STRIPE OLT

☎ 0207 043 7044
✉ hello@stripeolt.com

CYBER SECURITY USER EDUCATION

Turn your number one weakness, into your first line of defence.

Over 50% of all cyber security breaches are caused by human error, yet less than a third of businesses report their staff have undergone any formal training.

For a business to be truly prepared when dealing with a cyber-attack, their security strategy needs to go beyond Artificial Intelligence and Anti-Virus software – A wholly robust strategy adopts an offensive position and prevents through cyber security education.

At Stripe OLT, we understand there is no 'one-size-fits-all' solution, and when it comes to education, we believe different user groups require different forms of training. From phishing awareness, to tailored stakeholder workshops, our courses focus on specific areas of business risk and how to mitigate these appropriately.

WHO IS IT FOR?

Any company that wants to support their users, whilst protecting their business will benefit from our courses.

London

☎ 0207 043 7044
✉ hello@stripeolt.com

Bristol

☎ 0117 974 5179
✉ hello@stripeolt.com

STRIPEOLT.COM

UNDERSTANDING THE RISKS

RISKY PERSONAL DEVICES

Without clear security policies around the use of company data and personally owned devices, staff may connect their own devices to your network, which could lead to the inadvertent import of malware or compromise your sensitive data.

INEFFICIENT REPORTING

Without a robust cyber security culture and formal reporting process, you are unable to uncover potential issues or report genuine incidents.

LEGAL RISK

If your workforce is not supported and trained effectively, especially around how they handle particular types of sensitive information, it could leave you open to legal action.

OPEN TO EXTERNAL ATTACK

Your users are the primary focus for external attackers. Attacks such as phishing or social engineering rely on taking advantage of legitimate user capabilities and, in turn, can gain access rights.

OPEN TO INSIDER THREAT

Without the right processes in place, employees hold a lot of power. Dissatisfied employees can easily abuse their system level privileges or coerce other employees to gain access to information or systems to which they themselves are not authorised.

London

☐ 0207 043 7044

✉ hello@stripeolt.com

Bristol

☐ 0117 974 5179

✉ hello@stripeolt.com

STRIPEOLT.COM

OUR COURSES

At Stripe OLT we offer two levels of user education.

Staff Cyber Awareness (SCA)

In this course, we focus on the cyber risks to the individual and their role within the business. Hackers are becoming increasingly aware of how businesses operate and what they need to do to gain the attention and trust of an employee. Focusing on the technicalities behind social engineering, we look at the following areas...

What's included?

- Phishing emails & campaigns: What they are, how they work and what to do if you receive one.

- Introduction to Malware: We'll take you through a live WannaCry demonstration to show you exactly how the hackers operate.

- The importance of account hygiene: Why you need to keep your systems up to date and your passwords strong.

- Remote Working and the Risks: Focusing on wireless device security and the necessity of a closed Wi-Fi network.

- System Management and Maintenance: We'll demonstrate how hackers can gain your information and why they sell it on the Dark Web.

Executive Cyber Fundamentals (ECF)

The Executive Cyber Fundamentals (ECF) course covers one full day of training, where selected delegates will gain a relevant and up-to-date understanding of the current threat landscape and how to mitigate cyber security risks to their business. This interactive security training day is comprised of the following syllabus...

- Cyber Security Essentials: Immediate risks to your organisation, common attack vectors and principle security controls.

- Spear Phishing emails & campaigns: What they are, how they differ to phishing attacks and what to do if you receive one.

- Introduction to Malware: We'll take you through a live WannaCry demonstration to show you exactly how the hackers operate.

- The importance of account hygiene: Why you need to keep your employee systems up to date and the importance of multi-factor authentication.

- What is Social Engineering: How the hackers use your employees to gain internal information and credentials, including a live demonstration.

- Remote Working and the Risks: We'll cover the technicalities behind VPNs and when to use them, how to utilise Office 365 applications for device security, and the necessity of a closed Wi-Fi network.

- System Management and Maintenance: A demonstration into how hackers work, and why they sell your user credentials and company data on the Dark Web.

HOW MUCH DO OUR COURSES COST?

Depending on the number of users and type of course(s) provided, prices vary. Please get in touch with our security experts for a free discovery session, upon which we'll provide you with a quotation.

WHY STRIPE OLT?

The work we do is recognised by the UK government. As GCHQ-certified experts, we deliver cyber security training and consultancy to businesses all over the UK, providing them with the guidance and support they need to successfully educate their employees.

We educate in line with the Cyber Essentials scheme and in accordance with Information Security standards, such as ISO 27001.

We have already helped a large number of organisations build security awareness for employees, so understand how cyber security differs. No matter what size and industry, we have the experience and skills required to support your organisation.

BUSINESS TECHNOLOGY CLIENTS

ADDITIONAL SECURITY SERVICES

Phishing Simulation & Awareness Training

Prevent and protect your business through practical phishing attack training sessions.

Threat Intelligence

Our threat intelligence solutions gather raw data about emerging and existing threats, both internally and externally, helping you identify possible weaknesses, such as leaked credentials or newly identified exploits. In doing this we can help you prepare, prevent, and identify the threats that could take advantage of your valuable resources.

Gap Analysis

In undertaking a Cyber Security Gap Analysis our secuity experts will help you determine the difference or 'gap' between your organisation's current and ideal state of business technology security.

Managed Security Operations Centre

Our managed Security Operations Centre provides businesses of all sizes with enterprise-level threat detection and incident response capabilities, without the need for heavy internal resourcing costs.

Cyber Essentials & CE PLUS

Cyber Essentials is a national, government-backed certification that helps organisations safeguard their systems and employees against the most common types of cyber attack - and we'll take you through the process.

London
0207 043 7044
hello@stripeolt.com

Bristol
0117 974 5179
hello@stripeolt.com

STRIPEOLT.COM