How's BUSINESS

The How's Business guide to *Cyber Security*

What's How's Business?

Hello. First of all, we'd like to say a big thank you for downloading our guide.

We're How's Business, the growth hub for York, North Yorkshire and East Riding.

We're one of 39 growth hubs set up by the Department for Business Environment and Industrial Strategy.

Our role is to make it easy for business owners like you to find the support you need. This could be to locate funding, help with marketing, or advice on how to expand your set-up.

As our patch is quite rural, travel times can really cut into your day.
So, we try to focus on what's available locally. Our website plays a vital role in offering advice from anywhere with an internet connection.

We hope you find our guide really useful.

Introduction

This eBook aims to help make you and your business more cyber aware and give you some advice for staying safe online. It has practical tips that you can use to help protect your online assets and customer data as well as some ideas about where you can go to get extra help with protecting your business.

Contents

Disclaimer: This eBook is only a guide to basic cyber security. Always talk with an expert about any problems or questions you have about your safety online.

Chapter 1: Simple steps for protecting yourself online

Rhys Jones
McClarrons Ltd

Cyber security is a must in business as well as in your personal life. There are numerous ways that you can protect yourself, including simple, cost-effective steps. You don't have to be a tech expert to implement these security measures, but if you do want something a little more complicated, head to our next chapter, as every bit of defence helps.

Passwords

One of the easiest things you can do to keep yourself safe online is to have a strong password that you regularly update. But, be aware, cyber criminals can often detect when passwords change, which will demonstrate that an account is active. So, you shouldn't change your password too often, especially if it reduces the strength of your password.

Strong passwords include a mixture of upper and lower case letters, numbers, and special characters like !, @ and ? but they do need to be memorable, as it is very unsafe to have a document listing all your passwords. All staff should have their own unique passwords and there shouldn't be a need for everyone to

share the same password. Also, if your staff share the same account then this could jeopardise everyone if one person is hacked, so each member of staff should have their own profile.

If you are struggling to create numerous passwords for different accounts, you could use a system such as 1Password. Using this website will mean you'll need to remember only one password and the rest will be securely stored for you.

Don't fall into the trap of using guessable passwords. Make it something relevant to your business so that you'll remember it. Don't use any of these as they are the first things a hacker might try:

- Name of your product/service
- 1234 or 4321
- Access
- Admin
- Anonymous
- Database
- Guest
- Manage
- Pass
- Password
- Root
- Secret

With your passwords, you should also look out for suspicious activity – check any unauthorised access to your systems, failed log-in attempts or out of hours activity. Limit the number of times someone is allowed to try and log-in and make sure that the system is locked down once the threshold has been reached. Remove any accounts that are no longer being used so that they can't be accessed once the employee has moved on.

Software updates

We've all been there. Our computer tells us that they need to restart and install updates and we postpone them for as long as possible. In the interest of cyber security, you should allow your computer and other technology to update itself, as these often include security updates which will help keep you safe online.

Take a look at this site for some guidance on how to make sure all your devices have the latest software updates running.

Head to the next chapter to find out more about software techniques you can use to protect yourself against cyber-crime.

Use anti-virus software

It's in the name: anti-virus software helps to keep you safe online by keeping out viruses. If a virus gets into your computer systems or other technologies, then it can access whatever data you have and send it back to its creator. In some cases, viruses can corrupt or destroy data so that you can no longer use it.

Pick one anti-virus provider for your systems, not multiple. Using two anti-virus software programmes does not mean you'll have double protection. They'll cancel each other out, or cause your computer to freeze or become inoperable which will actually leave you unprotected.

There are lots of different, really great anti-virus programmes that you can install on your computer. Make sure you shop around and look at reviews before signing up to any. Check over what coverage they provide and look at some independent reviews before you make a decision.

Train your staff

It's always better to work with your staff than against them, and having everyone working towards the same goal will make your online security much stronger.

Have a look here for free online training for you and your staff provided by partners of the UK government.

Future Learn offer a free, eight week introduction to cyber security. If you and your staff spend just three hours per week on the course, you can learn how to make sure the work that you do is protected. Sign up here.

Email phishing scams

If something looks suspicious in your inbox then it probably is. Make sure you never open an email if it seems strange, and definitely don't open any attachments sent to you unless you know exactly who it has come from and were expecting it. Files can very easily hide the code for viruses that, once opened and allowed onto your computer, can be very hard to get rid of and can cause lots of damage.

Phishing is one way that hackers can gain access to sensitive personal details, such as usernames, passwords and payment details. This is usually done through emails, which contain malicious attachments or website links that will infect your computer or devices. The problem with phishing is that these emails often appear authentic from legitimate organisations, or even someone that you know.

When checking your emails, you should keep your eye out for:

- Vague terms like 'dear valued customer' as they're unlikely to know your real name and therefore shouldn't be opened.
- Odd spellings, random and excessive capitalisation and grammatical errors in the subject box – this is an attempt to get around spam filters.
- A mismatched URL – when hovering your mouse over any links within the email, you'll often see the actual hyperlinked address is different from the address that is displayed.
- Requests for personal details like your card information or passwords.
- A sense of urgency or threatening language in the subject line as phishing emails often play on your emotions.

Here are a few actions you can take to decrease the threat:

- Reduce unwanted email traffic with basic security protections, such as email filters, which should also block malicious intruders and alert you to suspicious activity.
- Make sure employees are aware that they shouldn't click links in suspicious emails but be cautious of email attachments from unknown sources. Sometimes viruses can fake the address of someone you know, so it's best to be cautious of any strange emails.
- Keep computers used for social media sites, email and general internet browsing separate from computers used for processing financial transactions.
- Regularly check for updates for your security software and web browsers, but ensure employees only install approved applications and are on the right website when downloading. You should double check the URL.
- Never reveal personal details when responding to emails. Even if you believe the organisation is genuine, you should always be cautious and check their legitimacy before revealing anything. Banks would never request sensitive information from you by email, so don't trust any email claiming to be your bank asking for private details.
- Never respond to a message from an unknown source, even unsubscribe links can be malicious.
- Don't believe everything that you see. Phishers are becoming more skilled at what they do, so be aware that an email with a convincing brand logo or a valid email address isn't necessarily legitimate.
- Use an EV certificate on your webmail. This is a certificate used for HTTPS websites to prove that the controller of the website is legitimate, which would prevent staff members from wrongly accessing a webmail created by a hacker. For more information on this, head here.

Physical safety

Your computers and other technology needs to be safe in the real world as well as in the cyber world. Control the access to your machines and don't leave them unattended in an unsecure place. If someone can directly access your technology because it isn't secure in your workspace, they won't need to turn to cyber crime, they can access your data straight from your devices.

Sign up to fraud alert

You can now sign up to Action Fraud alerts and receive direct, verified, and accurate information about scams and fraud in your area by email, text, or voice message. They will only send you alerts that are applicable to you in your area so you'll only receive relevant messages. Action Fraud provide this service for free, so sign up here today.

Back up your data

It's always a good idea to have other copies of your data in case something happens to it. If a threat enters your computer systems it can destroy your records, so having them backed up on an external drive can help lessen the impact.

Insurance Cover

It is possible to purchase insurance cover to protect businesses against the financial consequences of a cyber attack. The losses a business can suffer may be direct or indirect, i.e. paying compensation to customers whose data has been lost.

Cover can include:

- Costs of investigating breach and restoring data
- Business interruption
- Privacy costs
- Hacker damage
- Media liability
- Cyber extortion/ransom
- Social engineering e.g. telephone, e-mail
- Third party damages
- Costs incurred dealing with the Information Commission

Some of these covers are standard and others are optional, therefore, it is important to seek independent advice on your insurance needs to determine

which policy fits your requirements.

Insurers will also offer assistance should a loss occur with access to dedicated professional claims and IT specialists to help with everything from data restoration to dealing with a ransom demand.

For more information on cyber insurance, head to the next chapter.

Summary

There are lots of small things that you can do in your business to make sure you stay safe online. They don't have to cost a lot, and can really help you protect your business data online. Work with your staff to make sure cyber security measures are consistently followed in your business.

Further resources

Cyber Essentials

Designed by the government, Cyber Essentials is there to help protect your business against common cyber threats. This certificate also shows your customers that you are serious about protecting their data.

Action Fraud

If you see anything suspicious on your systems or online, you can report it to Action Fraud, the UK's national fraud and crime reporting centre.

Get Safe Online

Get Safe Online offer businesses great, free, expert advice about cyber security and have a tool where you can directly ask your questions.

The government

The government have a really detailed document specifically for business owners that you can access for free for more advice on how to stay safe online.

The National Cyber Security Centre

The National Cyber Security Centre have a really great free PDF that you can access which shows you common cyber threats, how you can help prevent them, and what to do if you are a victim of cyber-crime.

Chapter 2: Next steps for increasing your cyber security

Stephen Ridley
Hiscox

You should use a range of tools to help protect yourself against cyber crime, because this will help to build up your defences and make your business more resilient. You could even promote the steps that you've taken to safeguard your data and sensitive information, so that your customers will have more confidence in you. In the last chapter, we discussed some simple, cost effective steps to take (e.g. use stronger passwords, be careful when checking emails etc.), now we're going to show you how to up your game even further through ethical hackers, cyber insurance and patch management.

Certified Ethical Hackers

A certified ethical hacker is a skilled professional who understands how to search for weaknesses in your cyber security. They use the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to check the structure of your computer systems. To help improve your defences, they will attempt to breach your cyber security and find vulnerabilities that a hacker would exploit. Rather than take advantage of this, they work for you, and would document these instances and advise how to improve them.

The ethical hacker will have been trained professionally and certified by the EC-Council. The EC-Council, the International Council of E-Commerce Consultants, is the world's largest cyber security technical certification body and have developed the Certified Ethical Hacker, Computer Hacking Forensics Investigator, Certified Security Analyst and License Penetration Testing (Practical) programs. For more information, check out the EC-Council's website.

Hiring a certified ethical hacker can't guarantee your systems will become 100% secure, but it will help you to withstand automated attacks and unskilled hackers. Some standards even require you to test your security through an ethical hacker, such as the Payment Card Industry Data Security, for more information on this, head to chapter 4.

Before hiring an organisation or individual, you should thoroughly read through their service level agreement – this is a contract between a business and its IT supplier. For more information, check out the Tech Donut's website. Discuss with your ethical hacker how testing will be carried out and how their findings will be handled. They will be dealing with sensitive information, so you need ensure you hire a firm that you feel confident in and can trust. Plus, you will need to agree on a legal contract. If you're unsure about the contract, you might want to seek legal advice. You can search for a solicitor on The Law Society website.

Cyber Insurance

Buying insurance can also help to protect your computer systems and data. With cyber insurance, you'll have coverage for:

- Breach costs – the costs of investigating, remediating and responding to a data breach
- Business interruption – the lost revenue or increased costs suffered as a result of a cyber attack
- Data restoration – the costs of repairing / reinstating data that is lost or damaged as a result of a cyber attack
- Cyber extortion – the costs of managing an extortion incident, such as ransomware or threatened denial of service attack
- Privacy liability – legal costs and awards for legal actions brought by individuals affected by a data breach, or regulators that have jurisdiction over data protection matters
- Multimedia liability – legal costs and awards for legal actions brought against you as a result of your online content, such as website and social media feeds, for defamation, breach of intellectual property rights, or transmission of a virus.

You should strongly consider cyber insurance if:

- You hold sensitive customer data.
- You are reliant on computer systems to run your business.
- You have a website, especially if it's for eCommerce.
- You are subject to Payment Card Industry Data Standards Security which we discuss in chapter 4.

Cyber insurance is worth having as part of your overall security strategy. Despite this many businesses don't yet have the insurance and could face unnecessary charges. If your business is near the river, you wouldn't ignore insurance coverage for flooding, so don't ignore cyber insurance when technology often rules the running of your business.

Even if you use cyber security solutions, your company could still face unnecessary disruption in managing an incident. One of the biggest benefits of many cyber insurance policies is that they do not just provide financial recompense in the event of an incident; they will often provide access to a team of specialists that is on hand to do all of the heavy lifting straight away. This will ensure that the incident is handled as swiftly as possible, and will leave you and your staff free to carry on with running the business as best as possible.

Before you buy insurance cover, you should think about what expenses and incidents you would like to have covered. You should then either see a cyber security specialist broker (head down to further support to find these) or an insurance company. For more information on buying cyber liability insurance cover and what questions to ask, see these tips.

Patch Management

Without the technical jargon, patch management is simply about keeping software up to date and able to handle cyber attacks. Updating your systems can be a nuisance and disruptive to your day, but software becomes vulnerable if it isn't updated and hackers can take advantage of this. It's especially important that you keep your anti-virus or anti-malware products updated. Patch management will help to maintain updates and check which are appropriate and test systems after installing.

You should also avoid using unlicensed and unsupported software, as this would prevent you from receiving continuous updates. Most importantly, when those updates pop up, make sure you install them.

Summary

In the news, there are often cases of big businesses being hit by cyber breaches, but you need to be aware that these are risks that could still harm a small business. By following our tips, you could help to strengthen your security. With ethical hackers, you'll know where your weaknesses are and

how to correct them, whilst cyber insurance will be a security net for if anything does go wrong, preventing numerous costs to your business. For ideas on day-to-day changes you could make, head to chapter 1.

Further resources

Hiscox

Hiscox are one of the businesses that can offer you cyber insurance. They will protect your business by paying you if you suffer a breach, help you to minimise any losses and damage to your business. They also offer a range of tools to help you stay up to date with evolving risks and how to create a response plan. For more information, head to their website or give them a call on **0808 2743 517**.

British Insurance Brokers' Association

If you want to buy cyber insurance, you can get it directly from an insurer or from a broker. The British Insurance Brokers' Association has lists of brokers and you can find ones specialising in cyber insurance. Coverage for small businesses often covers between £100k and £5 million.

National Cyber Security Centre

National Cyber Security Centre is a source of advice, guidance and support on cyber security, including the management of cyber security breaches. Head to chapter 6 for more information about the centre.

Chapter 3: What to do if you've been a victim of cyber crime

By Laura Dempsey
TeraByte

No matter how careful you are, there is always the risk that you could be a victim of cyber crime. As this eBook has shown, there are lots of things that you can do to raise awareness for the potential risks and ways you can reduce the likelihood of being a target for cyber crime.

So, what can you do if you have been a victim of cyber crime?

Action Fraud

If you've been a victim of crime, you should contact Action Fraud. They are the UK's national fraud and cyber crime reporting centre. They are run by the City of London Police and work alongside the National Fraud Intelligence Bureau, so they can make sure that your crime report reaches the right place so the appropriate action can be taken. An investigation will be launched, and hopefully the cyber criminal will be caught.

Report the crime at any time here or call them on **0300 123 2040** between 9am and 8pm Monday to Friday

Disconnect from the internet

As soon as you notice that there is a threat in your systems, you should disconnect from the internet. Breaking the connection in this way is the best way to put an immediate stop to the attack.

If you are connected via an ethernet cable you can physically disconnect yourself from the internet by removing it from the device. If you are connected wirelessly, you will need to go to the start menu, click on settings, head to network connections and select disable. If you're using a phone or tablet, you will need to go to your settings, click on Wi-Fi then switch it off. With phones, you may also want to turn your data off, so you don't accidentally reconnect to the internet. For a Mac, you will click the Wi-Fi icon in the menu bar then click turn Wi-Fi off.

Contact your IT service

If you have an established IT service working within your business, you should contact them. They will be able to track the source of the problem and hopefully put a stop to it and recover any damaged files.

Scan your computer

Hopefully, you'll have an anti-virus software installed on your computer that can do a lot of the leg work for you. Your anti-virus can often detect and remove threats to your system.

Close accounts

If you have been a victim of fraud, then you should talk to your bank first, as money may be recovered and they can advise on the best course of action. Likely, you will need to close all the affected accounts within your bank to avoid any of your money being spent by the online thief.

Set up fraud alerts

You can set up a fraud alert with a consumer reporting agency. This will mean that your bank is aware you suspect fraudulent action might be taken using your name and accounts. The fraud alert will ensure creditors will contact you directly before making any changes to existing accounts or to open any new ones, so that criminals cannot make changes to your accounts or take money out in your name.

There are three agencies you can contact, and speaking to one will set up alerts with all three, so they do most of the hard work for you: Equifax, Experian, and Transunion.

Change your passwords

If you've been a victim of cyber crime, it's vital to change your passwords. For more support on creating passwords, head back to chapter 1.

Summary

You need to make sure that you and all your staff are working towards increasing your cyber security so that you don't come under cyber attack. But no matter how careful you are, there is always some risk that your business data might not remain safe. Knowing how to respond is vital, and can minimise the damage a virus or a criminal can do if they get into your systems.

Chapter 4: How to protect your customer's online payments

Andy Gambles
Servertastic

eCommerce has become a popular platform for business as it allows you to reach a new market and grow your business. But you need to be aware of security measures that should be put into place to protect customer data. Without effective payment security in place to prevent breaches, you could face severe penalties of up to £500,000.

To avoid this, you must comply with the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS is a worldwide security standard developed to protect cardholders' personal information.

What is Payment card industry data security standard (PCI DSS)?

PCI DSS is the Payment Card Industry Data Security Standard, which was set up to help businesses process card payments securely, protect cardholder data and reduce card fraud. The standard includes a set of requirements that you must follow if you handle credit or debit card payments.

However, depending on the website and card transaction processer that you use, you may not be directly responsible for all of these requirements. There is no one-size-fits-all method to ensure you are compliant – different procedures will be needed, depending on your card payment processing. If you have used a web developer to set up your eCommerce website then they may have integrated some of the PCI DSS requirements already, similarly certain websites (e.g. Etsy, eBay) and shopping carts should be PCI DSS compliant - to be safe though, you should always double check this.

If you're uncertain about what is required of you, then you may need to get in touch with your web developer, check out what information is available on your website host, or speak directly to your website host. Also, your payment gateway may be different to your website.

If you have set up your eCommerce independently and are responsible for payment transactions, you will have to make sure you have:

- A firewall to protect your data

  A firewall is software that stands between your computer and the rest of the network, which prevents unauthorised connections being made. Most routers, computers (Windows or Mac OS X), anti-virus software and servers already have firewalls built in which will provide you with a good amount of protection.

  Most importantly, double check that you're covered and that your firewall is on as some router's firewalls are automatically turned off. If you don't have a firewall on your server then you will need to install one or switch to a server with one already built in. Your firewall should also be configured to allow only traffic that is necessary for your server. Be sure to close unused ports and restrict those providng server acess to just the necessary IPs.

- Strong passwords for you and your staff

  Regardless of what platform you use, this will be your responsibility. For more support on this, head back to chapter 1.

- Encrypt all sensitive data

  It won't harm your business to have everything protected, including ecrypting your hard drives. Basically, anywhere that you store data needs to be made secure. Transport Layer Security (TLS, which is discussed later in this chapter) provides secure communications on the Internet for things such as data transfers.

- Regularly update all software, especially anti-virus

  Updates can often seem like a nuisance but if you do get a notification, don't ignore it. Keeping your programs up-to-date will help prevent vulnerabilities to your system. Some eCommerce websites, such as eBay, will handle their updates internally, so you won't need to worry about this, but you should ensure other systems that you use are still maintained. For more information on updates, head to chapter 1.

- Restrict access to sensitive data

  Ensure confidential data is only available to those who definitely need to access it. For example, not all of your employees need to know personal details such as the addresses of your customers. To help this, you could assign a unique ID to each person with access – this way you can monitor activities and ensure no one is wrongly using data. This also applies to physical access of cardholder data, it should be restricted to only those who definitely need to use it. Also don't keep data that you no longer need - dispose of it correctly. Head to chapter 5 for advice on data protection.

- Regularly test security systems

  If you use an eCommerce website such as eBay then they will likely invest in ethical hackers to test their systems. But, if you have your own independent website, you might want to try an ethical hacker (explained in chapter 2), hire mystery shoppers to test the process of buying on your website, and regularly run virus scans and subscribe to mailing lists that will give you cyber security updates.

- Ensure your staff are aware of their roles

  No matter how you handle your card payments, it's important that all of your team are on the same wavelength. Let them know what their responsibilities are and how they can ensure they are PCI DSS compliant. They should also be aware that they can challenge requests if they don't feel comfortable that they comply with the PCI DSS.

Who must use PCI DSS?

You need to comply with PCI DSS if:

- You are selling online, even if you have subcontracted all PCI DSS activities to a third party.
- Yu are a service provider, including software developer. If you're processing cardholder data then you must comply.

When is PCI DSS not relevant?

PCI DSS is always mandatory if you're taking a card type payment, regardless of what you're selling, your business size or the amount of payments you take. People often make the mistake that compliance depends on what website you are using, for example, many eCommerce websites, such as Shopify, already have PCI DSS built into their systems. Trusted payment providers like PayPal are also PCI DSS compliant. When using PayPal, customers will give their payment details over the provider's secured site.

However, you will still need to ensure you are being compliant with the standard, as there are other objectives involved - using a third party provider doesn't cover everything. Although outsourcing will reduce your risk of breach, you cannot ignore PCI DSS. Achieving and maintaining compliance requirements can be challenging and time-consuming, but it is necessary.

How to be compliant?

As we've mentioned, it's necessary for all businesses who accept card payments to comply with PCI DSS, and you might already be taking steps to uphold this without realising. For example, you probably update your anti-virus software and this is one of the requirements of PCI DSS. But, this is not enough, you must also prove your compliancy, which is when things can get a little complicated.

Sometimes your bank will get in touch with you to inform you that need to prove your PCI DSS compliancy and you can ask them to support you through the necessary steps. However, you are responsible for making sure you are compliant, so don't wait until your bank asks you specifically.

In simple terms, here's the steps you need to take:

1. Determine your level

There are four levels of PCI DSS compliance, which are based on the number of transactions you process annually.

- Level 1: more than 6 million transactions per year.
- Level 2: 1 million to 6 million transactions per year.
- Level 3: 20,000 to 1 million eCommerce transactions per year.
- Level 4: less than 20,000 eCommerce transactions per year or less than 1 million other transactions.

The more transactions you process, the more complex the PCI DSS compliance becomes. Most small businesses will fall into Level 4, which includes less rigorous compliance processes. All that you would need to do is complete a submission of an annual self-assessment questionnaire (SAQ).

If you're unsure, you should speak to your bank, as all banks have teams dedicated to PCI DSS and security issues. Your bank makes the final decision over what level you are, so it is worth seeking their advice.

For more information, check out the information provided by the PCI Compliance Guide blog.

2. Find your Self Assessment Questionnaire (SAQ)

Not only are there different levels, there are also different SAQs, which depend on how you process your payment transactions. This is a necessary step even if you are outsourcing your payment card processing to a third party (e.g. PayPal).

See the chart below from PCI Compliance Guide website to determine which is right for you:

Processing Method	**Description**	**SAQ code**
Shopping cart - Entire Internet Presence Outsourced	Your customers enter their credit card information into a website to make online purchases, payments, or donations. All eCommerce pages including all payments acceptance and processing are delivered directly from a 3rd party PCI-validated service provider.	A
Shopping Cart - Payment Page Entirely Outsourced	During the payment process, the consumer's browser is redirected to a checkout/payment page (URL or iFrame) that is entirely controlled entirely by a PCI-compliant 3rd party service provider.	A
Shopping Cart - Payment Page Partially Outsourced	During payment process, the consumer's browser is redirected to a checkout/ payment page (URL or iFrame) that is controlled by a PCI-compliant 3rd party service, BUT some elements (javascript, CSS, etc.) are passed from the merchant page to the 3rd party payment page.	A-EP

Shopping Cart - Payment Page Direct Post	During payment process, the checkout/ payment page directly posts payment information from the merchant website to a 3rd party service provider, but the page resides on the merchant website.	A-EP
Shopping Cart - Payment Page Not Outsourced	During payment process, the consumer enters credit card information on a checkout/payment page that is part of the merchant website.	D-Merchant
POS Terminal	You are using POS (Point of Sale) software installed on a computer or other device. Computers with POS software are often combined with devices such as cash registers, bar code readers. In addition, POS systems typically have functionality beyond just payment processing, such as inventory management, and are usually designed for a specific business sector (e.g. restaurants, hospitality, gyms, grocery stores, etc.)	C
Virtual Terminal - Manual Entry	You use a web browser on a computer or mobile device to access a merchant services site for entering and authorizing credit card purchases. You should have a username and password and be able to access the site from any online computer. You never swipe the card, but instead use a keyword or keypad to manually type in the credit card information.	C-VT
Virtual Terminal - Card Reader	You have a card reader connected to your computer that reads the card information and enters it into the virtual terminal.	C

3. Complete the SAQ

The list of SAQs can be found on the PCI Security website with instructions and guidelines.

4. Send your SAQ to your acquiring bank

Do you need to renew your PCI DSS compliance?

Each year, you will need to renew your PCI DSS compliance in case you have changed your processes or the standard may have been changed to adapt to new security threats. Luckily, the PCI DSS compliance tends to be easier to fill out after the first submission.

Why are these requirements important?

If you don't follow the rules set out by the PCI DSS then you'll be leaving your business exposed and open to cyber risks. Plus, this will reduce the confidence that your customers have in your website. Then if you do suffer a security breach and you're not compliant, you could face Card Scheme fines and you may have to pay the losses that your customers have faced.

Transport Layer Security (TLS)

One useful tool you can use to uphold some of the PCI DSS compliance is a Transport Layer Security (TLS). This is not the only step you will need to take - you'll have further requirements, but TLS does demonstrate your website is legitimate.

Transport Layer Security is based on Secure Sockets Layer (it's predecessor), which you may still see it referred to as. To complicate matters, you may even sometimes see Transport Layer Security called HTTPS certificate. Essentially, these things are the same and involve ensuring all data passed between the web server and browser is protected by remaining private. TLS is an industry standard and is used by millions of websites in the protection of their online transactions.

To use TLS, you will need to get an TLS certificate. When you have this certificate, your website will display a padlock symbol in your customer's web browser when your site is opened and the https prefix in front of your URL address in the browser. This demonstrates to your customers that your website is secure and they will likely feel more confident making online payments with you. Google also likes secure websites, so you're likely to rank higher in search results with an TLS certificate.

When taking payments, you'll need a TLS certificate with one of the highest levels of security, which can cost a few hundred pounds. Be aware: different providers offer varying levels of certificates. To get your certificate, you should contact a TLS Certificate Issuer (also known as Certificate Authority or CA).

Summary

Tech jargon can be a lot to take in and some of the abbreviations might be giving you a headache. But, it's important to be aware of the regulations for taking online payments, which are especially relevant if you don't use a payment provider.

Further Resources

PCI Security Standards Council

PCI Security Standards Council was created to help improve the understanding of security standards for payment account security and their website includes a range of sources, such as training, assessors to check the strength of your security, and tips for preventing cyber risks.

The UK Cards Association

The trade body for the cards payment industry in the UK is the UK Cards Association and their website includes some useful information on Payment Card Industry Security Standards – what it is, why it's important, a compliance checklist and advice on data breaches and fraud.

The EC-Council Global Services (EGS)

The EC-Council Global Services includes information on Payment Card Industry Data Security Standard, including why your business will need to use it.

Do I need an TLS certificate?

If you're still unsure whether the TLS certificate is appropriate for your business, check through this article - it explains why it can be useful if you use PayPal, what the SEO benefits are and if you're using data other than credit card information.

Chapter 5: Data Protection Compliance

Samantha Dunwell

Dunwell Data Protection

Having excellent cyber security measures can help protect you against fraudulent theft and other expenses. On average, businesses lose over £1000 when they've been a victim of cyber crime, and that's just for legal fees and setting things right. Being secure can also make your customers feel more confident in buying your products or using your services as they know their data is safe. These are all great reasons to be cyber secure, but you are also legally obliged to protect customer data under the Data Protection Act.

With Principle 7 of the Data Protection Act, you have to ensure that the personal data that your business collects and uses is fully protected – this includes ensuring it is secure on your systems and can't be stolen through cyber crime. Without appropriate cyber security, your systems could be breached and you may be liable to a fine of up to £500,000 for breaching data protection legislation. So, you need to ensure you use the appropriate technical and physical security measures to safeguard the data you collect and use.

Principle 7 of the Data Protection Act

Many businesses are unaware of their responsibilities outlined in Principle 7 of the Data Protection Act and simply associate data protection with appropriately processing personal data. However, Principle 7 is just one of the legal obligations you must comply with and states you must have appropriate technical and organisational measures in place to safeguard the personal data you process from unathorised or unlawful processing and against accidental loss or destruction of, or damage to. Your employees must also uphold this principle and act responsibly when handling all types of personal data.

Having the appropriate defences to prevent cyber crimes within your business will keep you on the right side of the law. You will need to design your security around the nature of your data, be clear about the responsibilities of your employees, ensure you have both physical and technical security, and be ready to handle any breaches. This might sound a little daunting and expensive, but you don't need to worry about your bank account taking a hard hit. You aren't expected to have state-of-the-art technology protection, only what is appropriate to safely protect the type of personal data you process. Make sure you review your security as technology advances, keep software up-to-date and follow the tips from this eBook. For a refresh, head back to chapter 1 and chapter 2.

What should you do if there's a security breach?

Despite all the precautions that you put in place, there is still the chance that you could become a victim of cyber crime. Rather than panic, if this does happen, there are four steps that you can take to minimise the damage. The Information Commissioner's Office (ICO) proposes these four steps:

1. **Containment and recovery**
   You should have a recovery plan in place to help deal with the breach and handle any damage caused by the breach. If you have cyber insurance (which we discuss in chapter 2), you'll be better prepared for this situation and will save your business money.
2. **Assessing the risks**
   It is important to assess the risks associated with the breach as this will help determine the actions you need to take. For example, a laptop that is irreparably broken but its files were backed up and can be recovered has different risks to the theft of a customer database whereby the data obtained can be used to commit identity fraud. Assessing the risk helps you learn from the incident and strengthen your security to prevent future breaches.
3. **Notification of breaches**
   You'll need to think about who should be notified of the cyber attack and why. This is likely to include the people whose data has been compromised, the police, the Information Commissioner's Office and

other third parties such as banks or the media.

4. **Evaluation and response**
   Finally, you should investigate what caused the breach and evaluate your response to it. Take on board what you find and update your security, policies and procedures where necessary.

For more information on handling a data breach, check out the ICO's guide which includes useful tips and checklists to ensure you can respond to a breach to the best of your abilities.

Or, head back to chapter 3 to find out what to do if you've been a victim of cyber crime.

General Data Protection Regulation (GDPR)

Although the General Data Protection Regulation (GDPR) came into force in all EU member states, including the UK, in May 2016, it doesn't become directly applicable until 25th May 2018. This is to allow businesses time to make the necessary changes to their data protection processing to become compliant with GDPR from 25th May 2018. The UK Government has announced that the UK will still be adopting GDPR on this date. GDPR replaces the Data Protection Act 1998 and affects all UK businesses who process personal data and is especially relevant for UK businesses operating internationally. The security of data plays a big role in the new GDPR, as it includes stricter obligations which you must follow.

For cyber security, the GDPR covers three main areas, which you are required to follow:

Security of processing

- You need to implement the appropriate technical and organisational measures to ensure a level of security appropriate to the risks. These risks include accidental or unlawful destruction, loss, or alteration; the unathorised disclosure of or access to data sent, stored or processed in any other way.
- That employees who process the data have the authorisation to do so.
- If you use another business to undertake any of your work that involves the processing of personal data, it is your responsibility to ensure the sub-contractor complies fully with the security requirements of GDPR.

Notification of a personal data breach to the supervisory authority

- If there is a risk to the rights of the individuals whose personal data have been breached you must notify the Information Commisioner's Office no later than 72 hours from discovering the breach. If reported later than 72 hours, you must provide reasons for the delay.

- The following must be included in the breach notification: the nature of the personal data breach, who's been affected, the name and contact details of the data protection officer where more information can be obtained, the expected consequences of the data breach and how you will respond to the breach.

Communication of a personal data breach to those affected

- If the data breach is likely to result in a high risk to the rights of the individuals concerned then they should be notified immediately. You should clearly describe the nature of the breach to them and the action you have taken/will be taking.
- However, communication to an individual is not required if: you've implemented appropriate protective measures to the data such as encryption, which makes the data unintelligible to hackers; you've minimised any risks to the individuals so that there will no longer be a high risk to their rights; or if a large number of individuals have been affected and it would be difficult to contact them all separately – in this case, you should communicate the incident publically so that all individuals are informed.

Summary

The security requirements of the Data Protection Act and the General Data Protection Regulation might seem like a lot to take in, but take a deep breath because they're not as intense as you might expect. Remember if you keep personal data secure and fully protected and follow the tips in our eBook then you are following the security requirements of the Data Protection Act and General Data Protection Regulation.

Further resources

Information Commissioner's Office (ICO)

The ICO offer a range of support, including details on General Data Protection Regulation and the Data Protection Act, security tips to prevent cybercrime and what to do if you have a security breach.

Government Legislation

For more information on Principle 7 of the Data Protection Act, take a look at the government's legislation for it.

Chapter 6: What is the Government's involvement

The National Cyber Security Strategy 2016-2021 is the UK government's plan to ensure that Britain is secure and resilient online. The strategy explains the government's approach to managing cyber threats in the UK and how they aim to make Britain the most secure place in the world to do business online. There are going to be investments of £1.9 billion into defending online systems and infrastructure and deterring potential cyber criminals.

It has 3 objectives:

- To defend – to ensure UK networks, data and systems in the public, private, and commercial spheres are protected against a cyber attack.
- To deter – by making sure that the UK's cyber security is neither time nor cost effective to break into should act as a deterrent to cyber criminals.
- To develop – the UK will invest in the education and training to ensure that there are talented and qualified cyber security professionals continuously working to strengthen cyber security.

The National Cyber Security Centre (NCSC)

The National Cyber Security Strategy operates through The National Cyber Security Centre. They work with the government, the police and academia to make sure that they are constantly strengthening cyber security. There is lots of really useful information on the website that you can access to make staying safe online much easier.

They produce great articles that you can read through with focus on specific cyber security problems and solutions. You can access their advice here.

Some of their most popular articles are:

- 10 steps to cyber security
- Password guidance: simplifying your approach
- I'm gonna stop you little phishie

The Centre for the Protection of National Infrastructure (CPNI)

The Centre for the Protection of National Infrastructure work closely with The National Cyber Security Centre to help protect the UK's online presence. They have great resources that you can access for free to increase the cyber security.

Security awareness campaigns

The centre runs security awareness campaigns that you can access for free to help you and your staff work together to keep your business safe online.

Employee vigilance campaign

This campaign will explain what makes good and bad employee security behaviour and show you how you can help your employees be more secure with their work.

My digital footprint campaign

The digital footprint campaign shows you what gets left behind whenever you go online. There are great resources that you can access, helping you to track your digital footprint, how to be more two-faced online, and much more

Workplace behaviours campaign

The things your staff do when in the workplace have a big impact on the security of your business, both in the real world and the online one. The toolkit provided here helps you work with your employees to increase safety.

You can also access advice for personnel and people security, physical security, as well as cyber security on their website.

Summary

The National Cyber Security Strategy 2016-2021 has been set up and is implementing change to the way the UK currently protects itself against cyber threats. It is investing lots of money into the innovation and implementation of new protective measures to ensure that the UK is one of the safest places to conduct business.

Further resources

Read the full PDF which details exactly what the National Cyber Security Strategy aims to do and how they intend to do it.

Visit the Centre for the Protection and National Infrastructure's website for useful tips and resources that you can use to keep your business safe.

Next steps

We hope you've found this guide really useful and that it has given you some practical ideas of how to keep yourself and your business safe online. Before we go, we'd like to point you towards other places that you can head to find out a bit more.

The Centre for the Protection of National Infrastructure (CPNI)

The CPNI have great resources and advice that you can access from their website for free.

The National Cyber Security Centre

The centre have lots of guidance that you can look at as well as alerts for the current cyber security threats that you might need to be aware of.

Action Fraud

Head to Action Fraud if you know that you have been the victim of a cyber crime. You can also sign up to Fraud Alert for free to be notified of threats in your area.

How's Business

There are loads of great articles, networking events, eBooks, and expert advice that you can access on the How's Business website.