Cyber Crime

Cyber Crime resources for businesses.

Cyber Crime in the UK

According to the telephone operated Crime Survey for England and Wales, there were 1.7 million Computer Misuse Act offences (hacking, malware, etc).

In the same time period, there were as many as 4.5 million fraud offences. 80% of all fraud in the UK is considered cyber enabled.

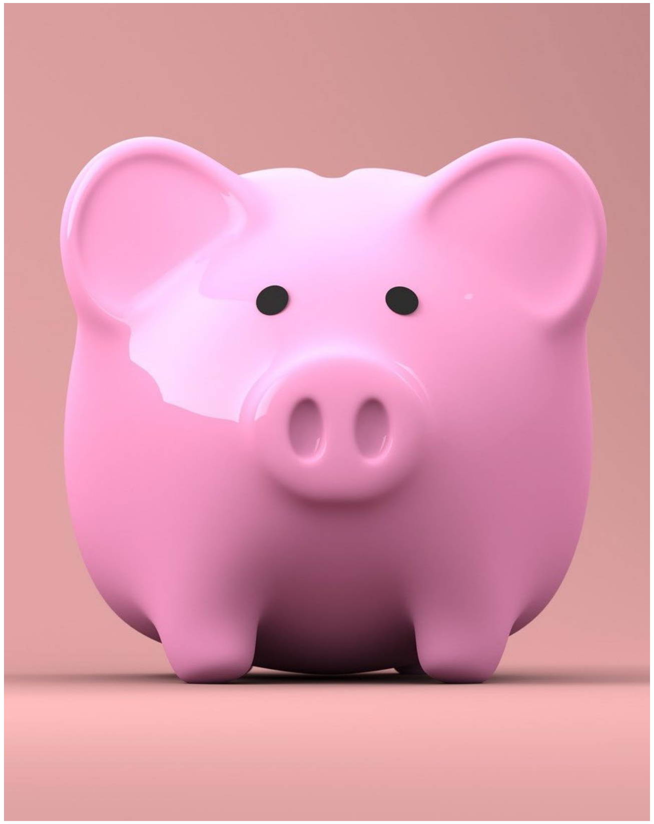
This means, according to the survey, there were roughly 5.3 million cyber crimes in the UK in one year.

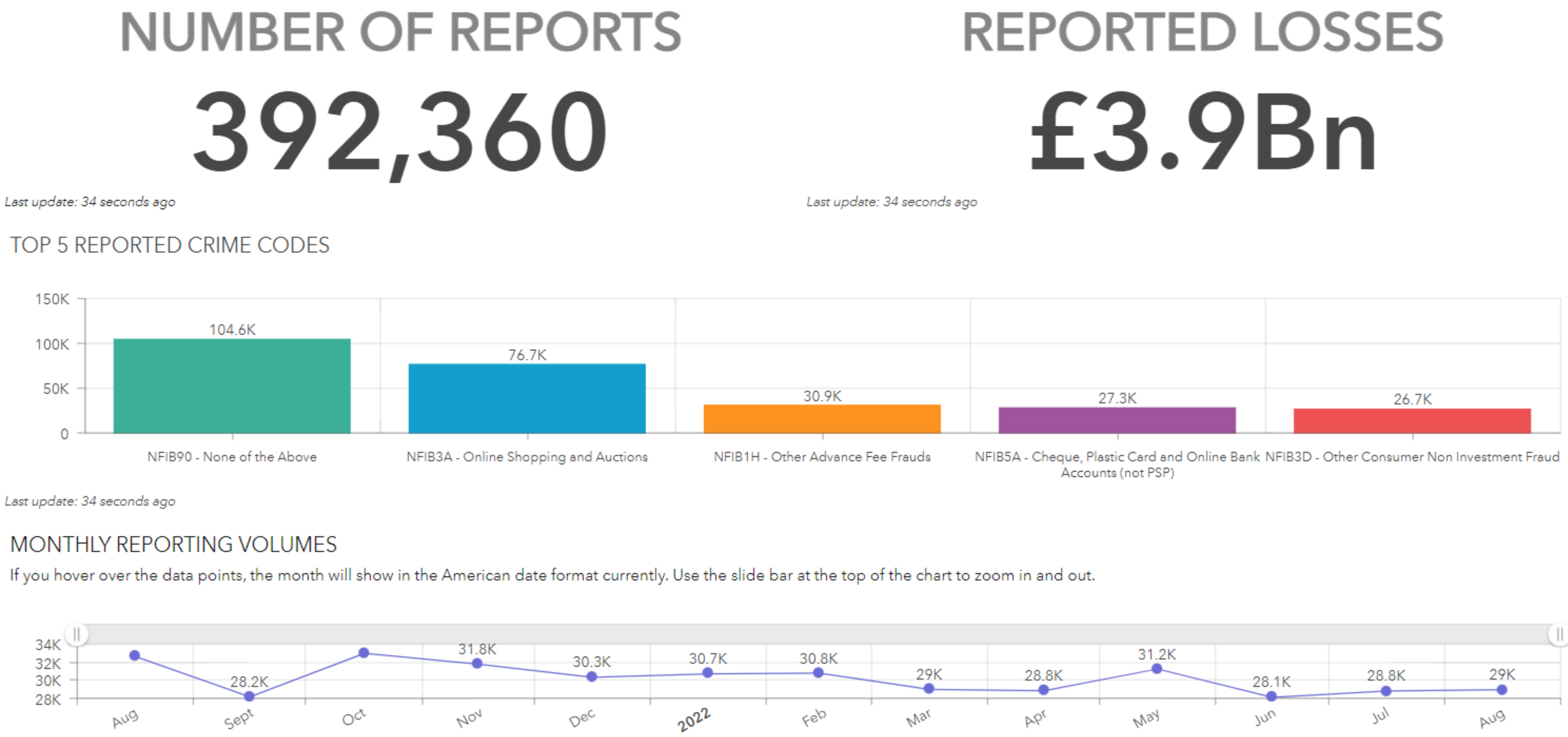
Financial impact

According to the data from Action Fraud, cyber crime cost the UK economy as much as £3.9bn in the last year

In Dorset, there were 5,276 reports and a total of £20.7m lost.

Cyber crime often goes unreported, with 1 out of 10 people actually making a report to Action Fraud. As such, it's likely that the losses are actually much higher.





NUMBER OF REPORTS

392,360

Last update: 34 seconds ago

REPORTED LOSSES

£3.9Bn

Last update: 34 seconds ago

TOP 5 REPORTED CRIME CODES

150K
100K
50K
0
104.6K
76.7K
30.9K
27.3K
26.7K
NFIB90 - None of the Above
NFIB3A - Online Shopping and Auctions
NFIB1H - Other Advance Fee Frauds
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)
NFIB3D - Other Consumer Non Investment Fraud

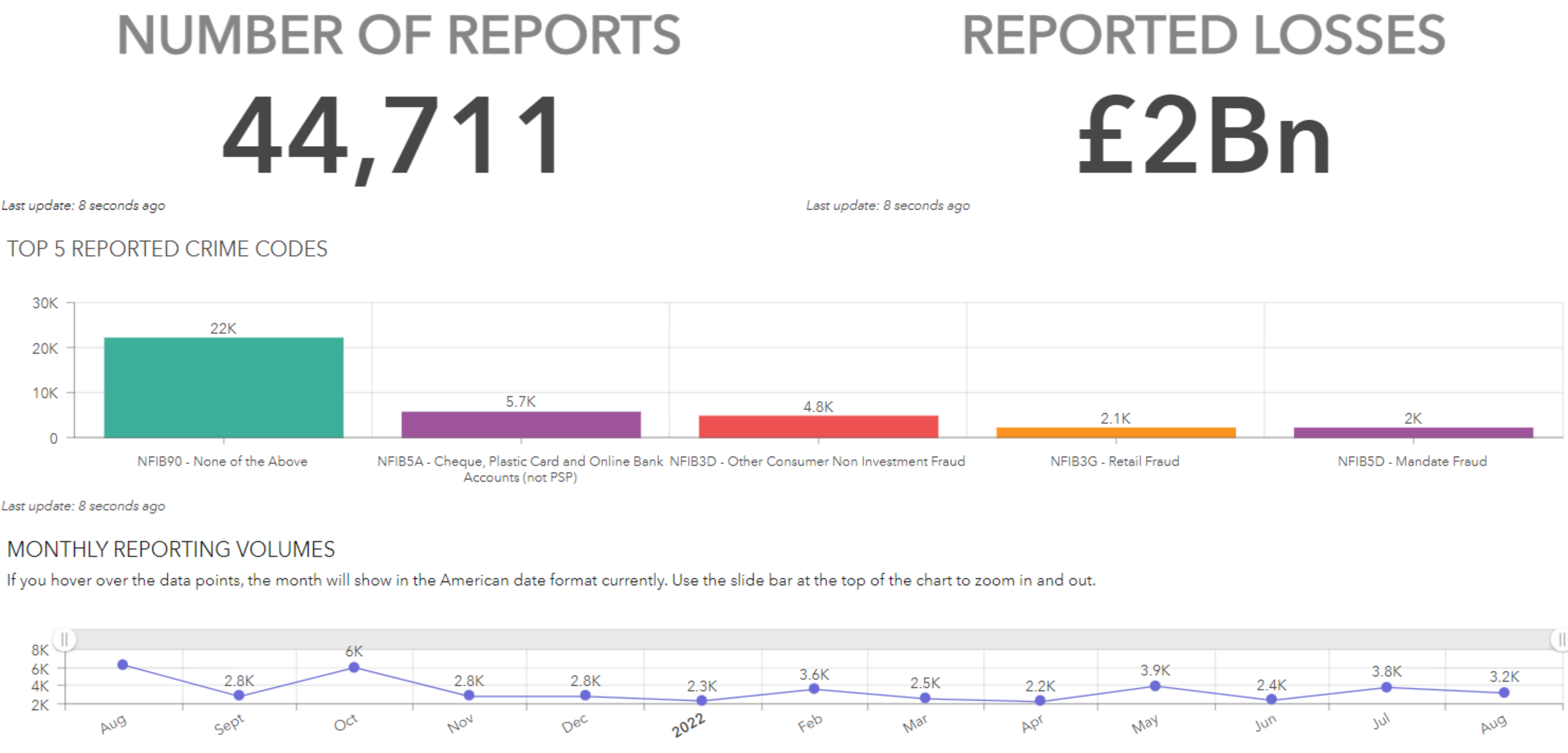
Last update: 34 seconds ago

MONTHLY REPORTING VOLUMES

If you hover over the data points, the month will show in the American date format currently. Use the slide bar at the top of the chart to zoom in and out.

34K
32K
30K
28K
28.2K
31.8K
30.3K
30.7K
30.8K
29K
28.8K
31.2K
28.1K
28.8K
29K
Aug
Sept
Oct
Nov
Dec
2022
Feb
Mar
Apr
May
Jun
Jul
Aug

Dorset Police



NUMBER OF REPORTS

44,711

Last update: 8 seconds ago

REPORTED LOSSES

£2Bn

Last update: 8 seconds ago

TOP 5 REPORTED CRIME CODES

30K
20K
10K
0
22K
5.7K
4.8K
2.1K
2K
NFIB90 - None of the Above
NFIB5A - Cheque, Plastic Card and Online Bank Accounts (not PSP)
NFIB3D - Other Consumer Non Investment Fraud
NFIB3G - Retail Fraud
NFIB5D - Mandate Fraud

Last update: 8 seconds ago

MONTHLY REPORTING VOLUMES

If you hover over the data points, the month will show in the American date format currently. Use the slide bar at the top of the chart to zoom in and out.

DCMS Cyber Security Breaches Survey 2021

1,419 businesses took part in the 2021 survey. Almost 40% of those identified a cyber attack or breach in the last 12 months. The average cost of these attacks was £8,460.

83% of businesses identified phishing attacks, 27% were impersonated in order to scam other businesses, and 13% suffered malware attacks (including ransomware).

82% of those who fell victim to ransomware paid their attacker in order to recover their data.

Mandate fraud

One of the most common cyber crimes affecting businesses.

It relies on a criminal successfully compromising a suppliers emails. From there, they amend invoices with new payment details before sending them out to unsuspecting customers.

In the last 12 months, across the UK, businesses lost as more than £153,000,000 to mandate fraud. However, the impact isn't just financial. The reputational damage caused by a compromise can have a much longer lasting effect.

If you're on the receiving end of an email asking you to change payment details, the best thing to do is to verify that contact. But what can you do to stop yourself being compromised as the supplier?

DCMS Cyber Security Breaches Survey 2021

Account compromises usually start with a phishing email, stealing credentials from an authorised user.

So, on this basis, you might assume that the end user is the weak point in an organisations cyber security.

The reality is that phishing emails are often very convincing, and if you’ve not been shown how to tell them apart, there’s a good chance you might be caught out.

End users are not an organisations weak point. Untrained end users are. Despite this, a mere 14% of the businesses surveyed say they train their staff on cyber security.

Staying safe

It’s easy to feel overwhelmed when it comes to cyber safety. The reality is that the vast majority of common cyber crimes can be thwarted with some relatively simple protective measures.

That’s why the National Cyber Security Centre (NCSC) created their Cyber Aware campaign.

The campaign focuses on six top tips to improve your cyber security, and protect you from the most commonly reported forms of cyber crime.

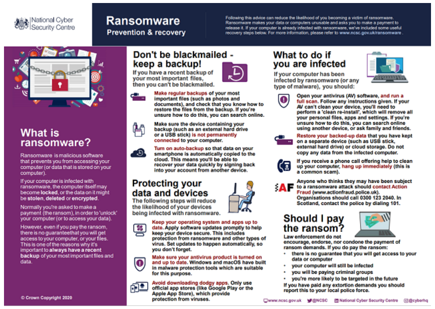
Cyber Aware

NCSC Cyber Aware

The six tips 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 step verification (2SV)
5. Update your devices
6. Back up your data

NCSC Resources



National Cyber Security Centre

Ransomware
Prevention & recovery

Following this advice can reduce the likelihood of you becoming a victim of ransomware. Ransomware makes your data or computers unusable and asks you to make a payment to release it. If your computer is already infected with ransomware, we've included some useful recovery steps below. For more information, please refer to www.ncsc.gov.uk/ransomware .

What is ransomware?

Ransomware is malicious software that prevents you from accessing your computer (or data that is stored on your computer).

If your computer is infected with ransomware, the computer itself may become **locked**, or the data on it might be **stolen**, **deleted** or **encrypted**.

Normally you're asked to make a payment (the ransom), in order to 'unlock' your computer (or to access your data).

However, even if you pay the ransom, there is no guaranteethat you will get access to your computer, or your files. This is one of the reasons why it's important to **always have a recent backup** of your most important files and data.

© Crown Copyright 2020

Don't be blackmailed - keep a backup!

If you have a recent backup of your most important files, then you can't be blackmailed.

Make regular backups of your most important files (such as photos and documents), and check that you know how to restore the files from the backup. If you're unsure how to do this, you can search online.

Make sure the device containing your backup (such as an external hard drive or a USB stick) is not permanently connected to your computer.

Turn on auto-backup so that data on your smartphone is automatically copied to the cloud. This means you'll be able to recover your data quickly by signing back into your account from another device.

Protecting your data and devices

The following steps will reduce the likelihood of your devices being infected with ransomware.

Keep your operating system and apps up to date. Apply software updates promptly to help keep your device secure. This includes protection from ransomware and other types of virus. Set updates to happen automatically, so you don't forget.

Make sure your antivirus product is turned on and up to date. Windows and macOS have built in malware protection tools which are suitable for this purpose.

Avoid downloading dodgy apps. Only use official app stores (like Google Play or the Apple App Store), which provide protection from viruses.

What to do if you are infected

If your computer has been infected by ransomware (or any type of malware), you should:

Open your antivirus (AV) software, and run a full scan. Follow any instructions given. If your AV can't clean your device, you'll need to perform a 'clean re-install', which will remove all your personal files, apps and settings. If you're unsure how to do this, you can search online using another device, or ask family and friends.

Restore your backed-up data that you have kept on a separate device (such as USB stick, external hard drive) or cloud storage. Do not copy any data from the infected computer.

If you receive a phone call offering help to clean up your computer, hang up immediately (this is a common scam).

AF Anyone who thinks they may have been subject to a ransomware attack should contact Action Fraud (www.actionfraud.police.uk). Organisations should call 0300 123 2040. In Scotland, contact the police by dialing 101.

Should I pay the ransom?

Law enforcement do not encourage, endorse, nor condone the payment of ransom demands. If you do pay the ransom:

- there is no guarantee that you will get access to your data or computer
- your computer will still be infected
- you will be paying criminal groups
- you're more likely to be targeted in the future

If you have paid any extortion demands you should report this to your local police force.

www.ncsc.gov.uk @NCSC National Cyber Security Centre @cyberhq

The NCSC have a range of free to use infographics that can be printed and distributed freely.

Some of the topics include Malware, Ransomware, Phishing, Passwords, Video Conferencing, Incident Response and Password Policies.

The NCSC have also created a free e-learning package aimed at small charities and small businesses. This can be used as a standalone product, or incorporated in to your existing e-learning platform.

Find out more about these at www.ncsc.gov.uk.

NCSC Resources

Exercise in a Box helps organisations test and practise their response to a cyber attack. It is completely free and you don't have to be an expert to use it. It provides exercises, which your organisation can do in your own time, in a safe environment, as many times as you want. It includes everything you need for setting up, planning, delivery, and post-exercise activity, all in one place.

The Cyber Security Information Sharing Partnership is a platform for businesses to share information about cyber incidents – successes, shortcomings, lessons learnt etc. It is free to join, and can help to keep your organisation ahead of the curve, by learning from others in similar industries.

You can sign up at www.ncsc.gov.uk/cisp

South West Cyber Resilience Centre (SWCRC)

The South West Cyber Resilience Centre (CRC) is a not-for-profit partnership with business and academia. Funded by the Home Office, the centre aims to help businesses and charities in the region protect themselves from cybercrime.

There are a few membership options, offering a range of services including cyber awareness training to vulnerability assessments. The SWCRC can also leverage a network of approved partners to make recommendations to businesses around purchasing technology.

Find out more at www.swcrc.co.uk.

THE
CYBER
RESILIENCE
CENTRE
FOR THE **SOUTH WEST**

Dorset Police Cyber Crime Unit

As part of the Cyber Protect network, we offer free and impartial cyber awareness training to businesses of all sizes. No business is too small (so far, our record is 4 people) or too large.

We are also able to run cyber awareness sessions for your board – one of the more popular activities we run is the Decisions and Disruptions game. Aimed at decision makers and budget holders, the game puts participants in charge of a Lego powerplant and tasks them with making decisions on how to spend their budget over the course of four quarters.

If you think your organisation would benefit from free cyber awareness training, at any level, get in touch. We can discuss your needs, and make sure we deliver a session that best suits your needs.

Contact us

Feel free to get in touch if you have any questions or concerns about cyber security.

Send us an email at:
cybercrimeprevention@dorset.pnn.police.uk