National Cyber Security Centre

Small Organisations Newsletter

Coffee Break Cyber

Edition 1 March 2021

Cyber Aware

Cyber Aware is the government's advice on how to stay secure online.

Cyber Aware Campaign

At the National Cyber Security (NCSC) we have a key aim: to make the UK the safest place to live and work online. We're committed to helping businesses and individuals protect themselves from cyber criminals and our Cyber Aware campaign outlines six practical, actionable steps everyone can take to avoid falling victim to the majority of online crime. These are:

1. Use a strong and separate password for your email
2. Create strong passwords using 3 random words
3. Save your passwords in your browser
4. Turn on two-factor authentication (2FA)
5. Update your devices and apps
6. Back up your data

Last Friday (26th February 2021) we released the next phase of the campaign with the launch of a free service to business owners which they can use to assess their own cyber security. It takes just five to ten minutes to complete but it could help arm people with the knowledge to better protect themselves and their business.

You can visit cyberaware.gov.uk to find out more.

Threat Reports

12th February 2021

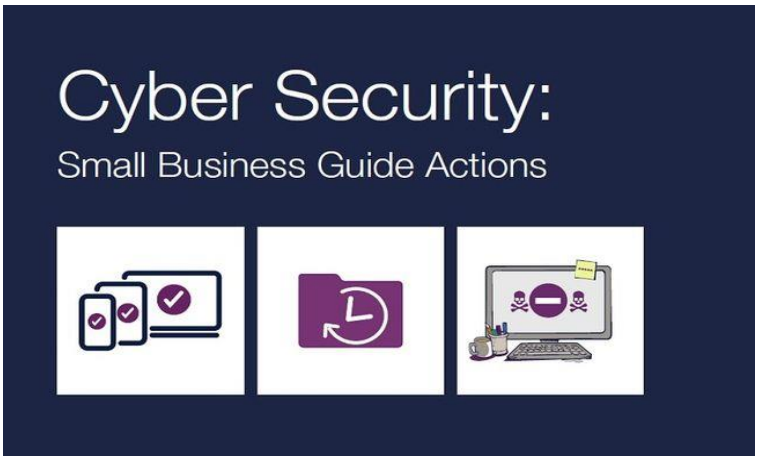
5th February 2021

NCSC News

Cyber Security for Farmers

Secure Second-Hand Devices

Post Data Breach Scams



Small Business Guide

Cyber security needn't be a daunting challenge for small business owners. Following the five quick and easy steps outlined in the guide could save time, money and even your business' reputation.

This guide can't guarantee protection from all types of cyber attack, but the steps outlined below can significantly reduce the chances of your business becoming a victim of cyber crime.

Step 1 - Backing up your data

Tip 1: Identify what data you need to back up
Tip 2: Keep your backup separate from your computer
Tip 3: Consider the cloud
Tip 4: Read our cloud security guidance
Tip 5: Make backing up part of your everyday business

Step 2 - Protecting your organisation from malware

Tip 1: Install (and turn on) antivirus software
Tip 2: Prevent staff from downloading dodgy apps
Tip 3: Keep all your IT equipment up to date (patching)
Tip 4: Control how USB drives (and memory cards) can be used
Tip 5: Switch on your firewall

Step 3 - Keeping your smartphones (and tablets) safe

Tip 1: Switch on password protection
Tip 2: Make sure lost or stolen devices can be tracked, locked or wiped
Tip 3: Keep your device up to date

Upcoming Events

Digital Loft Events 2021

Join the NCSC Economy & Society Team for a series of webinars covering essential cyber security topics. All webinars are free, sign-up. Click on the dates below to book a space.

Cyber Aware with NCSC

03.03.21 - 11am-12noon

Cyber Exercising

10.03.21 - 10.30am-11.30am

Introduction to NCSC

10.03.21 - 9am- 10am

Glossary of Terms

Phishing - Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Tip 4: Keep your apps up to date
Tip 5: Don't connect to unknown Wi-Fi Hotspots

Step 4 - Using passwords to protect your data

Tip 1: Make sure you switch on password protection
Tip 2: Use two-factor authentication for 'important' accounts
Tip 3: Avoid using predictable passwords
Tip 4: Help your staff cope with 'password overload'
Tip 5: Change all default passwords

Step 5 - Avoiding phishing attack

Tip 1: Configure accounts to reduce the impact of successful attacks
Tip 2: Think about how you operate
Tip 3: Check for the obvious signs of phishing
Tip 4: Report all attacks
Tip 5: Check your digital footprint

For more information, click here

Two-Factor Authentication (2FA) -The use of two different components to verify a user's claimed identity.

Ransomware Explained

A type of malware that makes data or systems unusable until the victim makes a payment.

Protecting your data & devices

- **Keep** your operating system and software (apps) up to date.

- **Make** sure your antivirus product is turned on and up to date.

- **Avoid** downloading dodgy apps only use official app stores (Google Play, Apple App Store) .

Next month...How to defend your organisation against ransomware

Error! Reference source not found.