net technical solutions

The ultimate secret

to keeping your business data safe

net technical solutions

As business IT professionals, we've seen some things.

Things that would horrify you.

Things you would never want to encounter in your own organisation.

We're talking security breaches, data theft and file corruption. Activities that have brought entire businesses to their knees.

This is something that you really wouldn't want to happen.

It only takes one click on a bad link from a well-meaning member of your team and it could mean the difference between a thriving business and disruption so severe, it makes trading impossible.

We also know that data loss can lead to a huge loss of confidence from your clients.

And often the cost of rectifying a situation such as this can be phenomenal.

So we want to share

the secret behind keeping your business data safe

Let's assume you have a blended IT Security package in place right now, providing the right mix of security products that protect you and your team, without inconveniencing you while you're trying to work.

But there's something else, that in our view every business should invest in, every year.

Cyber security training.

Though it may sound simple, you'd be surprised to learn how many businesses underestimate the importance of **company-wide security awareness.**

And yes, we really do mean company-wide.

Your whole business, from the new entry level person to the CEO, should take part in formal data security training on a regular basis.

A strong cybersecurity culture is one of the best ways to keep your business safe from the increasingly sophisticated threats out there.

Hackers use automated tools to look for vulnerabilities in every business, all the time.

And this includes yours. Remember, it only takes one click from a well-meaning member of your team on one bad link. And that can unwittingly let hackers into your system.

“But my people are savvy professionals. They’re not going to fall for a scam”

We hear this often.

And yes, your people are savvy, but so are cyber criminals.

Cybercrime is evolving and there is always another scammer or hacker around the corner waiting to take advantage of a technology flaw or stressful situation (such as the global pandemic).

Your business can never be too prepared.

Take a look at **phishing** for example. You’ve heard of that, right?

But do you and your team actually know what it is?

Phishing is a common tool used to extract information such as login credentials or credit card details by email, telephone or even text message.

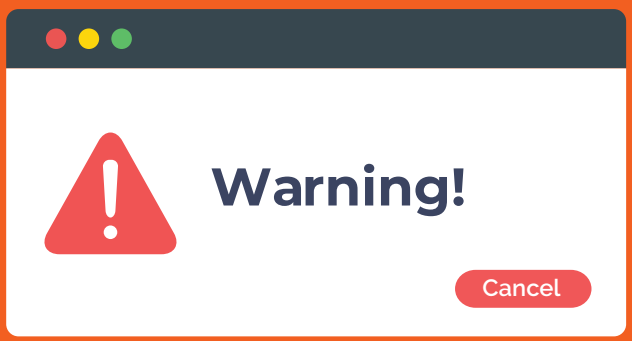
You may think that your team are above falling for an email from their ‘long lost uncle abroad’. But phishing scams have come a long way since those days.

Today, phishing emails are far more convincing. They often claim to come from someone credible, such as your bank, a client, or someone else you know.

They’ll ask you to click a link to update your details, or change a password. However, instead of being taken to a legitimate website, you’ll be taken to a very convincing duplicate.

And once your details have been entered, you’ve given them away.

Other times, you’re sent an attachment - again, seemingly from someone you know - which, when opened, will install malware on your device (or across your whole network).



This can then allow criminals to steal data or deny you access to your own information (that's called **crypto locking).**

Then we have **spear fishing.** Instead of phishing, which is aimed at anyone, this is targeted at specific individuals.

Typically the attacker has spent time learning a lot of information about you (your name, role, company information, etc), and then uses this to their advantage.

If they target someone at the top this is called **whaling** (also known as CEO fraud).

They're targeting people at the top as they have access to the most sensitive data.

Whaling attacks are often planned for a long period of time. And when they work, give huge financial gain to the cyber criminals.

Then there's **pharming,** which asks you to take an action on what looks like a familiar website.

Except if you look very carefully, the website address is slightly different from normal. It's a scam site, and any information you enter will go to the criminals.

There is a worse version of pharming where the criminals manage to divert traffic going to the real website. These are really hard to detect.

Often there are tiny little clues though that give the fake sites away, if you know what to look for.

Spoofing is the term for when you receive an email pretending to be from someone you know - such as your accounts department asking you to go to a link to reconfirm your details.

This type of scam is often used to download malware or ransomware rather than to steal your credentials.

Then we have **smishing,** which is phishing with text messages (SMS). And **vishing,** which is phishing on the phone or voice phishing. For example:

You receive a phone call from a blocked or unusual number. The caller will pretend to be from somewhere familiar and ask you to carry out actions or make a payment.

These are fairly common. So if you or your team are ever unsure, hang up, then call the company back on the number you have for them (and never the number the caller gives you).

Can your business really afford to underestimate the importance of good cyber security training?

As you can see, it really does take just one action to open up your business to this kind of threat.

This is not an exhaustive list. There are plenty of other ways that cyber criminals will attack your business.

You many think your people are hot on cyber security and hopefully you've got the latest security software protection across your whole network.

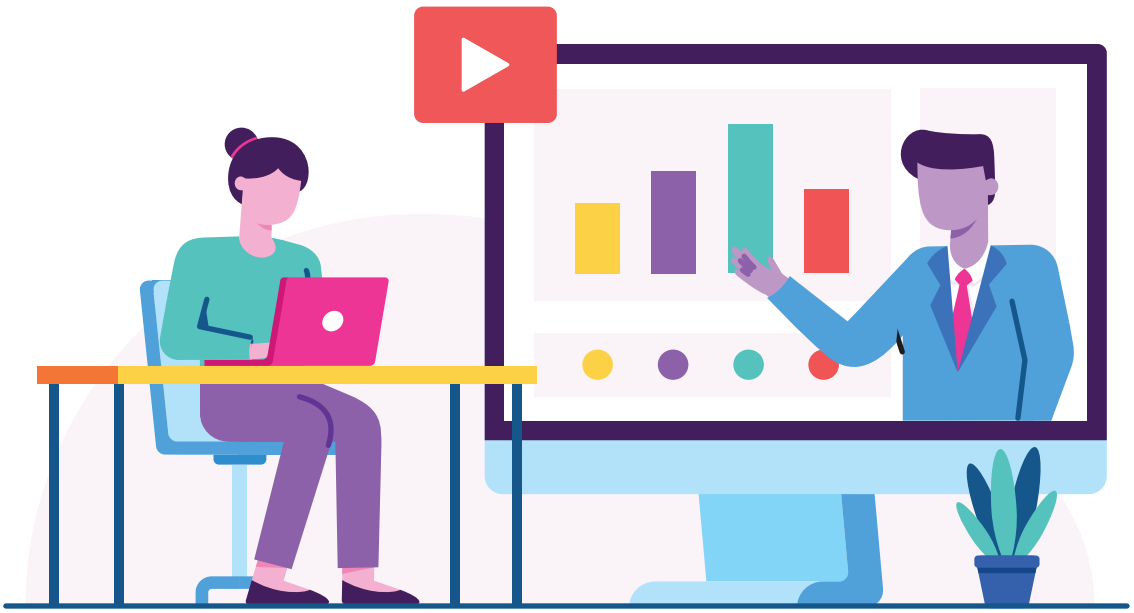
However, it's always a great idea to add another level of human protection. This is because businesses like yours really are prime targets for cyber criminals.

If you've never implemented security training before, now is the perfect time to start creating new habits. After all, your team will have seen enough change this year to be open to just about anything!

Employee education is one of the best business tools you can invest in. It could end up saving your organisation from disaster.

The benefits of regular training don't end there though. It's a great motivational tool, too. Your team will feel invested in when they have relevant training, increasing engagement all round.

Remember to make sure that everyone, from the bottom to the top, undertakes regular training. A cyber criminal really isn't fussy about who clicks that link... just as long as someone does.



If you would like us to deliver phishing awareness or data security training to your business, please contact us today.

Our team of experts is on hand to help keep you informed and protected.

01252 235 235
security@ntsols.com
www.ntsols.com

net technical solutions