



SECURITY
AWARENESS
TRAINING

Fun & engaging training delivered by experts

Educating employees on the importance of cyber security

Cyber security awareness training for staff is a critical (but all too often overlooked) part of protecting a business. Our awareness programme uses a range of fun, engaging methods to educate employees on their role in keeping the business they work for safe.

Our methods teach best practice about data storage, application downloads, passwords, spam email, backing up work and much more. We find this is best delivered through practical exercises such as simulated phishing attacks and testing users' passwords with our password cracker.

Keeping security in the forefront of employees' minds and driving home the importance of due diligence is imperative.

It's a fact that your end-users are the weakest link in your network security. The strongest defences are rendered useless if an attacker can dupe an employee into handing over login details.

The threat to UK businesses is real and we are working with organisations to help them stay one step ahead of cyber criminals. Being cyber secure no longer needs to feel daunting. Our team of specialists are on hand to guide you every step of the way.

At a glance

- Make staff cyber-aware
- Education is key
- Regular cyber security promotion
- Simulated attacks to raise awareness

Our Education Service:

Monthly phishing attacks – company wide

We'll attempt to compromise your users' accounts and identify employees who are not working with cyber security in mind and have weak passwords and network security. Month-on-month an improvement in employee cyber behaviour is expected.

Bi-annual spear attacks – high risk departments

Typically targeting departments that have access to business finances, we'll attempt to scam specific groups of employees and steal data. Issues can be quickly pinpointed and addressed with departmental training.

Annual whaling attacks – executives and directors

Once a year we'll target your executives and directors with sophisticated attack methods. The higher up the chain an employee, the more access they have to valuable information and the more to gain for the attacker. All outcomes will be reported on and training provided to prevent repeat incidents.

Quarterly password check

Four times a year we'll run state-of-the-art password checker to pinpoint passwords that do not adhere to password protocols. We'll inform employees that need to change their password and offer advice on how to set a secure but memorable password.

Bi-annual USB drop & desk check

Twice a year we'll arrange formal opportunities for staff to rid themselves of USB drives, also known as flash drives or memorysticks. They pose a big security risk to businesses; plug in an infected USB drive to a computer and you could cripple your whole network. We'll also take a look at your work spaces to ensure best practice for secure working is being followed.

On-demand video training

Access to engaging video content on the issues around cyber security. Available on-demand to all staff, or purely to those with learning requirements.

Quarterly cyber security newsletter

Delivered every quarter to your employees with useful hints, tips and ideas for working securely.

CyberGuard Technologies - Raising visibility, managing threats

“ Being 97% secure also means
being 3% insecure! ”

Source: Law Gazette, February 2017



Expert security advice available

It's a fact that your end-users are the weakest link in your network security. So what are the most common ways employees are targeted by cyber criminals?

- ✔ Ransomware
- ✔ Malware
- ✔ CEO fraud
- ✔ Compliance failure
- ✔ Phishing attacks
- ✔ Spear phishing attacks
- ✔ Executive whaling
- ✔ Social engineering



Our cyber security
experts are waiting to
hear from you:



01299 873 805



security@cg-tech.co.uk



cg-tech.co.uk