Why my staff are better prepared for cyber threats than yours.

In 2021 alone, email spoofing and phishing increased by 220%. And despite billions having been invested into perimeter and endpoint security over the last two years, phishing and business email compromise (BEC) scams continue to be the primary attack vectors into organizations, often giving threat actors the toehold they need to wreak havoc on companies and their customers.

In fact, over $44 million in losses in 2021 were a direct result of successful phishing and advanced email scams.

The 2021 FBI Internet Crime Report reveals that spear phishing scams snagged more victims than any other type of internet scam last year. Phishing and related tactics are attempts to trick victims into disclosing their credentials and other sensitive information. Phishing represents 38.2 percent of all cybercrimes reported to the FBI in 2021 and has been the most reported cyberattack since 2018.

Spear phishing isn't a new tactic, though it has become more sophisticated over the years. Criminals will continue to use it because it is so successful as a pathway into otherwise secured networks. Some of the largest cyberattacks in the last decade began with spear phishing attacks.

With a recession looming and average cost of a breach increasing almost exponentially, email security is the highest priority for organizations around the world.

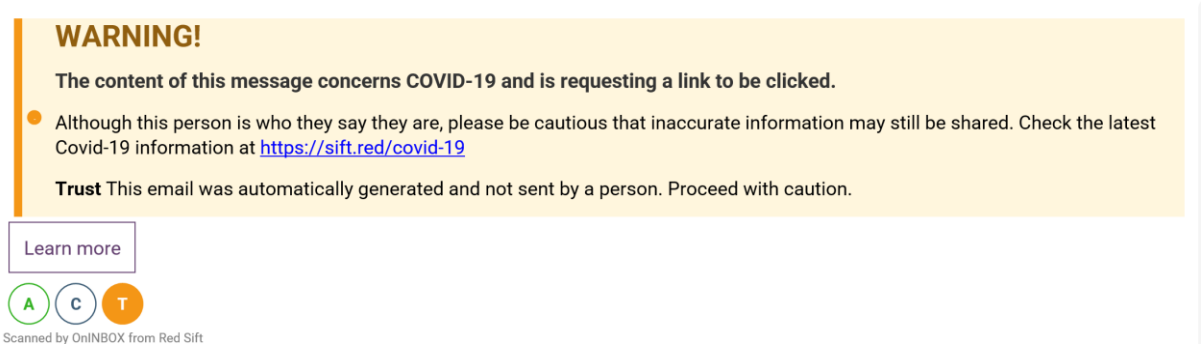
Yet many businesses rely solely on a legacy SEG (Secure Email Gateway) to defend against the relentless onslaught of ingenious and compelling email campaigns designed to extort, steal credentials, deliver advanced malware and to compromise critical accounts. Social engineering, the art of persuading somebody to do something they wouldn't ordinarily do, is at the heart of this.

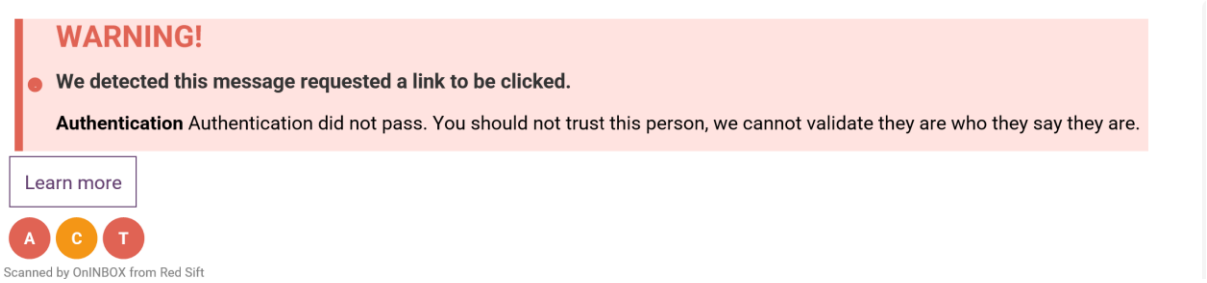
In today's ever-changing environment, an intelligent email security solution that includes AI, computer vision, automation, human reporters, and crowdsourced threat intelligence is an absolute must for organisations to stay protected from a breach.

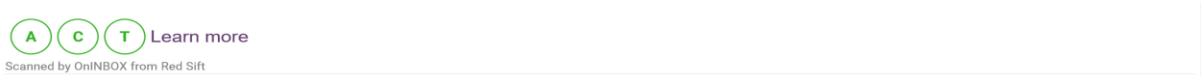
The user and their inbox are now your new line of defence. If you don't educate your staff, and change their behaviour towards security risk, your technology point products are futile countermeasures.

Octree Limited The Lloyds Building Birds Hill Letchworth Herts. SG6 1JE
T: +44 (0) 1462 416400 E: security@octree.co.uk U: https://octree.co.uk U: https://securapro.co.uk
Company No: 6773278 Registered Office: 28 - 31 The Stables, Wrest Park, Silsoe, Bedfordshire MK45 4HR

.

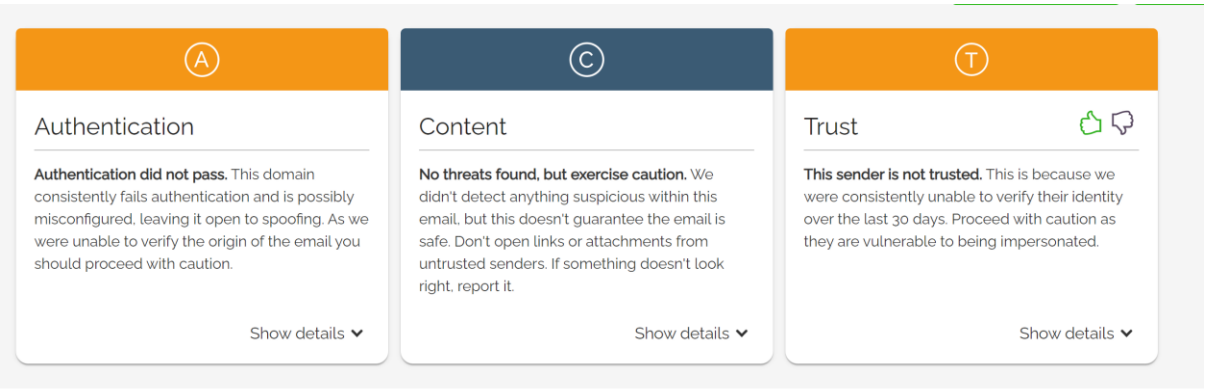






In our environment, sitting at the top of every email are clear, traffic light-coloured indicators that break down the trustworthiness of a sender's risk profile, allowing users to make informed decisions when they engage with their email, as shown above.

If the end user clicks on “Learn More” they can review a concise explanation of each decision around Authentication, Content and Trust. this helps end-users identify potential risks before engaging with the email, without interrupting productivity, or adding pressure to become a knowledgeable expert.



Combine this with an advanced threat protection solution that detects zero-day threats at the first encounter instead of days later. Traditional email security solutions depend on data from previously detected cyber threats and successful penetration tactics. This creates protection gaps for new, unknown threats to exploit, by which time its already too late.

And educate your staff, change the security culture of your employees. Influence specific security behaviours. Measure and reduce risk. CybSafe is software that helps security teams reduce avoidable incidents. It does so by supporting and educating people, by empowering and improving confidence, and by measuring and improving their security behaviours. Think «Fitbit» fitness tracker, but for personal security decisions.

This means security teams can see which elements of their security programme are working, and know why. You'll be more valued because you can prove reduction of human-cyber risk.

Finally, ensure your domain cannot be spoofed. Protecting domain reputation greatly influences an organization's email deliverability. Mailbox providers rely on domain reputation to determine trust. The better a domain reputation, the more likely receiving email servers will trust the emails. And of course, the worse the domain reputation, the less likely an email service provider will trust the emails. Email has become the biggest threat vortex for an organization's domain reputation because of the ease at which bad actors can take advantage of unassuming customers.

The InfoSec Institute has found that customers are 42% less likely to engage with an organization after a phishing attack. Unfortunately, bad actors are constantly looking for ways to take advantage of consumers. Prevalent methods include spoofing, misusing, or even creating a close cousin of an established domain to conduct a phishing campaign. This way, when a customer sees the phishing attempt, they trust the sender and are more likely to inadvertently give the bad actor access to their systems.

Implement email authentication protocols so mailbox providers can easily identify and respond to illegitimate messages. This includes Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) to validate the content through digital signatures. Then, organizations can implement Domain-based Message Authentication, Reporting and Conformance (DMARC) to direct mailbox providers to block or filter unauthorized messages spoofing your domain in the sender address of emails.

Register close cousin domains. Unfortunately, bad actors are eager to take advantage of common typos and misspellings to trick unsuspecting consumers into their phishing attempts. To thwart this, businesses should defensively register the scope of domains that bad actors could potentially abuse.

And that is why my staff, and my business, are far more secure than yours.