Office 365.
A Risky Business?

lis Lodge Information Services

helping you get IT right

Imagine if you woke up tomorrow to find that your business had suffered a huge data breach?

That's:

customer data leakage, all your business information – financials, confidential material, EVERYTHING exposed for suppliers, customers, competitors to openly access!

What's more, you know this has to be reported to ICO as it's a massive GDPR breach.

Then of course there's the massive reputational damage! Without even having to pay any fines, we all know that once your reputation has gone, customers will very quickly disappear too.

So, before you know it, your business, your livelihood, life as you knew it is... DEAD.

Of course, it's not all doom and gloom. Prevention is better than cure, so they say and that's where you can win. In the war against cybercrime, which now accounts for over 50% of crime in the UK, you have to make sure you keep a tight ship, with the guards posted and alerts fully operational.

Quite simply, just having IT support to keep your systems in a working state, with a simple antivirus, is no longer good enough.

The question to ask is, what is the weakest link in your business?

You'd be wrong if you thought anything technology and right if you thought it's people.

You can put in the most sophisticated technology (and you certainly should make sure that is in place), but if you overlook the people element, you will most certainly fall victim.

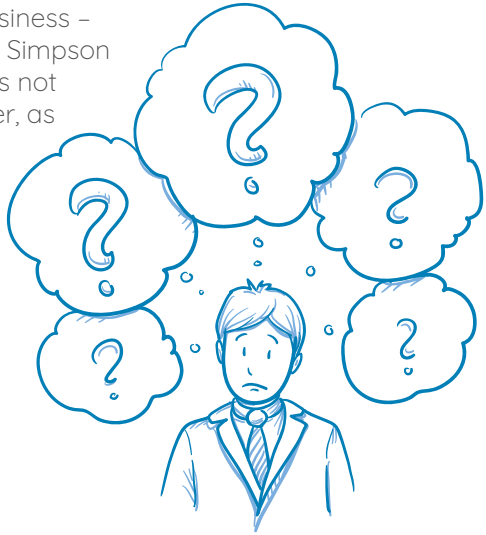
Cybercriminals are no longer doing scattergun attacks, just hoping to get lucky by someone clicking on a rogue link.

No, they are making targeted, strategic attacks on businesses. They find the right way to allure your staff into clicking a link to give away their usernames and passwords.

They are cunning social engineers, preying on human weaknesses and emotional vulnerabilities to give them a window of opportunity into your systems.

Can you be so sure that even if you wouldn't click a link, visit a rogue website, answer a suspect telephone call, use your business email address and password for personal stuff... that your staff would be so vigilant too?

Remember, you have to account for everyone in your business – that includes Homer Simpson in the corner! And, it's not all about being clever, as the true story below highlights about a team of solicitors who got caught out, big time.



It doesn't matter how clever you think you are:

A team of solicitors found this out the hard way, when they horrifyingly discovered that they had paid **£200,000** of a client's house sale money, into a cybercriminals account. Yes, that's right: £200,000!

Solicitors are clever people, just like you. They don't suffer fools, take short cuts or risk their clients' money, just as you wouldn't.

So, how had this happened?

Well, it may surprise you to learn that that average time a cybercriminal sits silently in a victim's account, watching and waiting for the right opportunity to strike is 197 days!

Yes, 197 days watching everything you are doing, without your knowledge. One of your staff is socially engineered into giving away their username and password for their Office 365 system and it doesn't matter how many fancy firewalls, etc you have on your system, once someone is entering a legitimate username and password, no antivirus or firewall is going to bat an eyelid at them.

To cut a long story short, the solicitors weren't a customer of ours, but they contacted us just before the incident because they felt their current IT support company weren't quite cutting it. However, before we got to the appointment date, we were hastily called in to check out the systems due to the £200,000 breach.

The current IT support company had told the solicitors that their systems were perfectly fine and they had nothing suspicious going on. However, they couldn't understand this because they had paid the money into an account supplied by email that was part of an email chain.

Within five minutes, we ran our new and advanced security alert checks to find a forwarder had been placed on the email account and cybercriminals had been watching every email that the solicitors had sent.

To be brief, once a cybercriminal has gained your username and password, they don't want to be spotted by logging in and out, so they place a 'forwarder' on your emails so that a copy gets sent to them too. You would have no idea that this is on and so you happily go about your business not knowing that someone is waiting their opportunity to strike.

Hence, when the £200,000 transfer was about to take place, the cybercriminals jumped into the email chain, changed bank details to their own and the rest is history!

Were the solicitors to blame?

Technically, yes – the cybercriminals had breached their system.

Was it their fault? Well they had given away their password.

BUT, even the IT support company hadn't spotted it.

A cybercriminal can set up a forwarder in three different places on an Office 365 account and it takes approximately 10 minutes per email address to check for them, and that's if you know what you're looking for, AND to be 100% certain you remain safe, you would have to do this consistently throughout the day. Could you do this? Do you have the skills? The time? The staffing levels?

Obviously our tool saved the day in sorting this and the solicitor has now become a valued and very appreciative client. They have, of course, been put through their paces by ICO and The Solicitors Regulatory Body, but thanks to the security measures that we have now put in place, not least the Office 365 tools to safeguard against this ever happening again, they have shown 'due care' and been given a glowing bill of health with their new security systems.

They weathered the storm and won! BUT, can you imagine what they went through? At one point they thought they would lose everything!

You can make sure you don't have to suffer like they did.

Here are the tools that they now take and why you need them:

Email Forwarding Alerts

What it does:

You, and us, are sent an email alert as soon as any forwarder is set up on your emails. The forwarder may be legitimate – you may, for example, want Pam from accounts to have a copy of your emails whilst you are on holiday.

With a simple click of a button contained within the email alert, you can accept or reject the forwarder. And don't worry if you miss the email. It won't stop sending to us or you until a response has been made.

Why you need it:

We know from the solicitor true story, that cybercriminals frequently put forwarders onto accounts once they have gained entry.

You need to be able to get rid of these fast before any damage can be done.

It would take a full-time knowledgeable member of staff all day/every day to do this for every email account you have. Do you have the resource/knowledge/time to do this?

Admin Monitoring

What it does:
This clever tool makes sure you (and us) are notified when any new admin account/ admin changes are made in your Office 365 accounts.

Why you need it:
With an admin account, a cybercriminal can gain access to everything in your business, make changes, give permissions. They have the driving seat.

You need to know who your admins are and be in control.

It's not just cybercriminals either, you need to know if your staff have made themselves an admin so you can remain in control of your business information and security.

Spoofing Protection

What it does:

I'm sure you've seen an email that looks like it has come from your colleague – it has their email address and looks very authentic, but they didn't send it. A cybercriminal is playing you and this can be done really easily – known as spoofing.

Whenever an email is sent to you, this clever tool automatically checks for possible spoofing by running checks against the name and the domain. If it finds a match it lets you know by splashing a warning across the email.

Why you need it:

You can't be watching your staff all the time. It's when you're pushed for time, feeling distracted, tired, busy that you are most likely to click on a rogue email. We've seen it done time and time again. We've even seen it in our own business.

It doesn't mean you've been hacked: it's just a clever method cybercriminals are using to fool you and ultimately gain access to your hard-earned money.

This tool takes away the guess work, by clearly showing you a spoofed email, so you can rest easier knowing you and your staff won't fall prey to this.

Location Monitoring

What it does:
Automatic alerts are sent to us and you whenever a login is spotted from a suspicious location. What's more you can choose the zone you want monitoring based on country, region, city, IP address. Exclusions can also be added if someone in your team is working away.

Why you need it:
Cybercriminals typically operate outside of the UK. You need to know instantly if your account is accessed from a suspicious location. You can choose to have this set to exclude certain areas, like your work locations (even in different countries), so you aren't constantly alerted.

Once notified, we can immediately take steps to make sure no damage is done.

Remember it's not about a brute force attack, but when someone has given away their username and password. It may even be that one of your staff or yourself have gone on holiday and accessed systems at a local internet café, for example. The wi-fi they accessed was a rogue one and now the cybercriminal can login with legitimate details. We all know you/your staff shouldn't do this, but how can you be sure?

With this clever tool, you know instantly and can lock it down before any damage is done. You are kept in control.

At the end of the day, security is a choice, but it's no longer one we can take lightly.

In the past it was good enough to just protect our businesses by putting on robust locks, then alarm systems to let you know if someone gained entry so you could do something about it before anything was taken.

In the intangible threat world of cybercrime, we now understand we have to have antivirus and firewalls, but just like we need an alarm system on our physical property, we need an alarm system on our Office 365.

You need to know instantly if anyone attempts to gain entry, so they can be booted straight out before any damage can be done.

These tools allow you to keep in control, so you can sleep easier.

It's always choices and consequences in life.

Can you afford to risk your livelihood and way of life as you know it?

The tools are there, the choice is yours. Over to you...

These tools are so simple to implement and they ensure that YOU stay in control.

For more information, contact us today:

Lodge Information Services

LIS House, Main Road Woodham Ferrers, Essex CM3 8RP

T: 01245 323900 **E: enquiries@lisltd.co.uk**

lis.helpdesk @LIS_Support @listechsupport

We can remove the stress and help you sleep easier in just one call.