Email Security

90% of cyber security attacks start with a simple email. **Why?**

itblue

Imagine this: You're sitting in your office, sipping your morning coffee, going through your emails. Everything seems routine until you stumble upon an alarming message from your bank.

You click the link and log in to your bank… but something feels wrong.

You go back to your email and look again. Your heart skips a beat as you realise it's not from your bank at all… it's a cleverly disguised phishing scam. This is where criminals pretend to be someone else. They've sent you to a fake bank login page and you've just handed over your banking login details without even realising it…

Now your business account has been compromised, and the criminals are already logging into your real bank account.

This scenario might sound like the plot of a dramatic novel, but unfortunately, it's a reality many businesses face every day.

With all the modern communication tools we have, most businesses are still overly reliant on email. This 50-year-old tool refuses to go away.

Criminals aren't just sending you fake emails, they are also trying to break into your inbox.

If you think about it, having access to someone's email gives you a huge amount of power. You can reset their passwords… see their purchase history and travel plans… and even pretend to be them while emailing other people.

This is why criminals are obsessed with your email. 90% of cyber security attacks on businesses like yours start in your inbox.

So how do you prevent one of these nightmare scenarios?

First, understand the risks

Email is the one communication tool every business uses… which makes it the primary method for cyber attacks. The most common threats are phishing, and attachments that attempt to load malware onto your computer.

Phishing scams especially have become increasingly sophisticated. Cyber criminals are using smarter tactics than ever to encourage you to give away sensitive information or click on malicious links.

The consequences of a successful email breach can be devastating for a business of any size.

Here are just a few potential outcomes:

Data breaches

Cyber criminals may gain access to sensitive company or customer information, such as financial records, intellectual property, or personally identifiable information (PII). The exposure of this data not only compromises individual privacy but also exposes your business to regulatory penalties and lawsuits.

Financial losses

Email scams can result in financial losses through unauthorised wire transfers, fraudulent transactions, or ransom demands. These losses can have a significant impact on your bottom line and erode trust with customers and stakeholders.

Reputational damage

A breach can tarnish your business's reputation and undermine customer trust. News of a data breach spreads quickly and can have long-lasting repercussions, driving away customers and damaging relationships with partners, investors, and suppliers.

Operational disruption

Dealing with the aftermath of a security breach can disrupt normal business operations, leading to downtime, productivity losses, and increased stress for your team.

Then build a strong foundation for secure email

Choose a secure email service

The first step in strengthening your email security is to choose a reliable and secure email service provider. Look for providers that offer robust encryption protocols, secure authentication methods, and comprehensive spam filtering capabilities. You should also consider solutions that offer advanced threat detection and prevention features to safeguard against threats like phishing scams and malware attacks.

Implement strong authentication

Passwords are often the first line of defence against unauthorised access to your email accounts. Make sure your employees use strong, unique passwords for their email accounts.

Ideally give all your team a password manager. This can generate long random passwords, remember them, and securely input them so you don't have to. Better security with less work for humans is smart.

Consider implementing multi-factor authentication (MFA) to add an extra layer of security. MFA requires people to provide additional verification, such as a one-time code sent to your mobile device, before accessing your accounts. This makes it significantly harder for attackers to gain unauthorised access.

Educate your team

Your employees are your first line of defence against email-based threats, but they can also be your weakest link if they're not adequately trained. Provide comprehensive training on email security best practices, including how to recognise phishing attempts, avoid clicking on suspicious links or attachments, and report suspicious emails to your IT support provider.

Regularly reinforce these training sessions to ensure that your team remains vigilant and up to date on the latest threats and tactics used by cyber criminals.

Secure mobile devices

Many of your employees use smartphones and tablets to access their work email accounts remotely. So, it's important to make sure these devices are also adequately secured with security measures like passcodes, biometric authentication, and remote wipe capabilities in case of loss or theft. You may also consider using mobile device management (MDM) to enforce security policies and monitor how devices are being used, to prevent unauthorised access to corporate data.

Regularly update and patch

Keep all software up to date with the latest security patches and updates. Cyber criminals often exploit known vulnerabilities to gain access to systems and networks, so regularly applying patches is essential for maintaining secure email. Consider implementing automated ways to streamline the patching process and ensure that critical updates are applied promptly.

And look at extra security

Email encryption

Email encryption is one of the most effective ways to protect your email. It scrambles the contents of your messages so that only the intended recipient can decipher them.

Implement end-to-end encryption to keep your emails secure both in transit and at rest. Also consider using email encryption protocols such as Transport Layer Security (TLS) to encrypt communications between mail servers.

Advanced threat detection

Traditional spam filters and antivirus software can only do so much to protect against sophisticated email-based threats. Implement advanced threat detection that uses machine learning and artificial intelligence to analyse email traffic in real-time. They're looking for threats like phishing scams, attachments with malware, and suspicious URLs.

This can help you proactively detect and block malicious emails before they reach your inboxes, reducing the risk of a successful cyber attack.

Email archiving and retention

Implement email archiving and retention policies to ensure compliance with regulatory requirements and to preserve critical business communications for future reference.

Email archiving solutions capture and store copies of all inbound and outbound emails in a secure, tamper-proof repository, allowing you to retrieve and review historical email data as needed.

As a bonus, email archiving helps protect against data loss by providing a backup of your email communications in the event of a server failure or other catastrophic event.

Employee awareness and training

Even with the most advanced technical safeguards in place, human error remains a significant risk factor in email security.

Continuously educate and train your employees on email security best practice, emphasising the importance of vigilance, scepticism, and caution with email messages.

If you really want to test your team, conduct simulated phishing exercises to find out their awareness and responsiveness to phishing scams. Then provide targeted training to address any areas of weakness identified during these exercises.

Lastly, monitoring and optimisation

Effective email security requires constant vigilance. Use robust monitoring tools and processes to continuously monitor email traffic, detect anomalies and suspicious activities, and respond promptly to potential security incidents.

What should you monitor though?

Email logs, server activity, and user behaviour will help identify signs of unauthorised access, unusual patterns, or potential security breaches.

Consider using security information and event management (SIEM) solutions to aggregate and analyse data from multiple sources and detect security threats in real-time.

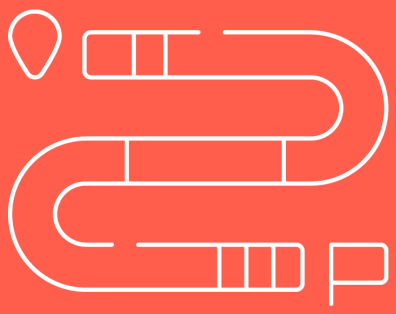
Develop a comprehensive incident response plan to guide your business's response to email security incidents. Define roles and responsibilities, establish how best to communicate when you can't trust email, and outline step-by-step procedures for investigating and mitigating security breaches.

You can also conduct regular exercises and simulations to test the effectiveness of your incident response plan and ensure that your team is prepared to respond quickly and effectively if there is a problem.

Regularly assess and audit your email security controls to identify vulnerabilities and areas for improvement.

How to stay ahead of the curve

Keeping up to date with the latest trends, threats, and best practices in email security is essential for maintaining effective defences against cyber threats.



But it's a full-time job. Which is another reason you should consider partnering with an IT support provider (like us) to keep you secure and ahead of the curve.

We subscribe to industry publications, newsletters, and blogs to stay informed about emerging threats, new attack techniques, and security vulnerabilities. We do it so you don't have to.

And we keep our clients safe by handling all the security aspects of their email, so they don't have to think about it.

Shall we talk about your email security?
Get in touch.

CALL: +27 21 880 2796
EMAIL: info@itblue.co.za
WEBSITE: itblue.co.za

itblue