30 Cyber Security Mistakes Small Businesses Make

A practical guide based on real issues seen in small organisations

Contents

Introduction

Cyber attacks increasingly affect small businesses because attackers assume security controls may be weaker than in larger organisations. In practice, many successful breaches occur because simple protections have not been implemented or maintained.

This guide highlights thirty common cyber security mistakes seen during reviews of small business systems. Each section explains the problem, provides a realistic scenario and suggests practical steps that organisations can take to reduce risk.

1. Weak Passwords

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

2. Reusing Passwords Across Systems

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

3. No Multi-Factor Authentication

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

4. Ignoring Software Updates

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

5. No Data Backups

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

6. Backups Are Never Tested

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

7. Using Public Wi-Fi for Business

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

8. Default Router Passwords

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

9. No Antivirus Protection

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

10. Too Many Administrator Accounts

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

11. No Security Awareness Training

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

12. Ignoring Phishing Risks

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

13. Sharing Passwords by Email

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

14. No Incident Response Plan

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

15. No Device Screen Locks

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

16. Using Unsupported Software

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

17. No Website Updates

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

18. Unused User Accounts

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

19. No Monitoring of Login Attempts

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

20. No Guest Wi-Fi Separation

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

21. Not Verifying Supplier Payment Changes

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

22. Opening Unexpected Attachments

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

23. Storing Sensitive Data Unencrypted

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

24. No Mobile Device Security

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

25. No Network Firewall

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

26. Insecure Remote Access

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

27. No Access Control Policies

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

28. Ignoring Security Alerts

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

29. No Cyber Security Policy

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

30. Assuming Small Businesses Are Not Targets

Why this matters

Many small organisations unintentionally create this vulnerability through everyday working practices. Attackers frequently use automated scanning tools to identify weaknesses across thousands of businesses at once. Once a weakness is found it may be exploited to gain access to systems, email accounts or sensitive data.

Real-world example

A typical example might involve a small company using common cloud services such as Microsoft 365, Google Workspace or a website management platform. If basic security protections are missing, an attacker may gain access to an account and use it to send fraudulent emails, steal customer data or deploy ransomware.

Practical ways to reduce the risk

1. Review your current security configuration and policies.
2. Apply basic technical protections such as strong authentication and updates.
3. Ensure staff are aware of common cyber risks.
4. Regularly review systems, backups and user access.

About Wellis Technology

Wellis Technology supports organisations with technology resilience, cyber security guidance and standards-based best practice. The focus is on practical improvements that help organisations reduce cyber risk and operate securely.

Website	www.wellis-technology.co.uk
Email	wellis.technology@gmail.com
Telephone	07976 806151

Guide written by John Ellis - Wellis Technology