


The Norfolk Cyber Conference 2025



Think Like a Hacker:

Simple Steps to Secure Your Business



A photograph of an empty casino floor, likely at MGM Las Vegas, showing rows of slot machines and gaming chairs. The floor has a colorful, patterned carpet. A red text box is overlaid on the image.

MGM Las Vegas casino under
cyberattack, empty and not
functioning Wednesday 9/13
2.30 Pacific time

TikTok
@casinocompwallet

Casino giant MGM expects \$100 million hit from hack that led to data breach

Reuters

🕒 2 minute read · Published 9:40 PM EDT, Thu October 5, 2023



M&S cyber-attack disruption to last until July

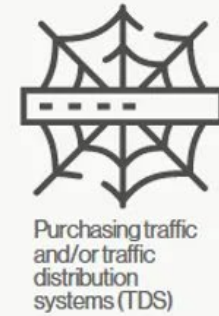




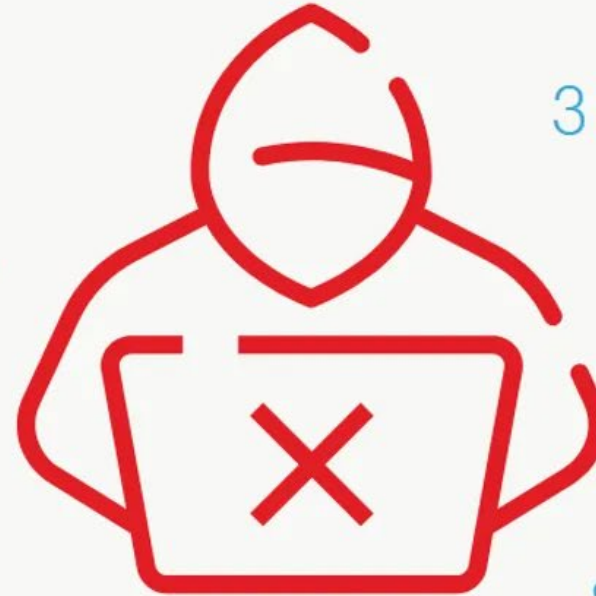
1 Services



2 Distribution



3 Monetization



Faces behind the Hacks

Noah
Urban



Ahmed
Elbadawy



Tyler
Buchanan



Arion
Kurtaj



30%
40%
56%

Credential Theft: Attackers Prefer Logging In, Not Breaking In

Stats

- 56% of incidents involve valid credentials without MFA.
- 1.8 billion credentials stolen in first half of 2025.
- Credential theft up 160% year-over-year.

Insert source information here



30%
40%
56%

Credential Theft: Attackers Prefer Logging In, Not Breaking In

Why it matters

- Attacker bypass perimeter defences
- Enables ransomware, data theft and supply chain compromise

Insert source information here



30%
40%
56%

Credential Theft: Attackers Prefer Logging In, Not Breaking In

Defences

- MFA everywhere
- Password managers and strong policies
- Monitor for compromised credentials:
Dark web scans
- Zero trust: verify every access

Insert source information here





ORIGINAL

DEEPPFAKE

EM HONEST

Y *THIS* ONE

EM HONEST

Y *THIS* ONE



The AI Arms Race

AI: The New Weapon in Cybercrime

87% of organizations faced AI-powered attacks in the past year

AI-generated phishing emails now have a **54% click-through rate**
4.5x higher than human-written ones

Deepfake voice scams (“vishing”) use AI to impersonate CEOs,
vendors, and banks

SMBs are **3x more likely** to be targeted due to weaker defences.

**SMBs must adopt AI-driven defenses to
counter AI -driven threats**

Cybersecurity basics every business must get right

1	2	3	4
Cyber Hygiene Essentials	Employee Awareness	Access Control	Incident Response
<ul style="list-style-type: none">• Strong Passwords and MFA• Regular Patching and updates• Data Backups (3,2,1)• Malware protection	<ul style="list-style-type: none">• Phishing• Social Engineering• Embed a Cybersecurity culture	<ul style="list-style-type: none">• Principle of Least privilege• Monitor 3rd party access• Smartphones	<ul style="list-style-type: none">• Create a written down plan• Very basic is better than none• Practice this



National Cyber Security Centre

www.ncsc.gov.uk/section/advice-guidance/small-medium-sized-organisations

Cyber Security Small Business Guide

Backing up your data

Take regular backups of your important data, and test they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

- **Identify what needs to be backed up.** Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.
- **Ensure the device containing your backup is not permanently connected** to the device holding the original copy, neither physically nor over a local network.
- **Consider backing up to the cloud.** This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

- **Switch on PIN/password protection/fingerprint recognition** for mobile devices.

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at

www.ncsc.gov.uk/smallbusiness

- Configure devices so that when lost or stolen they can be **tracked, remotely wiped or remotely locked**.
- Keep your **devices** (and all **installed apps**) **up to date**, using the 'automatically update' option if available.
- When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.
- **Replace devices that are no longer supported by manufacturers** with up-to-date alternatives.

Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

- **Use antivirus** software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.
- **Patch all software and firmware** by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.

- **Control access to removable media** such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.

- **Switch on your firewall** (included with most operating systems) to create a buffer zone between your network and Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

- Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.
- **Scan for malware** and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).
- Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

- Make sure all laptops, Macs and PCs **use encryption products** that require a password to boot. Switch on **password/PIN protection or fingerprint recognition** for mobile devices.
- **Use two factor authentication (2FA)** for important websites like banking and email, if you're given the option.
- **Avoid using predictable passwords** (such as family and pet names). Avoid the most common passwords that criminals can guess (like password).
- **If you forget your password** (or you think someone else knows it), tell your IT department as soon as you can.
- **Change** the manufacturers' default passwords that devices are issued with, before they are distributed to staff.
- **Provide secure storage** so staff can write down passwords and keep them safe (but not with their device). Ensure staff can reset their own passwords, easily.
- **Consider using a password manager**, but only for your less important websites and accounts where there would be no real permanent damage if the password was stolen.

The essentials of cyber security

Cyber Essentials scheme

Self-assessment questionnaire
optional on-site Audit (CES+)

Firewalls
Configuration
Patches
Malware
User accounts

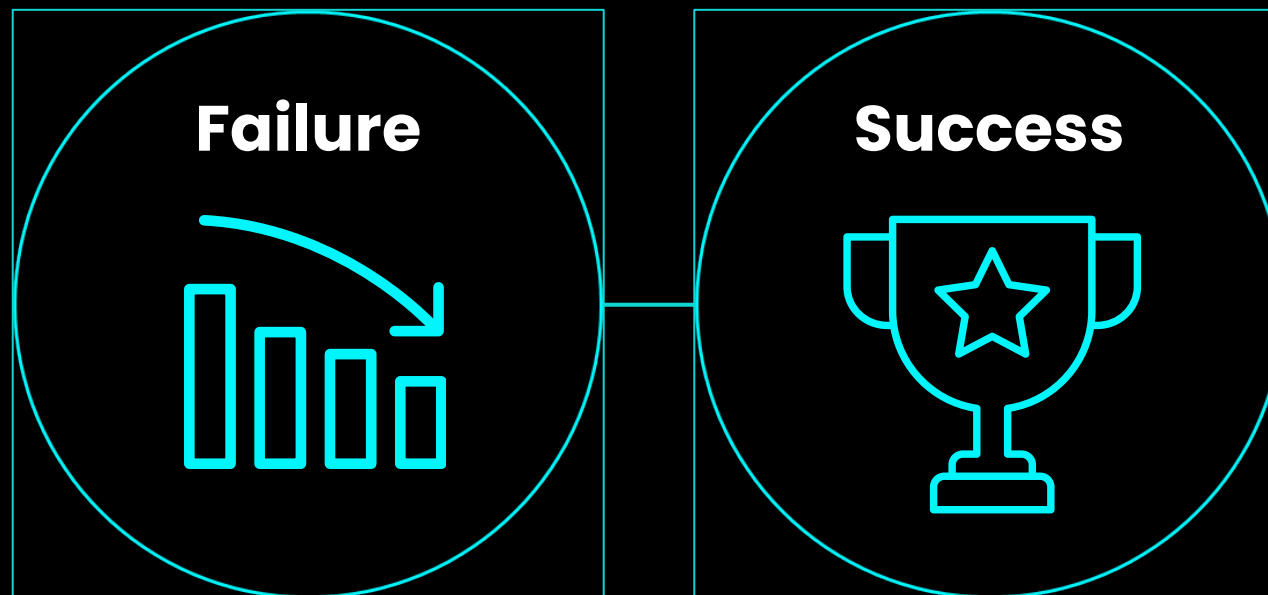
The Government wants every
organisation in the UK to be
Cyber Essentials Certified

Cyber Essentials is a simple but effective, UK Government backed scheme that will help you to protect your organisation, whatever its size, against a whole range of the most common cyber attacks.

Cyber attacks come in many shapes and sizes, but the vast majority are very basic in nature, carried out by relatively unskilled individuals.

There are 2 levels of certification





Vulnerabilities | OS out of date | Admin controls | Cloud Services MFA



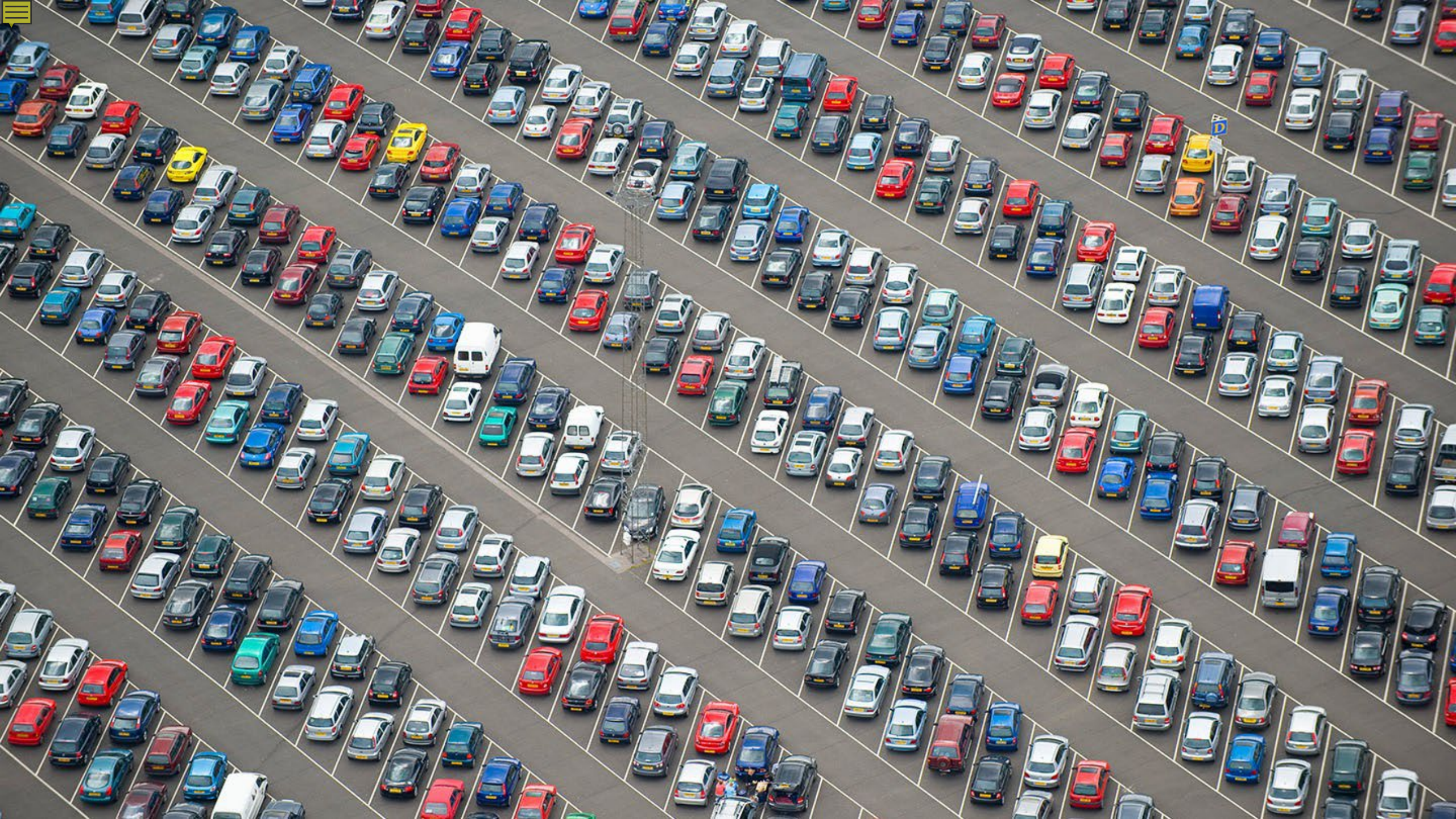
Insurance companies

Insurance companies report that companies with CE controls in place are 92% less likely to claim on Cyber insurance than ones without CE controls in place



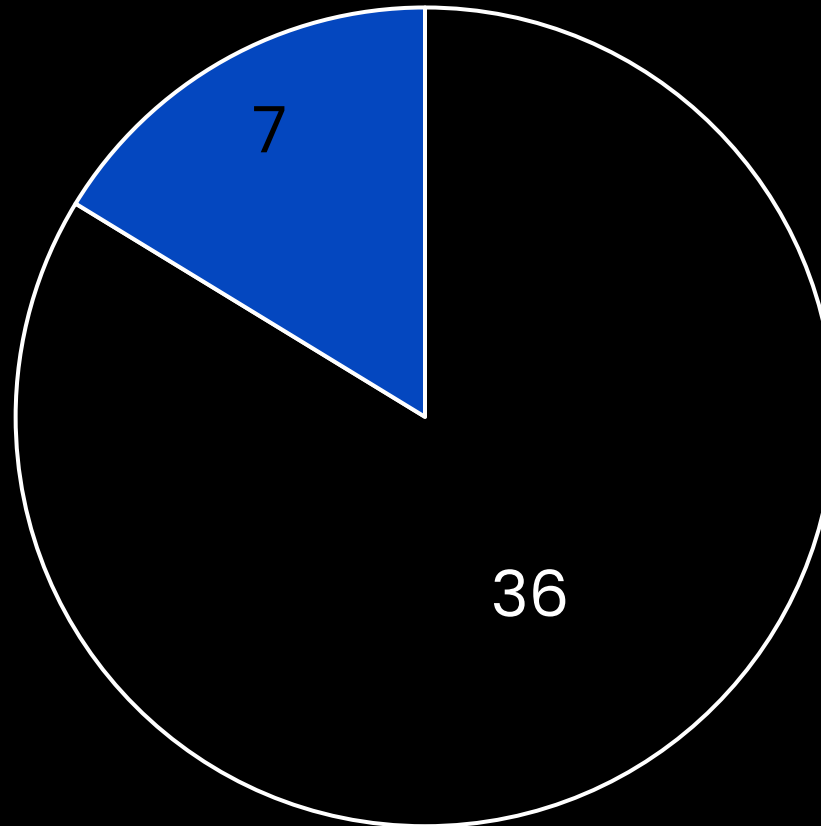
Cyber Essentials Certification





SPF configuration

Norfolk Cyber Conference Nov 2025



□ SPF, Correct

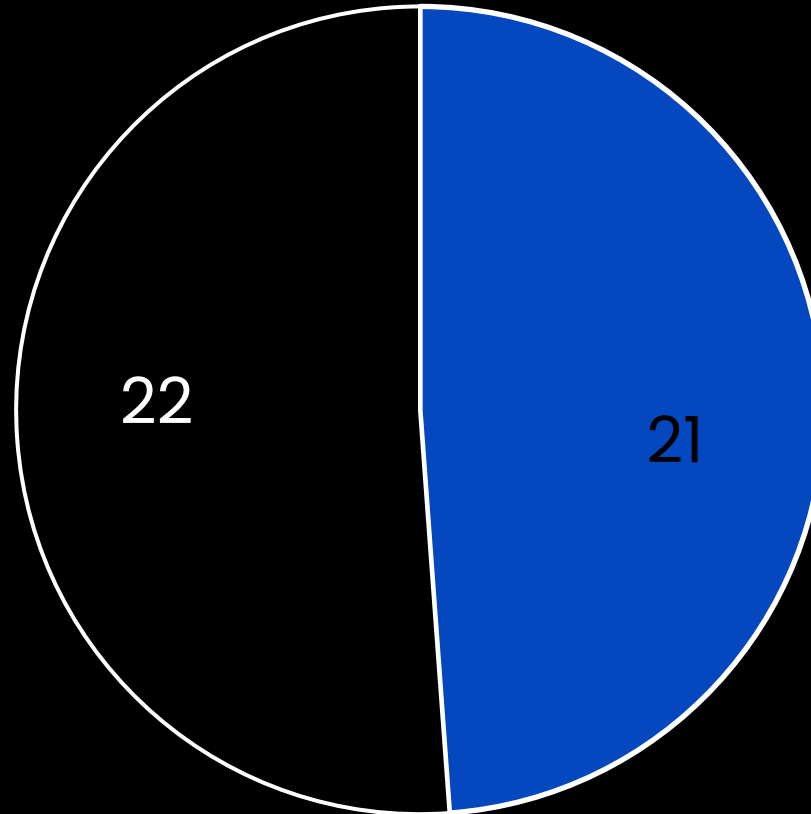
■ SPF not configured correctly

Sample size 43



SPF and DMARC configuration

Norfolk Cyber Conference Nov 2025



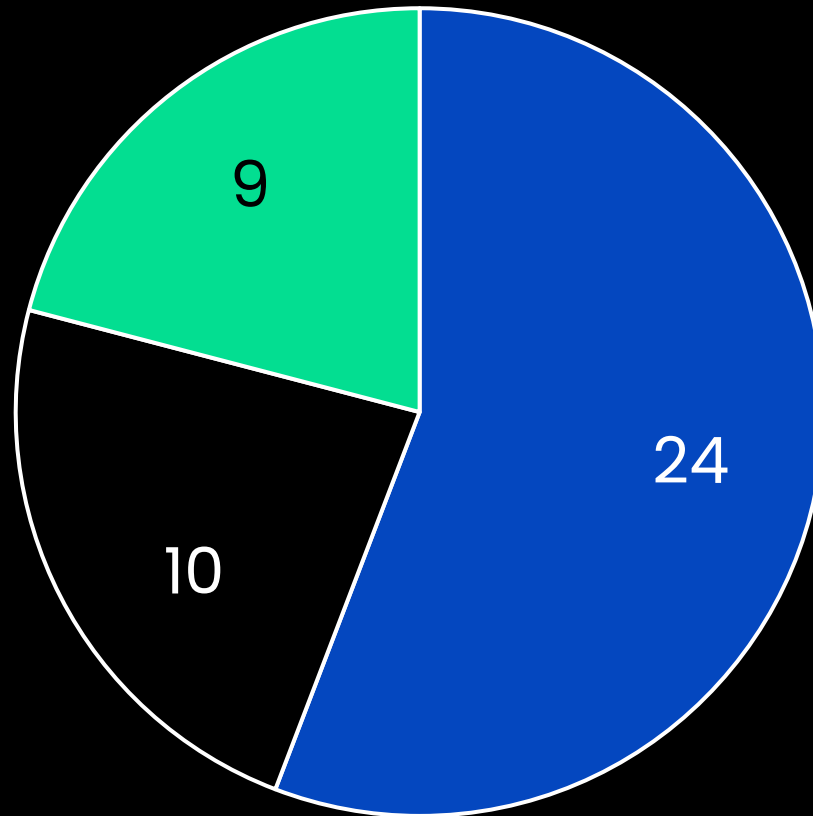
■ SPF, DMARC NOT Correct

□ SPF or DMARC Correct



Website basic vulnerability scan

Norfolk Cyber Conference Nov 2025



■ Rating A/B

■ Rating C

■ Rating D-F

5 Laws of Cybersecurity

Law 1: If there is a vulnerability, it will be exploited, no exceptions

Law 2: Everything is vulnerable in some way

Law 3: With Innovation comes opportunity for exploitation

Law 4: Humans can trust when they shouldn't

Law 5: When in doubt, see Law 1



Key Takeaways

1

Enable MFA
Everywhere

2

Train ALL your
staff
(Phishing &
Deepfakes)

3

Cyber
Essentials
Certification

4

Build and test a
response plan
(no matter how
basic)

Mostyn Thomas

Senior Director of Security, Pax8 EMEA

25 years experience working with MSPs, including founding and running Astrix integrated systems in 2001, which he sold in 2018 to concentrate on cybersecurity.

Much of his work with MSPs is to deliver effective cybersecurity solutions to the MSP company itself and their customers through best practice and awareness training.

In addition to his unique experience, Mostyn holds security certifications from Comptia, the British Computer Society, the National Cyber Security Centre and is a qualified Cyber Essentials assessor.

E: mthomas@pax8.com



Mostyn Thomas NCSC CCP
Entrepreneur | Technologist |
Cybersecurity for MSPs | NED



