EMAIL SECURITY

Your business email needs to be
as secure as it can possibly be.

PiSYS .net
A COMCEN COMPANY
We make IT easy

Example...

Everyone in the company gets an email at 6am. It comes from the head of IT and instructs everyone to follow a link to install an update.

Some people don't spot that the head of IT's name is spelt slightly wrong – a simple spoofing technique straight out of the cyber crime textbook.

By 9am people start losing access to their files. They've been encrypted. The link installed ransomware that's making its way through the network. Customer data, employee information and other vital files are skimmed, ready to be sold on the dark web. The criminals demand £75,000 to release the data back to the company.

The company tries for more than a week to remove the ransomware, but eventually they give in and pay the money. It takes another two days to get the decryption key, and when they open their files, half of the data is corrupt.

This happens a lot.

Owners of small and medium-sized businesses often make the mistake of thinking that they aren't on the criminals' radar. In reality, more than 40% of cyber attacks are aimed at small businesses – precisely because they often don't take the same security precautions that larger companies do, and they're more likely to pay a ransom.

It is essential for small companies to prioritize email security, as the impact of a cyber attack cannot be quantified solely in monetary terms. Such an attack can also lead to decreased productivity and a loss of confidence from customers.

According to research conducted by Deloitte, the majority of cyber attacks (91%) originate from phishing emails, which are fraudulent messages that appear to be from a legitimate source, but are actually sent by criminals.

This is the method used to attack web giant Yahoo a few years ago, allowing the contents of half a billion user accounts to be exposed to criminals. Though major incidents like these receive a lot of attention, small and medium-sized businesses are also vulnerable to these types of attacks.

Studies show that 60% of small businesses that suffer a data breach close their doors within six months of the attack.

What to know!

If you don't already use business email, you should. It looks more professional to have your business name after the @, and you get additional benefits too.

Things like an integrated calendar, notes app, document cloud, and chat and video call facilities.

But you'll also benefit from a higher level of security than you'll get with your personal email account.

Using business email also gives you the ability to control employee accounts.

So when someone leaves you can block their access immediately.

There are several aspects to email security: secure gateways, encryption, multi-factor authentication, malware protection, and further authentication protocols. If this sounds like so much jargon, don't worry. We're experts at this stuff and we're here to help all the way.

What is a phishing attack?

Phishing emails aim to deceive you into clicking on a link, opening a file, or taking any other action that leads to harm. These attacks come in various forms, all with the intention of achieving a similar outcome.

Many phishing emails are distributed to thousands of individuals indiscriminately. It may seem like it is from a company like Amazon, requesting that you update your personal information, but the attackers are simply casting a wide net, hoping that some recipients will fall for the scam. These types of emails usually lack a personal greeting and may appear 'suspicious' compared to legitimate messages from the company.

Look carefully and you'll see that the address it's sent from isn't Amazon's standard email address. The link will take you to a spoof page that will steal your credentials as soon as you enter them.

Spear phishing is more targeted. It might include your name in the greeting, or it may be a more sophisticated Business Email Compromise attack. BEC attacks are usually targeted at a senior employee, or even the business owner, and try to trick them into transferring money or handing over sensitive information.

CEO fraud happens where a company executive or the business owner is impersonated in emails to colleagues. This can involve email address impersonation – or spoofing – and they often request funds to be transferred. Attackers take time to study emails to get the right language and tone to convince the recipient that it's a genuine email.

What's the damage?

The impact of phishing attacks can vary, but the criminals have three main objectives:

Data Theft

Data theft – scammers will use 'credential phishing' to steal your customers' personal information.

Malware

Malware - some attacks will install malicious software onto your device, which can potentially spread through your network. This could include spyware, which can log your keystrokes and track you online; or ransomware, which encrypts your data and demands a ransom to get it back.

Wire Transfer Fraud

Wire transfer fraud - CEO fraud and BEC attacks in particular attempt to persuade a target to transfer money to an account controlled by the attacker.

A people problem

All email-based attacks rely on human error within an organisation for success. Therefore, it is crucial to adopt a sense of security within the company to decrease the chances of a "social engineering attack" - a type of scam that persuades individuals to take a specific action- from being successful. Employees should be educated on how to identify potential threats and the steps to take in case of an incident, including who to inform and what immediate measures to implement.

Have an email use policy that sets out how your people should use their business email account, and the importance of following the rules.

And consider putting your team to the test from time to time… maybe by simulating a phishing attack, or holding refresher sessions where you quiz them on their knowledge.

Failure to make your whole team aware of the importance of good cyber security can be a costly mistake.

We can help

By providing staff training as one of the most potent resources at your disposal, we can complement your efforts by implementing a range of technical measures that will minimize the likelihood of an attack occurring and mitigate its consequences if it does.

We can create a gateway to block or quarantine suspicious emails, scanning both incoming and outgoing email for malicious content.

We can install software to help protect you from email spoofing, and from your email being used in BEC attacks, phishing scams, and spam email.

And we can deploy end-to-end encryption, which stops anyone from reading the content of your email unless they have the correct encryption key. That means your email is only ever received by the intended person and data can't be tampered with.

Better password management?

You already know the drill here. Long, strong randomly generated passwords all the way.

Probably the easiest way to do this is by using a password manager. Not only will it create impossible-to-guess passwords, but you won't have to remember them (or write them down on a Post-it note). Your password manager will keep your passwords secure and autofill them for you when required. This also stops the problem of passwords being reused for other online accounts, which is a huge security risk.

You should enable multi-factor authentication (MFA), too. As a second line of security, this sends you a single-use password or PIN via your mobile device or a USB key each time you log in. Biometrics are another form of MFA, where you provide a fingerprint or retinal scan in addition to your password.

All this may make logging in a little more time consuming, but it can go a long way towards keeping your accounts secure.

And we always advise that updates and patches should be installed immediately to keep you protected against new threats.

It may seem overwhelming, but email attacks are a significant security risk for small businesses and should be given proper attention.

If you need assistance from experts or are concerned about potential disruptions from implementing these measures, do not hesitate to reach out for help. We are experienced in dealing with these issues on a regular basis.

CALL: 01792 464748 |
EMAIL: hello@pisys.net
WEBSITE: www.pisys.net

PiSYS .net
A COMCEN COMPANY
We make IT easy