System Force I.T.
Secure IT Simplified

PROTECTING YOUR ORGANISATION'S IDENTITY ONLINE

Email & Identity Security

Post-Webinar Summary & Key Takeaways

System Force IT – March 2026 Client Webinar Follow-Up

Thank you for attending our March webinar, "Protecting your Organisation's Identity Online."

This session focused on one of the most critical areas of modern cybersecurity: email and identity security. As organisations increasingly rely on cloud services, collaboration platforms, and remote access, identity has effectively become the new security perimeter.

This document summarises the key learning points from the webinar and highlights practical actions organisations can take to reduce the risk of fraud, credential theft, and email-based attacks.

1

WHY EMAIL REMAINS THE PRIMARY ATTACK VECTOR

Email continues to be the most common entry point for cyber attacks against organisations.

Modern attackers rarely attempt to break into systems directly. Instead, they attempt to trick users into giving them access by stealing credentials or persuading employees to take unsafe actions.

Common risks include:

- Clicking malicious links in phishing emails
- Entering credentials into fake login pages
- Opening malicious attachments
- Responding to impersonated messages from executives or suppliers
- Granting access to malicious applications

When attackers obtain valid login credentials, they can gain access to:

- Corporate email accounts
- Cloud services such as Microsoft 365
- Internal systems and shared files
- Financial information
- Sensitive customer or employee data

In many cases, attackers do not need to "hack" systems at all — they simply log in using stolen credentials.

2

THE HUMAN ELEMENT IN CYBERSECURITY

Research consistently shows that the majority of cyber incidents involve a human element.

Attackers exploit human behaviour and psychology rather than technical vulnerabilities.

Common manipulation techniques include:

- Urgency – "Your account will be suspended"
- Authority – "The CEO needs this urgently"
- Fear – "Immediate payment required"
- Curiosity – "You've received a secure document"

Because these tactics create pressure to act quickly, people may respond before fully verifying the legitimacy of a message.

This is why cybersecurity awareness training remains one of the most important defensive measures available to organisations.

3

HOW EMAIL ATTACKS WORK TODAY

Email-based attacks have become significantly more sophisticated.

Common techniques include:

- **Credential Harvesting**
  Attackers send emails directing users to fake login pages designed to steal usernames, passwords, or personal information.
- **Business Email Compromise (BEC)**
  Attackers impersonate senior executives, finance staff, or suppliers to request urgent payments or sensitive information.
- **Email Spoofing**
  Messages are sent that appear to come from trusted sources such as:
  - Company directors
  - Finance departments
  - Suppliers
  - HMRC
  - Microsoft or other service providers

These messages may use:

- Look-alike domains
- Forged sender addresses
- Display name deception

Because email systems were originally designed to deliver messages rather than verify identities, these attacks can appear extremely convincing.

4

PRE-TAX SEASON FRAUD AND HMRC IMPERSONATION

During the webinar we also discussed a common seasonal threat: tax-related phishing campaigns.

Fraud attempts often increase around important financial deadlines, particularly during self-assessment tax return periods.

Common examples include:

- HMRC impersonation emails
- Fake payment requests
- Payroll diversion fraud
- Messages claiming urgent action is required

Because organisations may already expect tax-related communications, employees may be more likely to trust these messages.

Attackers exploit this urgency to encourage quick responses.

5

IDENTITY IS THE NEW SECURITY PERIMETER

Historically, organisations focused on protecting the network perimeter.

Today, the reality is very different.

Cloud services and remote working mean that access to systems is primarily controlled through user identity rather than physical location.

If attackers compromise a legitimate account:

- They appear as a trusted user
- Security alerts may be harder to detect
- They can move through systems more easily
- They may access email, files, and financial systems

In effect, once attackers log in as a legitimate user, they bypass traditional security controls.

This is why protecting identity has become central to modern cybersecurity.

6

MODERN PASSWORD BEST PRACTICE

Traditional password practices are no longer considered sufficient.

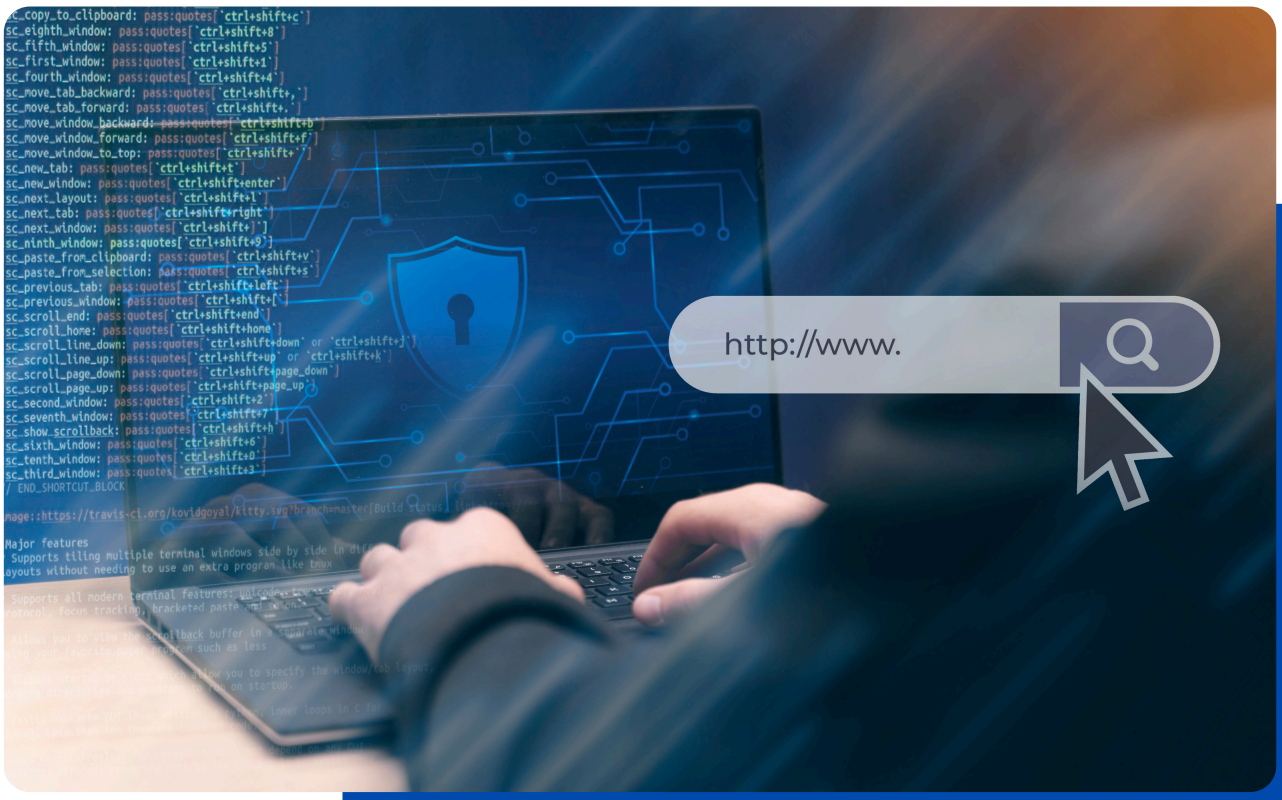
Mandatory frequent password changes often lead to predictable behaviour, such as:

- Password1 becoming Password2
- Winter2024 becoming Winter2025
- Passwords written on sticky notes

Instead, modern best practice recommends:

- Using long, unique passwords
- Avoiding password reuse across systems
- Using a password manager to securely store credentials
- Blocking commonly used passwords
- Encouraging memorable passphrases rather than complex short passwords

If one password is compromised and reused across systems, attackers may gain access to multiple services.



7

MULTI-FACTOR AUTHENTICATION (MFA)

One of the most effective security controls discussed during the session was Multi-Factor Authentication (MFA).

MFA requires users to provide more than one form of authentication before accessing systems.

This typically includes:

- Something you know – a password
- Something you have – a mobile authenticator app or hardware token
- Something you are – biometric verification such as fingerprint or facial recognition

Even if a password is stolen, MFA adds an additional layer of protection.

Research shows that enabling MFA can prevent the vast majority of automated account takeover attacks.

For modern organisations, MFA should now be considered a baseline security control rather than an optional feature.

8

SECURING MICROSOFT 365 ENVIRONMENTS

Many organisations rely heavily on Microsoft 365 for email, collaboration, and document management.

Key security recommendations include:

- Enforcing MFA for all users
- Implementing Conditional Access policies
- Protecting administrator accounts
- Ensuring administrative accounts are not used for everyday tasks
- Regularly reviewing permissions and access controls

Failure to configure these protections correctly remains a common weakness in many organisations.

9

TECHNOLOGY ALONE IS NOT ENOUGH

While tools such as Microsoft Defender and advanced monitoring solutions can help detect threats early, technology alone cannot eliminate cyber risk.

People remain the key decision-makers within organisations.

A strong cybersecurity culture includes:

- Regular staff awareness training
- Clear incident reporting procedures
- Ongoing phishing awareness
- Access control policies
- Practised incident response plans

Training should be continuous and role-relevant, rather than a once-per-year exercise.

10

COMPLIANCE AND REGULATORY EXPECTATIONS

Cybersecurity also plays an important role in regulatory compliance.

UK organisations must consider obligations under:

- UK GDPR and the Data Protection Act
- Information Commissioner's Office (ICO) expectations
- Cyber Essentials security standards

Where enforcement action occurs, it is often because:

- Known risks were ignored
- Basic controls were missing
- Staff were not adequately trained

Cybersecurity is therefore not just an IT issue — it is a business risk management responsibility.

KEY TAKEAWAYS FROM THE SESSION

The most important messages from this webinar were:

- Attackers increasingly target people rather than technology
- Email and identity compromise remain the most common entry point for cyber incidents
- Password hygiene and MFA are essential security controls
- Cloud services make identity protection critical
- Staff training plays a major role in reducing risk

> **As one key message from the session highlighted:**
> "Attackers don't break in – they log on."

HOW SYSTEM FORCE IT CAN SUPPORT YOU

System Force IT can help organisations strengthen their security posture through:

- Microsoft 365 security configuration reviews
- Identity and access management improvements
- Multi-Factor Authentication deployment
- Security awareness training programmes
- Phishing simulation campaigns
- Cyber Essentials readiness support
- Incident response planning

Our goal is to help organisations build sustainable, practical cybersecurity processes that align with both operational needs and regulatory requirements.

FINAL THOUGHT

Cybersecurity is no longer just a technical issue. It is a business resilience issue.

The organisations that successfully defend against modern cyber threats are those that:

Protect identity
Verify trust
Train their people
· Continuously review their security posture

Protecting your organisation's identity online is not a one-off task — it is an ongoing discipline.

System Force I.T.
Secure IT Simplified

SYSTEM FORCE IT

sales@systemforce.co.uk

Sales: 0330 0167 681

Support: 0330 0167 680

Fax: 0330 0167 689

If you would like a follow-up discussion or a security review, please contact our team.