Red Helix

Email Security Demystified: The Essential Playbook for Securing Your Inbox

CONTENTS

What is Email Protection?	3
DMARC & BIMI	4
What does Security Awareness Testing & Training do?	5
Endpoint Detection & Response	6
Ransomware Protection	7
Email Security with Red Helix	8

What is Email Protection?

Email is the backbone of modern communication, but it is also the most exploited entry point for cyber threats. With **3.4 billion phishing emails sent daily,** the need for robust email security has never been more urgent. Businesses must adopt comprehensive email protection strategies to safeguard sensitive data, financial assets, employees, and brand reputation from evolving cyber threats. Here we will explore the layers of email security, providing an essential roadmap to securing your inboxes against phishing, ransomware, and other malicious attacks.

What Does Email Protection Do?

Email protection services offer advanced threat detection to guard against phishing, ransomware, spam, malware, and brand impersonation. These email security solutions use a multi-faceted approach, including employee **Security Awareness Testing & Training,** protocols like DMARC, and real-time threat monitoring. Advanced threat intelligence and machine learning scans identify potential threats earlier, stopping email-borne attacks before they spread and cause greater damage.

Email protection services provide advanced threat detection to guard against:

- Phishing – Preventing cyber criminals from tricking employees into revealing sensitive information or clicking on malicious links.
- Ransomware – Stopping malware from encrypting data and demanding ransom payments.
- Spam & Malware – Filtering out unwanted and potentially harmful emails.
- Brand Impersonation – Protecting your brand by ensuring only authorised senders use your domain.

By leveraging Security Awareness Training, DMARC, and real-time threat monitoring, businesses can proactively detect and stop attacks before they cause harm. At Red Helix we specialise in building bespoke solutions so, if you are not sure which layers you need, get in touch.

DMARC & BIMI

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a policy and reporting protocol that marks the first step in securing your domain against abuse. It prevents cyber criminals from impersonating you in phishing attacks by allowing email recipients to check the authenticity of incoming emails. This ensures that all emails sent from your domain will be legitimate.

The service will help you to protect your brand reputation by ensuring only authorised senders can use your domain, reducing the risk of fraudulent activities. DMARC will also improve your visibility and control by providing you with reports and insights of email delivery and authentication.

As part of our DMARC service we will monitor and secure your domain names against DNS attacks. We will monitor your DNS records for unauthorised changes and detect lookalike domains. This helps to protect your customers and supply chain from those wanting to impersonate you as well as ensuring the integrity of your domains.

BIMI

The next step is to introduce **BIMI (Brand Indicators for Message Identification)** which is a standard that displays your organisation's trademarked logo beside every email. As it is achieved through a combination of a fully configured DMARC record and a digital certificate (a VMC), it ensures a stronger email security for your organisation.

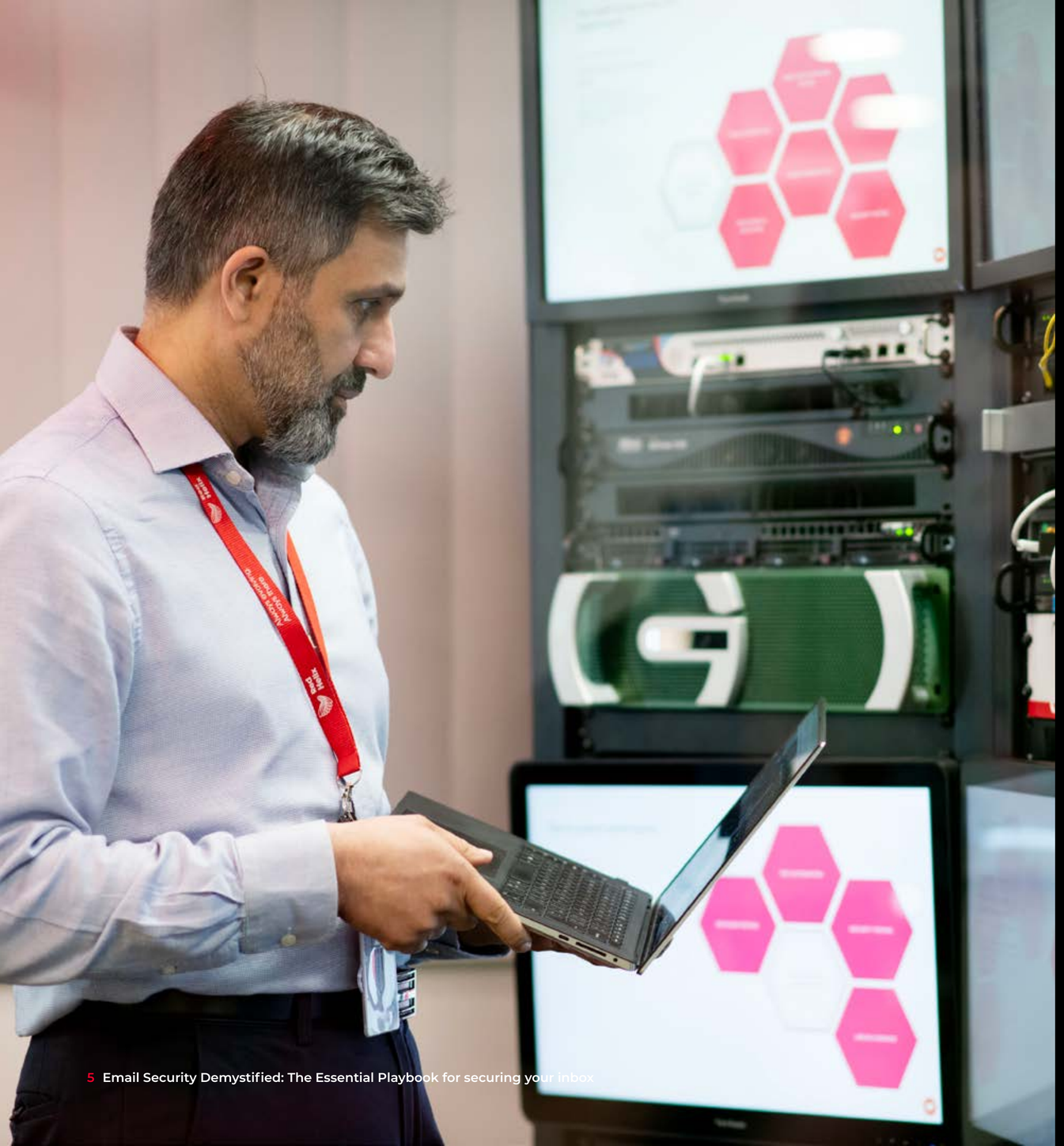
Email continues to be the most popular way that companies communicate with their customers and using a logo when your email hits their inbox adds valuable brand impressions, improved open rates, and increased customer confidence.

It's a simple way for your email recipients to recognise an email from you and know they can trust that it really is from you. Because of this improved trust it can radically transform your email ROI.

Finally, our automated security scanning and assessment tools will help you to evaluate your web infrastructure, SSL/TLS configurations, email security, DNS and more. With all of this in place, cyber criminals will see there's no point trying to impersonate you.

"With spoofing protection from Red Helix, I can rest easy knowing our brand, team, customers, and supply chain are shielded from domain impersonations. This invaluable defence ensures we can focus on our core business objectives without distraction, thanks to Red Helix's continued vigilance and expertise."

LDC



What does Security Awareness Testing & Training?

Cyber security is not just about technology; it requires continuous employee education. Human error is at the root of most security breaches, making training an essential part of any email security strategy.

Why do you need Security Awareness Testing & Training?

After the first full year of training, our training partner KnowBe4 see an improvement of 82% across all industries. With this level of awareness, employees can prevent attempted phishing and ransomware attacks which is evidenced by employees phish prone percentage decreasing from 33.2% to 5.4%. This is only achievable when security training and testing is repeated regularly. There is a minimum level of awareness that needs to be upkept. Therefore, a constant revising of employee knowledge is necessary.

It doesn't matter the size of your organisation; big and small companies alike are susceptible to phishing attacks. Don't risk tarnishing your brand's reputation by falling victim to a phishing email.

Security Awareness Testing and Training also ensures a level of compliance which is necessary nowadays to remain in accordance with Cyber Insurance policies. Many industry standards now state that organisations must have gone through security awareness training to be eligible for a claim if they are breached.

Endpoint Detection & Response (EDR)

Why do you need EDR?

Even with security awareness training and domain protection in place, mistakes can happen. If an employee accidentally clicks on a malicious link, Endpoint Detection & Response (EDR) provides real-time threat detection and mitigation to stop the attack before it spreads.

What is EDR?

Endpoint Detection and Response (EDR) is a cyber security solution designed to continuously monitor an organisation's endpoint activity across devices such as computers, mobile devices, and servers. It detects, investigates, and responds to potential threats, providing threat intelligence that helps security teams understand how attacks occur and how to prevent future incidents. By giving visibility into activities happening at the endpoint, EDR enables security teams to detect suspicious activity that may have otherwise gone unnoticed. It also contains threats before they spread across the network, and guides security teams on how to respond effectively.

Managed EDR

At Red Helix, we partner with CrowdStrike to provide a managed Endpoint Detection & Response (EDR) service. While CrowdStrike's platform is cutting-edge, many SMBs face challenges managing its advanced tooling, keeping up with updates, or allocating the dedicated personnel required for 24/7 monitoring.

Outsourcing endpoint security to a Managed Security Service Provider (MSSP) allows organisations to concentrate on growth rather than managing security challenges.

By leveraging shared licensing models, we provide SMBs with access to the advanced CrowdStrike solutions at an affordable cost. Our predictable monthly pricing model ensures organisations can scale their security as needed without overinvesting upfront. The democratisation of advanced cyber security tools means that SMBs can finally level the playing field, staying protected with the same tools and expertise used by the world's largest organisations.

Ransomware Protection

If all other security layers fail and ransomware still infiltrates your systems, a strong anti-ransomware platform ensures that your data remains protected.

Our partners at Halcyon have developed a platform to recognise the behaviour of ransomware, stop it in its tracks, and in the unlikely event of a successful breach, will synchronously decrypt all affected data and devices to keep your company running.

Halcyon blocks known ransomware threats and detects and stops previously unseen strains. And if any encryption does take place, Halcyon has a copy of the encryption keys and is able to build a decryptor for unlocking your data and systems.

This means, even if the attack manages to evade Halcyon's preventative measures and locks your data and systems, Halcyon already has the keys needed to efficiently decrypt everything.

Email Security with Red Helix

Email security requires multiple layers of protection to guard against ever-evolving threats. A strong defence includes:

- **DMARC and BIMI** to prevent brand impersonation.
- **Security Awareness Training** to educate employees and reduce human error.
- **EDR solutions** to detect and contain threats at the endpoint.
- **Ransomware protection** to mitigate worst-case scenarios.

By implementing these layers, businesses can significantly reduce their risk exposure and ensure their email communications remain secure.

At Red Helix, we specialise in bespoke cyber security solutions tailored to your environment. If you're unsure which security layers your business needs, contact us today for a free consultation. Secure your inbox today, email security is too important to leave to chance.

Contact Red Helix today and revolutionise your IT security.

+44 (0)1296 397711

info@redhelix.co.uk

Phoenix House
Smeaton Close
Aylesbury
Buckinghamshire

Red Helix

redhelix.com