

Cablers



365 SECURITY - EMAIL SUPPORT TO GIVE YOU PEACE OF MIND

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.

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. 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 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.

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 both internally or rogue and be in control.

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. It doesn't mean you've been hacked: But, 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.

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

THE SECURITY REPORT

What it does:

It instantly collates all of your Office 365 admin security at the touch of a button, revealing key information such as: who your admins are, what forwarders are on your account, who shares what mailbox, are there any external documents being shared and much, much more. It keeps you in control and compliant.

It provides a clear, detailed report of your Office 365, which is fully searchable.

Why you need it:

We all need to be on the ball when it comes to being in control of our business information/ systems and this clever tool allows this. It's really clear and easy to understand, coming with a user-friendly glossary. You really can be in control of your systems and if you're a regulated industry, it really is a must to show you are doing all of the necessary compliance measures.

It also helps you to keep track of your employees and see which ones may be letting you down by not operating a strong password or having multi-factor authentication on their accounts.

Call us to discuss pricing:

 01787 221166

 hello@cablers.co.uk

 www.cablers.co.uk



Cablers