5 MAJOR CYBER SECURITY IMPROVEMENTS IN 5 DAYS

Red Helix

With so many cyber security tools available and new launches every week, navigating the complex landscape of digital defence can be daunting. To simplify your choices, here are our top five cyber security enhancements that can be deployed swiftly to drastically reduce your risk.

From bolstering protection against phishing emails to leveraging AI to combat ransomware, these solutions offer a strategic and cost-effective approach to safeguarding your digital realm.

Phishing Email Protection

01

Phishing emails are one of the most common cyber security threats. To protect against these, companies are heavily reliant on the human firewall, i.e. their staff's ability to spot these attacks for what they are. Fortunately, the cost of online security awareness training that strengthens the human firewall is miniscule compared with the price of sophisticated perimeter security tools – which often miss phishing emails.

Based on data from 10 million users worldwide, 33% of a company's workforce can be easily duped by a phishing email if a security awareness training program is not in place. However, within 12 months of starting a program, companies should expect that number to drop to just 5%.

Network Detection & Response

02

Given the speed at which ransomware attacks can inflict loss and disruption, the action of rolling out capabilities that alert to, and stop, such attacks needs to be equally fast.

Network Detection & Response technology, using AI, takes under a week to roll out and can spot attacks, isolate the infected device and close the door that was exploited to prevent future attacks getting through without any human intervention.

Automated Security Testing

03

Automated Breach & Attack Simulation (BAS) persistently tests security measures against new and existing threats, showing companies where attacks can get through and advising on what needs to be adjusted or updated to close the gaps.

As security misconfigurations and environment drift can quickly open the door to attacks, setting up BAS can have a massive impact, for a fraction of the price spent on other security tools.

Zero Trust Network Access (ZTNA)

04

In today's hybrid working era, companies are transitioning from Virtual Private Networks (VPNs) to Zero Trust Network Access, for secure access to data, applications and network drives. ZTNA assumes all connection requests are hostile, allowing for the creation of tailored authentication policies for granting secure access.

Alongside its large security benefits, many companies have also found ZTNA to be a good replacement for their Wide Area Network (WANs) – as it connects straight to the desired location instead of going through the corporate firewall and slowing down the user experience.

Impersonation Protection

05

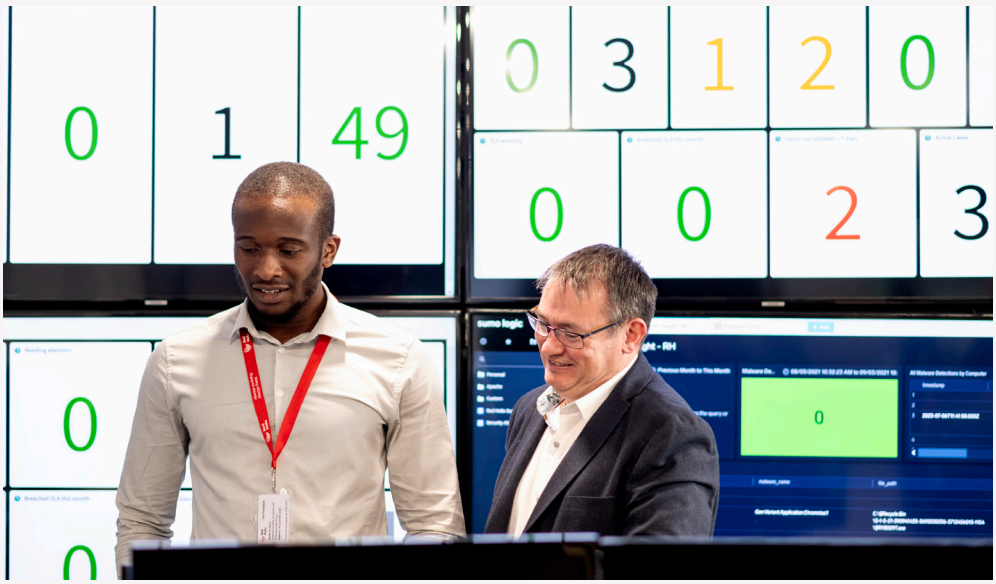
Criminals often pose as company executives, or even as the company itself, to exploit relationships with clients and suppliers. With publicly available information on a company's email configuration and authentication status, attackers can easily see which companies are unwittingly making it easy to spoof their email domains.

Fortunately, spoofing protection technology can help businesses take action before harm is caused. Such technology can immediately audit your domain status, advise on what needs to change, and ensure that only authorised senders can use your domain. It can also alert you the moment someone tries to set up a company that impersonates your brand.

Red Helix

We can support on any or all of the above.

Our managed services and solutions integrate seamlessly with your teams to ensure robust and compliant security.



Contact Red Helix

+44 (0)1296 397711
info@redhelix.co.uk
www.redhelix.co.uk

Red Helix

bsi ISO 9001 Quality Management Systems CERTIFIED FS 11766
ISO/IEC 27001 Information Security Management CERTIFIED IS 725251

CYBER ESSENTIALS CERTIFIED PLUS