Cyber security for farmers:

Practical tips on how to stay safe

National Cyber Security Centre
a part of GCHQ

NFU

Sarah Lyons NCSC Deputy Director Economy & Society Engagement

The National Cyber Security Centre (NCSC) is delighted to partner with the National Farmers' Union (NFU) in producing this guide to help the Farming Community protect themselves from the most common cyber attacks.

If you are unfamiliar with NCSC, we are the UK Government's national technical authority for cyber security and our aim is to make the UK the safest place to live and work online. To help us achieve this, we work very closely with key companies and organisations of all sizes and sectors of business including Agriculture.

As the advantages of technology impact on all sectors, including farming and growing, we want to help you feel better prepared to understand and respond to the challenges too, today and in the future. We aim to do this by making cyber security less daunting - providing advice and guidance in a clear way and in an easy to implement style. This is particularly important now for farming and rural communities adapting to life outside the European Union and responding to the impact of the pandemic on business models.

Our aim is to get businesses to think about cyber in just the same way as you would protect your property against other types of crime. To do this, we hope that the guide provides you with enough information to start this journey or enhance your current cyber maturity.

Whilst we cannot guarantee protection for your business against all the cyber crime threats it faces, we can increase your ability to deal with them and to be aware of who can help you.

This booklet is the first of many collaborations and we look forwarding to working with the NFU and the wider agriculture sector. Only together can we protect farming in cyber security, now and in the years to come.

Stuart Roberts, Deputy President of the National Farmers' Union

As the agricultural industry embraces and champions new technology, it is increasingly important for farmers and rural communities to look at their growing exposure to cyber risks and how to best protect themselves and their data. The NFU is delighted to partner with the National Cyber Security Centre (NCSC) to produce this important guidance for farmers, landowners, and the rural community.

Cyber attacks can be devastating for businesses and the individuals who are victims to fraudulent activity. It can affect agricultural businesses in a number of ways, including leaking of confidential data or financial losses. As farms rely more on technologies such as GPS, remote sensing and unmanned vehicles, the risks increase.

Cyber criminals are becoming increasingly sophisticated and savvy; finding new ways to exploit us or find vulnerabilities in our technological security to steal passwords, money, or data.

Cyber crime is a significant threat to businesses of all shapes and sizes. I cannot stress enough how it is not just the larger organisations who need to invest in cyber security. Farmers have been targeted by cyber criminals, so it is important to be aware of the risks and invest in our own cyber security.

The NFU is committed to ensuring farmers are aware of this potential threat and understand the benefits of investing in security measures to start to protect themselves against cybercrime.

I hope this booklet will provide farmers and growers across the country, as well as those in rural communities, with the practical, step-by-step guidance they need to easily implement the appropriate security and build greater resilience to cyber criminals.

Why cyber security matters in Farming

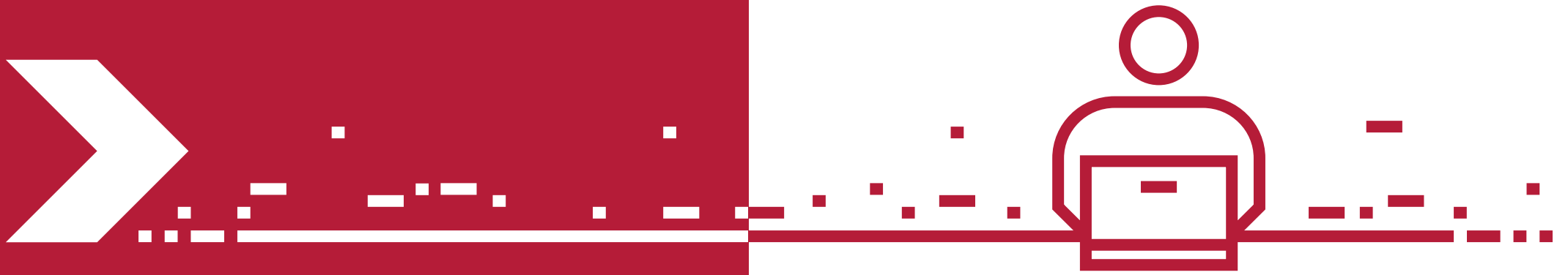
We all keep information about ourselves and our businesses electronically. This is particularly true for the agricultural sector, which makes use of many 'smart', internet connected systems as well as the usual email and accounting packages.

These internet-connected technologies have become central to the way we live and do business today. As a direct result, they have become an attractive target for cyber criminals. This is why it's so important to secure all the digital aspects of your business.

So, what are the digital aspects of your business? Firstly, your IT and other computerised equipment. This means everything from the computer where you do your emails and run your farm management software, to the automated machinery, security cameras and smart phones which help you run your farm.

The second aspect to keep in mind involves your online activity. You must consider all the online accounts that you use. This means banking, email and social media but also things like the Rural Payments service, HMRC online services, online shopping and cloud document storage (e.g. Office365, Google Docs, DropBox etc).

This guide has been produced by the NCSC and NFU to help you protect your devices and accounts from the unwanted attention of Cyber Criminals. By following the steps in this guide, you should be in a much more secure and resilient position.



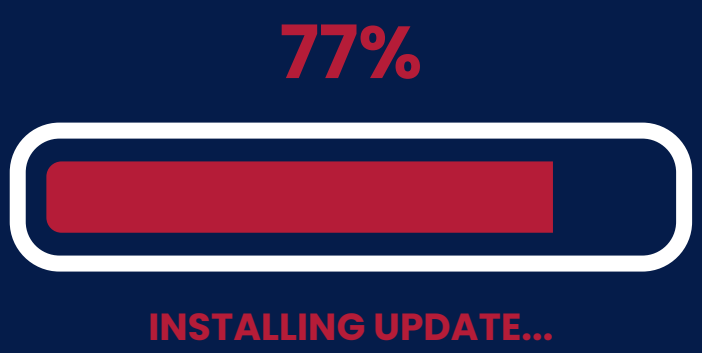
Keep your devices up to date

Like any piece of machinery, computers and mobile phones need regular maintenance and servicing to ensure they work effectively and securely.

Most of this essential maintenance can be achieved by ensuring the operating system and installed software on your devices are regularly updated.

This process is known as 'patching.'

The easiest way to make sure that your device and your apps are kept up to date is to set updates to be installed automatically. This is always true for the major operating systems: Windows, macOS, iOS and Android. However, other software may require you to manually install updates.



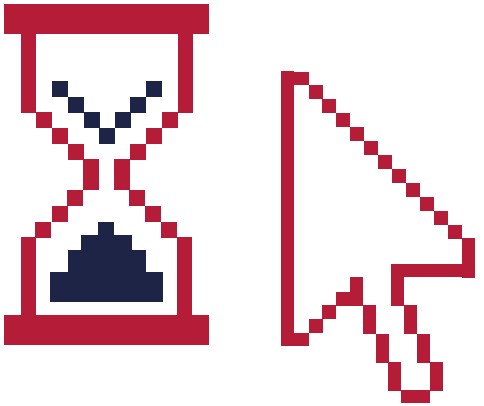
Old machines

If your computer equipment is old, it will be more vulnerable to attack from viruses and malware. It will also be more likely to develop faults that could result in the loss of data.

Eventually, your operating system (i.e. Microsoft Windows, Apple macOS and iOS, Google Chrome OS and Android) will become obsolete and no longer receive updates.

For example, a computer running Windows XP will no longer receive updates.

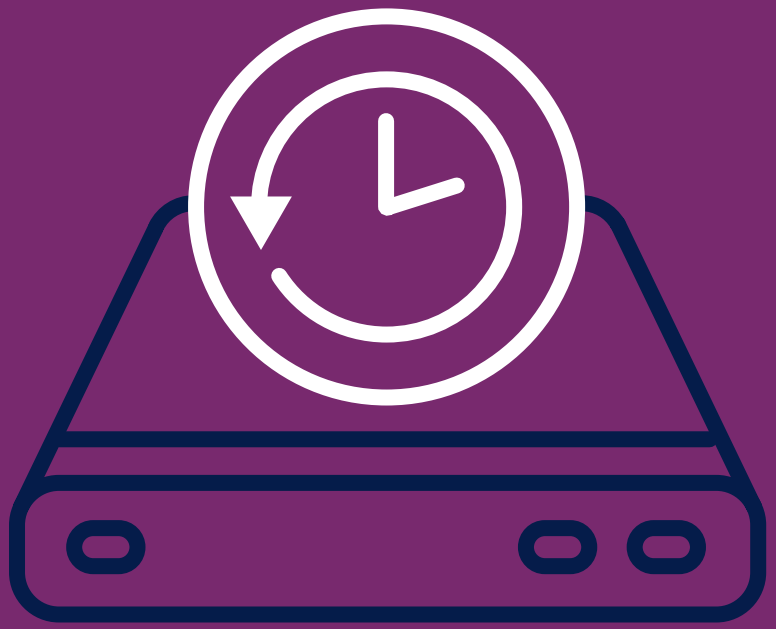
When this happens, you should look to update your operating system or replace the device in question.



Backup your data

You probably have quite a lot of data that you rely on: emails, invoices, contacts, orders, quotes.

Making regular backups of your important data and keeping these backups somewhere physically separate will save you from the worst of effects of a malware or ransomware attack.



How to back up your data

1

Identify what data you need to back up.
This is the information without which you and your farm and business couldn't function.

2

Keep a safe backup of your important files.
Regularly create a backup copy of the data that is most important to you, and perhaps add a recurring appointment to your calendar to remind you. Keep the copy separate from your computer, possibly on a USB storage device, separate hard drive, or separate computer. You could also use cloud services to back up your files, so that a fire or theft from site won't result in you losing both copies.

Keep your devices safe

Phone, laptop, PC and tablet - you probably use more than one device on a day to day basis.

You should take steps to keep all of these safe, particularly if you use the same devices for business and personal work.

Switch on password protection. Enable a screenlock password, PIN, finger print/FaceID, or other authentication method for each of your mobile devices. Protect your home and/or office computer too.

Use an encryption product. This means BitLocker for Windows, or FileVault for macOS. These are built into the operating system, all you need to do is turn them on. Encrypting your data will prevent unauthorised access to your information.

Lost and stolen devices

Most devices include free, web-based tools that you can enable to...

Track the location of the device

Lock it remotely

Erase data remotely

Retrieve a backup of data stored on the device.

Protect your farm from malware

The name 'malware' comes from the joining of two words: **mal**icious soft**ware**. This is the slightly more technical term for 'a computer virus.'

Malware is usually designed to steal or extort money from you, often by holding your data to ransom.

Malware can attack your laptop and your phone, but it can also target less obvious 'devices.' Anything which connects to the internet is at risk from malware.

For example, malware could:

- Lock your device or make it unusable
- Immobilise your farm vehicles
- Steal, delete or encrypt your data
- Interfere with any automated systems which you use
- Use services that cost you money, such as premium rate phone calls
- Divert your confidential farm data into the public domain

Protecting against malware

Keep a safe backup of your important files. Create a regular backup copy of the data that is most important to you. Keep the copy separate from your computer, and consider using cloud services to backup your files.

Update your operating system and the apps you use. Follow the prompts when your software tells you updates are available, or set your devices to do this automatically

Make sure your antivirus product is turned on, and is up to date. Antivirus software is often included for free within popular operating systems. It should be used on all computers, laptops, and on mobile phones if possible. For example, in Windows, go to Settings, enable Virus and Threat Protection, and you'll be safer immediately.

Switch on your firewall to create a buffer zone between your network and the internet. Locate the network security settings on your device and check that your Firewall is switched on.

Always use passwords

Most systems require usernames and passwords. Criminals rely on the fact that a lot of people use the same password for all of their accounts, or use simple passwords such as “password”.

Cyber criminals trade stolen username and password combinations which they try out on accounts around the internet. They also try common, easily-guessed passwords randomly against different accounts, hoping to strike lucky.

This is why you should use separate passwords for each of your devices and online accounts, especially email accounts.

Wherever possible, make the password strong. And for your most important accounts, make it unique. NCSC guidance on passwords can be found at **https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0**

Using passwords well

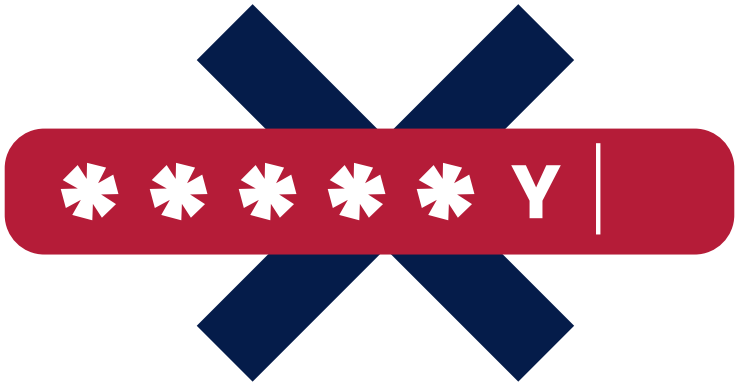
- **Change all default passwords.** For every new device you start using, including your Wi-Fi network, change the manufacturer’s default password to a new one of your own.
- **Choose strong passwords.** Combine three random words to make a short, memorable phrase.
- **Have a different password** for each online account if you can, especially your primary email account. If criminals are able to access and control your email, they may be able to reset passwords and gain control of your other accounts
- **If you write down your passwords,** store them securely, away from your device.
- **Consider using a password manager.** For example, most modern web browsers will offer to save your passwords for you.

Do not choose weak pa$$w0rds

When coming up with a password, do not use information which anyone trying to break into your account could find out about you.

Your passwords should not include:

- **Family names**
- **Your pet's name**
- **Your place of birth**



- **Your favourite holiday**
- **Something related to your favourite sports team**
- **A list of numbers (eg123456) or words like "password" or "qwerty"**

Turn on two-factor authentication, 2FA

Two-factor authentication (also known as 2FA, or Two-Step Verification) is a free security feature that provides an extra layer of protection to your online accounts.

2FA double-checks that it's really you trying to log into your account. It means that even if a criminal knows your password, they won't be able to access your accounts. So, if you are given the option to turn on 2FA, you should do it.

With 2FA in place, anyone trying to access your account must know your password **and** have access to your second proof of identity.

Often, this second source of proof involves a code being sent to your smartphone, or created by an authenticator app or device.

Check the Settings for each of your important accounts to see that 2FA is enabled. Visit Cyber Aware **(https://www.ncsc.gov.uk/cyberaware/home)** for step by step instructions on how to turn on 2FA for your email, social media and online bank accounts.

Secure your online presence

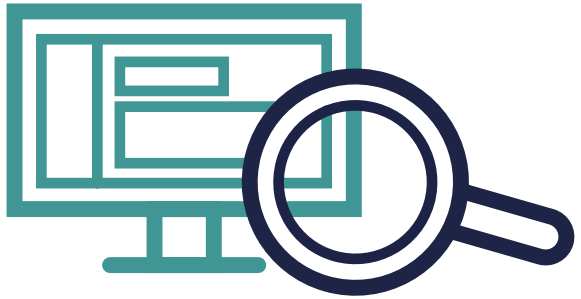
Having an online presence can have a number of advantages. It can allow businesses to share digital content, build communities, access wider audiences and communicate effectively with each other.

It is important to take steps to ensure the information being shared online by yourself or employees is not increasing the vulnerability of your business.

When using social media think about what you are posting, and who has access to it. Have you configured the privacy options so that it is only accessible to the people you want to see it? You should control who can access these accounts, making sure to use unique passwords and 2FA.

On your website or social media account, consider what your followers and friends need to know, and what detail is unnecessary (but could be useful for criminals).

Check that your website host is a legitimate company with the correct security settings, further NCSC guidance that you may find helpful can be found at **https://www.ncsc.gov.uk/guidance/moving-business-from-physical-to-digital.** Also think about the protection you might need if you have an online shop or booking system.



Dealing with scam emails, text messages and phone calls

A typical scam email or text message will try to convince you to click a link, sending you to a website which could download viruses onto your computer, or steal your passwords and personal information.

Some online scams promote bogus investment opportunities, advertise fake machinery for sale through what may appear to be a legitimate dealership organisation, or claim to be from HMRC, offering tax rebates.

Some criminals may even telephone and pretend to be from legitimate companies in a bid to trick you into giving away information, which would allow them to take money from you or access your business accounts.

How to spot suspicious messages and callers

The first things to consider when receiving a call or message is “am I expecting this?” and “Is the sender or caller who they claim to be?”. If you are unsure, check by contacting the person or business via the contact details you have in an original document or via their business website. *Do not use the numbers or addresses contained in the suspicious messages.*

Don’t forget that the Rural Payments Agency, your bank, or any other official source, will never ask you to supply personal information in an email or text.

How to spot suspicious messages and callers

Most scams rely on the same methods. Tricks to look out for are:

Authority
Is the message claiming to be from someone official?

Urgency
Are you told you must respond "immediately" or "within 24 hours"?

Emotion
Does the message make you panic, fearful, hopeful or curious?

Scarcity
Is the message offering something in short supply? Fear of missing out can make you respond quickly.

Current Events
Are you expecting to see a message like this? Criminals often exploit current news stories or specific times of year: they know the dates of the BPS payment window.

If you have received an email you are not quite sure about, forward it to NCSC's Suspicious Email Reporting Service, SERS, at **report@phishing.gov.uk**

Suspicious text messages should be forwarded to **7726** – it's free of charge.

Where to go for help

If you're looking for information on common IT security problems, such as fraudulent emails or websites, a hacked account or infection with malware, visit the NCSC website at **www.ncsc.gov.uk**.

If you receive a potential phishing message, you can report it to the NCSC using our Suspicious Email Reporting Service, SERS. Just forward the message to **report@phishing.gov.uk**. If the message is found to link to malicious content, it will be taken down or blocked, helping prevent future victims of crime.

Suspicious text messages should be forwarded to 7726. This free-of-charge short code enables your provider to investigate the origin of the text and to take action, if it is found to be malicious.

If you are unlucky enough to experience cyber crime you should report it to Action Fraud using their fraud reporting tool at **www.actionfraud.police.uk**, or by calling **0300 123 2040**.

If you live in Scotland you should report to Police Scotland by calling **101**.

National Cyber Security Centre
a part of GCHQ

NFU

All advice is based on NCSC guidance as of November 2020. For print-ready files of this document, please visit:

https://www.ncsc.gov.uk/guidance/cyber-security-for-farmers

@ncsc

National Cyber Security Centre