Cyber Security Basics

Inform.
Transform.
Protect.

VENOM·IT

Cyber Security Basics

Everyone Should Know

Welcome

When it comes to taking proper cyber security measures, your organisation is really only as strong as its weakest link.

In this guide, we will explain the basics of cyber security so that anyone in your organisation can understand and apply the principles for a secure working environment.

We will focus on two things: your people and your system. Because depending on whether you have properly educated your workforce and updated your systems, they can be either your best asset or greatest liability.

Cybercrime is only set to grow exponentially over the next few years. Most Industry and government experts agree that all businesses and individuals need to be supported and action taken. Understanding the very nature of the threat first will help to know which measures is best to take to successfully prevent them.

Cyber security means CIA

Confidentiality, integrity and availability are known as the CIA triad. These are the three main principles or 'legs' of cyber security. Remove any one of the three legs and the entire system fails. Let us explain.

Confidentiality

This is about who needs to have access to different parts of your system. And more importantly, defining who does not need access and whether they are properly excluded.

Integrity

Data integrity is essential. In other words, is the data in your system whole and correct? Ensuring data integrity means protecting it from being changed or erased – either on purpose by an unauthorised party or by accident by someone with authorised access. It also means making sure that any damage can be reversed.

Availability/Access

This is about making sure the right people can access the data they need. There's no point putting security measures in place that are so strict that the data becomes inaccessible. It's also important to make sure the data will still be secure when accessed remotely by a legitimate user from a non-secure location.

The Fourth Principle: Balance

Of course, CIAB sounds nowhere near as good as CIA. But in any security scenario, the need for balance is essential. Just as you shouldn't spend more on security than what the asset is worth, neither should you try to protect a high-value asset using the cheapest security solution you can find.

Your analysis of cyber security should consider cost vs convenience vs protection. Inconvenient rules might increase security in theory, but they are more likely to be broken or disregarded. When weighing cost vs protection, lean towards protection.

Did you know?

53% of all crimes reported in the UK are computer-related? Cyber security is becoming more important than ever before. Stay safe!

Backups

Backups in IT can be compared to spare tyres in cars. Without a spare wheel or roadside assistance, you could be in quite a bit of trouble when disaster strikes.

Similarly, regular data backups can prevent huge amounts of lost time, anger and frustration after a cyber disaster happens. This could be a hard drive failure, a fire, an accidental deletion by a member of staff, or a hacker getting into your system and causing havoc.

There are two types of backups – on-site, hard copies (like having a spare wheel) or cloud backup (like having roadside assistance). Each offers its own unique advantages, and ideally you should have both.

How regularly should you back up?

- The rule of thumb is every eight hours' worth of work should be backed up. Whether one person works for eight hours, or eight people work for one hour, all that work should be backed up. In an organisation of 20 or more people, it quickly becomes evident that only automated, 'live' backups will suffice.

How secure are your stored backups?

- Your backups should be secured both electronically from intrusion attempts, as well as physically from damage, theft or loss. It is pointless leaving backup devices plugged in all the time as that opens them up to attack. There are numerous cases of backups suffering the same ill fate as the main computer network, simply due to being on site or still plugged in.

Should you use incremental or complete backups?

- Referring back to the rule of eight, the most sensible way is to create one full backup, with incremental backups done on-the-fly during the day. Further full backups or backups of the backups should be kept as the dataset grows.

Cloud storage is a useful solution for all of the above. Instead of incremental backups, certain cloud services can offer live replication, which means your data exists in two or more places at once, thus limiting the potential for disaster.

Top tip…

Public Wi-Fi is notoriously unsecured – use your own mobile data wherever possible.

Hardware and Software Firewalls

A firewall is probably the most important part of your defence against attacks and intrusions.

There are two types of firewalls. A hardware firewall protects your system from attacks from the outside world, while software firewall protects a device within your system. Both types of firewall do the same thing, which is to protect your data, but each does it in a slightly different way.

By way of illustration, a firewall can be compared to the system of security fences, cameras and guards walking around a large factory. Low-end firewalls can be thought of as just a fence, with very limited detection capabilities. On the other hand, high-end firewalls are not only a 'fence' protecting your data, but also have proactive monitoring of the environment, raising the alarm when intrusion attempts are detected.

Firewall questions you should be asking

- Do you have a hardware firewall?
- Does each computer on your network have a software firewall?
- Are all the firewalls up-to-date, with the most recent security patches installed? Remember that hardware firewalls also have on-board software called 'firmware' that sometimes needs updating.
- When was a penetration test last done on your system?
- Have the firewall default passwords been changed?

Top tip…

Be careful when installing new mobile apps—take the time to read through the permissions and deny anything that looks suspicious (e.g. a game wanting access to your address book or calendar).

Antivirus Software

Not all antivirus software is created equal. While most of us realise the importance of using some sort of protection, there are still some considerations that you need to keep in mind.

1. Use business-grade antivirus software in your workplace – there is a big difference to domestic software. Home versions are stand-alone systems, which means each machine needs to be individually managed. However, business-grade antivirus solutions cannot be turned off by the user and can be managed centrally, meaning the IT department can force updates and scans without sitting in front of that particular computer.
2. Stay away from free antivirus software. The two main problems are that either they are inadequate due to limited functionality (usually the reason why they are free) or worse, they are fake and designed to infiltrate your system under the guise of protecting it.
3. Top-notch antivirus programs also scan for vulnerabilities such as weak passwords, outdated operating systems or very old apps and programs that are no longer secure.

You should always be asking whether the antivirus software on each machine on your network is up-to-date. Make sure the same applies to the mobile devices used by reps and consultants, as well as remote workers.

Did you know?

A common mistake in larger companies is a file & data structure that's far too lenient - too many people have too much access to too much data.

Ransomware

Around 70% of all cyber-attacks take the form of ransomware. They usually come as innocent-looking emails, attachments or even the occasional free download.

This class of malware loads an encryption program onto your hard drives, allowing hackers to extort money from you to unlock the drive. Alternatively, they can blackmail you with the threat of going public with what they've found or posting it on the dark web.

Most business-grade antivirus programs have some form of ransomware protection built-in and there are cloud-based solutions that can also mitigate the risk of ransomware.

But the question that has recently been in the limelight is whether to pay or not. Here are some considerations before you decide:

	Pay	Don't pay
PROS	◇ You can immediately start working again	◇ There might be a way to unlock your computer for free. Law enforcement agencies have been collecting encryption keys and various tools to circumvent the ransomware. ◇ Regular backups could save the situation ◇ Not paying is the only long-term solution. The Italian government found this out during the 80s, when Mafia kidnappings of famous or wealthy individuals spiralled completely out of control.
CONS	◇ You're actively supporting crime and they now have more money with which to buy infrastructure to commit even more crimes ◇ You might not actually get your unlock codes as promised ◇ Money unnecessarily spent ◇ You are statistically more likely to be targeted again, because "Hey, this person pays!"	◇ Takes longer to get back on track ◇ Repairs could cost more than the ransom amount ◇ Depending on your back-up capabilities, some work might still be lost

Did you know?

The average age of cyber criminals is 17 – children need to be taught what's right & wrong, especially when it comes to the world of computers.

Software updates and patch management

Security patching is a proactive defence mechanism and equally as important as having suitable antivirus software on each machine.

Security patching is a proactive defence mechanism and equally as important as having suitable antivirus software on each machine.

Security patches are developed when so-called 'white-hat' hackers are employed by software developers and cyber security companies to break into their own computer systems or hack their software. This allows them to highlight the flaws and weaknesses in their system and address them with fixes and patches.

For you as the end user, good patch management simply means that each program on your system – especially the security suite and operating system – need to be up-to-date with the latest security upgrades. This means:

- Ensuring all the machines on your network are up-to-date
- Checking if any software on any machine is no longer supported by the vendor because it is so old.
- Checking if any machines use operating systems that are more than 10 years old, such as Windows 7, Vista, XP, 98 or (heaven forbid) Windows 3.1. The same goes for Mac OS Tiger, Panther, Jaguar, Puma, Cheetah, Kodiak or older.

How cloud keeps you up-to-date

Instead of using physical machines that need constant attention, all the time, consider using a cloud-based, virtual network populated with virtual machines.

In most cases, the monthly or annual fee for a virtual network is cheaper than upgrading physical machines on a like-for-like basis. The reason for this is economy of scale, meaning you always have the latest and the best system, always up-to-date and secure, tailored to your needs.

Top tip...

Configure remote data wiping on your mobile devices to prevent your data from ending up in the wrong hands if ever your device gets lost or stolen.

Access control

Parts of your system need strict access control, in much the same way as certain areas in a secure building would be off-limits to certain people.

Think of the three legs of cyber security – confidentiality, integrity and availability. Confidentiality needs to be considered before making data available, so here's what you need to consider:

- Make certain that all your most sensitive, valuable information is only available to those who truly need access to it.
- Ensure your user accounts work on the principle of least privilege for each user, meaning higher levels of privilege are assigned to a user for each data set.
- Check if you have a company data/user access matrix. This indicates exactly which member of staff may access what information.

Get a more robust access solution

Moving your server onto the cloud allows you to take advantage of virtual servers with banking-grade security encryption (IL4, 2048-bit) along with expert advice from Venom IT on how to manage your access control.

Did you know?

An advanced or next-gen Firewall has a faster Internet speed limit than a basic Firewall.

Educating your staff

Remember what we said about your people and your system? Well, unfortunately, the weakest link in the cyber security chain is very often the human one.

It's why educating your staff is one of the most fundamental necessities of ensuring a cyber secure workplace. It's your responsibility to make sure each member of staff understands:

- The importance of cyber security
- That under the latest legislation, they could personally be held accountable for any data breaches
- How to apply good password policy
- The risks of installing unverified apps
- The importance of running daily malware scans
- They must take personal responsibility for the security at your firm
- How to identify spoofs, phishing scams, social engineering scams, CEO scams and the like
- What to do when a cyber threat or attack is identified – just like a fire drill.
- Have you done any simulations of cyber attacks, to test your staff response?

We offer staff training packs and seminars. Please contact Venom IT for further details.

Top tip…

Secure your phone and tablet with reputable antivirus software—mobile fraud rose 24% in 2018 with 150 million attacks during the first 6 month alone.

Zero Trust: 10 principles to ensure better security

In the past, the concept of a safe zone was considered best practice.

The idea was to create a perimeter – usually through firewalls and segregated networks – which could block all intrusion attempts. This would create a safe zone for the machines and users within the network, similar in concept to the medieval castle with moat and walls – everyone on the outside is a foe, everyone on the inside is a friend.

However, a plethora of recent cases where the threats came from inside the organisation, has given rise to the concept of Zero Trust. This means you still have a strong perimeter to block outside attacks, but now each machine, user and service has to be more strongly authenticated and better segregated.

Access is also given to the network based on the principle of least privilege, meaning they must be proactively and individually allowed to access more sensitive parts of a system.

The National Cyber Security Centre has published the following 10 principles of Zero Trust:

1. Know your architecture including users, devices, and services
2. Create a single strong user identity
3. Create a strong device identity
4. Authenticate everywhere
5. Know the health of your devices and services
6. Focus your monitoring on devices and services
7. Set policies according to value of the service or data
8. Control access to your services and data
9. Don't trust the network, including the local network
10. Choose services designed for zero trust

Why cloud works for Zero Trust

Cloud services are built around the concept of Zero Trust, purely because the stakes are so high. The cloud provider simply cannot afford to allow a single user or a single device to contaminate the entire network. As a result, the above 10 principles are always in play. This is another reason why cloud-based infrastructures are generally more secure than most on-site versions.

Did you know?

Switching to cloud-hosted desktops and/or servers, you could gain access to top-end security without having to bear the huge costs normally associated with such high-end equipment.

BYOD – Bring Your Own Device

BYOD means allowing employees to access your organisation's systems via their personal devices.

Naturally, this has become quite popular in recent years, and merits special attention if your organisation relies on this method of operation. Obviously, there are some great benefits to BYOD, but also some major pitfalls. You should have a clear, well-thought-through BYOD policy that covers which devices to allow and which to ban, as well as regulatory compliance, usage agreements, and the following:

- Your IT department should do a first-hand inspection of devices and their capabilities:
  - Can the device record audio/ video and potentially be used as a spy tool?
  - The same goes for wearable gear, such as smart watches
- Use MDM (Mobile Device Management) or UEM (Unified Endpoint Management) tools. These make it easier for your IT department to manage how mobile devices interact with the organisation's system, allowing them to:
  - Secure devices, especially tabs and phones
  - Enforce password policy
  - Remotely wipe company data from lost or stolen devices
  - Manage/ push work content
  - Push relevant apps
  - Run updates and security patches
  - De-activate users who leave the company
- Devices should only be granted corporate network or Wi-Fi access through enrolment done by the IT department
- Any work-related data stored on the device should be encrypted
- Don't allow 'jailbroken' (Apple) or 'rooted' (Android) devices
- Educate your staff on the essentials of cyber security
- Did we mention educate your staff?
- Almost forgot: Educate your staff.

Top tip...

Learn how to spot fake emails. 41% of all people can't.

Password security

Passwords are the most common weak link in the cyber security chain – mainly because they have historically relied on humans for their strength. Good password policy can be summed up as follows:

- Minimum 12-character length, but the longer the stronger. Consider pass phrases as a more secure alternative.
- A mix of UPPERCASE, lowercase, numbers (0-9) and $pec!@£ characters
- Avoid complete words or commonly used themes and ideas for passwords like film titles, children's or pet names, birthdays and anniversaries etc, or anything you've ever posted on social media.
- Very forgetful users might need to write down their passwords, especially right in the beginning, but should only do so in a very secure place – not under the keyboard, under the mouse or behind the screen—or alternatively use password cards [1].
- You should have separate passwords for everything – especially your main email account, from which you normally reset all your other passwords.
- Never share your usernames and passwords with other people. Really, don't.

Other things to consider:

- Make sure each user on your network knows and applies good password policy.
- Do you have a recovery system in place in case someone forgets their password?
- Do you use two-step authentication wherever possible?

Educate your staff

Consider having a staff meeting with the sole purpose of explaining good password policy and the importance of keeping passwords safe. No system on earth can protect you from weak or leaked passwords. Ask about our staff training packages.

Did you know?

Windows 7 is no longer considered fit for use in business. Upgrade to the latest version of Windows for better security. Venom IT offers free Windows upgrades on all our cloud-hosted desktops.

[1] Password cards are 15x15 blocks (or more) of random letters, numbers and special characters, with each block containing one character. These are a handy tool for forgetful users – the user only has to remember the start letter of the password, and the approximate position in order to find their password. Do not, however, use password cards found on the internet, as these have already been compromised and uploaded into password data bases used by cyber criminals. If you decide to use password cards, create a new, unique card for each user.

Working from home

Recent world events have made working from home a reluctant norm in certain industry sectors, and many organisations were ill-prepared for it. Here's what you should consider:

- Both you and your employees should be able to securely login to your network from remote locations, without compromising the security of your entire network.
- Your intra-company emails must also be secure, or you risk your competitors intercepting them and seeing what you're doing.
- Each home worker needs to complete a security assessment. Ideally, they should have a work-issued laptop/mobile device, a domestic firewall, and business-grade antivirus on the device used to connect to the office network.
- If this is not the case, please refer back to the section on BYOD, as those same principles apply to home workers who have not been issued with laptops/ mobile devices by their organisation.

Security assessment questions

- Have the default passwords on all internet-connected devices at your home been changed to more secure passwords?
- Are all your Wi-Fi passwords at least 20 characters in length, mixed uppercase, lowercase, numerals and special characters?
- Is your internet router fully patched?
- What's the age of your router?
- Do you use only hardware and software provided by the organisation to do work?
- Do you keep all your devices up-to-date in terms of operating system security patches?
- Do you keep all your devices up-to-date in terms of antivirus protection?
- Can you lock away all work-provided hardware when not in use?
- Do you have a suitable work area at home, conforming to workplace health and safety standards?
- Would you be required to print work product at home? If yes, what storage do you use and do you have a shredder?

The answers you get back from some of your workers might require that you take additional steps to help them secure their home environments.

Remote working from the cloud

When using cloud hosting, logging in from remote locations is easy and secure from almost any device. In a manner of speaking, that device becomes a display screen for your virtual computer, which always looks and feels the same, and has all your treasured data ready for you, no matter where you are. The device you used to log in could fall and break, get lost or get stolen, but none of that matters, because your real machine is a virtual machine, and you can access it again simply by using another device.

Off-site work and travel

Travelling reps are nothing new, and neither is getting hacked at the airport lounge while quickly checking emails before boarding. The same two main questions apply to off-site and travelling work as to home working:

- Can you and your employees securely login to your network from remote locations, without compromising the security of your entire network?
- Are the intra-company emails you send secured? Or can your competitors easily intercept them and see what you're doing?

Security on the move

In addition to all the standard security measures such as antivirus, patching etc., travelling workers should know and have the means to:

- Avoid free/public Wi-Fi
- Avoid device theft
- Avoid shoulder surfing
- Avoid saying too much on social media

Practical steps you can take include:

- Issuing each worker with a VPN subscription (especially for international travel) and sufficient data bundles on their mobile phones (local travel) so as to negate the need for them to use Wi-Fi
- Issuing each worker with a Kensington lock for their laptops
- Adopting a policy of 'zero data on device' and issuing each travelling worker with a secured remote desktop
- Fitting each mobile device with privacy-protector film over the screen

Travel by cloud

As with home working, consider the benefits offered by cloud hosting, because exactly the same applies: Logging in from remote locations is easy and, more importantly, secure, and can be done using almost any device. In a manner of speaking, that device becomes a display screen for your virtual computer, which always looks and feels the same, and has all your treasured data ready for you, no matter where you are. The device you used to log in could fall and break, get lost or get stolen, but none of that matters, because your real machine is a virtual machine, and you can access it again simply by using another device.

Top tip...

Public Wi-Fi is notoriously unsecured—use your own mobile data wherever possible.

More software, more risk

The more apps and programs you have installed on your computer, the greater the security risk.

Many apps require opening their own network ports [3] and the more of these ports that are unnecessarily open, the greater the risk that they can be exploited. Here are three things you can do to address this today:

- Check and revise your company's policy on installing apps. Does it allow staff to install apps as they wish?
- Ensure each machine has the absolute minimum of apps it needs for each individual to still be able to perform their work.
- Make sure each app on each machine is from a trusted vendor. Remember that sometimes trusted apps get repackaged (legally or illegally) and resold by less-than-trustworthy vendors.

Why hosted desktops work better

Consider switching to a hosted desktop service that includes the management of each machine along with its operating system, software and apps. This way you can have peace of mind that all your machines are always up-to-date and secure, with no unnecessary software. We offer a variety of off-the-shelf and tailor-made systems.

Did you know?

An advanced Firewall scans the traffic for malicious content, detects & blocks attempted intrusions (hackers), and gives you full control of each user's access rights. A good firewall is your first line of defence.

[3] Think of a network port as you would of an outside door at a high-security building, like a bank . The more outward-facing doors the bank has, the easier it becomes for robbers to gain entry and escape afterwards.

Physical security

Another cornerstone of cyber security is taking good real-world precautions against data theft.

- Is your server securely locked? Bolted down? Entire server cabinets have been stolen in an attempt to get at the data inside.
- Are all the USB ports on all machines disabled where necessary? Persons with ill intent should not be able to simply walk up to a computer, plug in a thumb drive and upload malware or download your data. USB ports should be enabled only for users whose work depends on regularly using USB drives.
- Do you use cables or Wi-Fi? Cable networks are more secure, and Wi-Fi should be on a separately-firewalled network.
- How many people have your Wi-Fi password?

Reducing the physical risk

Consider switching to a hosted desktop environment, where each virtual machine that you use is secured with multiple layers of physical, real-world anti-intrusion protection. No need to worry about server cabinets or PCs being carried off with all your data inside of them.

Top tip...

Perform a review of your user access rights every 6-12 months. You'd be surprised at what you sometimes find!

The GDPR and UK DPA 2018

Why you should pay attention

The GDPR (General Data Protection Regulation) outlines the measures an organisation must take when handling personal data. It came into effect on the 25th of May 2018. The UK DPA 2018 is a similar set of legislation that adopts the GDPR as UK law, with a few small amendments and additions.

Failure to comply with either could see your company fined up to 4% of its annual turnover or €20 million, depending on which figure is higher. Jail time can result from certain infringements such as malicious intent or reckless disregard.

Most individuals found guilty of negligence have been handed financial fines commensurate with their income and the amount of damage done. Similarly, corporations found guilty of neglect have been issued some rather severe fines.

Apart from the financial implications, the damage to your organisation's reputation could be catastrophic, with potential customers unwilling to trust you to handle their data safely. It is therefore vital that you have a sensible plan in place to protect your data from cyber threats.

Data protection and security now forms part of GDPR compliance. In essence, it says that you should apply the appropriate technological and organisational measures to protect personal data against unauthorised or unlawful processing. In other words, "we got hacked" will not likely be accepted as an excuse if any negligence can be proven.

So what's the best way to prevent any vulnerability to prosecution under GDPR? Here are three questions to ask:

- How secure is the personal data of your customers, of which you are the custodian?
- If a breach did occur, could you prove that you had taken all reasonable precautions to prevent any such breaches, and that it was not negligence on your part that contributed to the data breach?
- If a data breach did occur, what systems, policies and procedures do you have in place to mitigate the damage? Do you know who to report data breaches to?

How to make sure you're protected

When it comes to protecting yourself enough that you can answer the rather important questions above, it is quite possible to go the DIY route. But that would require that you:

- educate yourself to a fairly high level of understanding of cyber security
- implement all the needed systems, policies and procedures
- continually assess and update all your systems. This could be very time consuming and take you away from your core business.

Outsourcing your cyber security, on the other hand, can provide you with peace of mind that all your systems are up-to-date and secure, which in turn can leave you with more time on your hands to take care of your business.

Did you know?

ISO 9001 and ISO 27001 count towards GDPR compliance? The good news is, if you don't have ISO 27001, storing your data with an ISO 27001-certified Cloud provider also counts towards your compliance.

Above all: prevention and common sense

In cyber security, just as in everything else, prevention is better than cure.

Go through the headings of this booklet again, and mentally review each chapter, then do some of your own research. Educate yourself, educate your staff.

Here are a few common sense rules to apply:

- Trust but verify
- Stop and think
  - Why is there an attachment? Was I expecting one?
  - Why are they asking for payment in this manner and at this time? Why do they wait till the decision makers are away?
  - Why are they being so pushy?
- Share fewer details on social media, especially details that could be classed as personal or sensitive.
- If your dog's name is on Facebook, and that is also your password… well guess what?
- Wait until you come back from holiday before posting holiday photos. Recent posts of your new 60-inch telly/ new car etc. + current post of your holiday far, far away = opportunity for crime.
- Get Cyber Essentials accredited – most cyber-attacks exploit basic weaknesses in your computers and software. Cyber Essentials shows you how to address those basics and prevent the most common attacks.
- Read. Really read what permissions apps want (and ask why). When installing apps, read what additional apps might be loaded on top of what you're installing (eliminate the unnecessary bloatware).

Top tip...

Use longer passwords or even a whole sentence. It takes a hacker 2 minutes to crack a 5-character, lowercase-only password. It takes 200 years to crack a 12-character password.

Saving the situation

What happens if, in spite of your best efforts, a cyber-attack occurs? Unless you are a genuine cyber security expert, do the following:

1. Don't panic
2. Call support
3. If this was a major incident, report it to the ICO and Action Fraud. The GDPR requires that all breaches involving personal data be reported within 72 hours.

Top tip...

Choose a business-grade email provider (rather than a freebie) that can check incoming emails for spam, malicious links and viruses, and 'sandbox' attachments to make sure that they are safe.

Common cyber attacks you should be aware of...

CEO Scams:

An attack during which online con artists use spoofing to create false instructions that ostensibly come from whoever is the highest authority within the company. These will typically be payment instructions (or refunds of 'accidental' payments) to fake companies. These are highly sophisticated attacks and often involve social engineering, bots that check for vacation auto-responders and a careful study of the target, their type of language and writing style etc.

Social Engineering Scams:

Very sophisticated attacks of a more direct nature and relying on social media, human interaction and human nature to succeed. This often involves the psychological manipulation of the victim in order to get them to release confidential information, make unauthorised payments or break certain rules or override certain protocols. They often form the foundation of CEO scams.

Trojan Horses:

Yes, just like the legend. Trojans are seemingly benign apps or programs such as games, electronic greeting cards, documents or the like. These secretly install malicious software like Keyloggers, Spyware, RATs or Backdoors, or even Ransomware. Sometimes the app is specifically written to be a Trojan and sometimes it is a well-known app that has been modified into a Trojan, usually from a dubious source. Red flags include when a mere game wants to access your contacts list or the message handler.

Ransomware:

Also known as crypto viruses, these encrypt the hard drives of an infected machine, effectively locking the user out and rendering the machine useless, unless a ransom is paid. They usually come in the form of innocent-looking attachments. Once the ransom is paid, the criminals promise to send you the unlock code… but they don't always keep their promise.

Keyloggers:

Malware that records every keystroke made on the machine. Keyloggers are used to harvest passwords and other sensitive data like banking details. One way of circumventing keyloggers is by using virtual (on-screen) keyboards and 2-step verification.

Spyware:

A rather broad term for programs that secretly record or gather information on a computer, with specific emphasis on user interactions. Spyware could be benign – some companies use what is technically spyware to check on the productivity of their employees – but more often than not, spyware is malicious.

RATs:

Remote access tools are used to gain surreptitious control of a computer, especially the webcam and microphone. RATs are sometimes used by voyeurs and industrial spies, the former could use their access for blackmail, and the latter for sensitive information or to eavesdrop on meetings etc.

Insider Threats:

The people within your organisation could be a threat too. A disgruntled employee might actively wish to harm the business, a careless employee may do so unintentionally, an overly helpful employee could do so with the best of intentions and a blackmailed/threatened employee might harm the business in attempt to protect themselves.

DoS and DDoS Attacks:

Hackers use armies of compromised computers to simultaneously send the same request to a specific server, causing an overload in the system, which in turn causes either a loss of service, or opens a vulnerability which can be exploited.

Top tip...

In 2015, around 4000 infected apps were identified on the Apple App store and in 2017 around 800 infected apps were found on Play Store? The point is, less is more – fewer apps on your phone = better security.

Backdoors:

These could be relatively benign methods of bypassing the normal security measures of a computer, and could be used by administrators or developers to access their programs or systems in case of lockouts. Backdoors can, rather notoriously, be exploited by hackers to infiltrate a system without anyone being the wiser. Certain rootkits can also install system backdoors – these are almost invariably malicious.

Rootkits:

Malicious tools sometimes referred to as 'virus droppers'. These tools can infiltrate the computer operating system files (undetected) and then allow other, more malicious programs to enter and hide in plain sight, so to speak, making it very difficult for antivirus software to detect.

Worms:

Malware that self-replicates and then infects as many other computers as it can on the network.

Plastic Card Fraud:

A stolen card, or personal information stolen from a card, is used to commit fraud online. Fraudsters use the cards or details to purchase goods, or obtain unauthorised funds from accounts.

Weak Configurations:

Strictly speaking, this is not an attack, but user negligence, which makes the computer system more susceptible to attack.

Mandate Fraud:

Fraudsters obtain details of direct debits, standing orders or account transfer details and amend them to transfer monies to other accounts.

'419' Advance Fee Fraud:

A communication soliciting money from the victim for a variety of emotive reasons to assist the fraudster.

Romance Fraud:

The victim is befriended on the internet and eventually convinced to financially assist their newfound 'love' by sending them money.

Spoofs:

These are often fake alerts about viruses, sent in chain-email form. But they could also contain malware in their own right by warning about some supposedly detrimental cyber threat, and then 'kindly' offering a solution. This could be anything from a virus upload, a RAT, a fake antivirus for which you have to pay or ransomware. Spoofing could also refer to a hacker creating a spoof machine on your network, or anything fake used by cyber criminals to gain your trust.

Helpdesk Spoofing:

An old favourite among cyber criminals, and it still works. You might get a call from 'Microsoft' or your bank, with the friendly and helpful technician warning you about a virus on your machine/ someone trying to hack your account/ steal your money… well, guess who's the criminal here?

Email Spoofing:

This is different to spoof emails. Email spoofing is when a hacker uses a different address to send a mail, but cleverly makes it look as though it came from a trusted source. Their hope is that some people would be tricked into replying, downloading the Trojan they sent or going onto a fake website, such as banking, DVLA or HMRC scams.

Phishing Scams:

Often used in conjunction with email spoofing. A fake website is created (often one that almost perfectly resembles a banking website) and the user is tricked into entering their username and password, giving the thieves direct access to the victim's bank account. Vishing (voice + phishing) and Smishing (SMS + phishing) are similar, but instead of an email, the telephone is used. Spear phishing is directed at specific individuals within an organisation.

Common cyber security terms you should know

Browser Helper Objects (BHOs):

Not necessarily a bad thing, these apps plug into web browsers such as Internet Explorer, Edge or Chrome in order to provide greater functionality, but they can also be used by hackers to infiltrate a system or redirect web searches to malicious or spoofed websites. When prompted to install add-ons of any kind, always ask: Can I live without this? The answer is probably 'Yes'.

Browser Hijackers:

Malware that is designed to specifically attack your browser settings. If you find that suddenly webpages load very slowly, or your homepage or search engine has changed without your permission, then your machine probably has been infected with a browser hijacker.

Malicious LSPs:

LSPs (Layered Service Provider) are legitimate programs that help with the data transfer when a computer connects to the internet. A malicious LSP or an outdated, vulnerable LSP can be used by redirect web browsers to rogue websites, or to block access to sites like Windows Update or antivirus updates.

Diallers:

These can be useful, legitimate programs, or dangerous malware. Diallers, as you probably guessed, dial telephone numbers. Nothing wrong with that, unless the telephone numbers are premium numbers, with ludicrously high charges, and you never gave permission. Diallers can infect computers and mobile phones alike and, rather worryingly, can quietly run in the background without anyone noticing until the phone bill arrives.

Fraud Tools:

These are systems put in place to help prevent especially credit-card fraud during online transaction.

Adware (PUPs):

Adware, as the name implies, are apps or programs that add onto existing apps – for example the clickable telephone number or maps that you sometimes see on web searches – and are not necessarily harmful., yet unneeded and unwanted, hence the other name – PUP (Potentially Unwanted Program).

Bloatware:

Stand-alone Adware that most often comes with mobile phones, tablets and sometimes laptops. These could pose significant security risks and should be removed/disabled wherever possible.

2-Step Verification:

A way of signing into accounts by using a username, password and OTA (One Time Access) code. The OTA could be sent via SMS or generated by a keychain fob. This is far more secure than single-step verification that requires only a username and password.

White Hacker:

Also known as ethical hackers, or 'white hat hackers' in the US. These hackers are employed by software developers and cyber security companies to try and break into computer systems and, in so doing, highlight the flaws and weaknesses in the system and then create solutions to the problems they found. The term is a reference to the black-and-white era in film and television, when the 'goodies' in especially cowboy films would wear white hats and the 'baddies' would wear black hats, often with matching scarves, to make them more easily recognisable on account of the poor film resolution.

False Positives and Heuristic Viruses:

Sometimes antivirus programs will give a false positive – it will flag a program that is not a virus as being one.

Geo Tagging:

Geographical data about the user is sent to various vendors to enable better service e.g. finding a nearby petrol station or restaurant. This could be exploited by hackers who can then monitor your movements in order to lay digital traps or as part of e.g. CEO scams.

Nation State:

This is when countries attack each other in cyberspace. Usually there is civilian 'fallout' - i.e. businesses and individuals getting hit by malware not necessarily intended for them.

Remote Access:

Growing in popularity, this function can allow a user to login to their work desktop from a different location (home, internet café etc.) and work as though they are at the office.

Zero Day:

Vulnerabilities not even the software creators and vendors are aware of yet.

Top tip...

A cloud-hosted virtual desktop, such as the ones provided by Venom IT, is a very secure and convenient way of working remotely, and counts towards GDPR compliance by virtue of being ISO 27001-certified.

And remember

Always...

- lock your computer when you walk away, even for the briefest moment
- report suspicious activity
- perform regular backups
- double-check banking details before making large transfers
- make sure your antivirus software and operating system are up-to-date
- run regular antivirus scans
- check the permissions new phone apps are asking for
- use strong passwords
- take the time to educate yourself and your staff about cyber security
- make sure you comply with GDPR regulation
- block third-party cookies when practical

Be careful...

- not to open suspicious emails
- not to share your passwords
- not to leave sensitive data lying in plain sight
- of public Wi-Fi—it's not secure
- of unsecure computers such as at libraries, coffee shops etc.
- of calls out of the blue claiming to be from 'Microsoft', 'HMRC' or other well-known organisations
- not to give out personal/ sensitive company details without double-checking the validity of the request
- not to install software that has not been approved by your IT department
- not to allow unsecure private devices onto your company network
- not to post too much information on social media

Did you know?

Worldwide, over the past 5 years more than 5,000,000 organisations achieved ISO9001 certification, but fewer than 150,000 (3%) achieved ISO27001 certification. Venom IT is one of them!

More top tips

Top tips…

- Make sure you have proper consent before sending mass marketing emails. Historically, the ICO has written numerous fines for non-compliant marketing.
- Get Cyber Essentials Certified. It's a great way of checking both real-world and digital security measures, and having the certification makes your organisation more appealing as a partner.
- A degree of technological monitoring and control... balanced with age-appropriate education and guidance throughout their childhood – will show your children you care and go a long way towards keeping their digital lives safe and happy.
- Get a specialist cyber security company like Venom IT to perform a network audit at your organisation to ensure all your devices and systems are secure.
- Please share this booklet with someone—we should all stand together to face the growing menace of cybercrime.
- Download and read Venom IT's easy-to-understand companion booklet entitled GDPR Basics Every Business Owner Should Know

Did you know?

- There are around 6.4 billion fake emails sent worldwide every day!
- Venom IT is partnered with Microsoft, Fortinet, Veeam, Citrix, Webroot, 3CX and others. Our aim is to supply you with best-of-industry services that are tailor-made to suit your business, coupled with competitive pricing.
- The ICO recommends not using password expiration. Frequent password expiry "causes people to change a single strong password for a series of weak passwords."
- Venom IT runs 24/7 virus scanning on all its data centres? This means a much higher level of protection for your data than what is ordinarily available on an on-premises server.

Get in touch

Please contact us if you'd like to discuss any of the information outlined in this document

0330 202 0220
sales@venomit.com

Cyber Security Basics

venomit.com

Legal Disclaimer

Although the author and publisher have made every effort to ensure that the information in this book was correct at time of publication, the author and publisher do not assume and hereby disclaim any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause.

Venom it is not a law firm and does not provide legal services. Distribution of this booklet does not create an attorney-client relationship, nor does it constitute legal advice.

Please contact us if you'd like to discuss any of the information outlined in this handbook

0330 202 0220
sales@venomit.com

VENOM·IT