



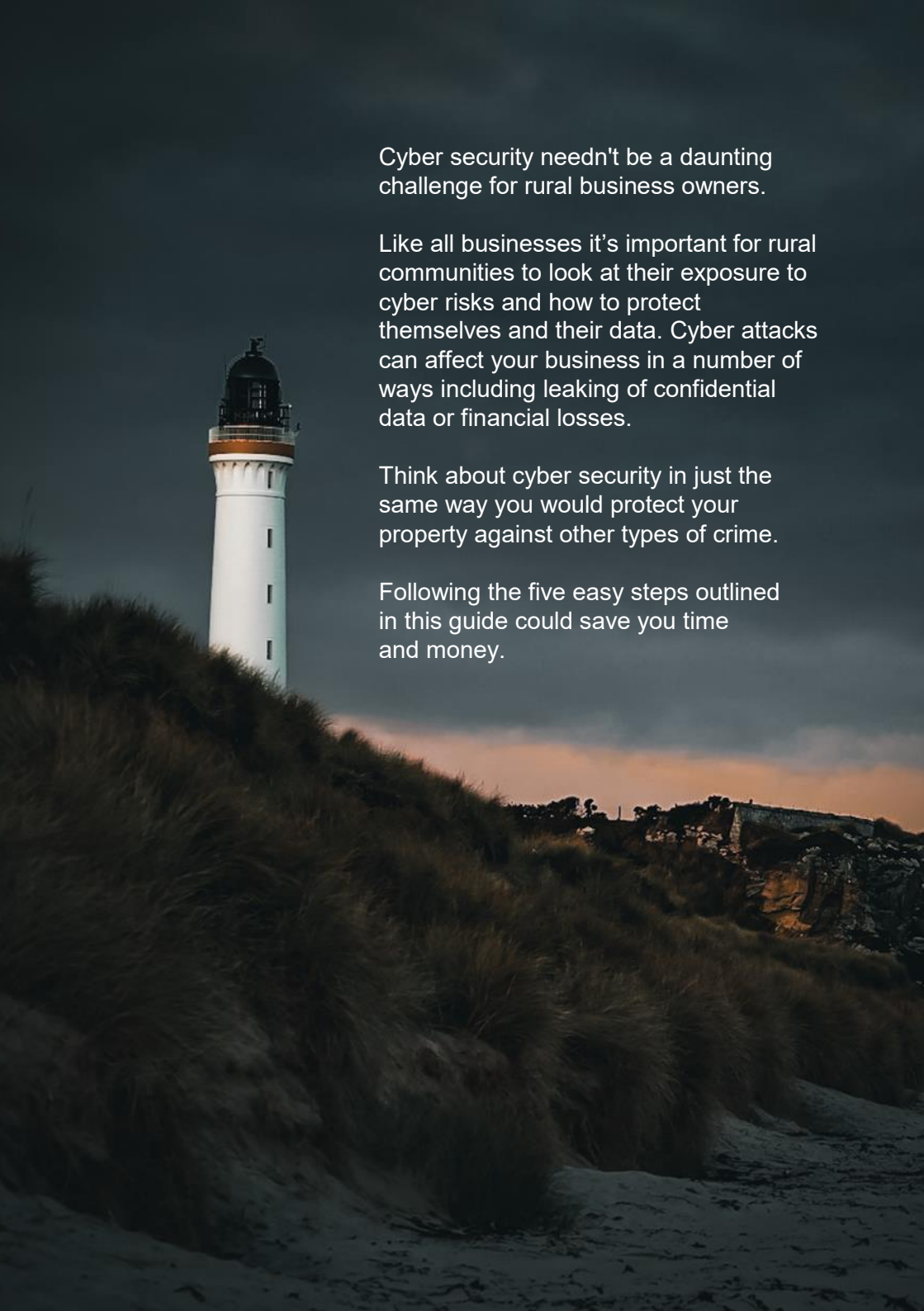
**POLICE
SCOTLAND**

Keeping people safe

POILEAS ALBA

Cyber Security for Rural Businesses





Cyber security needn't be a daunting challenge for rural business owners.

Like all businesses it's important for rural communities to look at their exposure to cyber risks and how to protect themselves and their data. Cyber attacks can affect your business in a number of ways including leaking of confidential data or financial losses.

Think about cyber security in just the same way you would protect your property against other types of crime.

Following the five easy steps outlined in this guide could save you time and money.

In this guide

- 1** **Back up your data**
4 things to consider when backing up your data.
- 2** **Protect your organisation from malware**
Free and easy to implement tips that can help prevent malware damaging your organisation.
- 3** **Keep your smartphones and tablets safe**
Quick tips that can help keep your mobile devices - and the information stored on them - safe.
- 4** **Use passwords to protect your data**
5 things to keep in mind when using passwords.
- 5** **Avoid phishing attacks**
Steps to help you identify the most common phishing attacks.

1

Back up your data

Think about how much you rely on your data such as customer details, quotes, orders and payment details. Now imagine how long you would be able to operate without them. Rural businesses should take regular backups of their important data and make sure that these backups are recent and can be restored. By doing this you're ensuring your business can still function following the impact of flood, fire, physical damage or theft.





Identify the data you really need

Identify your essential data - the information that your business couldn't function without. Normally this will be documents, photos, emails, contacts and calendars, most of which are kept in just a few common folders on your computer, phone, tablet or network.

Keep your backup separate from your computer

Whether it's on a USB stick, on a separate drive or a separate computer, access to data backups should be restricted so that they:

- are not accessible by staff
- are not permanently connected (either physically or over a local network) to the device holding the original copy.

Ransomware (and other malware) can often move to attached storage automatically, which means any such backup could also be infected. For more resilience you should consider storing your backups in a different location so fire or theft won't result in you losing both copies. Cloud storage solutions are a cost-effective and efficient way of achieving this.

Consider the cloud

You've probably already used cloud storage during your everyday work and personal life without even knowing. Using cloud storage (where a service provider stores your data on their infrastructure) means your data is physically separate from your location. Most providers offer a limited amount of storage space for free and larger storage capacity for minimal costs to small businesses.

Make backing up part of your everyday business

The majority of network or cloud storage solutions now allow you to make backups automatically. Using automated backups saves time and ensures you have the latest version of your files should you need them. When choosing a solution you'll have to consider how much data you need to back up and how quickly you need to be able to access the data following an incident.



2

Protect your business from malware

Malicious software - also known as malware - is software or web content that can harm your organisation. The most well-known form of malware is viruses which are self-copying programs that infect legitimate software.



Install antivirus software

Antivirus software - which is often included for free within popular operating systems - should be used on all computers and laptops.

Prevent staff from downloading dodgy apps

You should only download apps for mobile phones and tablets from manufacturer-approved stores like Google Play or Apple App Store. These apps are checked to provide a certain level of protection from malware that might cause harm.

Keep all your IT equipment up to date

For all your IT equipment make sure that the software and firmware is always kept up to date with the latest versions from software developers. Applying these updates is one of the most important things you can do to improve security. At some point, these updates will no longer be available (as the product reaches the end of its supported life) and you should consider replacing it with a modern alternative.

Control how USB drives and memory cards can be used

We all know how tempting it is to use USB drives or memory cards to transfer files between organisations and people. However it only takes a single user to inadvertently plug in an infected stick to devastate your company. You can reduce the likelihood of infection by:

- blocking access to physical ports for most users
- using antivirus tools
- only allowing approved drives and cards to be used within your organisation - and nowhere else

You can also ask staff to transfer files using alternative means such as by email or cloud storage rather than via USB.

Switch on your Firewall

Firewalls create a 'buffer zone' between your own network and external networks such as the Internet. Most popular operating systems now include a firewall so it may simply be a case of switching this on.



3

Keeping your smartphone and tablets safe

More of our data is now being stored on tablets and smartphones. These devices are as powerful as traditional computers and because they often leave the safety of the office they need even more protection than 'desktop' equipment.

Switch on password protection

A suitably complex PIN or password will prevent the average criminal from accessing your phone. Many devices now include fingerprint recognition to lock your device, without the need for a password. Always check they are switched on.

Make sure lost or stolen devices can be tracked, locked or wiped

Staff are more likely to have their tablets or phones stolen or lost when they are away from the office or home. Fortunately, the majority of devices include free web-based tools that are invaluable should you lose your device. You can use them to:

- track the location of a device
- remotely lock access to the device (to prevent anyone else using it)
- remotely erase the data stored on the device
- retrieve a backup of data stored on the device

Keep your device up to date

No matter what phones or tablets your organisation is using it is important that they are kept up to date at all times. Manufacturers release regular updates that contain critical security updates to keep the device protected. This process is quick, easy, and free; devices should be set to automatically update, where possible.

Keep your apps up to date

All the applications that you have installed should be updated regularly from the software developers. These updates will not only add new features, but they will also patch any security holes that have been discovered.

Don't connect to unknown Wi-Fi hotspots

When you use public Wi-Fi hotspots (for example in hotels or coffee shops) there is no way to easily find out who controls the hotspot, or to prove that it belongs to who you think it does. If you connect to these hotspots, somebody else could access:

- what you're working on whilst connected
- your private login details that many apps and web services maintain whilst you're logged on

The simplest precaution is not to connect to the Internet using unknown hotspots and instead use your mobile 3G or 4G which will have built-in security. You can also use Virtual Private Networks (VPNs), a technique that encrypts your data before it is sent across the Internet. Only use VPNs provided by reputable service providers.

4

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised users accessing your devices.





Make sure you switch on password protection

Set a screenlock password, PIN, or other authentication method (such as fingerprint or face unlock). If you're mostly using fingerprint or face unlock you'll be entering a password less often so consider setting up a long password that's difficult to guess.

Use 2 step verification for important accounts

If you're given the option to use 2-step verification (also known as 2SV) for any of your accounts you should do; it adds a large amount of security for not much extra effort. 2SV requires two different methods to 'prove' your identity before you can use a service, generally a password plus one other method.

Avoid using predictable passwords

Passwords should be easy to remember but hard for somebody else to guess. A good rule is 'make sure that somebody who knows you well couldn't guess your password in 20 attempts.' Remember that your IT systems should **not** require staff to share accounts or passwords to get their job done. Make sure that every user has personal access to the right systems, and that the level of access given is always the lowest needed to do their job, whilst minimising unnecessary exposure to systems they don't need access to.

Change all default passwords

One of the most common mistakes is not changing the manufacturers' default passwords that smartphones, laptops and other types of equipment are issued with. Change all default passwords before devices are distributed to staff. You should also regularly check devices, and software, specifically to detect unchanged default passwords.

RURAL MATTERS

PoliceScotland

5

Avoid phishing attacks

Scammers will send fake emails to thousands of people asking for sensitive information such as bank details or containing links to bad websites. They might try to trick you into sending money or steal your details to sell on.

Check for the obvious signs of phishing

Expecting your staff to identify and delete all phishing emails is an impossible request. However, many phishing emails still fit the mould of a traditional attack, so look for the following warning signs:

- Many phishing scams originate overseas and often the spelling, grammar and punctuation are poor. Others will try and create official-looking emails by including logos and graphics. Is the design (and quality) what you'd expect from a large organisation?
- Is it addressed to you by name or does it refer to 'valued customer' or 'friend' or 'colleague?' This can be a sign that the sender does not actually know you and that it is part of a phishing scam.
- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately.'

Look out for emails that appear to come from a high-ranking person within your organisation requesting a payment is made to a particular bank account. Look at the sender's name. Does it sound legitimate or is it trying to mimic someone you know?

If it sounds too good to be true it probably is. It's most unlikely that someone will want to give you money or give you access to some secret part of the Internet.

Email filtering services attempt to send phishing emails to spam/junk folders. However the rules determining this filtering need to be fine-tuned for your organisation's needs. If these rules are too open and suspicious emails are not sent to spam/junk folders, then users will have to manage a large number of emails, adding to their workload and leaving open the possibility of a click. However, if your rules are too strict, some legitimate emails could get lost. You may have to change the rules over time to ensure the best compromise.

If you believe that your organisation has been the victim of online fraud, scams or extortion you should report this to Police Scotland on 101.

We have put together a glossary of cyber security terms that we think everyone should know.

Antivirus Software

A type of software that can identify and detect different types of malicious code in order to prevent malware incidents.

Cloud

Technology that allows users to access files through the internet anywhere in the world.

Domain

A group of computers, devices or printers that are interconnected and governed as a whole. Domains are often found in workspace environments.

Firewall

Defensive technology that is either hardware or software-based and used to prevent hackers from entering your network.

Malware

Malware is specifically designed to harm a computer, a system or data.

Phishing

Phishing is an attempt to entice a person into providing sensitive or confidential information. In a phishing scam, cybercriminals distribute electronic content specifically designed to trick the user into engaging in a specific activity, such as clicking a link or responding to the email. The victims, thinking the content is real, provide the phisher with personally sensitive information such as usernames, passwords, banking, financial and/or credit card details.

Ransomware

A form of malware, ransomware limits or blocks users from accessing individual files or entire systems until a ransom is paid.

Spyware

Spyware is malicious software that spies on the computer user, capturing keystrokes, emails, documents or even turning on the video camera.

Virus

A form of malicious software that infects a system or computer and damages or alters the data on the system.

Virtual Private Network (VPN)

A tool that allows users to secure their network traffic and remain anonymous while surfing the internet by masking the location of your device.

Keeping Our Rural Communities Safe

North East Division Crime Reduction Team

Moray (Elgin)

PC Richard Russell

richard.russell@scotland.police.uk

Aberdeenshire (Stonehaven)

PC Mike Urquhart

michael.urquhart@scotland.police.uk

Aberdeen City (Nigg)

PC Mark Irvine

mark.irvine@scotland.police.uk

Wildlife Crime Officer (Elgin)

PC Hannah Corbett

hannah.corbett@scotland.police.uk