SpySecure

Cybersecurity Checklist

For small and medium-sized businesses

For management teams, CTOs, IT managers and external IT partners to assess how complete and effective an organisation’s cybersecurity really is.

Checklist

Cybersecurity checklist

Each level builds on the previous one.

SpySecure

LEVEL 1

The basics

Minimum protection if you use very few cloud services.

- [ ] Endpoint Protection

LEVEL 2

Standard

Essential for small and medium-sized businesses using Microsoft 365, Google Workspace or other SaaS apps.

- [ ] Email Security
- [ ] Cloud Security
- [ ] Identity Security
- [ ] Employee Security

LEVEL 3

Advanced

When customers require proof of security or you must meet NIS2 or ISO requirements.

- [ ] Backups
- [ ] Compliance Management
- [ ] Business Password Management
- [ ] Domain Protection

ALWAYS · ACROSS EVERY LAYER

Fully managed service

24/7 monitoring & response

- [ ] Install tools & keep security settings up to date
- [ ] Monitoring · review security alerts
- [ ] Detection · investigate suspicious activity
- [ ] Response · contain threats & resolve incidents
- [ ] Monthly security reports

Tools alone provide little protection without continuous monitoring and response.

LEVEL 1 · THE BASICS

Endpoint Protection

SpySecure

What to check

Ask for evidence—not just a yes or no.

- [ ] **Central device management**
  All business devices are enrolled, visible and assigned to an owner.
- [ ] **Operating system patching**
  Security patches are deployed promptly and failed updates are followed up.
- [ ] **Software updates**
  Common business applications are updated centrally, not left to individual users.
- [ ] **Next-generation antivirus (NGAV)**
  Behaviour-based malware protection is enabled on every supported device.
- [ ] **Endpoint detection & response (EDR)**
  All running processes and device activity are monitored for suspicious behaviour—not just files.

WHY IT MATTERS

Every laptop and desktop is a route into company data. Antivirus alone cannot detect and contain modern attacks.

EVIDENCE TO REQUEST

- ✓ **Monthly endpoint security report**
- ✓ **Device inventory and patch status**
- ✓ **Detected threats and actions taken**

FULLY MANAGED SERVICE

24/7 security operations

- [ ] **Monitoring**
  Continuous review of security alerts
- [ ] **Detection**
  Investigate suspicious activity
- [ ] **Response**
  Contain threats and resolve incidents

LEVEL 2 · STANDARD

Email Security

SpySecure

What to check

Ask for evidence—not just a yes or no.

- [ ] **Phishing filtering**
  Deceptive messages, sender impersonation and payment scams are detected and filtered.
- [ ] **Attachment filtering**
  Attachments are scanned and malicious files are blocked or quarantined.
- [ ] **Link filtering**
  Malicious URLs are detected and blocked at delivery and when employees click.
- [ ] **Content Disarm & Reconstruction (CDR)**
  Documents are rewritten to remove or disarm risky content while retaining usable information.
- [ ] **Outgoing data loss prevention (DLP)**
  Outgoing emails are checked to prevent sensitive information being sent without authorisation.
- [ ] **Employee warning banners**
  In-email warnings explain suspicious signals, helping employees learn and make safer decisions.
- [ ] **Employee reporting**
  Employees can easily report suspicious emails; each report is reviewed and acted on.

WHY IT MATTERS

Email is a common entry point for phishing, malicious links, unsafe attachments and invoice fraud.

EVIDENCE TO REQUEST

- ✓ **Monthly email security report**
- ✓ **Blocked threats and outbound data alerts**
- ✓ **Warning banners and report follow-ups**

FULLY MANAGED SERVICE

24/7 **security operations**

- [ ] **Monitoring**
  Continuous review of security alerts
- [ ] **Detection**
  Investigate suspicious activity
- [ ] **Response**
  Contain threats and resolve incidents

LEVEL 2 · STANDARD

Cloud Security

SpySecure

What to check

Ask for evidence—not just a yes or no.

- [ ] **Cloud detection & response**
  Activity across critical cloud and SaaS platforms is monitored centrally.
- [ ] **Suspicious cloud activity**
  Unusual downloads, sharing, mailbox and administrator changes are detected.
- [ ] **Risky sign-ins**
  Impossible travel, unfamiliar devices and anomalous locations are investigated.
- [ ] **Connected application monitoring**
  Third-party applications and OAuth access are visible and reviewed.
- [ ] **Data loss prevention (DLP)**
  Sensitive data movement and external sharing are detected and controlled.

WHY IT MATTERS

Company data is spread across Microsoft 365, Google Workspace and SaaS apps. Unmonitored access, downloads and sharing can expose it.

EVIDENCE TO REQUEST

- ✓ **Monthly cloud activity report**
- ✓ **Connected apps and sharing settings**
- ✓ **Suspicious activity and actions taken**

FULLY MANAGED SERVICE

24/7 **security operations**

- [ ] **Monitoring**
  Continuous review of security alerts
- [ ] **Detection**
  Investigate suspicious activity
- [ ] **Response**
  Contain threats and resolve incidents

LEVEL 2 · STANDARD

Identity Security

SpySecure

What to check

Ask for evidence—not just a yes or no.

- [ ] **MFA enforced—not just enabled**
  Multi-factor authentication is mandatory for every user and administrator, with no optional setup.
- [ ] **Account security monitoring**
  Sign-ins, resets, forwarding rules and other risky changes are monitored.
- [ ] **Privileged account control**
  Administrator roles are limited, separated and reviewed regularly.
- [ ] **Leaked credential monitoring**
  Company domains and accounts are checked and exposures are actioned.
- [ ] **Inactive and former accounts**
  Unused and leaver accounts are disabled promptly and reviewed.

WHY IT MATTERS

A stolen, overprivileged or forgotten account can bypass device controls and access company data directly.

EVIDENCE TO REQUEST

- ✓ **Monthly identity security report**
- ✓ **MFA enforcement and account status**
- ✓ **Leaked credentials and actions taken**

FULLY MANAGED SERVICE

24/7 **security operations**

- [ ] **Monitoring**
  Continuous review of security alerts
- [ ] **Detection**
  Investigate suspicious activity
- [ ] **Response**
  Contain threats and resolve incidents

LEVEL 2 · STANDARD

Employee Security

SpySecure

What to check

Ask for evidence—not just a yes or no.

- [ ] **Security awareness training**
  Interactive e-learning at least monthly, tailored to each employee's role and behaviour.
- [ ] **Phishing simulations**
  Realistic phishing tests run weekly to practise recognising suspicious messages.
- [ ] **Targeted follow-up**
  Employees who click or share data receive relevant additional training.
- [ ] **New joiners enrolled immediately**
  New employees are directly added to the ongoing learning and phishing simulation programme.
- [ ] **Management reporting**
  Participation, risk and improvement trends are visible to management.

WHY IT MATTERS

Employees make daily security decisions. Their training must be continuous, relevant and measurable.

EVIDENCE TO REQUEST

- ✓ **Monthly employee security report**
- ✓ **Training completion and phishing results**
- ✓ **Personalised follow-up and progress**

FULLY MANAGED SERVICE

24/7 **security operations**

- [ ] **Monitoring**
  Continuous review of security alerts
- [ ] **Detection**
  Investigate suspicious activity
- [ ] **Response**
  Contain threats and resolve incidents

LEVEL 3 · ADVANCED

Backups

SpySecure

What to check

Ask for evidence—not just a yes or no.

- [ ] **Encrypted device backup**
  Critical local data is backed up automatically and securely.
- [ ] **Encrypted cloud backup**
  Microsoft 365, Google Workspace or SaaS data is backed up outside the existing environment.
- [ ] **Backup monitoring**
  Failures and missing devices or accounts are actively followed up.
- [ ] **Retention and immutability**
  Versions are retained and protected from deletion or tampering.
- [ ] **Recovery testing**
  Restores are tested and recovery time and data-loss targets are defined.

WHY IT MATTERS

Ransomware, deletion or a compromised administrator can destroy live data—and poorly protected backups.

EVIDENCE TO REQUEST

- ✓ **Monthly backup report**
- ✓ **Coverage, failures and retention settings**
- ✓ **Latest restore-test result**

FULLY MANAGED SERVICE

24/7 **security operations**

- [ ] **Monitoring**
  Continuous review of security alerts
- [ ] **Detection**
  Investigate suspicious activity
- [ ] **Response**
  Contain threats and resolve incidents

LEVEL 3 · ADVANCED

Compliance Management

SpySecure

What to check

Ask for evidence—not just a yes or no.

- [ ] **Scope and gap assessment**
  Applicable NIS2, ISO and customer requirements are mapped and assessed.
- [ ] **Security policy management**
  Policies have owners, approval dates and a defined review cycle.
- [ ] **Controls and evidence**
  Every relevant requirement links to an implemented control and current evidence.
- [ ] **Compliance reporting**
  Management can see gaps, priorities, actions, owners and status.
- [ ] **Vulnerability management**
  Weaknesses are identified, prioritised, remediated and evidenced.

WHY IT MATTERS

NIS2, ISO and customer requirements demand documented controls, accountable owners and verifiable evidence.

EVIDENCE TO REQUEST

- ✓ **Monthly compliance status report**
- ✓ **Gap assessment and control register**
- ✓ **Evidence and remediation progress**

FULLY MANAGED SERVICE

24/7 **security operations**

- [ ] **Monitoring**
  Continuous review of security alerts
- [ ] **Detection**
  Investigate suspicious activity
- [ ] **Response**
  Contain threats and resolve incidents

LEVEL 3 · ADVANCED

Business Password Management

SpySecure

What to check

Ask for evidence—not just a yes or no.

- [ ] **Business password manager**
  Business credentials are stored in a business password manager, not browsers, spreadsheets or chat.
- [ ] **Controlled password sharing**
  Access is granted without copying or exposing credentials where possible.
- [ ] **Access to team vaults**
  Employees receive access to the relevant team vaults and credentials for their role.
- [ ] **Audit logging**
  Credential use, sharing and changes are traceable.
- [ ] **Offboarding and recovery**
  Access can be removed centrally and emergency access is controlled.

WHY IT MATTERS

Shared and reused passwords create invisible access and often remain active after employees or suppliers leave.

EVIDENCE TO REQUEST

- ✓ **Monthly password management report**
- ✓ **Team vault access and adoption**
- ✓ **Access changes and offboarding log**

FULLY MANAGED SERVICE

24/7 security operations

- [ ] **Monitoring**
  Continuous review of security alerts
- [ ] **Detection**
  Investigate suspicious activity
- [ ] **Response**
  Contain threats and resolve incidents

LEVEL 3 · ADVANCED

Domain Protection

SpySecure

What to check

Ask for evidence—not just a yes or no.

- [ ] **SPF, DKIM and DMARC setup**
  Email authentication records are configured correctly for every authorised sending service.
- [ ] **DMARC enforcement**
  The policy progresses to reject instead of remaining in monitoring mode.
- [ ] **Continuous sender monitoring**
  New senders and authentication failures are investigated.
- [ ] **Domain spoofing protection**
  Lookalike and spoofing attempts are detected and addressed.
- [ ] **Brand Indicators for Message Identification (BIMI)**
  Where supported, a verified company logo is shown alongside authenticated emails.

WHY IT MATTERS

Criminals can spoof your company domain to deceive customers, suppliers and employees—even without breaching your systems.

EVIDENCE TO REQUEST

- ✓ **Monthly domain protection report**
- ✓ **Authentication and DMARC enforcement**
- ✓ **Authorised senders and spoofing attempts**

FULLY MANAGED SERVICE

24/7 **security operations**

- [ ] **Monitoring**
  Continuous review of security alerts
- [ ] **Detection**
  Investigate suspicious activity
- [ ] **Response**
  Contain threats and resolve incidents

SpySecure

All-in-one cybersecurity.

Fully managed.

SME-priced.

From €9.99 per licence per month

Need help?

Talk to our Security Operations Center.

Schedule a call →

More information on improving your security

Small and medium-sized businesses	See our packages
Professional IT partners	See our partner programme