Cybersecurity Awareness Guide for Businesses

Micro Maintenance

Important information

About this guide

This free guide is provided by Micro Maintenance and is based on our cybersecurity training course. It is intended as an introduction to the basics of cybersecurity for small & medium enterprise employees.

About us

Micro Maintenance is an ISO 9001 certified Managed Services Provider that provides IT support services and UK GDPR consultancy to businesses in Surrey and Sussex. You can find out more about us at http://micromaintenance.co.uk.

Liability

This book is meant to be advisory and is not a replacement for formal training, hardware and software based security, or insurance. Micro Maintenance and the author accept no liability whatsoever for the information provided. If you do not agree, please delete or dispose of this book.

Rights

About the author

This guide was written by Matt Boxall, who is the owner of Micro Maintenance Limited, an ISO 9001 certified managed services provider based in Southeast England. He has over 30 years of experience in the technology industry.

If you have any comments or questions about this guide, you can get in touch with Matt via email or LinkedIn:

book@micromaintenance.co.uk

https://www.linkedin.com/in/mattboxall

Version history

Initial release	October 2018
2nd Edition	November 2019
3rd Edition	March 2021
4th Edition	March 2022
5th Edition	January 2023

Index

The purpose of this guide

To explain the common types of cyber-attack that all businesses face every day.

To make you aware that you can't rely on technology alone to protect your business.

To provide you with advice to protect yourself and your business online, creating a *human firewall*.

To make you aware that every business is a constant target for cybercriminals.

Cybercrime statistics

1. 37% of respondents to a Sophos survey were hit by ransomware in the last year. More that half of those said the cybercriminals succeeded in encrypting their data.
2. The average ransom paid by mid-sized organizations was £130,000. However, on average only 65% of the encrypted data was restored after the ransom was paid.
3. You are far more likely to fall victim to cybercrime than any other kind of crime in the UK.
4. Only 32% of businesses have cyber risk insurance.

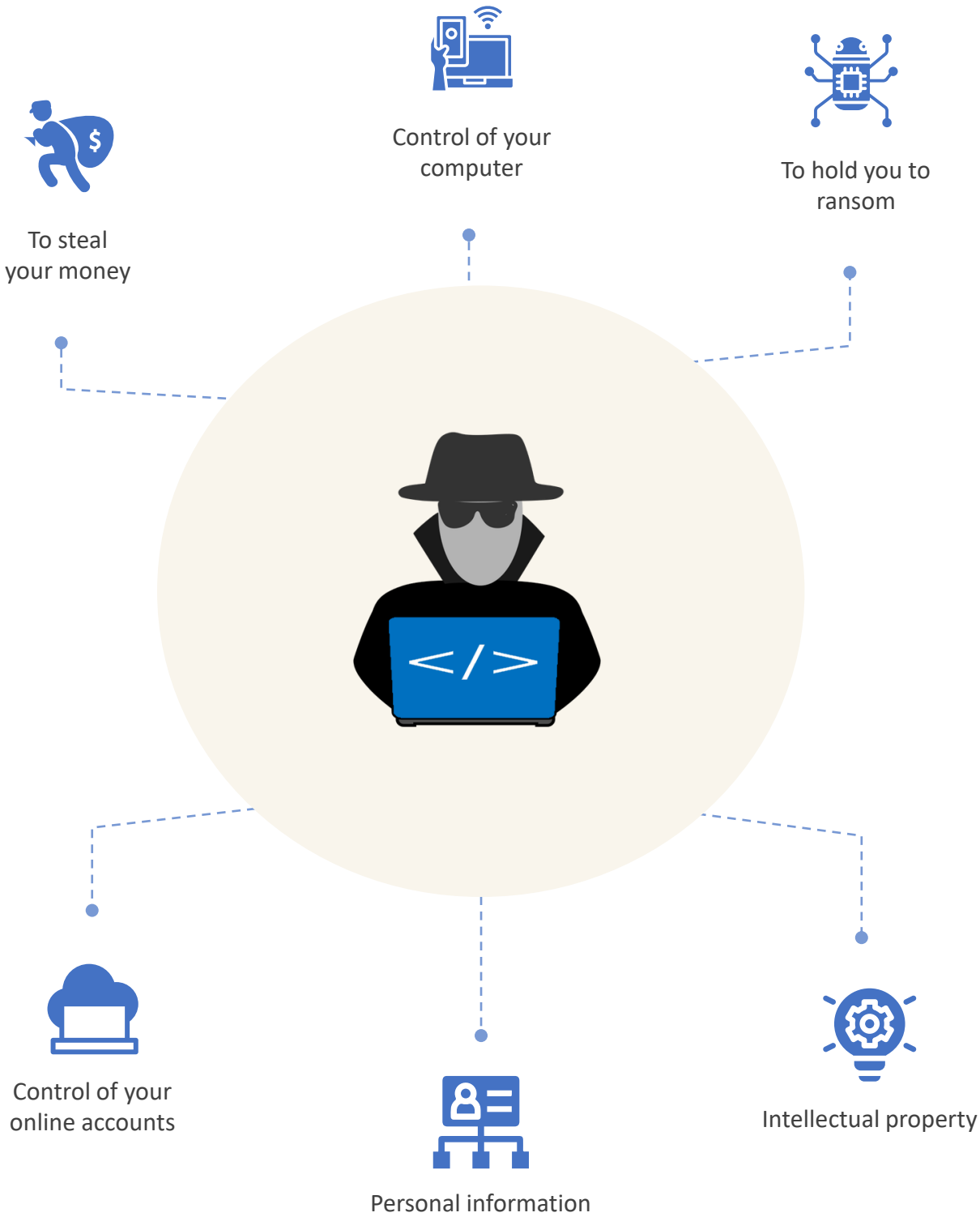
Sources:
Office for National Statistics 2020
Sophos - The State of Ransomware 2021

Who are cybercriminals?

Historically, cyberattacks were from hackers attempting to compromise systems or cause damage for fun or to prove their skills.

Contemporary threats are from organised crime, carried out on a massive scale by well-funded criminal gangs and nation states. The scale, determination and resources of these cybercriminals should not be under estimated. Every business, including yours, is a constant target.

What cybercriminals want



Financial theft

Cybercriminals want to steal your money, either by tricking you into making a payment, or by gaining access to your bank accounts. Common tactics include:

Account and device control

Cybercriminals want to gain access to your computer, typically for one or more of the following reasons:

To use your computer to access company resources like personnel records & intellectual property.

To install remote access software to spy on you.

To gain direct access your bank accounts via your computer, bypassing your bank's security features.

To install a crypto-virus (ransomware) to encrypt your data and hold you to ransom.

Ransomware

A ransomware (crypto-virus) attack is one of the most malicious and costly types of cybercrime.

1	Ransomware software infects your computer, often via a phishing email sent to you with a genuine looking attachment.
2	The ransomware will encrypt all your data and pop up a message asking for payment to restore it. The ransom amount can be tens of thousands of dollars or more.
3	Typically, you don't have long to pay before your documents are destroyed for good, but there is only a 65% chance that payment will actually result in recovery of your documents.
4	The ransomware will seek out any local backups, USB drives, network drives & cloud backups and try to destroy or encrypt that data too.
5	From there, the virus will try to replicate across your network affecting other computers, servers and backup devices.
6	If you don't have air-gapped backups of your data, ransomware could destroy your business. An example air-gapped backup system is multiple backup disks that are swapped and not left connected to your computer.
7	Cybercriminals often target specific business and do their homework, researching how much their target is likely to be able to afford.

Cryptocurrency

Cryptocurrencies, of which Bitcoin is probably the most well known, are virtual currencies that can be exchanged for real money.

Cryptocurrencies can be purchased and traded like other currencies, but they can also be “mined”.

Mining is carried out by running software that performs complex mathematical calculations to try and produce currency tokens.

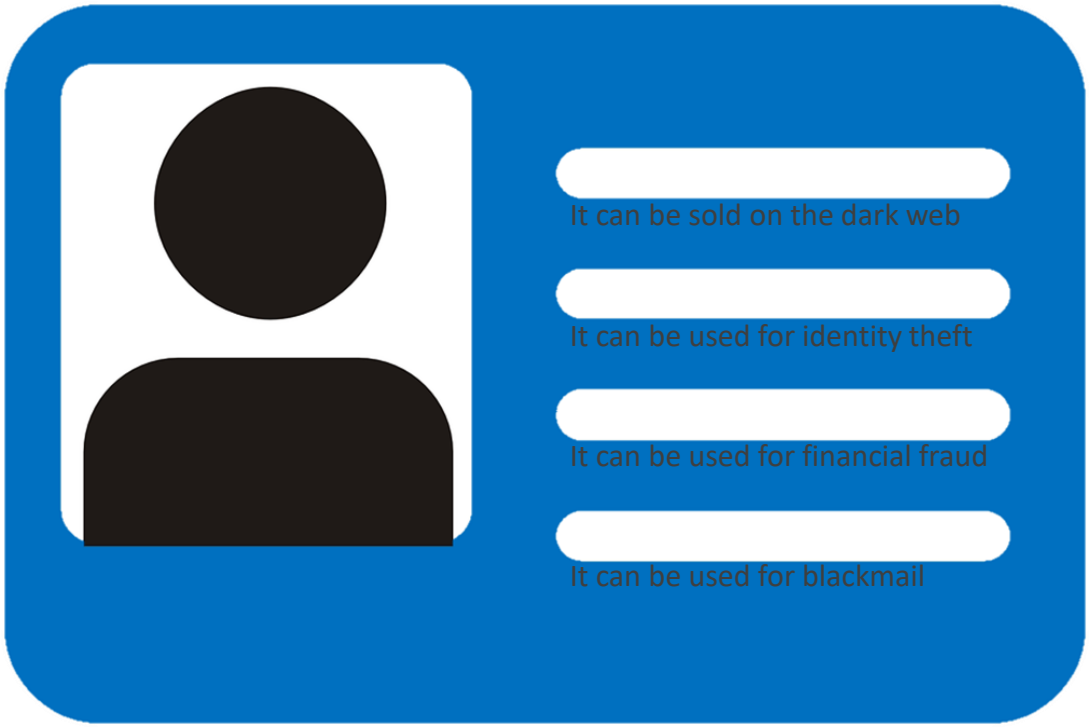
It is increasing difficult and costly to mine cryptocurrency, so hackers try to install mining software across as many computers as they can to increase their chances of generating the virtual currency.

A mining program can substantially slow down your computer or network and can add a significant cost to your energy bill.

It is likely that if your network has been compromised for mining purposes, other malicious activities are taking place.

Personal information

Personal information is a gold mine for cybercriminals, and it is frequently stolen in large quantities from unsecured databases on company networks and webservers. Information from multiple sources, including names, addresses, passwords, credit card information etc, is often combined into huge databases containing millions of records.



The principles of GDPR are a good starting place for applying protections such as encryption and data minimization. Micro Maintenance are qualified GDPR advisors.

Intellectual property

Your intellectual property is very valuable to you, and also to your competitors and cybercriminals who would like to steal it.

Many countries carry out state-sponsored hacking, phishing and social engineering on a huge scale, with the aim of stealing trade secrets and intellectual property.

It’s not just multinational companies that are targeted, businesses of all sizes are under constant attack.

If your business has unique manufacturing processes or other valuable information, you should take extra precautions to protect it.

The principles of GDPR are a good starting place for implementing protections such as encryption and data minimization.

Common methods of attack

Account Hacking

Phishing

Malicious Software

Social Engineering

Account hacking

It is the unauthorized access & use of your online accounts.

Massive databases of compromised usernames & passwords are freely available online, some of them with billions of account details.

These credentials are used repeatedly to try and access your online accounts.

You are very likely to be on one or more of these databases.

Reusing passwords put you at great risk.

You can check if your account details are included in any known data breaches at https://haveibeenpwned.com

Preventing account hacking

Here are some important tips on keeping your online accounts secure:

Never use the same password for more than one service. Having one account compromised in a data breach will result in your other accounts being breached as well.

Protect your email accounts with strong, unique passwords. This is a important as your email account can be used to request a password reset for your other accounts.

Use strong passwords. Totally random computer generated passwords are best, but multiple words is considered secure enough. For example the password *rock-press-inch-leader* is very hard to crack.

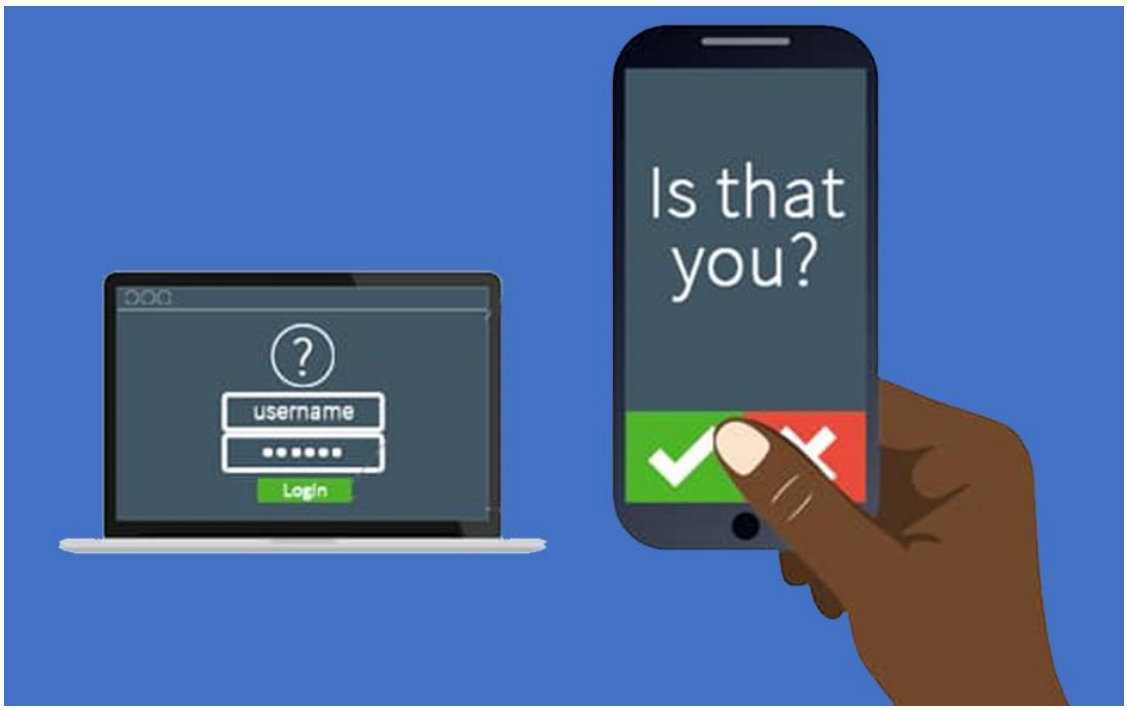
Consider using a password manager to create and store complex passwords for you, like 1Password or Bitwarden.

Avoid using options like Sign in with Facebook and Sign in with Google. One account hack could lead to multiple data breaches, and hackers can spoof these login pages on compromised sites.

Use fake answers (but keep a record) when setting up security questions like *What is your mother's maiden name?* Personal information like this can easily be obtained with social engineering techniques.

Multi-factor authentication

This helps keep your account secure. To log in on an unrecognized device, you need your username & password and another factor. This is also referred to as two factor authentication or MFA / 2FA.



Something you know and *something you have* provides multi-factor security and prevents a hacker from accessing your account, even if they know your username & password.

Some example second-factors (*something you have*):

- A one-time code from a security app on your phone which changes every 30 seconds
- Tapping the approve button in a security app on your phone
- A one-time code from a text message
- Inserting a physical security device into your USB port

Phishing

- A phishing email is an email that tries to trick you into providing your password or other information.
- They can be random, or they can be targeted at your organisation or even at you personally - this is called spear-phishing.
- Phishing emails can appear to be very genuine, even in the form of an expected reply from a co-worker or external contact.
- Outlandish offers and poor grammar are often deliberate - only easy targets fall victim, saving the cybercriminal a lot of wasted effort.
- You can be phished in other ways, too. For example, by telephone, text message or social media. Phishing is a form of social engineering.

Example phishing attack

Step 1

Register a domain name similar to your own, for example micrornaintenance.co.uk instead of micromaintenance.co.uk. (Here, the letters r n combine to look like the m in rnaintenance).

Step 2

Find out the name of two people within the organization from your website, social media, via social engineering or even from Companies House.

Step 3

Create a fake email account using the first name, copy company logo and other info from website or social media for a convincing looking email signature.

Step 4

Send an email from this fake account to the second person, asking for an urgent payment to be made.

Step 5

Follow up with further requests for increasing amounts of money until the victim realizes they have been defrauded.

Preventing phishing attacks

Don’t click on links or open attachments unless you are sure of the sender and the content. Be very wary of requests even slightly out of the ordinary.

Verify any suspicious emails by contacting the sender via a different channel, for example by phone to a known number. Don’t call the phone number in the email.

Be wary of attachments that require you to log in to Microsoft 365, Dropbox or other service to view the content. They are very likely to be trying to capture your credentials.

Phishing emails often ask you to act urgently to minimize the chance that you will stop and check what you are doing. Always take the time to verify suspicious or unusual requests.

Malicious software

Malicious software comes in many forms:

Viruses or worms can replicate themselves. They cause damage to software, data and even hardware.

Potentially unwanted programs, or PUPs, cause annoyances like changing your browser homepage or search results, or popping up adverts on your computer.

Trojan horse software hides itself on your computer and brings in other unwanted software.

A remote access trojan, or RAT, gives cybercriminal remote access to your computer. They can copy files, spy on you using your webcam or microphone, or even access your bank accounts via your computer while you are logged on, bypassing many online banking security features.

And it can get on to your computer in many ways:

From a fraudulent website, for example by misspelling a website address.

From a genuine website that has been hacked or is hosting malicious adverts.

From unsolicited disks, eg free gifts and trade show handouts.

From a memory stick you “found”.

Preventing malicious software

Do not use company IT equipment for personal web browsing. Social media sites are one of the biggest sources of malicious links.

Never accept an offered download that you did not purposely look for, for example Adobe Reader, a browser update or a free virus scan.

A padlock in your browser address bar is no guarantee that you are on a genuine website, only that you are securely connected to it. Other security logos that may be shown on a website are meaningless as they are just graphics that are easily added.

Be suspicious of disks from an unknown source, for example hand outs at trade shows or unsolicited disks that arrive in the mail.

Never insert a disk you found into your computer. It could have been purposely dropped near your premises on the chance it will be picked up and connected to a computer. Malicious USB drives may even have keys attached or be labelled “confidential” or similar, or your company name.

Social engineering

- Social engineering is the art of manipulating someone into divulging information or performing actions.
- It takes advantage of human nature to be helpful.
- Even the simplest piece of information like a name or contact information can be useful to an attacker.
- For example, giving out the name and email address of an accounts team member, and revealing whether they are in the office can lead to a targeted phishing email containing very convincing information.

Preventing social engineering

Always be aware of who you are communicating with.

Don’t provide any information about yourself, your colleagues or company - even trivial information, unless you know exactly who wants it and why.

If an unknown caller requests information, ask who is calling before providing it. If in doubt, ask for the caller’s details and say a colleague will call them back.

Be aware of what information you are making public. Social media posts and out-of-office emails can give a hacker lots of useful information.

Micro Maintenance

Thank you for reading this guide, I hope you found it useful.

If you have any comments or questions, please do get in touch. You can reach me by email or on LinkedIn.

book@micromaintenance.co.uk

https://www.linkedin.com/in/mattboxall