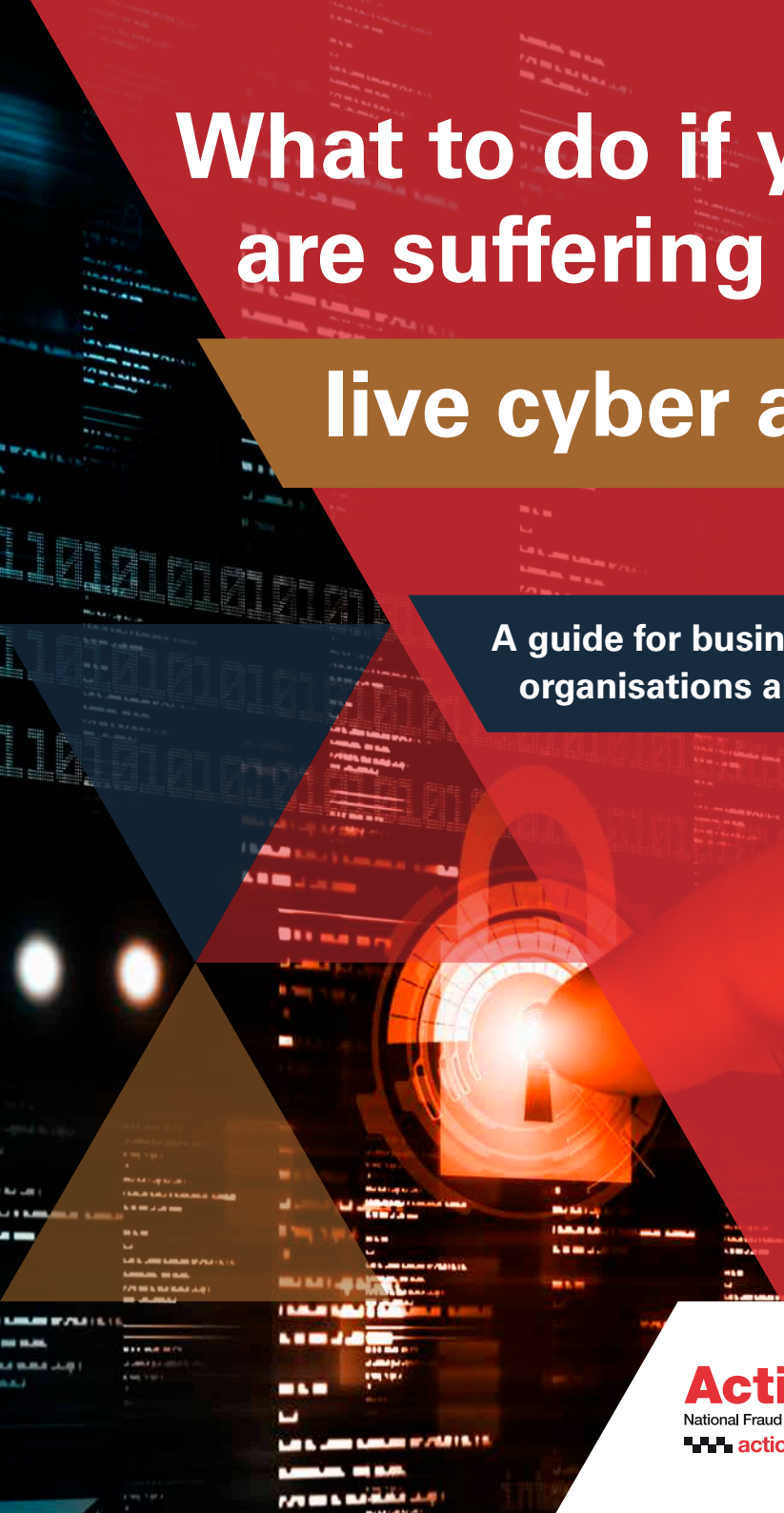
What to do if you are suffering a live cyber attack

A guide for businesses, organisations and charities



ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

What is a live cyber attack?

A live attack is one that is ongoing, that is still affecting your system and your ability to work... and there is an opportunity for law enforcement to stop the attack and/or secure evidence that will assist an investigation.

For example:

Cyber criminals have accessed your network and stolen personal information about your customers and are demanding payment for its safe return. This is also known as hacking extortion.

Or

Your website is being flooded with traffic – customers are not able to access it as a result. This is called a distributed denial of service (DDOS) attack.

How to report a live cyber attack 24/7?

If you are a business, charity or other organisation that is suffering a live cyber attack please call Action Fraud on **0300 123 2040** immediately, where our specialist advisors are waiting to take your call **24 hours a day, 7 days a week**.

Our advisors will ask you a series of questions to help identify what type of attack you are experiencing, give you advice/support and pass it immediately to the National Fraud Intelligence Bureau (NFIB). The NFIB sits alongside Action Fraud within the City of London Police.

What to expect after you report?

Once we have triaged your call to the NFIB, they will:

- Review your report and conduct a range of enquiries.
- Identify any connected reports or links to known criminals.
- Assess opportunities for police action.
- Send it to the relevant police agency.

Live cyber reports are sent to the relevant police agency within the UK in order to get the best response. This can be your local police force or the National Cyber Crime Unit (NCCU), which is part of the National Crime Agency.

Reports which are deemed significant and require cross government support are managed by National Cyber Security Centre (NCSC).

What type of cyber dependent crime should I report?

Cyber dependent crimes are offences carried out against computers, computer networks or other electronic devices in violation of the Computer Misuse Act 1990. These are crimes where unlawful access has been gained to a system or the system has been made unusable by the criminal.

An example of this is ransomware. This is a form of malicious software (malware) that infects your devices and encrypts all your files. The malware renders your system unusable and demands you pay a ransom, which is usually in a crypto currency such as Bitcoin.

Cyber criminals usually claim they will provide you with a decryption key once the ransom has been paid. However it is not guaranteed. There have been cases where the decryption key has not been sent after payment.

Other cyber dependent crimes include:

- Distributed denial of service attacks (DDOS).
- Network intrusion/hacking.
- Data breach.
- Malware – eg banking Trojans. A Trojan is a piece of malware hidden in what appears to be a normal file, which typically aims to steal data or take control of a user's computer.

Further cyber security advice and how to protect yourself

If you are an organisation (private, public or voluntary) that wants information about cyber security, refer to advice from the National Cyber Security Centre (NCSC). **www.ncsc.gov.uk**

The NCSC also have a small business guide which shows you how to improve cyber security – quickly, easily and at low cost. **www.ncsc.gov.uk/smallbusiness**

Register for the Cyber Security Information Sharing Partnership (CiSP)

CiSP is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment. **www.ncsc.gov.uk/cisp**

Follow @actionfrauduk on Twitter, or 'like' us on Facebook and keep up-to-date with the latest scams to watch out for.

@actionfrauduk

actionfraud

The Action Fraud website lists a handy A-Z of different fraud types as well as our top tips to protect yourself from fraud:

actionfraud.police.uk

You can sign-up for fraud and cyber crime alerts at:

actionfraudalert.co.uk

Or find out more at:

cyberaware.gov.uk

getsafeonline.org

@cyberprotectuk

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

CYBER AWARE

GET SAFE ONLINE .org

NCA
National Crime Agency

National Cyber Security Centre
a part of GCHQ

V1: November 2017