Cyber-Security for Schools

Maxxia
EDUCATION

Cyber-Security for Schools

With the frequency of cyber-attacks ever on the increase and the sophistication of them evolving, schools and colleges need to follow industry's lead in doing more to protect their systems from being breached.

A simple internet search of security breaches brings up countless stories of hacking and cyber-attacks on school computer networks. Educational institutions are now seen as playing catch-up in defending their systems and remain at risk of cyber-attack, unless they learn the lessons of industry and bolster their defences significantly.

However, the education sector is fundamentally different from the business world, in as much as it is populated to the larger extend by children, who either may not be aware of the problems with many cyber issues, or are more likely to have an uncaring attitude than adults. In many cases, this means that your school's IT strategies have to be more robust to be able to deal with these extra issues. And that requires a focused approach to the many problems that cyber-security brings.

This guide will examine many of the major security issues that may concern your school or college, and present coherent strategies to help counter the main types of cyber-attack.

Why Cyber-Attack?

In order to understand the potential risk to your school of cyber-attacks, we need to clarify the motivations behind those carrying them out. Some of the major reasons are:

Money

People are motivated towards committing cyber-crime to make quick and easy money from victims whom they believe they can either blackmail or coerce. Sometimes, particularly regarding data theft from schools, the motive can be to make money by selling the stolen information for reasons explained further on.

Revenge

A disgruntled student may try to take revenge on other pupils or the organisation itself in response to some perceived slight.

Fun

Many amateurs carry out cyber-crime simply for fun. They may just want to test the latest tool they have encountered online, or show their skills amongst a peer group.

Recognition

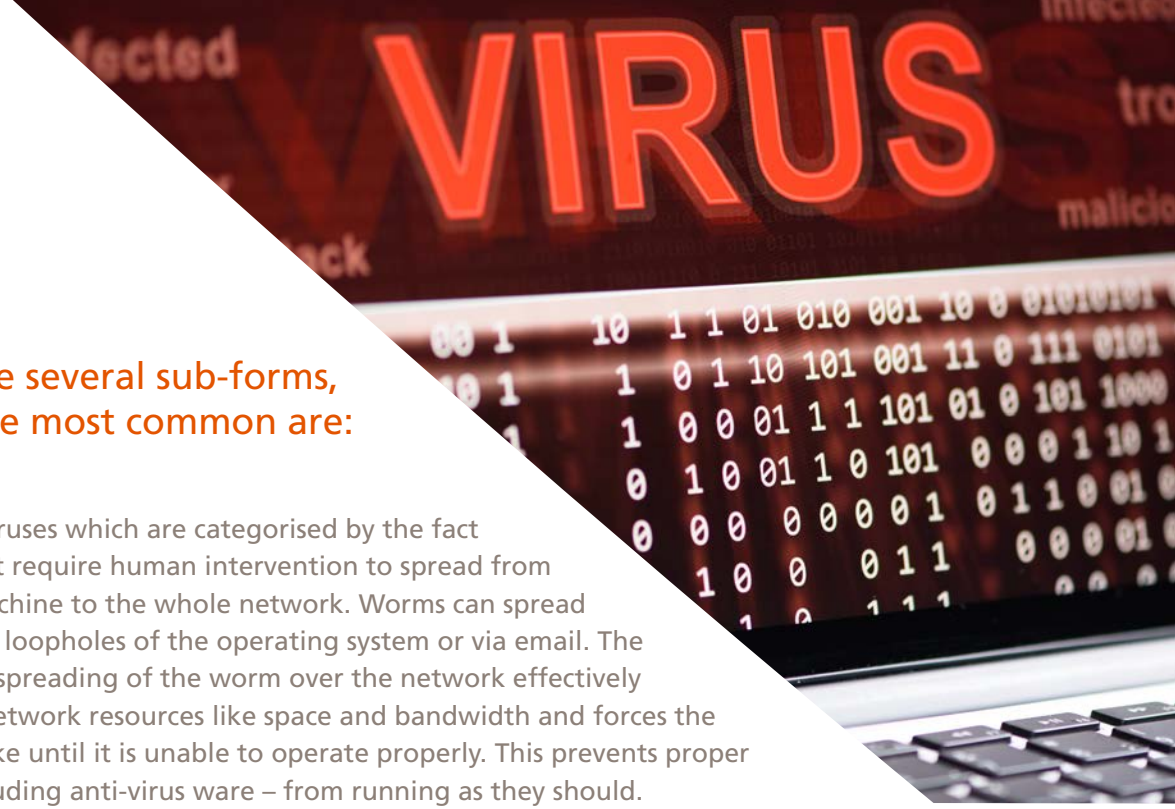
It is considered to carry huge kudos amongst the hacking fraternity if someone manages to hack the highly defended networks like defence sites or systems. This can lead many to try simply to get that acknowledgement from their peers.

Anonymity

It's possible that the anonymity that cyber-space provides motivates the person to commit cyber-crime, as there is a belief that they are much less likely to be caught than with other types of poor behaviour. Therefore, the motivation behind the crime is simple mischievousness, but the attacker is empowered by the knowledge that it will be difficult to locate and prosecute them.

Most of these reasons are global issues which can't be tackled by individual schools at source and the only credible way of countering such attacks is to have a robust security policy in place in your school which prevents attackers' access to the system. As you will learn throughout this guide, a major part of any such policy is the education of users – staff, pupils and, where relevant, parents – to not only identify potential attacks, but also to minimise their exposure to them. Let's look at some of the main threats and issues that could affect your school computer system.

Cyber-Security: Types of Attack



Viruses: A virus is a malicious code written to damage/harm the host computer by:

- deleting or adding a file
- occupying large amounts of memory space by replicating the copy of the code
- slowing down the performance of the computer
- formatting the host machine, etc.

It can be introduced via email attachment, pen drives, digital images, e-greeting, audio or video clips, etc. A virus may be present in a computer, but it cannot activate itself without the human intervention.

Viruses can spread when the software or documents they get attached to are transferred from one computer to another using a network, a disk, file sharing methods, or through infected email attachments. It would be very easy for school students to unwittingly import a virus into your school network via USB flash drives or memory cards, for example.

Some viruses use different stealth strategies to prevent their detection by antivirus software. For example, some can infect files without increasing their size, while others try to evade detection by killing the tasks associated with the antivirus software before they can be detected. Some viruses make sure that the "last modified" date of a host file stays the same when they infect the file.

Viruses have several sub-forms, of which the most common are:

Worms

A sub-class of viruses which are categorised by the fact that they do not require human intervention to spread from the infected machine to the whole network. Worms can spread either using the loopholes of the operating system or via email. The replication and spreading of the worm over the network effectively consumes the network resources like space and bandwidth and forces the network to choke until it is unable to operate properly. This prevents proper programs – including anti-virus ware – from running as they should.

Trojan

A Trojan – named after the Trojan horse from Greek mythology - is a type of malware that is often disguised as legitimate software. Trojans can be used by cyber-criminals and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated by the unsuspecting user, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system. These actions can include:

- Deleting data
- Blocking data
- Modifying data
- Copying data
- Disrupting the performance of computers or computer networks

Because virus attacks cannot instigate themselves, and the base program has to be loaded onto the target computer, this can usually only be achieved by fooling the user into doing it. Virus executable files are frequently attached to bigger programs which the user may download, unwittingly installing the virus at the same time. Again, introduction of a Trojan into the school system would be simple if your students are allowed to use their own flash drives or similar to upload onto your school network.

Phishing

This is a cyber-attack that uses an innocent-looking email as a means of trapping an unsuspecting computer user into believing that it is something that it isn't. The goal is to deceive the email recipient into believing that the message is something that they either want or need to open — such as an urgent request from their bank, for instance — and to click a link or download an attachment. The link is likely to take the user to a well-crafted replica of the expected site, which then requests the user's log-in details. Once those have been supplied, the attackers can log onto the real site using the duped user's credentials and typically transfer money to another account. Phishing relies on the target believing the validity of the email, and great attention is paid to making it resemble the expected site.

Phishing can also have variants such as the Advance Fee type where scammers ask the victim to pay a transaction fee up front in order to get financial gains or goods / services which never materialise. A similar scam involves the so-called account deactivation threat, where the victim is informed that their bank account is going to be closed by the bank and, to stop it happening, they need to prove their identity by passing across their log-in details, allowing the scammers to access their account.

The so-called 'spear-phishing' scam relies on emails which might appear to be from someone you know or a trusted source but are really a way of concealing an attack, such as downloading "malware". This is one of the most effective methods of phishing and is something that school pupils, or indeed staff, may well be taken in by.

None of the phishing scams are particularly elaborate and they rely on the victim's greed and/or gullibility in order to make them allow the scammer access to their account or details. In the context of a school, it is unlikely that children would be the victims of a banking-based fraud, but it may certainly be aimed at teaching staff, and could be used by the scammer to gain access to the school computer system. It's also possible that the phishing scams can extend out via the school system to parents who have their email details on the school system.

Bots

Short for *internet robots*, these software-based entities in the form of self-propagating malware are designed to bombard a system or cultivate data. The blanket term 'bots' also includes spiders, crawlers, and web bots. Malicious bots are defined as automated malware that infects a host computer and connects back to a central server or servers. The server functions as a command and control centre for a 'botnet', or a network of compromised computers and similar devices that can be controlled via the bots.

They can:

- Gather passwords
- Log keystrokes to uncover bank details
- Obtain financial information
- Relay spam to other computers on a network
- Launch Distributed Denial-of-Service (DDoS) attacks
- Open back doors on the infected computer for unlimited access
- Exploit back doors opened by viruses and worms.

A computer that has been infected may show slow internet connection speeds, irrational crashes, fast fan speeds when the computer is idle, slow running programs and changes to settings. While a computer infected with a bot may not show any outward symptoms, a bot may be programmed to exhibit certain functions. These might include scare tactics where a message is displayed requesting that a link is activated to prevent a virus being installed. The link then leads to a virus location.

Most up to date antivirus software will scrub bots from your system. It's vital that your school puts such software in place and that it's updated regularly. Ideally, someone on the staff who has computer skills should be made responsible for initiating, checking, updating and keeping a log of the security measures. If that's not practical, then it may be necessary to outsource the IT security to an outside company.

Ransomware

This is malicious software that aims to extort money from its victims via threats, usually associated with either infecting the computer with a virus or exposing some personal details of the user. This has become one of the most prolific criminal business models in existence today, mostly thanks to the multi-million dollar ransoms criminals demand from individuals and organisations that they attack. The demands of these kinds of attack are very simple: you either pay the ransom, or have your operations severely compromised or shut down completely, or data deleted irretrievably.

Usually, the first an organisation knows about the attack is when they receive an on-screen notification informing them that data on their network has been locked through deep-level encryption, and will be accessible once the ransom has been paid. This happened in the NHS system some time ago. Once payment is received, the company will be given the decryption key that will allow them to access their data. Failure to pay could result in the key being destroyed, and the data inaccessible. If backups aren't routinely carried out, a significant amount of data could be lost, and for organisations such as schools and colleges, that may include huge amounts of curriculum and student test results.

There are several different ways that ransomware can infect your computer. One of the most common is through malicious spam, sometimes called "malspam", which is unsolicited email that is used specifically to deliver malware to a computer. The email might include booby-trapped attachments, such as PDFs or Word documents, or it might contain links to innocuous-looking but malicious websites.

Malspam uses social engineering in order to trick people into opening attachments, or clicking on links, appearing as legitimate by seeming to be from a trusted source, making them quite difficult to identify.

Hacking

Quite simply, hacking is the process of gaining unauthorised access into a closed computer system, or group of computer systems. Usually accomplished through cracking of passwords that give access to the systems, the hacking can be carried out on single systems, a set or group of systems, an entire LAN network, a website or a social media site. The access to a password is obtained by the hacker through password cracking algorithms programs, giving them access to all areas in the system. Once in and behind the firewall, the hacker can change settings in the system, giving them access as and when they require it.

However, the most common intent of hacking is criminal or malicious, either to commit some fraud or to cause some financial or reputational harm to the person, group or entity so hacked. This is done through stealing confidential data or embezzlement of funds or other monetary resources, causing business disruptions, spreading of incorrect and malicious rumours, or other misleading information which is socially detrimental.

Unlike other forms of computer attack, hacking has a legitimate side and finds great use as a means of uncovering weaknesses in a system before unethical hackers can find the flaws and gain access. This has become big business, as companies race to prevent unauthorised access, and hire professionals who can examine their systems and advise them on how to plug any potential weak areas. Recent tests (April 2019) carried out by "ethical hackers" working for Jisc, the agency providing internet services to the UK's universities and research centres, showed that hacked access to sensitive data took less than two hours.

Compromised Emails

Usually, the first thing that we know about a compromised email is when our system fails, and it is too late to do anything about it. In the worst case, your system may shut down – or become locked – and you will have no way of accessing all of your information. Furthermore, a compromised email may mean that someone else has your details – including log-ons and passwords – and may be able to set up fake accounts in your name. According to leading websites, there have been over 4 billion identified stolen credentials and around 50,000 stolen credentials are identified daily! To help protect against the threat of compromised emails:

- Use a password manager and two-factor authentication (2FA) wherever possible
- Don't click suspicious links in email or texts
- Use a Virtual Private Network (VPN) on your computer and your phone to hide your identity, though this may be less of an option for a school or college
- Don't use public Wi-Fi or public computers when accessing personal accounts or data if possible. Or as above always use a VPN when accessing public Wi-Fi.
- Use a strong firewall and antivirus
- Ensure that your router and Wi-Fi are secure through a strong password
- Keep your computer and smartphone operating system, apps, programs and security software up-to-date. The recent NHS attack only occurred due to their entire desktop systems running unsupported Windows XP. If they had manually applied a single patch which was available for months preceding the attack, their network would not have been compromised with ransomware.

Password Cracking

Breaking into a system usually requires the cracking (or hacking) of passwords to allow unauthorised users legitimate access. Once in, they can cause all manner of chaos, so keeping unauthorised people out requires strong passwords that cannot be easily compromised.

That, however, can be a problem both in businesses and institutions such as schools and colleges, as the onus on creating a strong password often lies with the users. Many passwords are hacked because the authors create predictable words and phrases.

Investigations by IT professionals has shown that:

- There's a 50% chance that a password has at least one vowel
- Numbers that are used in passwords are usually the numbers '1' or '2' and are placed at the end of the password
- Capital letters are usually at the beginning and are followed by a vowel
- Women use personal names for passwords frequently
- Men frequently use their hobbies or favourite football team for passwords
- Most common symbols used are —~@#$%&?

Given that many people tend to follow these predictable paths, practiced hackers can break into systems quite quickly. In order to stop them, users need to create stronger passwords. That is possible by following a few simple rules.

To create a strong password:

- Have at least 12 characters: You need to choose a password that's long enough. There's no minimum password length everyone agrees on, but try to construct a password that is a minimum of 12 to 14 characters in length. An even longer password would be better but may become difficult to remember.
- You should include numbers, symbols, capital letters, and lower-case letters: Use a mix of different types of characters to make the password harder to crack, but mix it up so that you have capitals and symbols at random places rather than at the beginning and end only.
- Choose something that isn't a dictionary word (or combination of them either): Do not use obvious dictionary words and combinations of dictionary words, and any word on its own is equally bad. Any combination of a few words, especially if they're obvious, is also bad. For example, "house" would be a terrible password, but something combined like "Out house" would also be relatively easy to hack.
- Don't rely on obvious substitutions: Don't use common substitutions such as numbers for letters either. for example, "H0use" isn't strong just because you've replaced an "o" with a "0".

Of course, it is easy to give staff lessons in creating a strong password and they may then come up with examples such as 3o(t&gSp&3hZ4#t9, but then it becomes difficult to remember. If you instruct people to create something between the two extremes – and memorable – then it should be fairly safe.

Staff Privilege Misuse

Privilege misuse – or even outright abuse – can be a consequence of giving staff greater responsibility at work, and simply trusting them not to misuse that position. In the vast majority of cases, staff will play by the laid down rules and the problem will never occur. However, with a tiny minority, greater privilege is seen as an opportunity to extend their own agenda.

Privileged account abuse occurs when the privileges allowed on a particular user account are used inappropriately or fraudulently. This can be either malicious, accidental or even through wilful ignorance of your policies. According to a recent report, abuse of privileged accounts is now the second most common cause of security incidents and the third most common cause of breaches.

While only a small proportion of these kinds of breaches are intentional or malicious, institutions suffer a far greater threat from casual misuse. This usually manifests as accessing inappropriate and potentially unsafe sites, or the opening of personal emails on a work computer. The situation is amplified by the fact that few institutions actively monitor the extent of staff activity, particularly when it comes to accessing potentially dangerous content.

However, staff misuse of IT systems can be monitored fairly easily, and there are three steps that you can take to limit the problem:

Continuously assess and properly manage assigned privileges

- Review access rights and remove excessive permissions in accordance with the lowest-privilege principle. If people don't need extra access, don't give it to them!
- Review and update permissions whenever a user's role in the organisation changes
- Make sure your sensitive data is not exposed by verifying that access to it is granted based strictly on a specific need
- Pay special attention to your privileged accounts and assess who can use them and what permissions they grant
- Carry out regular audits of visited material and/or sites and determine who is accessing them

Gain visibility of your IT environment

Without solid checks in place, you are unlikely to know if there have been a suspiciously high number of failed attempts to access a critical file or database, or some unauthorised change to your security system or groups. In that case, this step is especially important to you. Without a complete and regular monitoring of all changes and user activity in the IT environment, it is impossible to detect threats, including privilege abuse, before they become dangerous.

Analyse user behaviour

Just by collecting data, it doesn't mean that you are using it effectively. Can you tell when your users exercise their privileges outside of normal working hours? Do you know whether their current behaviour deviates from the expected? User behaviour analysis will show you anomalies that are not always obvious if you just look at event logs.

Ask your IT provider to give you a monthly breakdown of computer usage and monitor this on an ongoing basis, to establish a baseline of current behaviour and to highlight any future changes that may expose your system.

Bring Your Own Device (BYOD)

Allied to employee misuse, there is a growing policy amongst many schools and colleges to allow staff and students to bring their own devices to school and, in some instances, connect them to the secure network. This is driven by the increasing personal ownership of laptops, tablet computers and mobile phones that are becoming an integral part of the learning experience. Many teachers and lecturers are using personal devices to construct lessons in their own time and find it onerous to transfer the data from their own device to the school system. It becomes expedient to allow personal devices on site, but there is also an increased risk with this policy.

The connection of personal equipment opens up the possibility of system attack through viruses or other damaging software entering behind your firewall and infecting the entire school system. Whether this is by a previously infected computer being connected to the network, or by an employee opening a link on a personal email, you need to be confident that BYOD will not adversely affect your system. There are a number of ways that you can minimise the risks from BYOD policies, including:

Control wireless network connectivity:

Wi-Fi and Bluetooth connectivity should be turned off when not in use, and employees should only connect their devices to trusted networks, and using strong personal passwords. Devices should be set to prompt users before connecting to networks so that employees aren't unknowingly connecting to unsafe networks. Or provide a separate Wi-Fi network with access to the public internet but blocked via a firewall or physical separation to the private or "business" network. Additionally via a firewall, a VPN could be created on the public Wi-Fi to permit authenticated access to the private network.

Control access and permissions:

Many devices have built-in access control features. Organisational IT and security teams should assist users in optimising their access control and app permission settings so that each application can access only what it needs to function and nothing more.

Keep OS, firmware, software, and applications up-to-date:

BYOD users need to ensure that all of their device operating systems and other software are updated to the latest standard. These often contain security patches to protect users from the latest threats or exploits.

Back-up system data regularly:

System back-ups should be performed at least daily and archives kept off site so, should something go wrong, previous data is easily accessible.

Never store personal financial data on a device:

Employees should avoid saving any financial or otherwise sensitive data on their devices. This precaution ensures that confidential data is safe even if a device gets compromised.

Beware of free apps:

Many free applications have been found to track users and share user information with advertisers or other third parties. Enterprise users should review app permissions prior to downloading and download only from trusted publishers. Furthermore, there is a growing trend for people to download pirated software, and these downloads can have viruses attached. All software used on any BYOD should be legitimate.

Run strong mobile antivirus software or scanning tools:

Employ strong firewalls and anti-virus software constantly so that any threat is almost instantly identified and dealt with. Also, ensure that BYOD users have similar conditions on their devices.

There are programmes available which support BYOD via a student lease scheme, and allows for the standardisation of the equipment provided – you can read more about this here https://maxxia.co.uk/blog/student-ipad-scheme/

eSafety: Countering the Attackers

Being safe online – eSafety – is an absolute must for schools and colleges. That means having a set of robust polices that help not only to protect your system from outside attack, but which protect users – primarily children – online too.

A recent report showed a number of traits concerned with eSafety:

- Parents typically use the internet regularly for a range of tasks including email and browsing but also commonly for shopping and banking. These are generally seen as safe pursuits as they usually involve trusted sites.
- While the parent's confidence in how to use the internet varied, most felt confident that they are able to do all or most of the tasks that they would want to do online successfully.
- Children tend to access the internet out of sight of their parents, and relatively few parents said that that their children are always supervised when online.
- The parent's view of the internet for their children was that it was a good educational tool, and could also be used for reward, once work had been completed.
- Many parents were concerned about the amount of screen time their children had, and the knock-on effects on inactivity and face-to-face social interaction, as well as being unsure as to what their children were accessing.

All of this means that, while parents are fairly happy with the concept of online safety, they tend not to know what their children are doing online and rarely actually observe it anyway. This is a difficult situation for parents to remedy, and the learned behaviour necessary for children to use good on-line strategies and habits has to be part of a school or college-led curriculum.

Social Engineering

Allied to phishing attacks, social engineering usually involves a tailored message to a small group rather than a blanket email. That can make it much harder to spot. Generally email based, it can also be carried out over the phone. The language used by the social engineer (essentially a hacker) is often persuasively urgent in context such as “please enter your password before your account expires” or “to increase your quota, please log into your account now”.

The social engineer may also use “verification of configuration” language during a phone call or in-person visit to the targeted location or individual that appears legitimate and official in nature. To prevent attack by a social engineer via email, always follow the steps below:

- If the email is from someone you don’t know or from a company you’ve never done business with, even if it appears to be a legitimate company, ignore it
- The sender’s email address may have an unusual ending, like “.uz”. Also, beware of spelling errors in the sender’s email address and in the body of the email.
- There is always a sense of urgency to open a link or to submit your personal information with a threat of losing your service or legal ramifications
- It may have suspicious links or attachments included
- The email doesn’t include your name or username, or addresses you simply as “Customer” or “Account Holder”

Social engineering is on the increase, and the social engineers themselves are becoming more refined in the types of language and attacks that they carry out.

Physical Security: How to Protect Your Computer

Below are some key steps to protecting the physical security your computer system from intrusion:

- Keep your firewall turned on: A firewall helps protect your computer from anyone who might try to access it. There are several free to use software firewalls that are highly effective if the software is kept up to date.
- Use antivirus software: This is software that is designed to prevent malicious software from activation on the system by detecting it and removing the threat. Key to running antivirus software is keeping it up to date as new threats are always arising.
- Use antispyware programs: Buy and install a reputable antispyware program to constantly run on your system. Like antivirus software, this needs to be kept up to date, and beware of free programs from the internet as they can actually install spyware on your system.
- Make sure that your operating system is up to date: Operating system providers are constantly testing their systems and periodically find problems that need fixing to prevent security breaches. Make sure that you download and install the latest version of your OS to maintain security.

Cyber-crime can be enormously damaging to any institution or business, but schools and colleges are more exposed than many. Deflecting or negating such attacks can become the major part of the IT department's activities, and with the sophistication of attacks ever rising, it is becoming increasingly important for a school's defences to be as robust as possible.

About Maxxia

At Maxxia, we arrange leasing solutions for a wide range of equipment and school improvements, from minibuses to temporary classrooms, or computers to catering equipment. Whatever funding requirements your educational establishment has, Maxxia gives you the most cost-effective, compliant and transparent leasing methods available.

We already work with many education establishments across the UK and we have helped them save money whilst keeping their assets up to date and making the student experience better. Our funding solutions meet the needs and regulatory requirements of each segment of the education sector.

In addition to funding, you can benefit from our relationships with numerous suppliers so as well as the finance, we may be able to help you negotiate a better deal for the equipment you require.

Need something even more innovative, like an iPad or laptop access scheme that is provided through the school, but where the items are actually funded by the parents? Talk to Maxxia.

Find out more about how Maxxia's leasing solutions benefit your school.

https://www.maxxia.co.uk/education

contact@maxxia.co.uk

Tel. 0845 643 1319

Maxxia Ltd, Corporate House, Jenna Way, Newport Pagnell MK16 9QB

Registered in England and Wales, company registration number 07807901

Maxxia