Nine ways

to get your staff on board with cyber security

Expert information and advice brought to you by:

iceconnect

Your Local IT Experts

020 3358 0000 | iceconnect.com

Nine ways

to get your staff on board with cyber security

Think you've got your cyber security covered?

Think again.

New strains of malware are constantly being discovered. That's because as businesses of all sizes have stepped up their cyber security software and procedures; hackers have upped their game, too.

The cyber threat landscape is constantly evolving. So it's imperative that you have an arsenal of weapons like firewalls, endpoint security, anti-virus software and email encryption to keep your data safe.

But that's only the start.

If you're going to stay ahead in the war against cyber criminals, it's essential that everyone in your business who goes anywhere near a computer or device is on board.

Your IT set up is only ever as strong as your weakest member of staff. And just one well-intentioned but badly trained person can undo all your hard work – and cost you a small fortune – in a matter of minutes.

Despite the constantly growing risks, there are still plenty of people who see cyber security as a lot of fuss about nothing, or "not my problem". And then there are those who struggle with anything vaguely techy and make silly little mistakes that can go on to cause huge problems for their business.

Nearly half of all cyber attacks are targeted at businesses with 250 employees or less. Why? Because smaller businesses often think they're not big or interesting enough for the hackers to target, so they don't take it seriously. And just like all criminals, cyber baddies like to look for easy targets. They know that smaller businesses don't always have much in the way of training budgets, which means lots of lovely ill-informed computer users to take advantage of.

The only way to keep your valuable data safe in 2020 is to promote a culture of cyber security awareness

But let's face it, it's not easy.

Getting everyone in your team to take cyber security seriously can feel like you're fighting a losing battle. Like any new initiative, there will undoubtedly be some resistance.

Nagging rarely works, and adopting a heavy handed approach like threatening disciplinary action if they fail to comply is likely to make some staff members down tools altogether.

But if your business is going to stay safe from cyber crime, you need to make sure that everyone – from the interns, up to senior executives and board members - are on the same page when it comes to cyber security.

When you meet a little bit of resistance (and you will!) think creatively about how to keep them engaged without feeling like they're being nagged.

Here are nine ways to change the way your employees think about cyber security and make it part of your business's culture.

1

Share information

Sure, cyber security can be complex. But that doesn't mean you should assume your employees won't be able to understand it or should be kept in the dark about the nitty gritty.

If you keep cyber threats to yourself just because you're the boss, you're not only in danger of alienating your employees and seeming elitist, but you're also missing an important fact.

Your staff are your most valuable defence against attack (and potentially your weakest link) so there should be no secrets when it comes to cyber security. This is a battle you have to fight together. Talk to your people about the latest threats and how hackers are constantly trying to find their way in, and you might be pleasantly surprised by how interested they are.

No-one wants their employer to go through huge pain, as it will directly affect them too.

2

Make it personal

We humans can be pretty selfish at times, especially when there's lots to do and not enough time. Employees are much more likely to care about issues that affect them personally, so it's important to explain the link between your business's data and their own.

Hackers are just as interested in employee data as they are company information - and your staff need to understand that. If they want to keep their own details safe, they need to understand the basics of cyber security in the workplace too.

3

Lead by example

Taking the “Do as I say, not as I do” approach is always going to rub people up the wrong way. And where cyber security is concerned it’s also a recipe for disaster. As the leader of a business or team it’s up to you to set a good example. So always be seen to do things properly.

At the very least, that means never sharing your password, actively participating in cyber security training programs and checking twice before you click on any link. Business owners and top tier executives are just as vulnerable to attack as anyone else. And if you’re the reason a hacker gets in... you’ll never live it down

4

Implement an easy to understand policy

You can’t expect people to behave in the right way if you don’t make it clear what’s acceptable in the first place. So create a policy document that’s easy to read and is shared among everyone in your business.

This should outline acceptable behaviour, standard practice and information on what to do in the case of a possible data breach. It should also clearly explain why multi factor authentication is best practice, and how you will enforce your policy.

5

Drill it in from the start

As the old adage goes, it’s never been easy to teach an old dog new tricks. Ingraining policies into existing employees’ minds is never going to be as easy as it is with your latest recruits. So take advantage of new blood.

As soon as a fresh team member starts in your business make cyber security a priority. So they don’t learn bad habits, and understand exactly what’s expected of them from the word go.

6

Make it regular

Unless you build regular cyber security awareness sessions into your diary it's likely that good intentions will soon fall to the wayside. The threat landscape is constantly changing. So you'll need to run an ongoing programme which allows everyone to get together to learn about the latest cyber attacks and how to spot them.

7

Start with the basics

Never assume that you're making it too simple. For everyone in your business to understand how to keep your (and their) data safe it's important to begin with the very basic stuff, like password management and security patches. Once you have a simple framework that everyone can understand, the more complex bits will fall into place much more easily.

8

Offer rewards

It doesn't have to be much, but a little thank you goes a long way when it comes to keeping your team on side. You can build good cyber security practices into your appraisal programme, or even encourage staff to look out for vulnerabilities in your system – and have a clear way to report them.

Try offering a monthly prize for anyone who spots a potential security risk and shares their findings. It's a great way to keep people engaged and informed. And will allow you to keep on top of problems in your system.

9

Run drills

Just like you have regular fire drills, it's a good idea to simulate cyber attacks too. Organising drills and fake hacks can help you monitor any gaps in knowledge, so you'll all be better prepared when a real attack happens.

9 simple ways to influence the way your staff think = one big outcome

Cyber security awareness is about a combination of knowing and doing. When that awareness becomes a part of your business's culture, your staff are much more likely to make good choices. Ultimately, we're all in this together. So understanding how to recognise threats is good for everyone.

Creating a cyber security aware culture doesn't mean you will be completely immune to cyber attacks. What it does mean is that you'll be much better placed to handle them when they do happen.

As the local experts in IT security, our goal is always to provide businesses with the tools they need to protect themselves against the ever growing threat of cyber attacks.

For us, that's about much more than simply putting the right defences in place. It's about sharing our knowledge too. When your team is properly educated about cyber crime, you'll sleep more soundly at night.

Contact us today to find out how we can help YOU sleep more soundly at night.

Expert information and advice brought to you by:

iceconnect

Your Local IT Experts

020 3358 0000 | iceconnect.com