HOW TO STAY CYBER SAFE

CYBER SECURITY GUIDE

Introduction

The last few years have shown us that Cyber Security is more important than ever before, with the rise of remote working and the automation of businesses leading to more time being spent in online spaces. In fact, the last two years saw 80% of UK organisations become the subject of successful cyber-attacks according to the CyberEdge 2022 Cyberthreat Defense Report. There are a lot of risks when it comes to operating in a technological space so it can be difficult or intimidating to formulate strategies on how to combat these dangers. However, there are several measures you can take to protect your organisation as well as yourself.

In this guide, we're going to take you through some tips and tricks to improve your cyber security, giving you safety and peace of mind, while also detailing how we at CSS maintain high standards of cyber security and data protec

Personal Measure

Following the COVID-19 Pandemic, remote online working has increased exponentially, and the recurrence of cyber threats and dangers has increased with it. Most home-based IT setups are not as well protected as IT environments for larger organisations. For example, 78% of Cyber Security and IT experts say remote workers are harder to secure (according to Splunk's State of Security 2022 study). With the statistic being that high, it's apparent that remote workers need more practices in place to stay safe. One measure you can take is to monitor your own activity. For instance: do not store sensitive data on a work device, make sure any webpages you visit are secure (there are some free browser extensions that can help you with this), don't open any links from senders you don't recognise (see Phishing). Small actions like this can make a world of difference when it comes to protecting yourself from cyber threats.

File Encryption

If you're sending files over an unstable connection or if these files contain sensitive data, then there are a few programmes that can encrypt your data so only you, and the people you share the key with, can view the files. Boxcryptor is a good example since this application can encrypt your files with 256-bit encryption, meaning it could take a computer years to crack through and so the data in those files is kept safe.

Furthermore, you can have e-mails encrypted so even if they are intercepted, they can't be accessed by hackers trying to farm your data or access sensitive information. Some services that offer this include: Mailvelope, Enigmail, and Thunderbird.

PHISHING - HOW TO SPOT AND AVOID IT

Phishing is one of the most common threats to online security and, according to APWG's Phishing Activity Trends Report for Q4 2021, phishing scams are more prevalent than ever, with 300,000 cases being recorded in December alone. It's something you're probably familiar with. They're commonly e-mail scams where a hacker or a group of hackers will masquerade as an official body (i.e., PayPal) and ask you to divulge personal information like banking details.

For example, you may receive an email from a service you currently use (Amazon, PayPal, Netflix etc.) saying your account has been frozen or compromised and that you need to verify your information to fix the issue. These details will be things no legitimate organisation would ask you to verify through e-mail such as your CCV number, your full national insurance number, or your account password. If you follow the links in these e-mails and enter this sensitive information, then that means these scammers now have your data and can do whatever they like with it. Remember, no legitimate organisation or service will ask you to verify your details through an e-mail, especially details as sensitive as the ones mentioned above. If you follow the link, you may see a webpage that is a dead ringer for the real thing, and this can add a fake air of legitimacy. However, if you were to check the URL and the rest of the page thoroughly, you'd begin to see some cracks. For example, the domain may be totally different to what the webpage claims to be, or it might be similar enough to the real thing but with a different spelling. A good way to check is to hover your cursor over a URL to display the actual name of the page.

Furthermore, these scam pages will most likely not have any additional pages, an 'About Us' section, or legitimate contact details.

If your details are compromised by this kind of scam, then the first thing you should do is notify your bank immediately and cancel or freeze any debit/credit cards, then you should change your passwords as quickly as possible to try and minimise the scammer's reach.

Thankfully, most of these scams are easy to spot since the URL is always suspicious, the sender will have an e-mail address incongruous with the organi sation they're claiming to represent, and the messag es are normally riddled with spelling mistakes or grammatical errors. So, if you receive an e-mail from "Payypal" it's for the best if you don't open it or follow any links.

VPN

The use of VPNs for personal browsing has increased due to a demand to access geo-locked content. However, a VPN (Virtu al Private Network) has more benefits than just giving you access to American Netflix. VPN's mask your IP address by hosting your connection via offshore servers, giving you total privacy and protection from any prying eyes. This means that you can browse the internet freely without having to worry about any hackers viewing your activity. This is important because some phishing scams (see phishing section), known as spear phishing, can target you directly by using information they stole while you were browsing unprotected sites. So, keeping your connection and your activity private is of paramount importance. Most VPN providers offer their services via a subscription model – with larger providers like NordVPN offering different tiers of features based on your subscription plan.

Some of these providers will even offer extra programmes bundled with their VPN, like a Password Vault, meaning you can guarantee privacy and security for a relatively inexpensive price. If you don't want to spend money on a subscription to a VPN, then there are some options that come free of charge like Proton VPN which offers both a free and paid model of the software. Although, with these programmes being free, you do get what you paid for – the bare minimum.

While these tips can help when operating online, it doesn't mean you're completely protected from security threats or ransomware.

Anti-Virus

Regularly running real-time or full system scans with antivirus software is half the battle with cyber security since it lets you stay on top of what might be lurking on your device. Not to mention that you should be updating your antivirus regularly to make sure the device is being protected by cutting-edge software. Most computers, smartphones, and tablets come with some form of antivirus software already installed but, depending on what you're using your device for, you may need to consider looking for alternative providers.

While some free antivirus programmes exist like Sophos it's always best to go with the larger, trusted providers like McAfee or Norton 360 since they have proven time and time again that they are reliable and robust antivirus programmes. These programmes that come with free models may be efficient but the programme itself is not going to perform as well as its contemporaries. You need to be careful when assessing antivirus options since some providers will collect and sell your data (Avast) to third parties.

To take this further, some antivirus programmes like Norton 360 Deluxe, offer an in-built VPN for use on public networks. This can be toggled on and off in the system settings to suit your needs. Features like this will add to the overall price but having a VPN or File Shredder (a programme that destroys files and any trace of them on the hardware) incorporated into your antivirus for a marginally higher cost is more than worth it for your peace of mind.

Password Management

Most of us are familiar with making passwords for new devices, e-mail addresses, or social media accounts. It can be a frustrating process to make a new password for every account and so you might be tempted to use one simple password, like “DOG123”, for all of them. However, it’s crucial to use a different password for every account and profile because this makes it harder for hackers to access multiple accounts.

Furthermore, your passwords should be strong and hard to crack. If you don’t want to use a Password Generator then a good rule of thumb is to include a mix of lower and upper case letters, numbers, and symbols, but try to avoid using personal information like a relative’s name as this would be easier to decipher. Furthermore, you should never share your password(s) with anyone over online channels or even in person. This could compromise the security of your device.

BROWSER EXTENSIONS

Some malicious content can infect a device through advertisements or advertisements can entice users to carry out certain actions like entering banking information or personal details. An easy way to combat this is by installing an ad-blocking extension onto your browser since these will filter out any and all advertisements. Most of these come free and even have versions that are compatible with iOS and Android devices, for example, AdBlock Plus (a Chrome extension).

Another important extension to consider would be something along the lines of HTTPS Everywhere, another free extension, because this redirects you to webpages with verified secure connections, therefore minimizing the risk of your data being intercepted or hacked.

Some other examples of browser extensions that can help protect your data and devices while online include DuckDuck Go (another free extension) and Ghostly (this extension comes with two paid plans). You don’t have to get just one either, most browser extensions work well together and can do things the other one can’t.

Security For Work

According to research from Atlas VPN, the number of cyber security companies grew by 21% in 2020. This growth in the market highlights the importance of maintaining security and privacy for businesses, both large and small. Most of these companies operate a consultancy model so they can cooperate with the IT officials in your organisation to ensure that the security systems in place are running at top capacity. While most workers can take measures to protect their devices and activity online for their own personal usage, this may only apply to personal devices. So, there is a need for businesses who supply workers with technology to hold up their end and provide security for the workplace as well.

SaaS (Software as a Service) organisations have become some of the biggest targets for cyber-attacks and data breaches in the last few years and most of this is due to poor device management and inadequate security measures.

VPN FOR BUSINESS

Just like with people using technology at home, VPNs are crucial for securing connections, especially for businesses utilising a remote or hybrid working model. If a company network is built on unsecured connections, then it's fair game to hackers or scammers.

This could lead to a ransomware attack which is when hackers will deploy a form of malware that captures data and won't release it until a ransom is paid. This kind of attack could wreak havoc on your systems and potentially halt operations until the issue is resolved. Not to mention that in the UK alone, the average cost of a ransomware attack can come up to approximately the equivalent of $1.08 million. This price tag alone is enough incentive to incorporate a VPN into your organisation.

Cisco is a provider equipped for the needs of big businesses because it allows remote workers to access a company network with an encrypted connection. This is ideal for businesses with remote-working employees since it allows them to continue working from home, accessing company servers and information, while still maintaining privacy and security. Furthermore, VPNs like Cisco require users to sign-in every time they access it, giving it that extra layer of protection if, for whatever reason, someone outside the business acquires a device with the programme installed.

Device Management

Device management refers to technology, specifically hardware, usage being monitored and regulated by the IT team. For example, work laptops can be configured by an administrator to block certain sites and downloads, limiting the risk of the laptop being targeted by hackers or people farming personal data. Not only does this encourage responsible use of work utilities, but it also allows for the IT team to closely monitor potentially risky activity.

Two important aspects of device management are identity verification and access authorization. These areas can be improved upon greatly by incorporating Two Factor Authentication to login processes.

TWO-FACTOR AUTHENTICATION

Most services, like e-mail providers, will push you to opt for this as you register with them. Two-Factor Authentication requires two methods of identity verification during the login process such as an ID and password, followed by a confirmation code.

While irritating, processes like these should be adopted as standard practice in order to minimise the risk of unauthorised access to work accounts. Moreover, it can double up as a recovery tool in case someone's login credentials have been compromised or need to be updated. Therefore, user-specific data and processes can be protected and insured against any major risk(s).

These programmes and practices are all equally essential for protecting your business' system and your workers' data. While initially they may take some time to configure and test out, they are worth the time and effort because they will demonstrate, almost immediately, how much safer you are both online and offline.

SECURITY WITH CSS

Here at CSS, we pride ourselves on our security measures, our defenses, and how we process data.

System Access

CSS employs single sign-on, meaning once a user has a secure login ID for one of our systems they can sign in quicker, granting better ease of access. Furthermore, the system grants access to administrators to edit login details in the case of these details being compromised, therefore compartmentalizing the sign-in process and providing an extra level of security in the event of a worst-case scenario.

Server Security

Our servers are hosted by Rackspace and all the data we transmit through our systems is protected by AES 256-bit encryption. These servers are secured by a back-up programme so if any data is compromised or a server collapses, the data is instantly backed up onto a server in a secondary location.

This means that in a worst-case scenario, sensitive data is still being kept secure from prying eyes. Not to mention that any critical data is stored on redundant disks – this means the same data is stored across multiple locations so there is always a backup.

When it comes to onsite security for these servers, there are several procedures in place to make sure they stay secure. The servers themselves are accessible only by authorized officials with biometric access points to ensure total control and visibility of system access. Moreover, the site is monitored 24x7 by a team of security officials to prevent any physical breaches to the systems. All of these measures are inspected and audited annually by independent firms to ensure full compliance with data protection guidelines.

ACCREDITATIONS

Building on this, it's important to us at CSS that we maintain high standards of cyber security and so we pride ourselves on our accreditations. We are proud to be part of, and hold certification for, the Cyber Essentials Plus Scheme. This shows how committed we are to maintaining excellency in data protection and cyber security. Additionally, we are on the ICO Data Protection Register meaning we proudly comply with the Data Protection Act 1998 and all its subsequent requirements.