ramsac
the secure choice

Cybersecurity training from ramsac

The Information Commissioners office (ICO) is the UK body that is responsible for prosecuting organisations that fail to keep data safe. They have recently mandated that staff and volunteers that have access to data, should receive cyber awareness training as part of their induction, and before they are given such access. Furthermore, they mandate that training should be ongoing for all employees, and that an organisation should be able to demonstrate completion of training and management of non-attendees.

Employee training and awareness are essential parts of your organisation's cybersecurity. Organisations collectively spend millions of pounds a year on firewalls, anti-virus solutions and security services, but they remain vulnerable because of one key factor: human error.

At ramsac we run a wide range of cybersecurity training courses offered either as in person workshops, online presentations or online learning to help protect your organisation against cybercrime.

ramsac
the secure choice

ramsac
the secure choice

Cybersecurity Board Briefing: The Human Firewall

Objective: This workshop on Cybersecurity has been designed to equip senior business leaders with vital skills and essential knowledge necessary in today's fully connected business environment. The agile nature of business, along with remote working technology, has left more companies open to the risk of cyber-attacks and it is vital that we understand the problem, know how to plan for it, talk about it and start to take action.

Course objectives: To equip attendees to;

- Understand how cybercrime can and will impact your business.
- Have an awareness of the latest scams being targeted at businesses of all sizes.
- Have the ability to direct and prepare for cybersecurity risks, knowing how to talk both to IT and the rest of the business.
- Understand the impact of cyber with regards to GDPR.

Outcomes: To equip attendees to;

- Understand current cybersecurity risks and how to mitigate them.
- Have an easy to understand approach for preparing for a cybersecurity attack.
- Have reassurance and confidence in a must-know subject with plenty of tips and useful anecdotes.
- Understand what needs to be done with cybersecurity for the GDPR

Learning format: Workshop aimed at the board of directors, partners or senior leadership team. With discussion and planning to leave the group with an understanding of their responsibilities, a plan for what they should do to protect their organisation from cybercrime and advice on what to do in the event of a cyberbreach.

Duration: 3 hours

Cybersecurity Board Briefing: Cybersecurity: A 10 Point Plan

Objective: This is a shorter workshop which is practical and a highly valuable session that works brilliantly as a remote session and can be delivered in 90 minutes for those who want a shorter speaker session. Vigilance starts in the boardroom and it is crucial that the C-suite take an active role in understanding the level of risk they are exposed to and establishing a meaningful and effective strategy.

The session is engaging, entertaining and thought provoking. At the end of it, delegates will have a checklist of at ten things that they should be doing in their business, questions that they need to be asking of their IT advisers and a strategy for minimising risk of prosecution.

Course objectives: To equip attendees to;

- Understand their liability and risks with regards to cybercrime
- Hear about the latest scams and cybersecurity risks
- Consider the additional challenges of a Work from Anywhere/Home culture
- Understand what the ICO and Insurers expect to see in play

Outcomes: To equip attendees to;

- Have a 10+ point action plan/check list
- Better understand the business challenge and how to tackle it at all levels.
- Know how to challenge and question your IT advisers (internal or external)
- Feel comfortable talking about a subject that may be alien to them
- Attendees with a cybersecurity background themselves will have a methodology for talking to businesses in a way that they understand and act.

Learning format: This workshop is suitable for all directors and board advisors, it can be consumed as a stand-alone session or in addition to the Human Firewall workshop

Duration: 90 minutes.

Cybersecurity Employee Briefing

Objective – To introduce the importance of cybersecurity and show employees how to be vigilant to protect themselves and the organisation they work for from cybercrime.

Outcomes: To equip attendees to;

- Understand how cybercrime can and will impact your workplace and personal life.
- Have an awareness of the latest scams being targeted at businesses of all sizes.
- Understand what steps you can take to protect yourself

Learning format: Workshop format available in person or online

Duration: 60 or 90 minutes.

Staff Induction Cybersecurity Training

Objective and outcomes: The Information Commissioners Office (ICO) now mandate that all staff should receive cyber awareness training as part of their induction to your organisation, and that this training should happen before they are given access to any databases. Furthermore, you should be able to evidence that this training has taken place. Our Induction training subscription will provide you with a personalised training video that you can integrate to your induction programme, and an online quiz to check learning which will result in a completion certificate being issued for your records.

Learning format: Video updated annually to reflect latest risks and cyber trends.

Duration: 60 minutes.

ramsac
the secure choice

Cybersecurity ‘speed awareness’ training

Objective: Cybersecurity Training is critically important in the battle for cyber resilience; indeed, it’s mandated under GDPR/DPA and should you suffer an incident, the ICO expect you to be able to prove that you and your business take this seriously.

We know that in every organisation there are two types of problems that hinder this. The first is your colleague who never takes part in the online training you’ve provided, the second is the one who repeatedly fails the cybersecurity tests or phish-threat exercises.

Unfortunately, when you have a breach, if you are a director or organisation official, their failings are your problem.

To assist you with this scenario we’ve created a training session which is delivered live online. Think of it as a speed awareness course for your repeat offenders! Book in as many colleagues as you wish and we’ll invite them to the next available course. We’ll issue a certificate of completion after the event so you can evidence their awareness training if the ICO ever ask you to do so.

Outcomes: Attendees will have a greater understanding of cyber security risks, GDPR compliance and the vital part they play in keeping your organisation safe from cybercrime.

Learning format: We run these sessions each quarter, they are delivered via Teams

Duration: 60 minutes.

ramsac
the secure choice

Cybersecurity awareness training

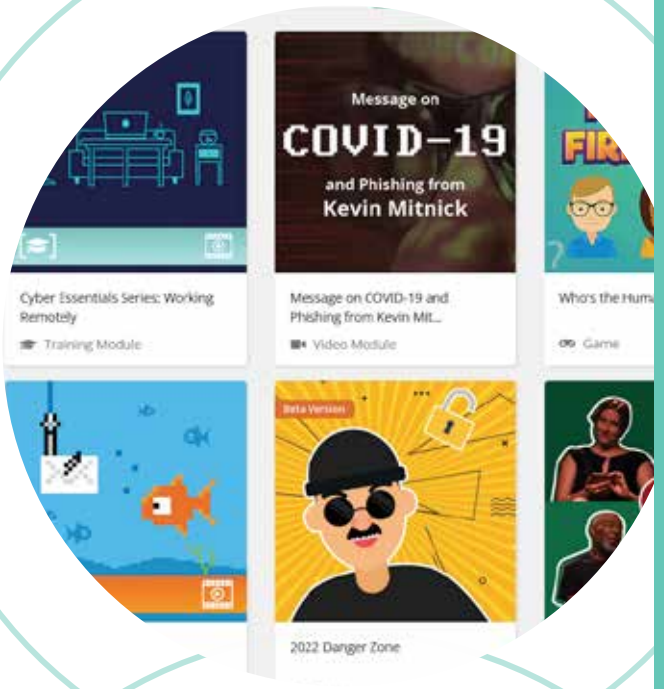
ramsac
the secure choice

What is the training?

ramsac have partnered with KnowBe4 – who offer the world's largest library of cyber training, on a platform that automates most of your management obligations.
KnowBe4 offers a vast library of content, including interactive modules, videos, games, posters and newsletters. Organisations can tailor training campaigns which can be scheduled to land in a user's inbox each month. The interactive training gives users a fresh new learner experience that makes learning fun and engaging, with our own favourite being a series of learning that feels more like watching a Netflix drama! And in the background, the platform records who has and hasn't completed the learning, and reminds non attendees – and their manager, if they are falling behind.

What makes it so effective?

This is not tech heavy, dryly delivered content. The most popular resource is 'The Inside Man' an award-winning original series that delivers security awareness principles embedded in each episode that teach your users key cybersecurity best practices and makes learning how to make smarter security decisions fun and engaging. From social engineering, insider threats and physical security, to vishing and deepfakes: 'The Inside Man' reveals how easy it can be for an outsider to penetrate your organisation's security controls and network. But it's delivered in a way that's entertaining – meaning users won't resent the activity and learning happens without feeling like an arduous task.



And because it's delivered regularly for a few minutes each month, it keeps the subject matter fresh and at the front of mind – and it stays up to date with changing threats and trends.

Learning format: Videos delivered monthly directly to users inbox

Duration: 5 -10 minutes.

Phishing awareness training

Objective: Phishing emails are becoming more sophisticated and harder for a user to spot, resulting in an increase in successful cybersecurity breaches. The key to protecting your data is ensuring that your staff know how to spot a fraudulent email and how to keep your business safe. That is why we offer a testing and awareness subscription to increase cybersecurity awareness and to train your "human firewall".

Outcomes: We will carry out random simulated phishing attacks, ensuring that every user receives a very realistic phishing email at least twice a year. The emails mimic real phishing emails and if the user clicks on a link they will be taken to a safe web page, that highlights what they have just clicked on and offers them an immediate online training session on how to spot attacks in the future. You will receive a report after each campaign showing you how many emails were sent, how many were opened and who clicked on links within the emails. The report will also show which users have undertaken the online learning

Learning format: Realistic phishing emails sent at least twice a year

ramsac
the secure choice

About ramsac

ramsac has a clear mission
- to be at the heart of IT

ramsac provide so much more than just IT support. We help our clients to get the best out of technology – implementing, managing and supporting secure, resilient, flexible IT solutions. We work with small and mid-sized organisations, providing them with strategic IT input, proactive management, jargon-free IT support and solutions that help them to grow their own organisations efficiently and securely. Our exclusive Cyber Resilience Certification programme helps organisation achieve the highest level of cybersecurity protection and allows them to demonstrate their commitment to their own stakeholders via our Gold certification standard.

Whether it's designing a new infrastructure, migrating services to the cloud, implementing enhanced security practices or providing end users with really efficient and friendly 24 hour IT support, ramsac manages IT on your behalf, so that you can focus on achieving your organisation's goals, safe in the knowledge that IT is secure, staff are working efficiently, and the IT investment is delivering tangible benefits to the business.

More information

For more information on ramsac's cybersecurity training courses please contact ramsac on
01483 412040, **email info@ramsac.com** or visit **ramsac.com**

ramsac
the secure choice

ramsac Limited
Godalming Business Centre
Woolsack Way
Godalming, Surrey
GU7 1XW

www.ramsac.com
01483 412 040

ramsac
the secure choice