Chasing users 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:	TOPIC:	MODULES:
Email Security	Phishing Overview Generic Phishing Spear Phishing CEO Fraud	Mobile and Wi-Fi	Smishing Applications Vishing BYOD Wi-Fi
Web Security	Pop-ups Toolbars Phishing Websites HTTP and HTTPS Suspicious URLs Links	Handling Sensitive Information	Handling Paper Based Information Handling Electronic Based Information
Physical	Removable Media Shoulder Surfing Leaving Technology Unattended Social Engineering ID Badges	Best Practice	Secure Passwords Keeping Technology Up To Date Email Web Physical Mobile



ALL TRAINING VIDEOS ARE DELIVERED AT YOUR END USERS' 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 IT END USERS NEED TO TAKE.

KEY BENEFITS

TIME

The whole SATT service is fully managed, taking up none of your time or resources.

TRAINING

Our service provides the best available security awareness training ensuring every user is trained on what is most relevant to modern day cyber security.

VIGILANCE

Senior management and employees know the test emails are there to catch them out. This makes and keeps them vigilant, meaning they actually apply the skills they have learnt in the training - which is exactly what stops security incidents.

BESPOKE

Everything is created and personalised for each individual organisation. We approach each organisation the same way a cyber-criminal would.

EXPERTISE

We are the experts and have a dedicated SATT team who research and create all the targeted emails, and manage the whole service personally for each customer.

LIBRARY

We have hundreds of templates and real-life examples that we tailor to each organisation.

REPORTING

Everything is reported on accurately – opens & clicks, training reports on every user's status and time spent watching the training. Monthly reports showing percentage at risk, any clicks and the training status of vulnerable users.

LANDING PAGES

Landing pages that look like the real page (baseline) and "oops you've clicked on a phishing email" (monthly phishing tests).

VULNERABLE USERS

Our service highlights vulnerable users, anyone who clicks on a targeted email after training receives instant remedial training. This is delivered immediately on the page they just clicked onto: "oops you just clicked on a phishing email", here is what to look out for so you don't make this mistake again.

ADDITIONAL TRAINING

Any vulnerable users are enrolled in specific 40-minute training.

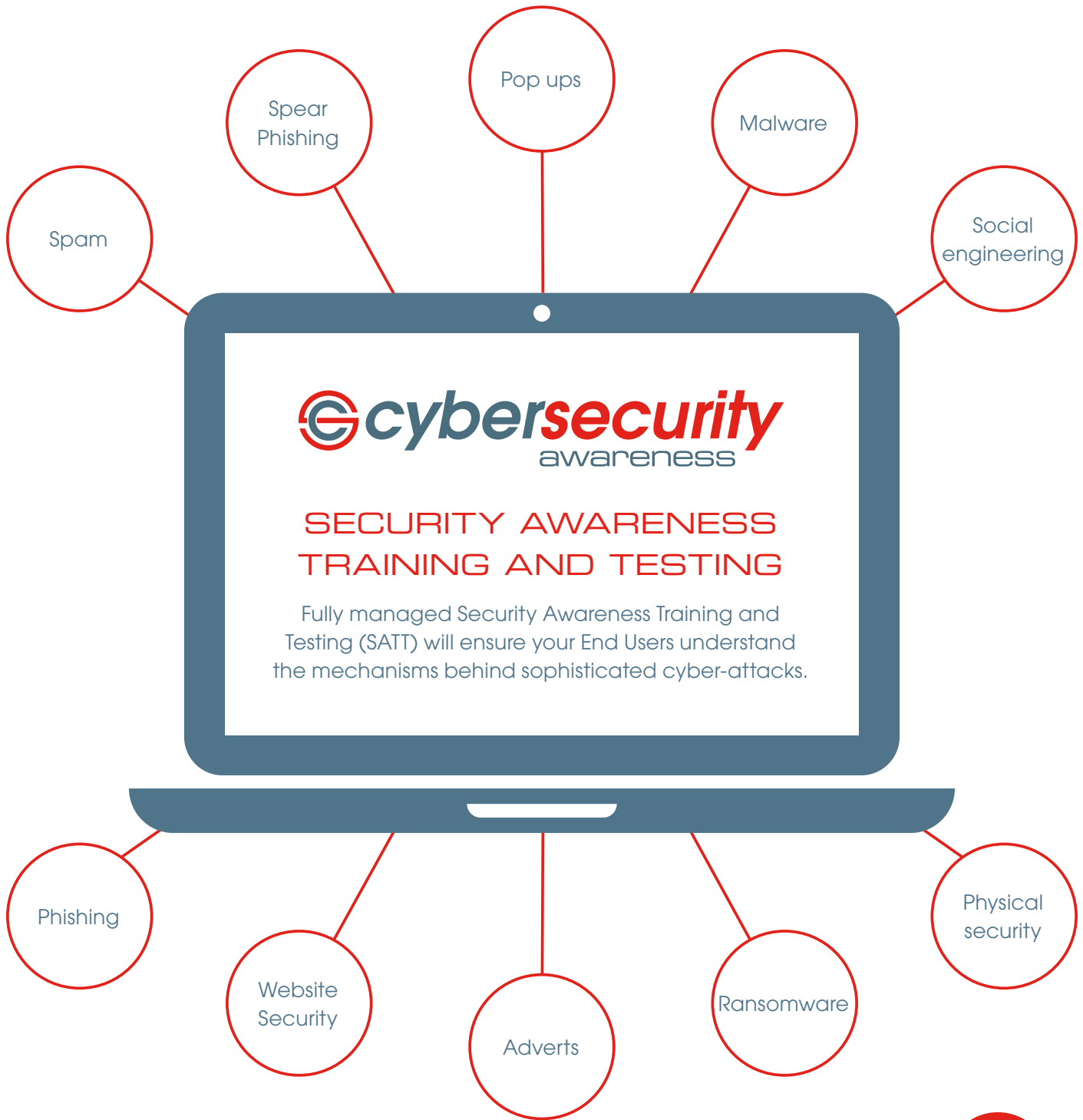
GUARANTEE

The SATT service comes with a full money back guarantee if we fail to reduce your end users' susceptibility to phishing attacks within 60 days

For more information see:

www.cybersecurityawareness.co.uk





THE SATT SERVICE IS COST-EFFECTIVE, REQUIRES A RELATIVELY SHORT AMOUNT OF EMPLOYEE TIME (AT THEIR DESKS), AND IS SUITED TO ORGANISATIONS OF ALL SIZES.
SATT IS DELIVERED BY INDUSTRY EXPERTS IN IT SECURITY AND TRAINING.

FOR MORE INFORMATION PLEASE CONTACT:

Deans Computer Services PLC
E: sales@deansplc.co.uk
T: 01937 541411
W: www.deansplc.co.uk



DEANS COMPUTER SERVICES PLC