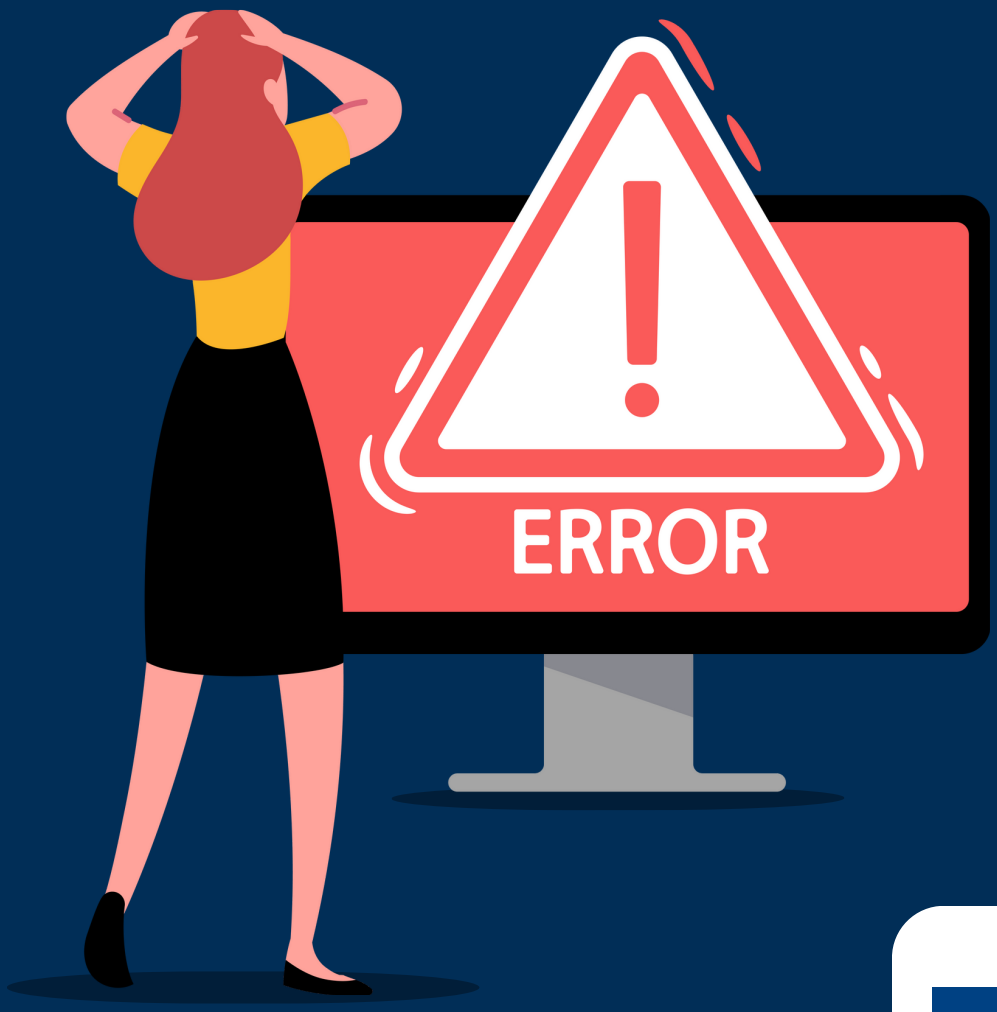
Human error. Your biggest cyber security risk

Why cyber security awareness training is so important for **you and your staff**



Shepherd IT
Securing your business

It was just an invoice. Nothing strange about that. And it didn't ring any alarm bells that the CFO emailed the accounts team asking for it to be paid urgently to keep a supplier happy. Oh, and they've switched banks – so if you could just update their details, that'd be great.

It's a small company where everyone knows everyone, so there wasn't a red flag in sight.

But something was very, very wrong.

Those new payment details belonged to a criminal gang. And the email didn't come from the CFO. This was the final step in a clever phishing scam known as CEO fraud, and it just cost the company thousands.

The crooks had gained access to the CFO's email account, intercepted a message and changed information to redirect a payment.

As is usually the case with cyber crime, it was simple human error that opened the door to the crooks.

No one knew to look for the warning signs that something wasn't right. And there was no policy that required everyone to confirm payment requests in person when details have to be changed.

This was a financial fraud. But every day the criminals are after more than just your money. Your business data is just as valuable to them, and they'll go to great efforts to get hold of it.

Small and medium-sized businesses are the most likely targets for all kinds of cyber attack – not just phishing scams like this one. That's because cyber criminals know that these companies are likely to have weaker security measures in place and will spend less time training their people.

The crooks know that your people are the weakest link in your security chain. Not because they'd do anything malicious, but because they're only human. Without training, they simply don't know the risks to look out for, or what they can do to keep your business safe.

That's why good cyber security awareness training – for everyone in your business – is vital.

Here's where to start

Find your baseline

Your training sessions needn't take a long time. But they need to be prepped properly.

Start by working out what your people's awareness levels currently are, and where you're exposed to security threats. It's an important part of the process and may open your eyes to some surprisingly risky behaviour.

You need to find the baseline level of staff cyber security knowledge – some people may be starting from zero. And if you're aware that your own knowledge has gaps, this is the point to seek some professional help.

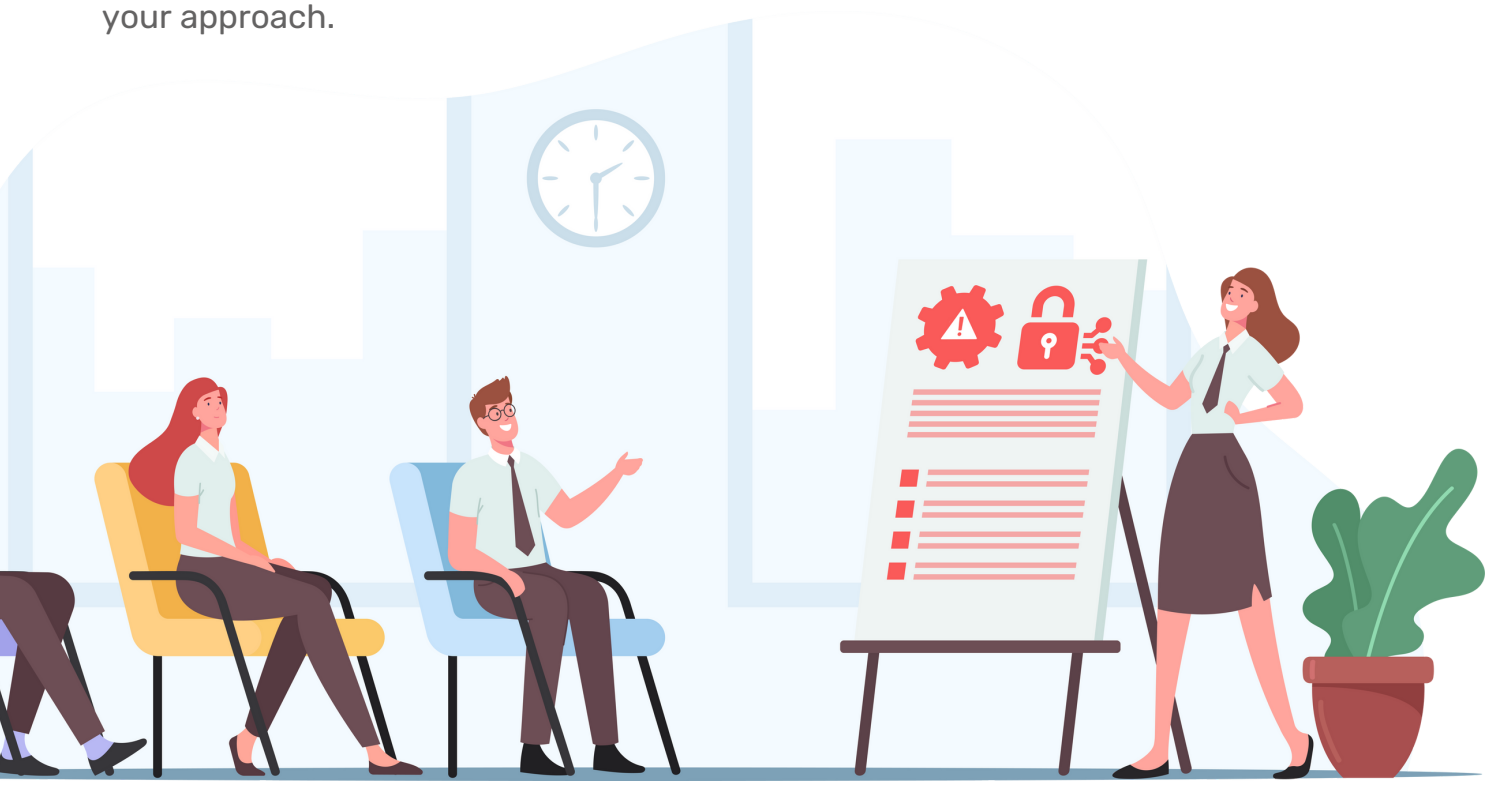
Examine the way everyone works to understand which risky behaviours are a threat to your business. There are countless kinds of cyber attack to protect against, so you need to be systematic in your approach.

Look at:

- Emails, communications and file sharing
- Logging-in behaviour
- Attitudes to policies around data protection and information handling
- General awareness of cyber threats
- …and more

Every business is different, so you should create your own priorities according to your needs.

Observe their behaviour rather than simply assuming that policies are being followed. That will give you the best idea of where your vulnerabilities lie, which can then give shape to your training sessions.



Assess the risks and prioritise

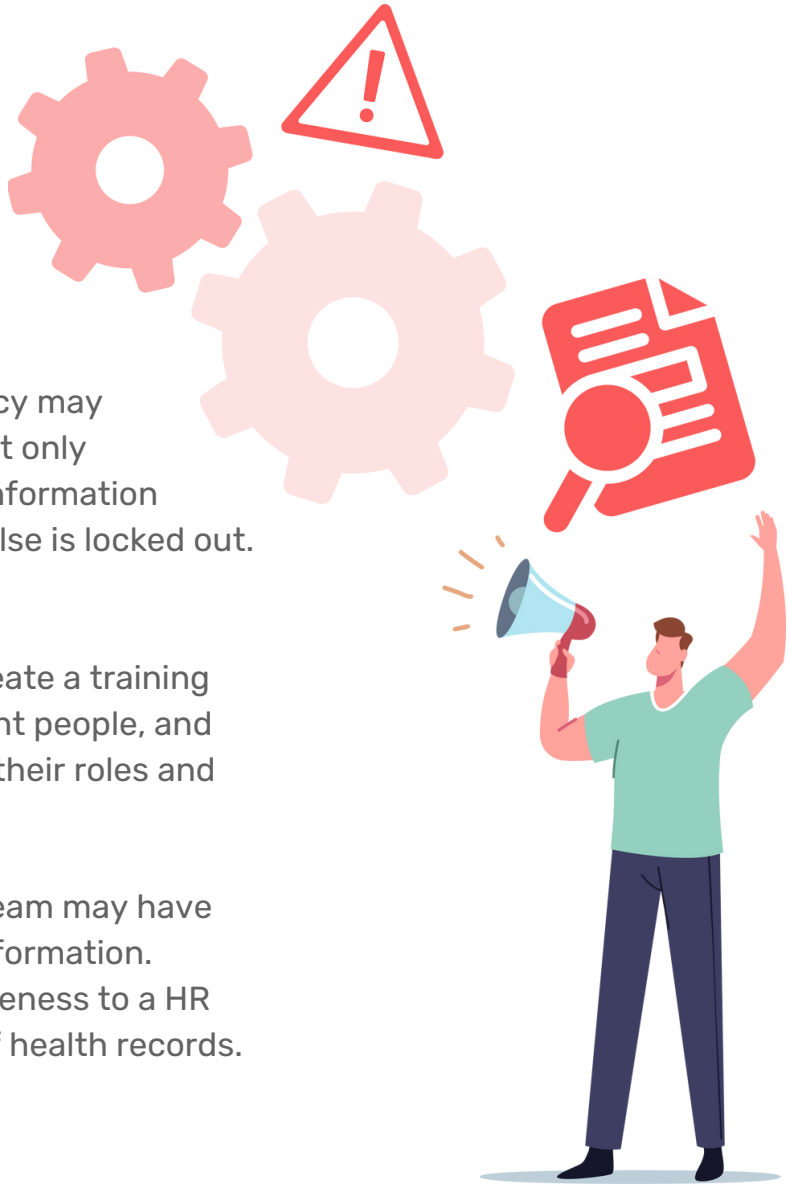
When you've taken the time to observe and understand your people's current security behaviours, you'll need to look at the most pressing risks you face.

There are security threats on many fronts. Prioritise training on the most immediate weaknesses, dealing with any obvious knowledge gaps first.

Risk assess your current systems, your network, and your digital assets. Look also at who has access to what information and why.

Re-assess as you go

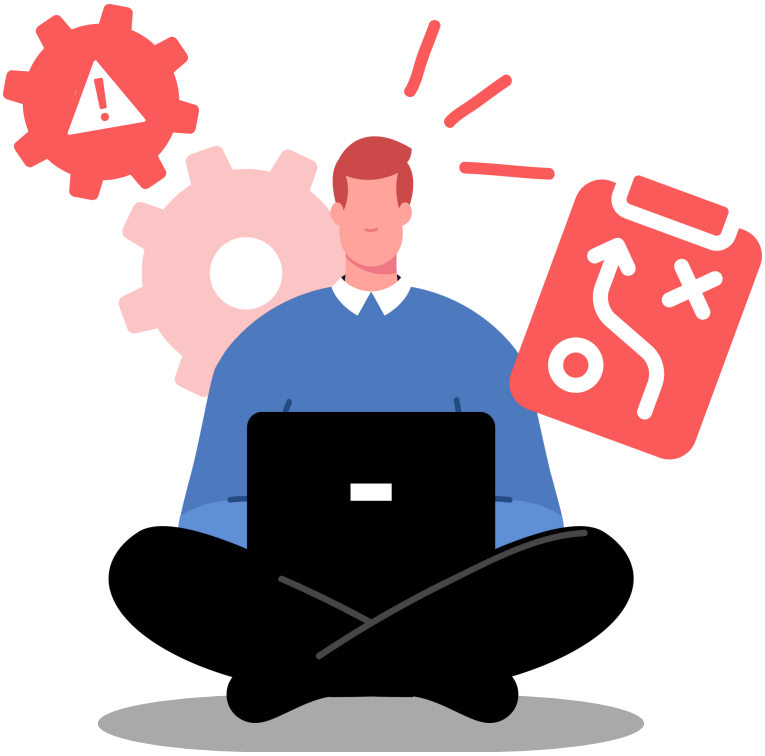
If you're dealing with sensitive data of any kind, take this opportunity to look at your wider policies alongside your training plan.



For example, a zero-trust security policy may be appropriate for you. This means that only people who need access to sensitive information are able to access it at all – everyone else is locked out. More on policies later.

These assessments will help you to create a training programme which is tailored to the right people, and pitched at the right level according to their roles and responsibilities.

For example, a warehouse fulfilment team may have access to private customer address information. That requires a different security awareness to a HR manager with access to sensitive staff health records.



Create your training plan

Once you've got to grips with the needs of your different employees and the wider business, match them with the resources available to you to create a training plan.

Lay out your objectives – the skills and knowledge you need to develop – as well as the attitudes and behaviours that you need to see at work.

Then break each objective down into topics or modules. For example, there may be a module on phishing emails, and one on data classification (where your data is grouped according to how sensitive it is – staff sickness records, customer financial information, sales process documents).

Sessions can be online or in-house and, where possible, training should be interactive and hands-on to help people retain information. Reading a guide or completing a workbook alone is unlikely to help someone understand and retain what they've learned.

But while the training should be as enjoyable as possible, the subject is a serious one.

So always reinforce the fact that the consequences of any data falling into criminal hands can be disastrous for a business. That's why, once everyone is trained, there should be clear repercussions for anyone who doesn't put that training into practice.

Begin training

Everyone should understand exactly why training is being introduced, the range of threats faced by the business, the desired outcomes, and the benefits both to employees and the company.

You may plan to carry out some or all of the training yourself, but more likely you'll bring in outside expertise. This will save you a lot of time, and reassure you that everything is being covered and that training materials are up to date. The training provider should work with you beforehand to cover everything you identified in your risk assessment and to suggest any additions.

Remember that training should be embedded for everyone in the business, so it should become part of your employee onboarding package, as well as part of the transition process when people change roles.

If you have an IT support provider they may offer this type of training and will already have some familiarity with your systems.

If you don't have an IT expert on hand, get in touch with us – our contact details are on the back page.

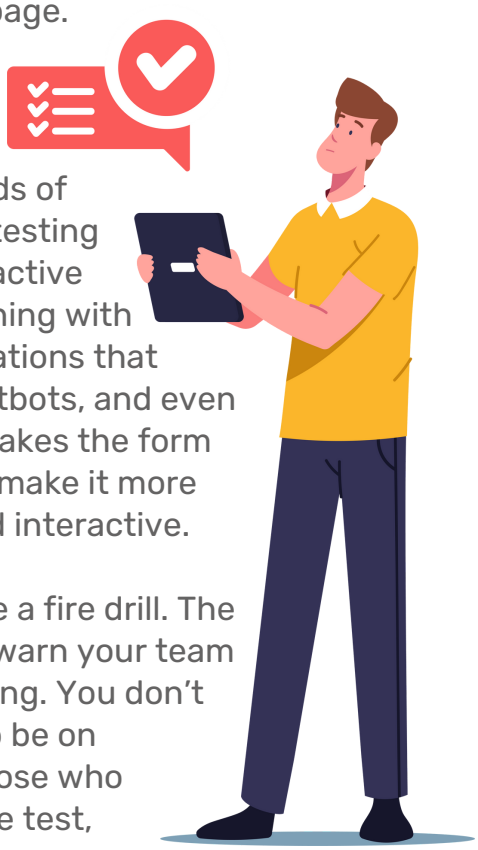
Put it to the test

When you've invested time and money into training, you want to be sure that it's doing its job.

Periodic written tests and quizzes are good, but a really effective way of finding out if your people can put their training to use is with a simulated phishing attack. There are platforms available to help you do this. There's also a lot you can do yourself.

A simple phishing simulation might just involve sending everyone an email with the aim of tricking them into taking action. It could invite them to click a link for a gift card as thanks for their hard work, or ask them to reconfirm their login details.

You can see who takes the bait, and who uses their training to spot the scam and take the required action.



Other methods of training and testing include interactive phishing training with online applications that work like chatbots, and even testing that takes the form of a game to make it more engaging and interactive.

Think of it like a fire drill. The key is not to warn your team a test is coming. You don't want them to be on guard. For those who don't pass the test, further training may be necessary.

Create new policies

If you don't already have a cyber security policy that sets out your expectations, it's time to create one.

Your policy should be detailed, but easy to understand. Describe the security controls you have in place and the threats they address. Include who is responsible for maintaining them, how incidents should be reported – and who to – as well as the consequences of not reporting a potential cyber security risk or attack.

Highlight your expectation that your people should use your security measures, follow protocols and use best practice at all times. Again, include the repercussions if someone knowingly fails to do so.

Include a remote access policy, acceptable internet use policy, and information about how updates are managed.

You may also consider a section on personal devices being used for work purposes, and how they should remain secured to protect company data.

Most people on your team will take protecting the company and its data seriously. But it's common for there to be an individual or two that won't. Enforcing your cyber security policy will make sure everyone recognises its importance and the serious risks you're protecting the business against.

When things are laid out clearly to employees, they'll feel more involved and more motivated to help protect the business… and they'll know the consequences of intentionally not doing so.

Stay updated

Cyber security training is never a set-and-forget thing. New scams and security issues arrive all the time, so keeping your people aware of the things they should be looking out for is crucial.

Plan for quarterly or six-monthly refresher sessions for everyone, from your apprentices to the people at the very top. This will ensure everyone has the most up to date cyber security knowledge while also, once again, reinforcing the ongoing seriousness of the threat.

Between sessions, keep everyone updated on the latest cyber security news. Share news stories of big data breaches, new malware and scams, and even insights on the security measures you use. You can set up news alerts or take a weekly scan through tech news sites – it's extremely worthwhile.

Creating your cyber security training plan is something that takes time and a fair amount of effort. But, done right, it plugs one of the biggest security holes in any business – human error.

A good IT support expert can help make the whole process run smoothly from first thoughts to routine refresher training.

If you'd like to know more about how we can handle cyber security training for your people, get in touch.

CALL: 01256596525
EMAIL: hello@shepherdit.net
WEBSITE: www.shepherdit.net

Shepherd IT
Securing your business