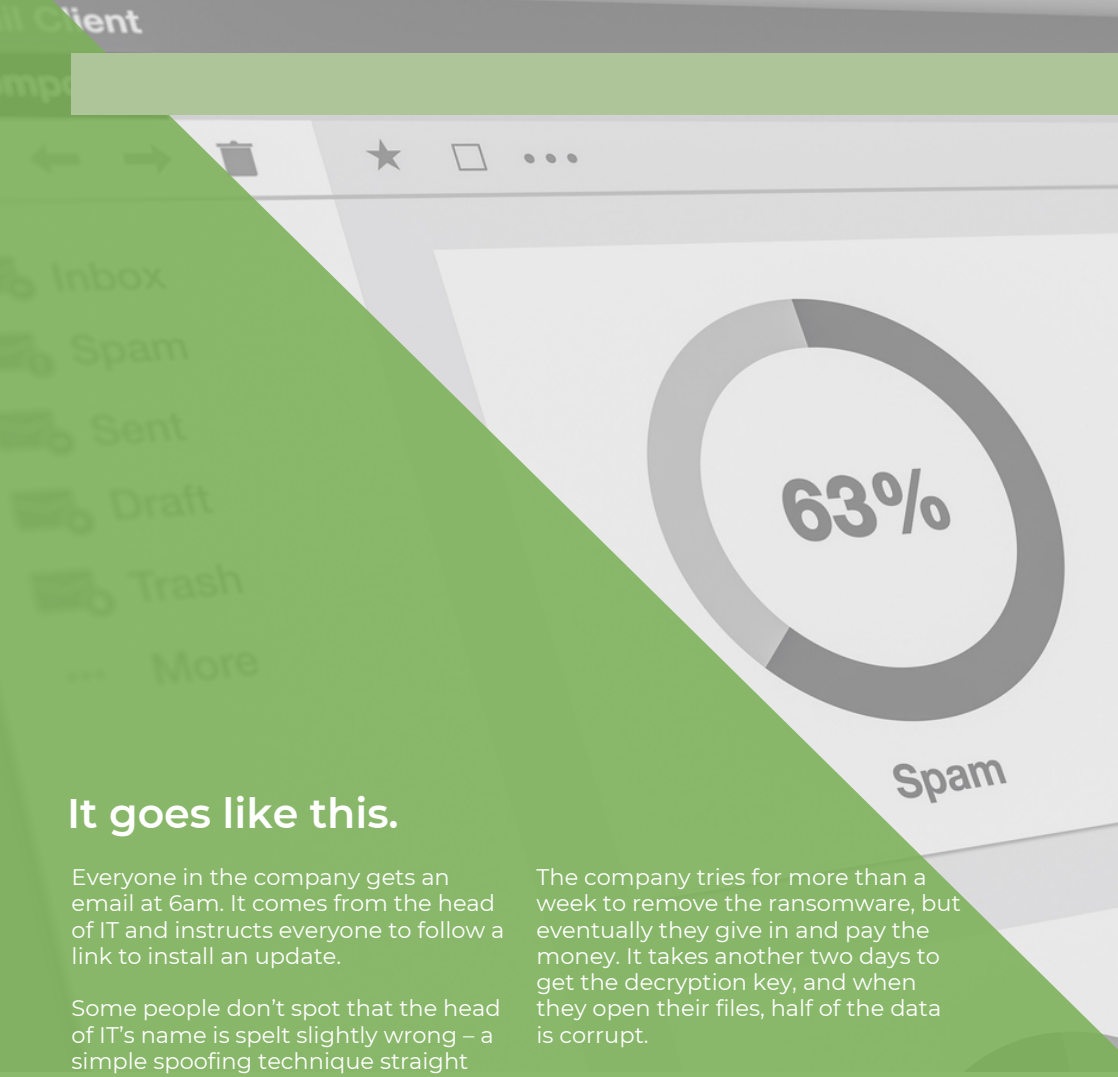
Getting to grips with email security



It goes like this.

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.

So smaller businesses must take email security seriously – because the cost of a cyber attack can't just be measured in financial terms. It comes with a loss of productivity and loss of customer trust.

Research by Deloitte found that 91% of all cyber attacks begin with a phishing email (an email that looks like it's from someone you know, but is actually from criminals).

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

That's how web giant Yahoo was targeted a few years ago, exposing the contents of half a billion user accounts to criminals. And though we often only hear about these high-profile cases, small and medium-sized businesses are prime targets for these attacks.

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

Here's what you need to know

First things first. If you don't already use business email, you should. Having your business name after the @ looks more professional, 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 trick you into clicking a link, opening a file, or taking any action that causes harm. Attacks take several forms, each with a different way of trying to achieve a similar result.

Most phishing emails are sent to thousands of people at random. It might look like it's from Amazon asks you to update your details, but the criminals have just thrown a lot of mud, hoping some of it will stick. There's no personal greeting, and it'll often look 'wrong' compared to a genuine email from the company.

Look carefully, and you'll see that the address it's sent from isn't Amazon's standard email address. Instead, 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 – scammers will use 'credential phishing' to steal your customers' personal information.

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

It's a people problem

All email attacks rely on someone in your business falling for the con. So it's essential to create a culture of security within your business to reduce the chances that a 'social engineering attack' – a scam that convinces someone to take action – will succeed.

Everyone should know what to look out for and what to do if they think an incident has occurred, including whom to report it to and what immediate action to take.

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.

How we can help

Staff training will be one of the strongest tools in your arsenal, but we can also help by putting a raft of technical measures in place to lessen the chances of an attack and to reduce the impact if it does happen.

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

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

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.

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 when required. This also stops the problem of reusing passwords 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's a lot to think about, but email attacks are one of the biggest security threats to small businesses. They need to be taken seriously.

So if you need expert support or are worried that making these changes might cause disruption, get in touch. We do this every day.

Contact.

+44 (0)333 202 6365

hello@better-it.uk

Better IT Limited, 3-3a Barrow Road, Sileby, LE12 7LW.