CYBER SECURITY FOR SMALL BUSINESSES

WHAT YOU CAN DO TO KEEP YOUR BUSINESS SAFE SECURE AND RESILIENT

Scottish Business Resilience Centre

Creating a secure Scotland for business to flourish in

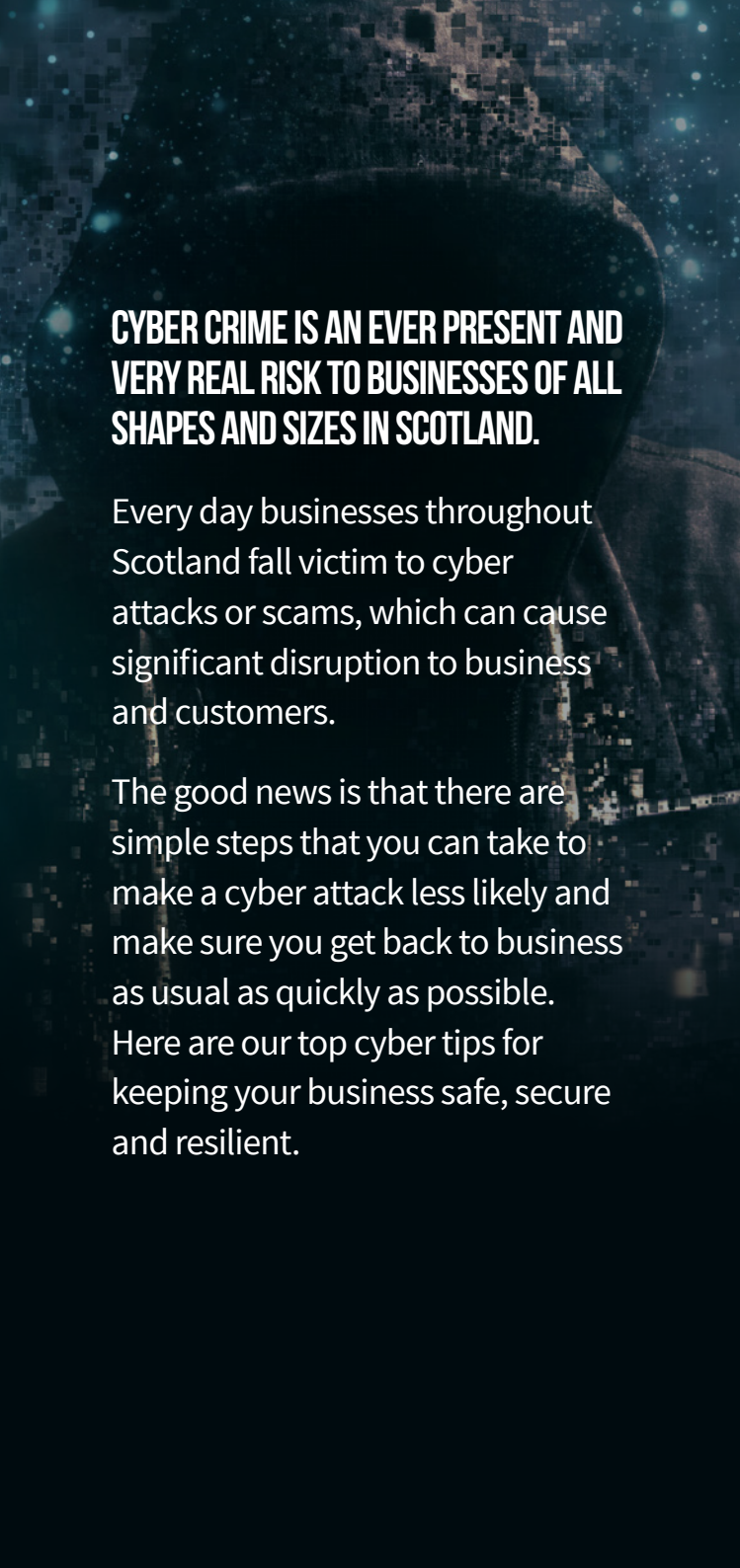
POLICE SCOTLAND

Keeping people safe

Scottish Government

Riaghaltas na h-Alba

gov.scot



CYBER CRIME IS AN EVER PRESENT AND VERY REAL RISK TO BUSINESSES OF ALL SHAPES AND SIZES IN SCOTLAND.

Every day businesses throughout Scotland fall victim to cyber attacks or scams, which can cause significant disruption to business and customers.

The good news is that there are simple steps that you can take to make a cyber attack less likely and make sure you get back to business as usual as quickly as possible. Here are our top cyber tips for keeping your business safe, secure and resilient.

SECURITY

THE MOST COMPLEX ANTIVIRUS SOFTWARE WILL NOT PROTECT YOUR COMPUTERS IF YOU DON'T DO THE BASICS.

You need to make sure that your office is secure with good locks, alarms, CCTV, controlled door entry, visitors policy etc. If you have an open office and use laptops, you might want to think about using tethers. Without these basic controls, someone could just walk out the door with you computer.

UPDATE AND PATCH

IT MAY SOUND SIMPLE BUT THE EASIEST WAY TO STAY AHEAD OF CYBER CRIMINALS IS TO MAKE SURE THAT YOUR OPERATING ANTIVIRUS AND SOFTWARE SYSTEMS (MOBILE PHONE AND COMPUTER) ARE ALL UP TO DATE.

When companies put updates out, it is normally because hackers have compromised an aspect of security and the update will fix this. If you do not update right away, then your system is at risk as the hackers know the way around the existing software security features. Cyber criminals often look for a quick hit and if you are up to date, chances are they will move on to someone else.

You need to understand how to update your systems and when to do it. You can normally find this information online. If you have an IT company you need to ask them when they update your systems and how often. Don't assume they do it right away as they may not and this could leave you vulnerable.

PASSWORDS

WHETHER IT'S THE PASSWORDS FOR YOUR COMPUTERS, ONLINE ACCOUNTS, SERVERS, CCTV AND MOBILE PHONE ACCOUNTS, YOU NEED TO MAKE SURE THAT YOU:

- Never share or re-use passwords.
- Never use passwords that can be guessed such as relatives or pets names, football teams, schools or bands.
- Use a passphrase of 12-15 characters, if possible. Lines from songs or poems are good, as long as you don't hum or say them out loud when entering them and don't make them too obvious. If everyone knows your favourite song, use another one.
- Use a password manager or vault but make sure you have a strong secure password protecting it from attack.
- Use the Scottish Business Resilience Centre's password strength checker to make sure your passwords are secure.

DATA BACKUP

IT IS VITAL THAT YOU MAKE SURE THAT YOU HAVE A BACKUP OF ALL OF YOUR BUSINESS INFORMATION. THAT WAY IF YOU ARE ATTACKED, YOU CAN RESTORE THE DATA THAT IS STOLEN OR ENCRYPTED.

However, you need to make sure that you back up regularly and that the attack would not get to your backup as well. If an attack hits your system and simply travels on to your backup then the backup will be lost. You need to make sure that your backup is safe or archived and can be retrieved. If you use a cloud or data centre backup, ask these questions and don't assume anything.

Finally, you need to regularly test your backup or have your IT provider do it for you. If the worst does happen, you need to be confident that your data can be restored quickly and easily.

MALWARE

MALWARE IS THE TERM THAT APPLIES TO ANY MALICIOUS SOFTWARE THAT IS DESIGNED TO ATTACK YOUR COMPUTER, PHONE OR NETWORK. THERE ARE ALL SORTS OF EXAMPLES FROM RANSOMWARE (WHICH ENCRYPTS YOUR INFORMATION), TO VIRUSES SUCH AS TROJANS, WHICH WILL HARVEST INFORMATION FROM YOUR COMPUTER.

One way hackers use to target companies is by sending e-mails which appear to come from legitimate companies and which include links which they try to persuade you to click on. Sometimes they will be addressed to you personally and claim to be from someone you know. These links, if clicked on, will then download malware to you computer, which will probably spread through your system. These are known as phishing or spear phishing e-mails.

Often the e-mails will contain poor grammar and incomplete sentences. They can be over familiar in tone and contain incomplete information about you. Often they will address you generically as customer or client.

These e-mails are socially engineered to pressurise you into panicking and taking a course of action you would not normally take. Often they will tell you something is wrong (e.g. you account has been compromised or needs updated), you need to take action immediately (e.g. click on the corrupted link to update your details) and that something bad will happen if you don't do this (your account will be closed or more money will be stolen from it).

If any of these things are present you need to stop and think who this e-mail is from and what you are being asked to do?

If you have any suspicions at all, remember the 5 Rs:

- **Roll Over** - Gently roll the mouse cursor over the e-mail address or click on it to expand it out and confirm who it is from. The address may have been designed to display as being from someone you trust or have done business with.
- **Reconcile** – If the information in the body of the e-mail says it's from a particular company then makes sure this tallies with the expanded e-mail address.
- **Review** – Review the contents of the e-mail. Are you expecting it, would it normally come to you at work, do you normally do business in this way?
- **Research** - Research the e-mail online. If it is malicious, you will sometimes find information about it, which can help you make up your mind what do. You can also check with the company or person concerned to see if the e-mail is genuine or not.
- **Reject** - If you have any doubts at all delete the e-mail. Do not take a chance with your cyber security.

PREPARE AND COMMUNICATE

THE STEPS DETAILED ABOVE WILL MAKE A CYBER ATTACK LESS LIKELY AND SHOULD MEAN THAT YOU RECOVER FROM ANY ATTACK FASTER AND WITH LESS DISRUPTION. YOU SHOULD THINK ABOUT HOW YOU WOULD RESPOND TO A CYBER ATTACK AND HAVE SOME SORT OF PLAN TO FALL BACK ON IF IT DOES HAPPEN.

This should include contacting the police immediately if you have been the subject of a successful cyber attack. Ideally this plan should be included in your wider business continuity planning process, which you should test from time to time.

You also need to make sure that all of your staff understand what the current cyber threats look like and what they should look out for. Remember that the person that gets the phishing e-mail might not be the manager or the security officer. They could be from the sales or admin team. If they know what to look out for and how to respond, they will be in a better position to protect you and prevent an attack from happening. Good, regular communication with all of your staff is a vital part of your cyber security.

RESOURCES

The Scottish Business Resilience Centre provides a comprehensive range of integrated cyber security services that help you assess, build and manage your cyber security capabilities, and respond to incidents and crises.

The Cyber Security Information Sharing Partnership (CiSP) offers organisations in the UK a safe portal in which to discuss and share intelligence that can assist the community and raise the UK's cyber resilience. Members are encouraged to share technical information and indicators of compromise so that the effects of new malware, and particularly ransomware, can be largely reduced. For more information contact Graham Bye, Scottish CiSP Coordinator.

The National Crime Agency (NCA) encourages anyone who thinks they may have been subject to online fraud to contact Action Fraud at www.actionfraud.police.uk. The NCA encourages industry and the public not to pay the ransom.

The National Cyber Security Centre (NCSC) runs a commercial scheme called Cyber Incident Response, where certified companies provide crisis support to affected organisations.