



## 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.

look forward 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

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 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

This guide has been produced by the NCSC and NFU to help you protect your devices and accounts from the

steps in this guide, you should be in a much more secure and resilient position.



---

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.



## 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 method for each of your mobile devices. Protect your

### Use an encryption product.

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: **malicious software**. This is the slightly more technical term for 'a computer virus.'

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:**



## Protecting against malware

---



Create a regular backup copy of the data





## 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>

## Do not choose weak pa\$\$w0rds

---

When coming up with a password, do not use information which anyone trying to break into your

## Turn on two-factor authentication, 2FA

---

Two-factor authentication (also known as 2FA, or Two-

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.



---

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,

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 will see. (On your Email and 2FA.

## Dealing with scam emails, text messages and phone calls

---

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

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

---

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.*

## 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

---

### **Urgency**

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

---

### **Emotion**

fearful, hopeful or curious?

---

### **Scarcity**

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

---

### **Current Events**

---

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](mailto:report@phishing.gov.uk)

## Where to go for help

---

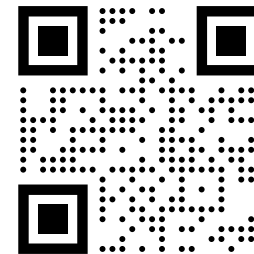
**If you're looking for information on common IT security problems**, such as fraudulent emails or websites, a hacked account or infection with malware, visit the NCSC website at [www.ncsc.gov.uk](http://www.ncsc.gov.uk).

**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](mailto: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 find out if a message is 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](http://www.actionfraud.police.uk), or by calling **0300 123 2040**.

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



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

