



Cybersecurity and IT Protection for Irish Businesses since 1996

25 Point Cybersecurity Checklist

A practical self assessment for Irish small and medium sized businesses

Use this checklist to identify simple, high impact improvements across your business. Tick Yes or No for each item, then use the notes column to record actions, owners or questions for your IT provider.

This is a general business health check, not a certification or legal assessment. NIS2 may apply to certain qualifying entities and sectors; it is not automatically a requirement for every SME. If it may be relevant to your organisation, ask for a readiness discussion.

Business details

Business name	
Completed by	
Date completed	

Your result

Count the items marked No. Focus first on the actions that protect accounts, email, backups and payment processes.

No answers	What this suggests	Recommended next step
0 to 4	Good foundation	Keep reviews and staff awareness regular.
5 to 9	Some important gaps	Prioritise the highest risk No answers over the next 30 days.
10 or more	Elevated exposure	Arrange a focused security review and recovery check.

MF Secure is the cybersecurity and IT protection service from MF Computer & ICT Services. We help Irish businesses identify practical risks, strengthen everyday defences and plan for disruption.

Talk to MF Secure: 086 262 0906 | mfcomputerservices1@gmail.com

1 Accounts and access

#	Check	Yes	No	Notes / action
1	Every staff member has their own user account. Shared logins are avoided or tightly controlled. <i>This makes it possible to remove access quickly and see who did what.</i>	☐	☐	
2	Multi factor authentication is switched on for email, cloud services, finance and administrator accounts. <i>A password alone is no longer enough.</i>	☐	☐	
3	Strong, unique passwords are used and kept in an approved password manager where practical. <i>Avoid reusing passwords between systems.</i>	☐	☐	
4	Access is removed promptly when an employee or contractor leaves or changes role. <i>Review leavers, role changes and external suppliers.</i>	☐	☐	
5	Administrator access is limited to people who genuinely need it and uses separate admin accounts. <i>Everyday email accounts should not normally have admin rights.</i>	☐	☐	

2 Microsoft 365 and cloud services

#	Check	Yes	No	Notes / action
6	Microsoft 365 security settings have been reviewed, including sign in, sharing and administrator controls. <i>A regular review helps keep settings aligned with how you work.</i>	☐	☐	
7	Email protection is in place to reduce phishing, spoofing and malicious attachments. <i>Check that junk and quarantine alerts are being monitored.</i>	☐	☐	
8	External sharing of files is controlled, with sensitive folders restricted to the right people. <i>Do not leave confidential files open to anyone with a link.</i>	☐	☐	
9	Company email domains have SPF, DKIM and DMARC configured or a plan to configure them. <i>These controls help prevent criminals impersonating your business.</i>	☐	☐	
10	Key cloud services and third party apps connected to company data are known and reviewed. <i>Remove old apps and unnecessary permissions.</i>	☐	☐	

3 Devices and network

#	Check	Yes	No	Notes / action
11	All computers, phones and tablets used for work have automatic security updates enabled. <i>Include devices used remotely or at home.</i>	☐	☐	
12	Business devices have reputable antivirus or endpoint protection and it is kept up to date. <i>Make sure alerts are checked and actioned.</i>	☐	☐	
13	Devices are protected by a screen lock and encryption where available. <i>This reduces exposure if a device is lost or stolen.</i>	☐	☐	
14	Wi Fi uses a strong password, modern security settings and a separate guest network where practical. <i>Keep business devices off the guest network.</i>	☐	☐	
15	The business router, firewall and any remote access tools are supported, updated and securely configured. <i>Replace equipment that no longer receives security updates.</i>	☐	☐	

4 Backups and recovery

#	Check	Yes	No	Notes / action
16	Important business data is backed up automatically and regularly. <i>Include email, cloud files, accounts data and critical systems.</i>	☐	☐	
17	At least one backup copy is protected from ransomware, such as an offline, immutable or separate cloud copy. <i>A backup connected all the time can also be encrypted by attackers.</i>	☐	☐	
18	Backups are tested by restoring a file or system at least every three months. <i>A backup is only useful if it can be restored.</i>	☐	☐	
19	The business knows which systems and data must be restored first after an incident. <i>Set realistic recovery priorities and responsibilities.</i>	☐	☐	
20	Backup arrangements are documented, including who checks them and how to contact the provider. <i>Keep this information accessible if normal systems are unavailable.</i>	☐	☐	

5 People policies and incident response

#	Check	Yes	No	Notes / action
21	Staff receive regular, practical guidance on phishing, passwords, payment fraud and reporting concerns. <i>Short, repeated training works better than a one off session.</i>	☐	☐	
22	There is a clear process for checking unusual bank detail or payment change requests. <i>Use a known phone number to verify, not the number in the email.</i>	☐	☐	
23	The business has simple written rules for acceptable use, remote working, passwords and handling sensitive data. <i>Keep policies short enough that people will use them.</i>	☐	☐	
24	There is an incident response plan covering who to contact, what to isolate and how to keep evidence. <i>Include your IT provider, insurer and key decision makers.</i>	☐	☐	
25	Cyber insurance, key supplier obligations and NIS2 readiness have been considered where relevant to the business. <i>NIS2 applies to certain qualifying entities and sectors; it is not automatically a requirement for every SME.</i>	☐	☐	

NEXT STEPS: Return to your IT provider or contact us below for a free consultation , no obligation,

Arrange your free consultation today!

086 262 0906

Martin Fleming
WhatsApp contact



Email : mfcomputerservices1@gmail.com

Book Online: <https://www.mfictservices.com/book-online>