

Getting control of your email security




Beck IT Systems®



63%

Spam

48%

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 spelled slightly wrong – a simple spoofing technique straight out of the cyber crime textbook.

By 9am people start losing access to their files. They have 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 receive the decryption key, if it arrives at all, and when everyone opens 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 it's vital that smaller businesses take email security seriously – because the cost of a cyber attack can not be measured in financial terms. It comes with a loss of productivity, opportunity 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.

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 possibly be.

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





Here's what you need to know

First things first. 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. Things like an integrated calendar, notes app, document cloud, and more. In addition, you'll also benefit from a higher level of security than personal email accounts provide.

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, data loss prevention and further authentication protocols. If this sounds like so much jargon, don't worry. We specialize in this and we are here to help.

What is a phishing attack?

Phishing emails try to 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. An email might look like it's from Amazon asking you to update your details, but criminals actually sent it in hopes it will fool people into providing their personal information to them. There's no personal greeting, and it will often look 'wrong' compared to a genuine email from the actual company.

Look carefully and you will see that the sending address is not 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. Business Email Compromise 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. This is called "Executive Fraud".

Executive 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. Don't fall

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 and your customers' personal information.



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



Wire transfer fraud – CEO fraud and Business Email Compromise 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 to submit to the false email. It is important 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 who to report it to and what immediate action to take.

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

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 technical measures in place to lessen the chances of an attack, and to reduce the impact if it does happen.

We can customize your spam filters to block or quarantine suspicious emails. BeckITSystems' email service currently scans incoming and outgoing email for malicious content.

We can use Artificial Intelligence systems in the Advanced Security service to help protect you from email spoofing, and from your email being used in Business Email Compromise attacks, phishing scams, Executive Fraud emails, and spam email.

Contact us to learn more about the Advanced Security Service from BeckITSystems, Inc.

Better password management

You already know the answer here. Long, strong pass phrases are considered the safest.

One of the easiest ways to do this is by using a password manager like RoboForm. Not only will it create impossible-to-guess pass phrases and passwords, but you won't need to remember them or write them in a Word document saved on your computer or the server.

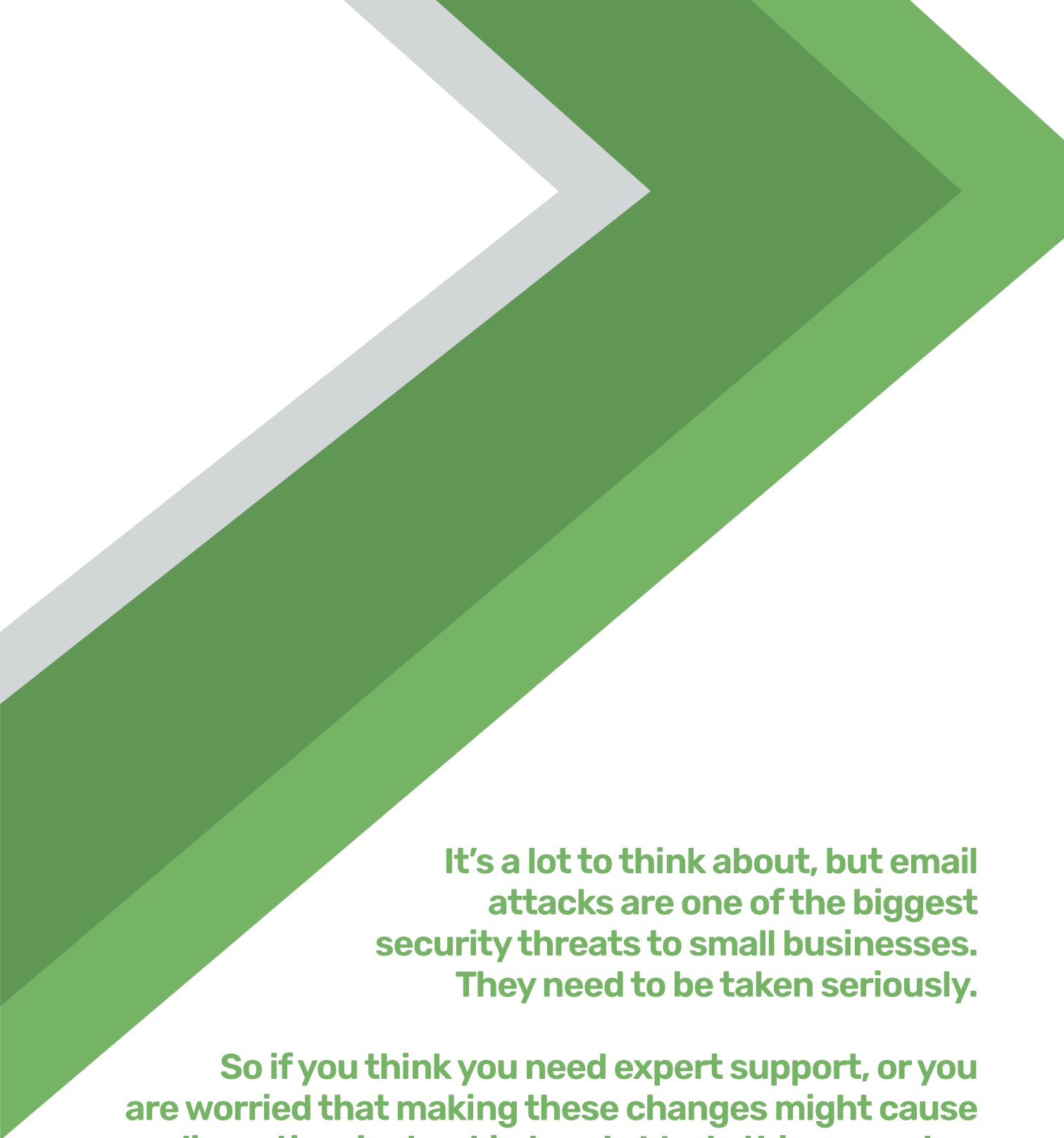
If your computer is compromised, the hackers will have passwords to everything that is in that document. This also stops the problem of passwords being reused for other online accounts, which is a huge security risk.

You should also enable multi-factor authentication (MFA) when it is available. As a second line of security, this sends a single-use password or PIN to your mobile device 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.

We also advise that updates and patches be installed as soon as they are tested and proven to work properly in order to keep you protected against new and emerging 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 think you need expert support, or you
are worried that making these changes might cause
disruption, just get in touch. We do this every day.

CALL: 703.433.0730
EMAIL: Tech@BeckITSystems.com
WEBSITE: BeckITSystems.Com

