secarma
CYBERSECURITY EXPERTS

SERVICE OVERVIEW

Security Awareness Training

Secarma's expert training team regularly run hands-on security awareness courses across the UK and remotely. Our training sessions feature an in-depth look at the security threats that modern businesses face, including an overview of hackers' motivations and methods. By learning to identify potential attacks, your workforce can become your organisation's strongest line of defence.

WHO IS IT FOR?

Our security awareness training course is for non-technical staff and is designed to give them up-to-date knowledge on the latest (and the well-established, but effective) security threats.

While the course is aimed at your non-technical teams, the session still covers aspects of advanced security awareness. Business security is everyone's responsibility within an organisation, so it's important to increase cybersecurity awareness at every level. We don't believe in oversimplifying security; because we're a team of penetration testers, we'll show your staff how an attack is carried out, so they get a better understanding of how it works, and therefore how to avoid it.

HOW CAN WE HELP?

We teach your staff why and how cyber-criminals may target your organisation, and arm them with the skills to protect your business.

You may have invested in the latest technology to keep your systems secure, but humans are still the weakest link in the security chain. We work with your teams to give them up-to-date knowledge on the latest and most effective threats that modern businesses are up against, and the part they play in defending against them.

As penetration testers, our experts draw on their own experiences, plus real-world examples to give your staff an idea of what an attack may look like.

WHAT WE TEST

Our security awareness training session provides an in-depth look at the following:

- **Why Hackers Hack**
  Covering a host of different reasons why a threat actor could target your organisation - there's more to it than just financial gain.
- **Potential Damage**
  Using real-world examples, we'll cover the potential damage a hacker could do once they've worked their way in to your systems; from ransomware, to defacing your website, to a dreaded data breach.
- **Types of Attack**
  An in-depth look at the different methods used to strike an organisation, including:
  - Exploiting insecure wireless
  - Physical access - tailgating and beyond
  - Sophisticated social engineering campaigns - targeting and tricking a user via email, text, social media, over the phone, and more.
  - Exploiting weak passwords
  - Exploiting known (and unpatched) vulnerabilities

Our sessions are completely customisable, so we can add specific sections and tailor the course to your organisation's needs.

- **Fighting Back**
  Not only will we show your teams what to look out for, but we'll also teach them how to stay vigilant against threats. This includes strong password policy, physical access prevention, and the importance of patching.