Micro Maintenance

IT Support & Cybersecurity Specialists

CYBERSECURITY

AWARENESS GUIDE

Protecting yourself and your organisation online

SIXTH EDITION

Micro Maintenance

IT Support & Cybersecurity Specialists

Prepared by

Micro Maintenance

IT Support & Cybersecurity Specialists

Micro Maintenance has been providing IT support, cybersecurity, and managed services to businesses across Surrey and Sussex for over 20 years. ISO 9001 certified, we help organisations of all sizes protect their systems, their data, and their people.

Phone	Email
01293 446677	**enquiries@micromaintenance.co.uk**

Website

micromaintenance.co.uk

Units 1 & 2, Courtlands Estate, Antlands Lane, Horley, Surrey RH6 9TE

Contents

1. The Threat Landscape

Cyber attacks are not a niche or distant risk — they affect organisations of every size, in every sector, every single day. Understanding who is behind these attacks and what they are after is the first step to protecting yourself and your organisation.

Who Are Cyber Criminals?

The popular image of a lone hacker in a dark room is outdated. The threat landscape has changed dramatically:

Then — Hackers for Fun

Historically, attacks came from individual hackers attempting to compromise systems or cause damage to prove their skills. Disruptive, but limited in scale.

Now — Organised Crime & Nation States

The threat today is from well-funded criminal gangs and nation states, operating on a massive, industrial scale — with dedicated teams, sophisticated tooling, and clear financial or political motives.

Key takeaway

Cyber criminals are professional, motivated and relentless. They run automated attacks against everything, all the time — not just interesting targets.

What Do Cyber Criminals Want?

Understanding what attackers are after helps explain why every employee — not just IT staff — is a potential target.

Money

Direct theft, financial fraud, and ransomware payments.

Personal Data

Usernames, passwords and identity information to sell or exploit.

System Control

Using your computer or accounts as a platform for further attacks.

Intellectual Property

Trade secrets, research and business-critical data.

Ransomware Leverage

Encrypting your files and demanding payment.

Disruption

Nation-state actors may attack simply to destabilise organisations or critical infrastructure.

2. Ransomware

Ransomware is malicious software that encrypts your files and demands payment for their decryption. It is one of the most damaging and costly forms of cyber attack facing businesses today.

How Ransomware Works

① Often has a countdown timer — the ransom increases the longer you wait, creating pressure to act without thinking.

② Once encrypted, it spreads across your network to servers and other workstations — a single infected device can compromise the entire organisation.

③ It seeks out and destroys backups to prevent recovery without paying the ransom.

④ Even if you pay, there is NO guarantee your data will be restored. You are dealing with criminals.

The Numbers

<50%	£100k+	7%
of UK businesses are insured against cybersecurity risks	Ransomware demands can reach hundreds of thousands of pounds	chance your data will be restored even if you pay the ransom

Sources: Gov.UK 2025, Hiscox 2024

3. Phishing & Email Attacks

Email remains the most common attack vector. Phishing emails are designed to trick you into revealing passwords or other sensitive information — typically via a fake login page. Attacks range from broad mass campaigns to highly targeted 'spear phishing' that uses personal details to appear convincing.

> **"Password phishing is the top security problem in the world today"**
> Microsoft, 2022

Recognising Phishing Emails

- Can be random mass campaigns or highly targeted 'spear phishing' attacks that reference your name, role or recent activity.
- Can be extremely convincing — even appearing as a reply to an existing email chain.
- Uses a link that leads to a fake login page to steal your credentials.
- Poor grammar and outlandish offers can be deliberate to weed out savvy targets — leaving only the most susceptible.

Preventing Phishing Attacks

✔ DO	**Verify suspicious emails** Contact the sender via a different channel — call a known number, not the one in the email.
✘ DON'T	**Don't click unverified links** Never click on links or open attachments unless you are absolutely sure of the sender and the content.
✔ DO	**Be wary of login prompts** Be especially wary of attachments requiring you to log in to Microsoft 365, Dropbox or similar services to view content.
✘ DON'T	**Don't ignore the EXTERNAL flag** Don't ignore the EXTERNAL flag in Outlook — report suspicious flagged emails to IT immediately.

Vishing — Voice Phishing

Phone calls are increasingly used to trick employees into revealing information or taking harmful actions.

How it works

The caller impersonates IT support, your bank, HMRC, Microsoft, or a supplier. They create urgency ('Your account has been compromised — act now'), may already know basic details about you to seem credible, and AI voice cloning can now impersonate real colleagues convincingly.

How to protect yourself

Hang up and call back on a number you find independently — not one given by the caller. IT and banks will never ask for your password over the phone. Urgency is a red flag — slow down and verify. Report suspicious calls to IT immediately.

CEO & CFO Fraud — Business Email Compromise

One of the most costly cyber attacks, targeting employees who handle money or sensitive data.

Typical scenario

You receive an urgent email appearing to be from the CEO or a senior director asking you to make an immediate bank transfer, purchase gift cards, or share sensitive payroll data — often while they are 'travelling' and 'unreachable by phone'.

✘ DON'T	**Urgency & secrecy** 'Don't tell anyone', 'needs to happen today' — classic pressure tactics to bypass normal process.
✘ DON'T	**Unusual requests** Requests to change a supplier's bank account, make an out-of-process payment, or buy gift cards.
✘ DON'T	**Slightly wrong sender** The email address may be one character off: ceo@company-name.co instead of ceo@companyname.co.
✔ DO	**Always verify independently** Call the requestor directly on a known number before acting. No legitimate request will object to a quick verification call.

4. Account Security

Account compromise is the unauthorised access and use of your online accounts using stolen or leaked credentials. Databases containing over a billion compromised usernames and passwords are freely available on the dark web, and these are used automatically to try and access many other accounts.

You are very likely to be in one of these databases.
Reusing passwords puts you at far greater risk — attackers will try your leaked credentials on every service they can find.

Preventing Account Compromise

Use unique passwords
Never reuse the same password for more than one service.

Protect email accounts
Email accounts are priority targets — they unlock everything else.

Use strong passwords
The easier it is to remember, the weaker it probably is. Use a password manager.

Avoid social sign-in
Avoid 'Sign in with Facebook/Google' where possible.

Beware public Wi-Fi
Attackers can create convincing fake hotspots to steal your login.

Use a password manager
Tools like 1Password create and store complex passwords for you.

Multifactor Authentication (MFA)

MFA requires something you know (your password) and something you have (your phone) to log in. Even if your password is stolen, attackers still cannot access your account without your physical device.

99.9%

of account compromise attacks are blocked by MFA (Source: Microsoft 2019)

Passkeys — The Future of Authentication

Passkeys are a new and highly secure method of logging in — no username, no password, no MFA code needed. They are based on strong cryptography and already supported by most major

platforms.

Simple to use Just approve a notification on your phone — no passwords to remember.	**Highly secure** Based on strong cryptography. Cannot be phished or stolen in the traditional sense.
Private by design Your identity information is stored on your device, not on the website's servers.	**No codes to enter** Unlike MFA, there are no one-time codes to intercept or enter manually.

5. Malicious Software

Malware can be delivered through many vectors — often without any obvious warning signs. Once installed, it can steal data, encrypt files, provide attackers with remote access, or use your device to attack others.

How Malware Is Delivered

- Fraudulent websites — e.g. a typo in a web address takes you to an attacker's site.
- Legitimate websites that have been hacked or display malicious adverts.
- Unsolicited disks or USB drives — e.g. free gifts from trade shows or events.
- A memory stick you found — a classic and surprisingly effective attack method.
- Email attachments from compromised or spoofed sender accounts.

Preventing Malicious Software

✘ DON'T	**Don't mix business and personal use** Don't mix business and personal use on the same device — use separate computers where possible.
✘ DON'T	**Don't trust unexpected pop-ups** Don't accept downloads from unexpected pop-ups — e.g. a surprise Adobe update, browser update or free virus scan.
✘ DON'T	**Don't connect unknown storage** Don't connect storage from an unknown source, such as trade show handouts or a USB drive you found.
✔ DO	**Keep software updated** Keep all software and operating systems patched and up to date — vulnerabilities are patched in updates.

Software & Updates

Unpatched software is one of the most common ways attackers gain access to systems. Every unpatched vulnerability is a known, open door.

Software updates patch known security vulnerabilities — delaying them leaves a known door open for attackers.

Enable automatic updates on all devices where possible — for the OS, browsers, and all applications.

Never install unauthorised software on work devices. Even legitimate-looking tools can carry malware or create security gaps.

If you need software for work, request it through IT — don't download workarounds or personal alternatives.

6. Social Engineering & AI Threats

Social engineering is the art of manipulating people into providing information or performing an action that helps an attacker — exploiting human nature rather than technical vulnerabilities. It is increasingly automated and augmented by AI.

How Social Engineering Works

- Takes advantage of human nature — helpfulness, authority, curiosity and urgency.
- Even the most trivial information (e.g. a colleague's name) can be a starting point for an attack.
- A phone call asking for the name of someone in finance is a classic and effective technique.
- AI is now used to automate social engineering calls — you may not know you're talking to a machine.

Preventing Social Engineering

✔ DO	**Always verify identity** Always verify who you are communicating with — especially if the request is urgent or involves sensitive information.
✘ DON'T	**Don't share information freely** Don't provide any information about yourself, colleagues or your organisation unless you know exactly who wants it and why.
✔ DO	**Be mindful of public sharing** Social media posts and out-of-office messages reveal more than you think — attackers use this to craft convincing approaches.
✘ DON'T	**Don't be rushed** Urgency and tight timescales are a classic social engineering tactic — slow down and verify.

Artificial Intelligence & Emerging Threats

AI is making attacks more sophisticated, more automated, cheaper and faster. Defences that worked last year may not be sufficient today.

Malicious Code

AI can write and improve malware, dramatically lowering the skill barrier for attackers.

Convincing Phishing

AI generates highly convincing, personalised phishing emails at massive scale.

Deepfake Voice & Video

AI can impersonate colleagues or executives in telephone and video calls.

Automated Attacks

AI makes it possible to run thousands of attack attempts simultaneously and cheaply.

7. Safe Working Habits

Many breaches are not the result of sophisticated technical attacks — they happen because of everyday habits and oversights. The following practices significantly reduce your risk.

Device & Physical Security

Cyber attacks don't always happen online — physical access and carelessness are real risks.

✔ DO	**Lock your screen** Lock your screen whenever you step away from your desk — even briefly. Use Win+L (Windows) or Ctrl+Cmd+Q (Mac).
✘ DON'T	**Don't leave devices unattended** Never leave devices unattended in public places such as cafés, trains or conference venues.
✔ DO	**Be aware of shoulder surfing** Be aware of people watching your screen in public. Use a privacy screen filter on laptops.
✘ DON'T	**Don't bin sensitive documents** Don't dispose of printed documents in general waste — always shred anything containing sensitive or business information.

Remote Working Security

Working from home or on the road introduces risks that don't exist in a managed office environment.

Always use the VPN
Connect to the company VPN whenever accessing business systems remotely. It encrypts your traffic and protects company data.

Secure your home router
Change the default admin password on your home router. Keep its firmware updated. Use WPA3 or WPA2 encryption.

Avoid public Wi-Fi for work
Coffee shops, hotels and airports have unsecured networks. Never access work systems on public Wi-Fi without a VPN.

Mind your surroundings
Don't take sensitive calls or work on confidential documents where others can overhear or see your screen.

Safe Data Handling

How you store, share and dispose of data matters as much as how you protect it.

Use approved channels only

Never send sensitive business data via personal email, WhatsApp or consumer file-sharing services.

Be careful with cloud storage

Uploading company files to personal Dropbox, Google Drive or iCloud creates uncontrolled copies outside the business.

Classify before you share

Think about who actually needs access to information before sending it. Less is more.

Secure your printing

Collect prints promptly. Never leave sensitive documents on a printer tray or in a meeting room.

Shred, don't bin

Paper documents with names, account numbers, or business information must be shredded, not placed in general waste.

Clear desk policy

Lock away sensitive papers and devices at the end of the day — a clean desk is a secure desk.

8. If Something Goes Wrong

No-blame culture

Anyone can be tricked — cyber criminals are professionals. Clicking a link or sharing information by mistake is not shameful. Not reporting it is what turns a near-miss into a crisis. The speed of reporting a suspected incident is the single biggest factor in limiting its damage.

What to Do

Clicked a suspicious link?

Disconnect from the network immediately. Don't wait to see if anything happens. Contact IT now.

Shared a password accidentally?

Change the password immediately and notify IT. Don't assume nothing bad will come of it.

Received a suspicious email?

Report it to IT using the Phishing Report button in Outlook or forward it to the IT security team.

Something feels off?

If your device is behaving strangely, report it. Trust your instincts — early reporting saves the business.

9. Consequences of a Cyber-Attack

Cyber attacks have real, lasting consequences — not just for the IT department, but for the entire organisation and everyone who works in it.

Financial Loss

Cleanup costs can be tens of thousands of pounds. Cyber insurance premiums will dramatically increase following a breach.

Business Disruption

Cleanup of affected systems can take weeks, halting operations entirely and affecting customers and suppliers.

Data Loss

Trade secrets and personal data may be sold to other criminals and circulated for years — it cannot be recalled.

Reputation Damage

Disclosure of a breach can be legally mandatory under UK GDPR — clients, partners and the public will know.

Business Failure

A significant proportion of cyber-attack victims cease trading within 3 years. Small businesses are especially vulnerable.

Cybersecurity is a shared responsibility. Every employee who stays alert, questions the unexpected, and reports concerns promptly makes the entire organisation safer.

About Micro Maintenance

Micro Maintenance has been delivering expert IT support and cybersecurity services to businesses across Surrey and Sussex for over 20 years. ISO 9001 certified, we combine technical expertise with a personal approach — acting as a trusted IT partner rather than just a helpdesk. Whether you need full managed IT support or help with a specific challenge, our experienced team is here to keep your business secure, efficient and future-ready.

Managed IT Support

All-inclusive support contracts covering unlimited remote and on-site support, hardware, software and proactive monitoring — for a fixed monthly cost with no nasty surprises.

Cybersecurity Consultancy

From risk assessments and Cyber Essentials certification to endpoint security and staff awareness training, we help you build robust defences against modern threats.

IT Helpdesk

A responsive helpdesk staffed by qualified technicians ready to resolve issues quickly — by phone, remote access or on-site visit — minimising disruption to your working day.

GDPR & Compliance

Expert guidance on UK GDPR obligations, data protection policies and ongoing compliance monitoring, helping you avoid regulatory penalties and protect customer trust.

Microsoft 365 Solutions

As a Microsoft Silver Partner we advise on and implement M365 including email hosting, SharePoint, Teams and OneDrive — keeping your team connected and productive.

Network & Infrastructure

Design, installation and maintenance of cabling, wireless networks, fibre optics and servers — reliable, future-proof infrastructure tailored to your business.

20+	ISO 9001	5–100
Years in business	Certified quality	Employees supported

Get in touch for a free consultation

Concerned about your organisation's cybersecurity posture? Micro Maintenance offers a free initial consultation to assess your risks and recommend practical next steps.

01293 446677 • enquiries@micromaintenance.co.uk • micromaintenance.co.uk

Units 1 & 2, Courtlands Estate, Antlands Lane, Horley, Surrey RH6 9TE