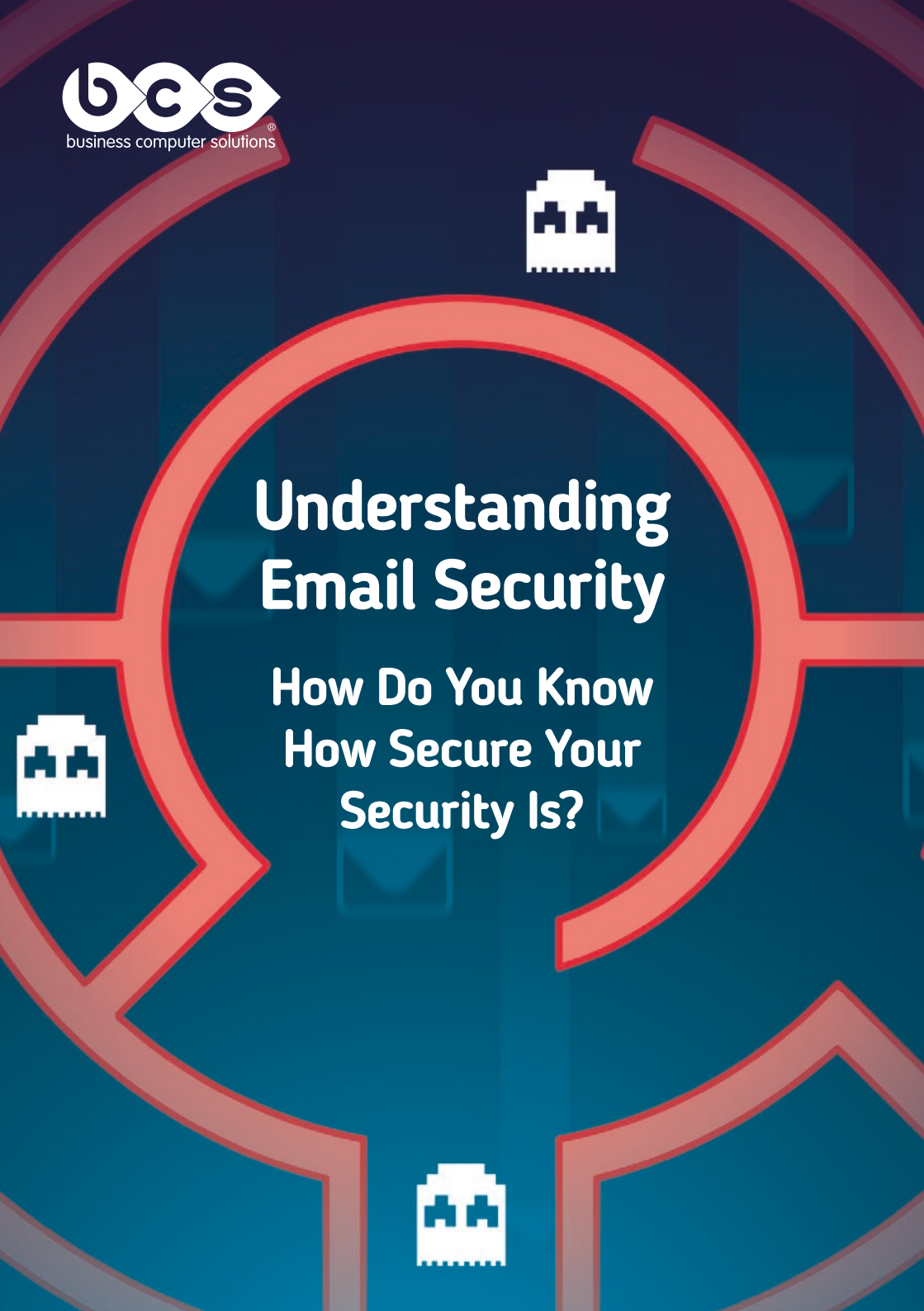
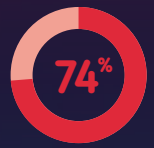

bcs
business computer solutions
Understanding Email Security
How Do You Know How Secure Your Security Is?

Email Security Explained

Cyber threats are on the increase. Falling victim can result in losses in revenue, sales, customer confidence and lead to compliance issues, even business closure. With most threats originating via email, and the sophistication and diversification of these threats ever evolving, email security is more critical than ever. Effective Email Security relies on three pillars. **Preventing** malicious emails ever making it into company inboxes. **Training** your team on the risks and best practises when opening email. Correctly **backing-up** emails for compliance, and access, if something does goes wrong.



Of Attacks Start Via Email*

Standard Solution Overview

Business owners are often surprised to find that the standard security, that comes from email or domain providers, is often not that secure. Basic prevention leaves considerable gaps and poor backups are unreliable at best. Training is often all but missing!

Advanced Solution Overview

In stark contrast to standard systems an advanced system is fully integrated. Multiple prevention tools work in real-time to keep most threats ever getting in. Robust, structured and automated backups keep everything safe and available. User training is at the heart of the system, ensuring that should a threat make it through the recipient can spot it and remove it.

Standard Solution V Advanced Solution

Prevention

Basic Virus Protection
Basic SPAM Protection

Training

Ad-hoc Warnings

Backup

No Guarantee If Lost
Deleted Emails Can't Be Restored
No Sharing Archives

Prevention

Advanced Virus Protection
Advanced Spam Protection
Anti-Phishing
Domain Imitation Protection
Outbound Email Encryption
Email Continuity
Ai-Based Threat Detection
Targeted Attack Protection
Account Takeover Protection

Training

Cyber Security Training
Attack Simulation
Security Webinars
Targeted Training

Backup

Guaranteed If Lost By Users
Restoration Of Deleted Emails
Auto-Archive
Sharing Archives

*2017 Threat Landscape Survey. SANS Analyst Program.

Powerful Prevention

Stopping malicious threats reaching your business in the first place is key. Standard protection is no longer enough. Your cybersecurity setup needs to be not just reactive but proactive in identifying threats before they cause harm. Standard protection is often lacking in real-time protection, lacking AI & Machine Learning advancements. This makes it unreliable. Threat protection is like a maze, trapping and destroying threats before they have a chance to escape.

Advanced Virus Protection

With a constantly updated catalogue of all known threats, Advanced Virus Protection utilises a vast knowledge base to deal with a variety of vulnerabilities. With new threats uncovered daily, this system continually educates itself on how to deal with new threats before they reach your business.

Advanced Spam Protection

Just like virus protection, spam filtering uses AI to spot the tell-tale signs that give a malicious email away. This saves you taking the risk, with the email in question not even touching your inbox. Known spam addresses are blocked straight away, and this system also keeps track of new threats.

Anti-Phishing

Phishing is one of the most common email threats, and that doesn't look like changing any time soon. Advanced Protection comes in the form of a safety net so if you do click on a dodgy link, Anti-Phishing will jump in front of the proverbial bullet before you're compromised.

Domain Imitation Protection

Cybercriminals are using new ways to catch people out. Domain imitation is one way of adjusting a URL, for example, instead of heading to facebook.com, you'll end up at faacebook.com, which could be filled with all sorts of harmful stuff. By scanning the URL before you access it, you can rest assured you're visiting a legitimate website.

Outbound Email Encryption

Emails are nowhere near as secure as people think. This makes them an easy target for attackers. Encrypting your email in transit makes it much harder for the contents to be snooped on, meaning you can send important documentation without worry. If you don't use encryption, your messages can easily be viewed.

Email Continuity

Could you survive a day or even a week without email? Continuity systems are crucial for ensuring continued access to important messages. Systems such as these give you a failsafe in the (hopefully) rare event that your email provider goes down. This means you won't lose anything.

Ai-Based Threat Detection

Traditional AV systems are great for finding issues after they've taken a hold on your system(s). With AI threat detection, threats are identified at a vastly quicker rate. This helps remove issues before they can become troublesome. This also means you can continue working whilst threats are eliminated in the background.

Targeted Attack Protection

If you are unfortunate enough to be the victim of a personalised or bespoke attack, then having a robust system in place to do what must be done is vital to minimising impact. Targeted attack protection uses a combination of tools to stop any damage.

Account Takeover Protection

If your account is accessed from a location or machine that is unrecognised, then account takeover protection will prevent a bad actor from undertaking potentially catastrophic actions. By temporarily locking your account, through to asking for extra verification, it makes it incredibly difficult for attackers to begin causing havoc.

More at: bcs365.co.uk/email-security

Smart Backups

A regularly kept backup is only good enough when it's quick and easy to access and get working again. The majority of the time this is unfortunately just not the case. With smart backups, you'll have regular snapshots of your data saved, meaning your backup is always up-to-date, and always accessible. You can get your data back and start working again in a pinch thanks to an intuitive system that is constantly working away to keep your data safe.

Guaranteed If Lost By Users

If your user accidentally deletes that important file or folder, it can be restored. With regular snapshots being taken of all data at your business, if one user or even a whole department loses something, your data is retrievable. It happens to the best of us, but with a smart backup system in place, you need not worry that that vital document disappears when you need it most.

Restoration Of Deleted Emails

Just like your data, if you delete an email from the trashcan and you think it's completely gone – don't worry – it's not. Whether it be from today or 6 months ago, retrieving deleted emails is straightforward. This is also the case for the emails of ex-employees, so if you need to restore an item for compliance purposes, this can be achieved with a smart backup system.

Auto-Archive

With all your emails and associated contents being archived regularly, it can be easy to forget that this will constantly accrue more storage space. What happens once you've reached a potential limit? Do your emails stop being saved? With validated auto-archiving, you need not worry. They will dynamically adjust the space needed for your archive so you can continue to rest easy knowing that all your emails are safe.

Sharing Archives

Despite your archives auto-expanding, it's easy to backup shared mailboxes as well. Archiving is a complete solution that packages up all email content in your business. Because it's easy to put these archives into one easy to deploy file, it makes it easy to share and reinstate email files across your business. This is ideal when roles change and people leave/join your organisation.

More at: bcs365.co.uk/email-security

Effective Training

Technology can only do so much. All it takes is one compromised email to get through and be opened. This is why people are the biggest risk to email security. For many organisations, guidance on email handling or formal training doesn't exist. It should be at the heart of email security – your users are your final line of defence before a threat reaches your business. Invest in your staff and they will invest in your business!

Cyber Security Training

Training comes in all shapes and sizes, but the important thing is to get across the key areas that matter, and what actions your staff can take. It doesn't have to be complicated, even simple tips can make a massive difference. Use online training as an easily accessible option for your staff. This allows them to take the courses whenever is suitable, meaning they can really absorb and understand they information.

Attack Simulation

Some people prefer to "do" rather than read or watch. Attack simulations are a great way to see how much people really know when it comes to combating threats. From a compliance standpoint, it's a fantastic way to get an accurate picture of how well protected your business really is when the time comes, and you face a cyberattack.

Security Webinars

As the cybersecurity landscape is ever evolving, it makes a difference to have cybersecurity champions at your business who understand and appreciate the latest threats to your business. Cybersecurity and the prevention of threats never really stops, so even when you've mastered the basics, it still pays to be aware of the latest trends out in the wild. BCS Security Webinars are a great way to maintain such knowledge.

Targeted Training

Take advantage of the knowledge of those that live & breathe cybersecurity. If you use email every day, you may benefit from phishing training. If you work remotely, again, you may benefit from a different type of knowledge check. Each business is different, so learning tricks and tips that are relevant to the way your business works is key to ensuring a successful security setup. Our security specialist Lee Hutton is BCS' go-to-guy.

More at: bcs365.co.uk/email-security

Secured & Assured

Planning to rely on standard email security can be planning to fail. Advanced email security and management solutions are far more effective in combating cyber threats and the resulting losses in revenue, sales, customer confidence and compliance issues. Once in place the risk is minimised and you can be confident that your people and systems are ready to recognise and remove malicious emails.

Would You Like To Know How Many Threats Are In Your System?

As part of our extensive BCS Security Audit, we will deep scan your email server to identify active and dormant threats contained in emails & attachments. We also undertake a unique scan of known dark web threats too. So if you've been involved in a data breach, we'll be able to tell you.

FREE BCS Cybersecurity Training For Kent Businesses

Our bespoke Cybersecurity training focuses on your staff. They're at the heart of your email security as well as being a key asset in the fight against cyberattacks. This is why we designed the training to transform what can be your greatest vulnerability into your strongest defence!

We Hope That You Found This Guide Useful

Educating and supporting other Kent businesses, in all things IT, is one of our core values. More handy articles can be found at www.bcs365.co.uk/blog

BCS is a Thanet based, Employee Owned, IT company serving local businesses and organisations. If you'd like to talk to us about anything IT related, drop us an email or pick up the phone, we'll be happy to help.

Best regards

Martin

Martin Hynes
Managing Director
martin.hynes@bcs365.co.uk

BCS, Unit 16, Leigh Road, Haine Ind Estate,
Ramsgate, Kent, CT12 5EU

Freephone: 0800 6521 365 Out Of Hours Option 1

hello@bcs365.co.uk bcs365.co.uk