totalityservices

Cyber Security Guide for Small & Medium Sized Businesses

Table of Contents

Foreword

On behalf of the totality services team, I would like to wish you a Happy New Year. I hope the festive period was enjoyable and you're looking forward to a successful 2019!

Over the last few weeks, I have found myself reflecting on some of the IT security nightmares covered in the media, but also described to me by industry colleagues and prospective clients. Staying on top of IT security for our clients is critical, as they all hold and / or own confidential data - so I decided to create a guide to help businesses protect their data from cyber-attacks.

Cyber-crime is a serious threat to businesses in the UK. However, in the last few years we've seen cyber-attacks evolve from targeting large, blue-chip companies (e.g. TalkTalk and Tesco) to more vulnerable small to medium sized businesses – in fact 81% of all breaches happen to SMBs. Each year, businesses are faced with newer, more potent forms of malware and ransomware, so staying on top of these threats is critical.

It's common to believe that your business is invincible to cyber-crimes. However, there's a 50% chance that small to medium-sized enterprises could be victim to a cybersecurity breach, if the right measures and solutions aren't in place. What's more, such a breach could cost your business 20 million euros or 4% of revenue (whichever is greater) under the new GDPR guidelines. This guide is aimed at helping small businesses protect themselves from such cyber-crimes and huge fines.

On average, 90% of a businesses' assets are digital. This includes customer data, product data, marketing data, financial data and employee data. As such, this data is prone to serious threats from malicious online entities. Viruses, malware and hackers could attack and deplete / steal your confidential data, meaning that major segments of your business' operations could fail with a digital malfunction or security breach.

The good news is that the most common types of cyber-attacks can be prevented by investing in security solutions. The first step in implementing such solutions is understanding the different types of cyber threats. Next, you have to explore the solutions available in the market to learn how to defend against these cyber-attacks. This guide delves into the five easiest steps which your business can defend itself against cyber-attacks.

In this guide, we will explore the proper method of using passwords, which can help you prevent many potent cyber-attacks. Next, we'll discuss how you can safeguard your smartphones and tablets from malware attacks. We'll also go into common ways in which malware attacks occur, so you can set-up defences against them. Then, we'll touch on disaster recovery, business continuity and secure ways to backup organisational data, so your business will be less impacted by cybercrime. Finally, we'll discuss phishing, common methods used for phishing attacks and how you can prevent them from occurring within your organisation. Through these five chapters, you can ensure that your company has sufficient protection to evade most scams, frauds and security threats.

Yours sincerely,

Pedro Martins

Pedro Martins
Co-Founder & Technical Director

Chapter 1 - How to Work with Passwords to Protect Data

Most organisations store confidential and business-critical data on cloud solutions, servers, Windows devices, Macs and smartphones. This data needs to be easily accessible by your employees but safeguarded from unauthorised personnel. The easy way to do this is by using strong, secure passwords. But you'd be shocked to know that 86% of the passwords created by employees are at high risk of being hacked. So, what's the correct way of using passwords? Here are five tips to create effective passwords:

1. Ensure that your screen-lock is enabled. Most devices offer protection in terms of screen-lock passwords, PINs, fingerprint or face unlock. When creating passwords, choose a mix of lowercase, uppercase and special characters. If you're enabling face or fingerprint unlock, pair it with a super-long word password that is impossible to crack. This way, you won't be burdened to remember it as you'll be using face or fingerprint unlock anyway.

You should also ensure encryption software is implemented to safeguard client and employee data on PC and laptop hard disks (e.g. mailboxes and data synced with cloud storage solutions).

2. Encourage the creation of more secure passwords. Create an IT policy that explains the importance of secure passwords for employees. Ideally, the policy should also express in easy and clear steps how one can create a secure password. Passwords should be easy to remember, but not at the cost of account security. They should be hard for someone else to guess. A good way to ensure this is by checking if someone close to you can guess your password within 20 attempts. In addition to this, employees should most certainly steer clear of universally generic passwords that are easy to guess, such as "password," "123456" or "1111111." There are easy tips to create more secure passwords. One such tip is to use one uppercase and special character in your password.

We strongly recommend central security management systems such as InTune, Hosted Active Directory for Windows or Jamf for Mac to manage enforced and regular password changes for all staff members. Specific rules can be put in place regarding a mix of uppercase, lowercase and numeric characters. These platforms also offer many other enhanced security functionalities.

3. Roll-out Multi-Factor Authentication (also known as 2-Step Authentication) for sensitive accounts. This solution doubles your security at low cost and effort. What does Multi-Factor Authentication mean? Well, it requires you to use two screen lock methods. Typically, this involves password protection and one more method to prove your identity before you access a device or service (e.g. mailboxes or cloud data storage). This could also be in the form a one-time code generated per session and sent to your smartphone (as in the case of certain online payment methods). Remind your staff that they shouldn't share passwords or access for any purpose. Ensure that every employee has a separate and personal access point, so there's never a need to share passwords. When providing employees access, take care to give the lowest required access for each employee to complete his or her job. Avoid unnecessary exposure of sensitive information where possible.

4. Refrain from using default passwords. If you are using default passwords at present, have all of them changed by system users. Default passwords or "umbrella passwords" can pose serious threats to the security of your organisation's data. Some users even retain the default passwords set by manufacturers, opening their devices to serious hacking threats. Ensure that all your devices have non-default passwords that are complex enough to ward off common cyber-security threats.

Chapter 2 - How to Keep Your Smartphones and Tablets Safe

Many staff members today use mobile devices to access mailbox data, and sometimes files and documents. This entails the storage of sensitive and confidential data on such devices. Further, these devices leave the office environment often, making them more prone to physical and cyber-attacks. That makes them require protection more than PCs, laptops and other devices on which organisations tend to focus their cybersecurity efforts. Bearing those details in mind, here are five tips to keep your mobile devices and data secure.

1. Begin by enabling password protection with a sufficiently complex password or PIN. Avoid using a simple password or PIN that can be guessed using your profile image as a reference. Most smartphones and tablets today have fingerprint and face unlock systems built into them. However, these features are usually not enabled when dispatched, so you have to ensure to do that manually. Further, you could opt for Multi-Factor Authentication for devices housing important accounts and data.

2. Keep all mobile devices updated. Irrespective of the mobile device brand or version of OS (Windows/Android/iOS), mobile device manufacturers release updates on a regular basis. These updates typically address previously raised security concerns and breaches. Installing such updates should address critical security concerns and keep your devices protected. Updating your devices takes no time or money investment. You could even set your devices to be automatically updated when possible. During the lifetime of most mobile devices, manufacturers stop releasing updates. It’s at this point when you should be considering replacing them with new devices.

3. Update your apps regularly. It’s not just operating systems of devices that need updating. It’s essential to update all apps regularly. Such updates offer new features, functionality and ramp-up existing security measures. Ensure that your employees are aware of this fact and know how to keep their apps updated, so they never face security issues created by apps.

4. Track all lost and misplaced devices. If you can’t successfully retrieve them, then invest in having them wiped out or disabled so that the theft won’t result in a cybersecurity breach. Employees are more susceptible to theft when away from the office environment, that is, at home or in the field. The good news is that today’s devices have free online web tools that can be used to track them or wipe their data. You can leverage these tools to track the location of your device, enable backup of the data on the device or remotely have the data wiped out. Installing such software on an organisation’s devices can be a painful task at first, but you can use mobile management software to set up standard configurations effortlessly.

5. Avoid connecting to public Wi-Fi hotspots. The danger in using public hotspots is that you are unaware of who is controlling them. Another issue is that anybody can connect to these hotspots and even access what you’re working on while connected. Through this invasion, third-party groups can gain your login details for apps and web services. The simplest way to evade such outcomes is by not connecting to unknown Wi-Fi hotspots. Alternatively, you could use your mobile 3G or 4G network, which most certainly have built-in security measures. Yet another alternative is VPNs or Virtual Private Networks. These networks encrypt your data before uploading it on the internet. If you are working with third-party Virtual Private Networks, ensure that you have the technical ability to configure it yourself. Also, take care to use only VPNs that are offered by reputable service providers. You could also use “tethering” to connect your phone 3G or 4G connection to your laptop or tablet.

totality services offer and support a range of end-to-end Mobile Device Management solutions which enforce security polices such as the above and more.

Chapter 3 - Safeguard Your Organisation from Malware

The 2017 WannaCry Outbreak made the world nervous about malware. What exactly is malware? Well, it's malicious software or web content that can pose a serious threat to your organisation. The most common form of malware is viruses, which are self-replicating malicious programs that can invade and infect other legitimate software. To prevent the impact of such malicious software, there are certain precautions that you can take. Here are five such tips to help you safeguard your organisation from malware.

1. Invest in professional Anti-virus software. Anti-virus software usually comes pre-installed on operating systems for most PCs and laptops, however it's strongly recommended that a professional, paid-for solution is rolled out. At totality services, the majority of our clients have Webroot Endpoint Protection installed. This solution has an enterprise level toolset, so for example our helpdesk is made aware of any malware across all the workstations we support, automatically and instantly. When dealing with smartphones and tablets, you may be required to follow a very different approach. Sometimes, ads are responsible for introducing malware on your devices. You can prevent such an invasion by installing an ad blocker on your smartphone browser.

2. Update your IT equipment regularly. Ensure that all updates available for your devices are installed, so you have the best possible security measures implemented. Ensure that software and firmware for all your PCs, laptops and mobile devices are the latest versions provided by vendors and software developers. Installing these updates is a process that is referred to as patching. All operating systems, apps, PCs, laptops and phones should ideally be configured to update automatically once tested, through central security management tools. There are a number of platforms available to manage this across Windows and Mac IT estates.

3. Create an IT policy about downloading using office Wi-Fi. Ensure that your employees never download sketchy apps or visit dodgy websites using the office Wi-Fi. This could put every device connected to that Wi-Fi at risk. You can create a list of pre-approved websites (like the Google and Apple app stores) from which your employees can download content. Forbid employees from downloading apps or data from unverified sources and vendors. Try and limit access to certain domains to prevent the most massive of threats. You can give employees just enough access to perform their jobs comfortably. These types of rules and security measures should be implemented at the Firewall level.

4. Restrict the usage of USB drives and other peripherals. Employees focus majorly on convenience when trying to fulfil their responsibilities. This could tempt them to share/carry data between offices or people through hard disks, USB drives or other such peripherals. However, even one infected USB drive could cause the downfall of your entire organisation. Malware are hard to detect and track. They only show signs of infection once they have entered your system. You can prevent the spread of malware by following these tips. Block all USB / DVD Drives using appropriate centrally managed software, using Anti-virus software, or restricting the use of the drives to one department of your organisation. Ensure that only approved drives and memory cards are plugged into your system. Make all of these rules your company policy, so they are easy to enforce. Finally, consider alternative methods of storing data, such as the cloud.

5. Set-up robust, business grade firewalls. Firewalls act as buffer zones between your organisation's network and external networks. Depending on your requirements (e.g. type of confidential data held), Meraki or Datto devices / software may be required for enhanced security protection.

Chapter 4 - How to Securely Backup Your Data

Consider how critical your data is to your business. Content writing agencies store client contact details and project specifications. HR companies store candidate profiles and client details. IT companies have all of their algorithms and projects stored alongside client data. Hospitals store patient records and financials.

How can any of these businesses operate without their data? Businesses of all sizes, in any industry, should backup their data securely from time to time to ensure no loss of data. If you have regular backups of data with ample retention rates, you won't lose data to ransomware threats. Ideally, businesses should also take precautions to prevent the effect of flood, fire, theft or other physical threats.

When backing-up business data, there are certain best practices that you should follow. Here are five such practices to consider when backing up your data.

1. Take stock of your data that needs to be backed-up. Without a plan, you can't structure your investment to securely store your data. First, make a document listing all of your data that has to be protected. Typically, this will include official documents, contacts, emails, photographs and calendar events. However, this list may extend to include customer information, sales and marketing notes, intel and company projections and financials. Also, consider all the information stored in shared folders and company accounts.

2. Plan a backup method that's separate from main data repository. Keep your server, NAS, Office 365, G Suite and other data backed-up on a compliant cloud-based solution. Ensure that access to this backup is restricted. It should especially be kept away from storage devices and systems that are suspected to have Ransomware or any other malware. This is because malware can be transmitted to any storage automatically, leaving all such backup potentially infected, so you have no recovery. For strong backup, you should store your backups in various UK data centres, so threats such as theft and fire leave them unaffected. Cloud backups with decent retention rates are the safest way to stay safe from malware.

3. Incorporate automatic back-ups into your daily schedule. Most cloud storage software today enable automatic backups; for instance, when you save new files to certain folders. Leveraging this automatic backup option saves you a lot of time and ensures that the latest versions of your files are stored for future reference. Most of these ready-to-use network and cloud solutions are super-easy to set up. They are also affordable when you consider the protection they offer to your invaluable business data. Before you choose a cloud solution, analyse how much storage space you need, the retention rates and how quickly you want to be able to access your data after an incident.

4. Invest in cloud storage, and backup that data. Many small and medium-sized businesses are already using cloud storage in Office 365, Azure, AWS or G Suite. If you decide to use cloud storage, a service provider will store your business data in their storage infrastructure. That means that there's a physical separation between your office location and where your data is stored. It's important that this data is also backed up on another 3rd party cloud storage platform to fully protect your files and documents. totality services offer a wide range of cloud solutions and cloud data backup platforms with full support included.

5. Evaluate cloud service providers carefully. Before entrusting your precious data with someone else's storage hardware, it's important to evaluate their reputation and services. Ask the cloud service provider to describe its services and provide validation for all of its claims. Assess the service provider's security measures such as anti-virus software, firewalls, data encryption and regular security checks.

It's also useful to check if the storage location is prone to natural disasters such as floods or earthquakes. The service level agreement is a crucial part of your cloud service experience. Check if the promises on this agreement meet all of your requirements.

Chapter 5 - Preventing Phishing Attacks

What exactly is a phishing attack? Typically, phishing is when scammers lure victims into sharing sensitive information such as passwords or bank details through suspicious looking emails. Sometimes, these scammers also send links to malicious websites or trick victims into sending money. Other scams involve stealing data to sell to advertising or political firms and gaining access to large organisations through stolen employee information.

Phishing emails are not always easy to spot. They could trick even the most observant of internet users. It doesn't matter if yours is a big or small business, you can be the victim of a phishing attack. This chapter of the e-Book is aimed at helping small businesses recognise phishing emails so they can protect their data and accounts. But remember that this isn't the perfect solution. There's a limit to what you can expect from employees.

1. Stay alert to the most obvious signs of phishing. It's not easy to identify and delete all phishing emails. Asking this of your employees could be more harmful than helpful. Ultimately, such an effort-heavy task could put the stops in your business productivity. However, most phishing emails follow the same general pattern, so you can request employees to keep an eye out for the red signals. Here are some of those signs.

- ✓ Most phishing scams are from non-English speaking countries. Usually, phishing scams come in emails with poor spelling, punctuation and grammar. These emails usually appear very official. They include logos and well-made graphics.
- ✓ Check if the email design is what you would expect of large organisations.
- ✓ Note how the email is addressed. Does it have your name? Or is it addressing you through generic terms such as sir/madam, friend or colleague? If the sender of the email doesn't know you, it could be indicative of a phishing scam.
- ✓ Does the email convey urgency? Many phishing scam victims fall prey to them because of the urgent/emergent tone of the email. Is it compelling you to do something unwise? Beware of words like "reply with your details within 24 hours" or "your email has been hacked, click here right now."
- ✓ Some scammers go as far as to impersonate people within your organisation. Watch out for emails from your CEO requesting you to make a payment to a random bank account. This type of scam is common in large organisations.
- ✓ Check the sender's name. Verify on LinkedIn or Facebook if possible. Does it seem legitimate? Does it appear to imitate someone in your contacts?
- ✓ Does the claim in the email sound plausible? Phishing emails usually offer rewards, prizes and access to the inaccessible. Assess if the claim in your email is legitimate before clicking on any link or giving up any private details.

2. Carefully analyse how you operate. Critically assess how a hacker may launch a phishing attack on your organisation. Figure out your weak points, and ensure that all employees are aware of how they can be targeted. This should be done with special attention to exchanges with other organisations. It's through these channels that phishing attacks are made. Your employees should be equipped to identify the normal ways in which phishing occurs.

Common attacks involve sending invoices for unknown services. When attachments such as these are opened, the malware is automatically downloaded, without your knowledge or consent. Yet another means of attack is convincing employees into transferring money or data through emails that appear fully authentic. List these types of common attack methods and figure out how to make them less effective. Here's an example. Give your staff a process of how to deal with unsolicited emails and requests even when it's from managers or customers. Many times, hackers impersonate your contacts and launch attacks. Show employees how to verify identities before taking any action.

Make sure that you understand all the relationships that your business runs regularly. Scammers often use these contacts as identities to initiate conversations that lead to phishing attacks. Sometimes, cybercriminals pose as large banks or insurances hoping that you have a relationship with someone from those companies. When such emails show up in your inbox, ask employees to tread with caution. Ask them to report such emails even if they appear to be legitimate and important. Treating the email with suspicion could prevent a major mishap.

3. Manage your accounts such that the impact of phishing attack is reduced. Manage staff accounts so that you give employees only necessary access. Use the “least privilege” principle in deciding how to provide your employees with access. This means that your staff members should have the minimum clearance required for them to complete their jobs. This ensures that the impact of a phishing attack through them is controlled and limited to a miniscule part of the organisation. You can further limit the damage caused by the loss of login details or malware by advising employees not to use their admin accounts when browsing the internet. Request them not to check emails when logged into the admin account either.

Admin accounts are typically those that have the power to make changes affecting other employee accounts. Admin accounts can also control security settings, install software and hardware and access all data on all systems connected to your network. To prevent the misuse of that power, request employees with admin access to use Multi-Factor Authentication on important email accounts. So, even if a hacker accesses your passwords, they won’t be able to get past the second line of defence.

4. Create a system to have all attacks reported. Ensure that your employees have the support to request help when such an event occurs. Even if an employee thinks they are being targeted by a cybercriminal, they should be able to raise a request for help. Once that’s done, you should launch an effort to scan all systems for malware. All passwords should ideally be changed to prevent misuse of those stolen during such an event. Don’t resort to punishment if an employee is a victim to phishing. This can be counter-intuitive, especially if it discourages others from coming forward when they suspect that there has been a phishing attack. It could also scare employees into spending unnecessary time and energy scrutinising every email that they receive. Each of these things could set your business back in the long run. In the event that your company is victim to online scams, fraud or extortion, you can report this to the Action Fraud website.

Attackers are always trying to infiltrate organisations using different attack methods that overcome cyber protection measures. That’s why it’s important to stay updated on the latest methods being used by cybercriminals to run online scams. You could do this by signing up for the free newsletter sent by Action Fraud Alert to receive accurate and verified information about scams.