nTrust
Your IT support partner

Get Cyber Fit in 2025

Strengthen Your Digital Defences in 12 Weeks

Just like physical fitness requires a plan, discipline, and the right exercises, achieving cyber fitness demands a focused approach.

That's why we've developed the *Get Cyber Fit in 2025* programme. It's a 12-week journey designed to fortify your organisation against cyber threats.

Each week introduces a vital action step, tailored to help you build a resilient, secure digital environment while reducing risks and ensuring compliance.

Think of it as your business's cybersecurity workout plan:

- Week by week, action by action, you'll strengthen your defences, from identifying vulnerabilities to implementing robust policies and processes.
- By the end of the programme, your business will be leaner, stronger, and more prepared to tackle the ever-evolving cyber threat landscape.

The reward? Peace of mind, minimised downtime, enhanced trust with your customers, and significant cost savings from avoided breaches or data loss.

Are you up for the challenge and ready to commit to your company's digital health? Let's get Cyber Fit!

Compete at least one of these tasks every week for the next 12 weeks and you'll increase your Cyber Security Position:

Change all default passwords on boundary firewall devices: Access the firewall's administrative interface, locate the password settings, and replace the default password with a strong, unique one.

Enable multi-factor authentication (MFA) on all cloud services: Configure your cloud services to require MFA for all users. This typically involves setting up an additional verification method, such as a text message code or authentication app.

Set a minimum password length of 12 characters with complexity requirements: Implement a password policy that requires passwords to be at least 12 characters long and include a mix of lowercase and uppercase letters, special characters, and numbers.

Limit access to data and systems based on roles: Ensure employees only have access to the data and systems necessary for their roles. This can be achieved through role-based access control (RBAC) policies.

Regularly review and update user access rights: Periodically review user access rights to ensure they are still appropriate for their roles. Remove or adjust access as needed.

Implement strong password policies: Encourage unique, complex passwords and use a password manager for storage.

Automatically lock out accounts after five failed login attempts: Configure your systems to automatically lock user accounts after five consecutive failed login attempts. This helps prevent brute force attacks and unauthorised access.

Conduct regular employee training on cyber security: Provide regular training sessions to help employees recognise phishing emails and other social engineering tactics.

Use encryption for sensitive data: Ensure all sensitive data, whether in transit or at rest, is encrypted to protect it from unauthorised access.

Implement robust email filters: Use email filtering solutions to block malicious content and reduce the risk of phishing attacks.

Establish a process for handling compromised passwords or accounts: Create a written policy outlining how to handle situations where passwords or accounts are suspected to be compromised. This should include steps for changing passwords and notifying affected users.

Regularly back up critical business data: Automate backups of critical business data and systems to a secure, offsite location or cloud service. Periodically test recovery processes to ensure backups are functional and accessible during emergencies.

Stay on Track with Your Cyber Fit Goals

We understand that implementing all 12 steps in the *Get Cyber Fit in 2025* programme can feel overwhelming, especially if you're juggling other business priorities.

But remember, you don't have to go it alone. If you're struggling with any of the steps—or even just need a nudge to get started—we're here to guide, support, and motivate you every step of the way.

Our team of experts is ready to help you overcome any challenges, tailor solutions to your needs, and ensure you achieve your cyber fitness goals.

Our desire is for you to build a stronger, more secure digital future for your business.

Are you up for the challenge and ready to commit to your company's digital health?

Let's get Cyber Fit!

Contact nTrust

Mark Cody

Commercial Director

T +44 3331 50 60 70

E m.cody@ntrustsystems.co.uk

W www.ntrustsystems.co.uk