PiSYS .net

A COMCEN COMPANY

Why do 90% of cyber security attacks originate from a seemingly harmless email?

We make IT easy

You‘re in your office, enjoying your morning coffee, when you check your emails and find a message that appears to be from your bank.

You click a link and enter your login details.

But then, doubts creep in as you revisit the email and the reality hits you—it’s a phishing scam. This clever ruse has directed you to a fake banking site where you’ve inadvertently handed over your login information.

Now, your business's financial security is under threat as these criminals could be breaching your actual bank account at this very moment.

This is an everyday reality for numerous businesses.

Email, an indispensable yet aged tool at over half a century old, continues to be a critical communication medium. Unfortunately, it's also frequently exploited by attackers.

The access gained from hacking someone’s email is extensive:

- altering passwords,
- monitoring transaction histories,
- viewing upcoming travel, and even
- masquerading as the victim in further emails.

This fixation on breaching email systems explains why a vast majority of cyber security attacks on businesses originate from compromised email activities.

How can you safeguard your business from these frightening scenarios?

Know the risks

Email remains the most widely used communication tool in businesses, positioning it as the main target for cyber security attacks. Common threats include phishing and malicious attachments that try to install malware on your devices.

Phishing scams have evolved significantly, with cyber criminals employing more cunning methods to trick you into divulging sensitive information or clicking harmful links.

A successful breach through email can have severe consequences for businesses, regardless of their size.

Here are a few possible impacts

Data breaches

Data breaches occur when cyber criminals access sensitive company or customer data, including financial details, intellectual property or personally identifiable information (PII). This exposure compromises privacy and subjects your business to potential regulatory fines and legal actions.

Financial losses

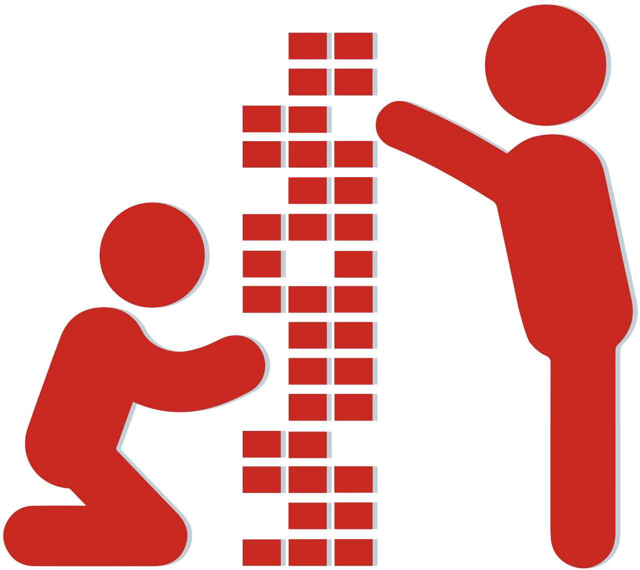
Financial losses stem from email scams through unauthorised wire transfers, fraudulent transactions or ransom demands. These losses significantly affect your bottom line and diminish trust among customers and stakeholders.

Reputational damage

Reputational damage occurs when a breach tarnishes your business's reputation and erodes customer trust. News of a data breach spreads rapidly and can lead to enduring repercussions. This damage often results in lost customers and strained relationships with partners, investors and suppliers.

Operational disruption

Operational disruption follows the aftermath of a security breach, which can interrupt normal business activities. This leads to downtime, reduced productivity and heightened stress for your team.



Then establish a strong foundation for secure email

Choose a secure email service

Start by selecting a secure email service. Enhancing your email security begins with choosing a dependable and secure email provider. Opt for services that provide strong encryption, secure login procedures and thorough spam filtering. Additionally, look for solutions equipped with advanced features for detecting and preventing threats such as phishing scams and malware attacks.

Implement strong authentication

Strengthen authentication measures. Passwords serve as a crucial first barrier to unauthorised access to your email accounts. Ensure your team uses strong, unique passwords for their email access.

Introduce a password manager for your team. This tool can create and store complex, random passwords and automatically fill them in, enhancing security with minimal effort.

Add an extra security layer by implementing multi-factor authentication (MFA). MFA demands additional verification, like a one-time code sent to a mobile device, before account access is granted. This significantly reduces the risk of unauthorised entry by attackers.

Educate your team

Employees often represent the first line of defence against email-based threats. However, without proper training, they could also be the most vulnerable. Deliver detailed training on email security best practices. Teach them to identify phishing attempts, steer clear of dubious links or attachments and report any suspicious emails to the Pisys IT support team. Consistently refresh this training to keep your team alert and informed about the latest cyber criminal strategies and threats.

Pisys eCampus offers **free training to every user** within each customer organisation. Our online learning platform is designed to enhance the professional development and technical skills of individuals across various industries. This e-learning environment offers a catalogue of courses ranging from cyber security to Microsoft 365, Windows 10 and 11, leadership training, wellbeing and more. Tailored to meet the needs of today's fast-paced business environments, Pisys eCampus provides engaging, flexible and accessible training solutions.

Secure mobile devices

A lot of your employees access work emails via smartphones and tablets remotely. Ensuring these devices have proper security is crucial. Equip them with passcodes, biometric authentication and remote wipe capabilities to handle loss or theft situations. You might also consider implementing mobile device management (MDM). This helps enforce security policies and monitors device usage to block unauthorised access to corporate data.

Regularly update and patch

Always keep your software updated with the latest security patches. Cyber criminals exploit known vulnerabilities to infiltrate systems and networks. Applying updates consistently is crucial for securing your email systems. Consider automating the update process to ensure timely application of crucial patches.

And look at extra security

Email encryption

Email encryption is a powerful tool for protecting your emails. It encodes the content of your messages, ensuring that only the intended recipients can read them.

Adopt end-to-end encryption to secure your emails during transit and while stored. Additionally, utilise protocols like Transport Layer Security (TLS) to encrypt interactions between email servers, enhancing your email security.

Advanced threat detection

Advanced threat detection is crucial for combating sophisticated email-based threats. Traditional spam filters and antivirus programs are not always enough. Integrate advanced threat detection that leverages machine learning and artificial intelligence to monitor email traffic continuously. This technology targets phishing scams, malicious attachments and suspicious URLs.

By implementing these advanced systems, you can proactively identify and block harmful emails before they enter your inboxes, significantly lowering the risk of a successful cyber attack.

Email archiving and retention

Email archiving and retention policies are essential for meeting regulatory compliance and preserving vital business communications for future use.

Implement email archiving solutions that securely capture and store all incoming and outgoing emails in a tamper-proof repository. This allows for easy retrieval and review of historical email data whenever necessary.

Additionally, email archiving acts as a safety net by creating backups of your email communications, safeguarding against data loss due to server failures or other catastrophic events.

Employee awareness and training

Employee awareness and training are critical, even with advanced technical safeguards. Human error still poses a significant risk to email security.

Regularly train your employees on the best practices for email security, stressing the need for vigilance, skepticism and cautious handling of email communications.

To truly gauge your team's preparedness. Pisys can organise simulated phishing exercises. These will test their alertness to phishing scams. Following these exercises, offer targeted training to strengthen any identified areas of weakness.

Lastly, monitoring and optimisation

Effective email security demands ongoing vigilance. Employ strong monitoring tools and processes to constantly watch over email traffic, identify unusual activities and quickly react to potential security incidents.

What exactly should you monitor?

Keep an eye on email logs, server activity and user behaviour to spot signs of unauthorised access, odd patterns or potential security breaches.

Consider deploying Security Information and Event Management (SIEM) systems. These solutions gather and analyse data from various sources, detecting security threats in real-time.

Create a detailed incident response plan. This should outline your business's approach to handling email security incidents, specifying roles, establishing non-email communication protocols and detailing procedures for investigating and resolving breaches.

Regularly conduct exercises and simulations to test your incident response plan's effectiveness, ensuring your team is ready to act swiftly and effectively if an issue arises.

Continuously evaluate and review your email security measures to find weaknesses and areas that need strengthening.

How to stay ahead of the curve

Staying current with the latest trends, threats and best practices in email security is crucial for upholding robust defences against cyber attacks.

Maintaining email security is a full-time job, which is why partnering with Pisys is a smart choice to stay secure and proactive.

We stay ahead by subscribing to industry publications, newsletters and blogs, keeping abreast of emerging threats, new attack methods and security vulnerabilities. We handle this so you don't have to.

We ensure our clients' safety by managing all aspects of their email security, allowing them to focus on their core business without worrying about these risks.

This is something we help businesses like yours with all the time. If we can help you in 2024,

Get in touch.

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

PiSYS .net
A COMCEN COMPANY