Protect

4 Simple steps you can take today to protect your business

Don’t Pay

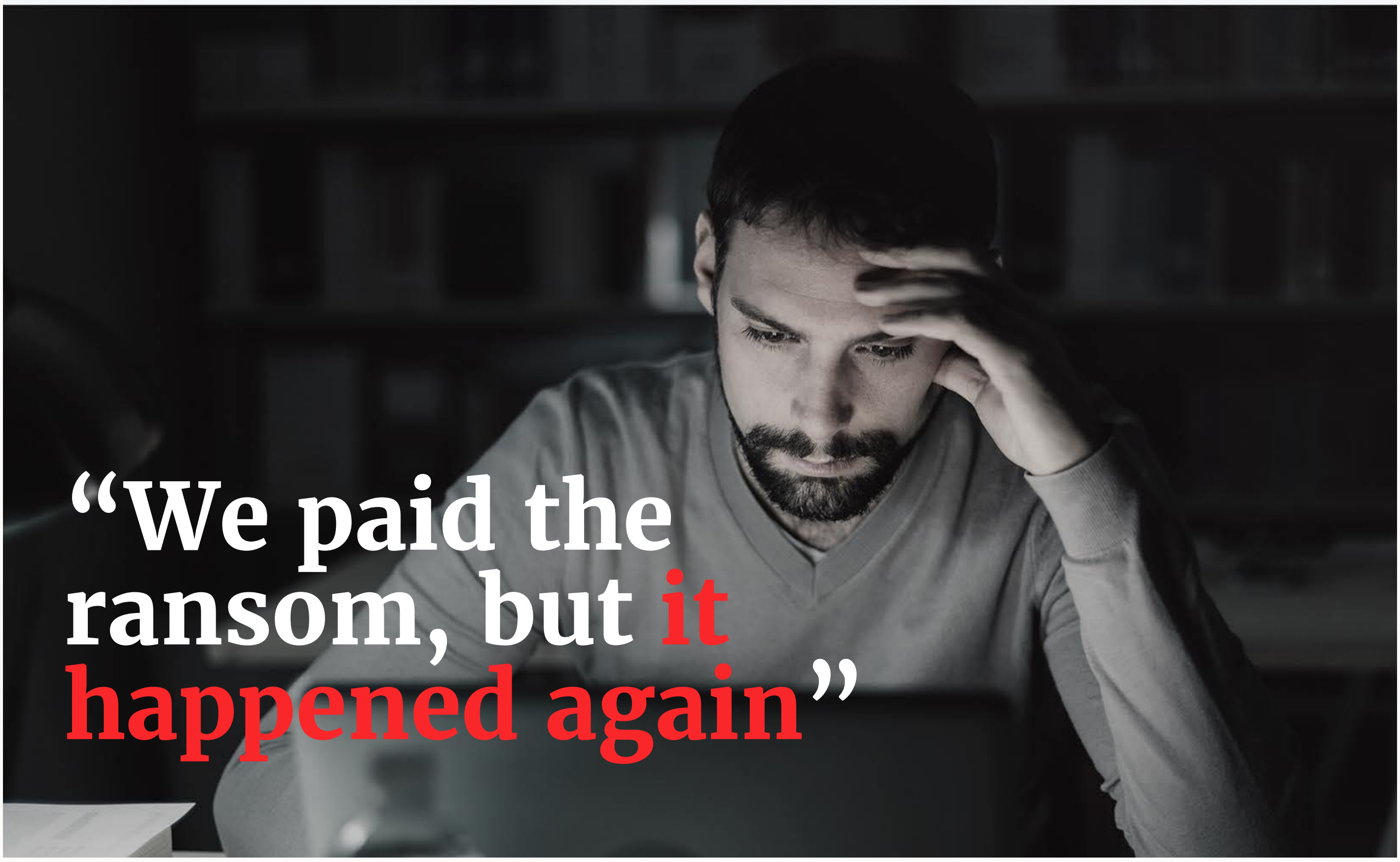
3 Reasons why you shouldn’t pay the ransom

Small businesses that almost lost everything to ransomware

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

CYBER AWARE

@CyberProtectUK



“We paid the ransom, but it happened again”

We originally noticed that none of our applications were working, all the computers just froze one after another. Once we restarted them, they all displayed a box with a message on it asking for payment. We tried restarting the computers again, but the same message was still there. I’m not very good with technology and I didn’t know how to fix this, so I called the number on the screen and a man told me that they would return my computer to normal if I paid them £350 in something called Bitcoins.

I paid the money and they gave me a code to type into all of the computers. It worked, all the computers were back to normal. Yesterday it happened again, the same message from two weeks ago has reappeared on our computers.

Reported by a small business in the North East

A company is hit with ransomware every 40 seconds.

https://securelist.com/

"...we realised that we'd been scammed"

“We gave them the money, but they weren’t going to unlock our files”

Our school was hit with a Ransomware attack last Friday. We’re still not sure how it happened, but most of our computers seem to be locked. They’re all displaying a dialog box that’s asking for Bitcoins and provides a phone number and Russian email address we can contact. We had an emergency staff meeting to discuss what we should do and it was decided that paying the ransom was our best move. The school can’t function properly without computers in classrooms, so we didn’t have much of a choice.

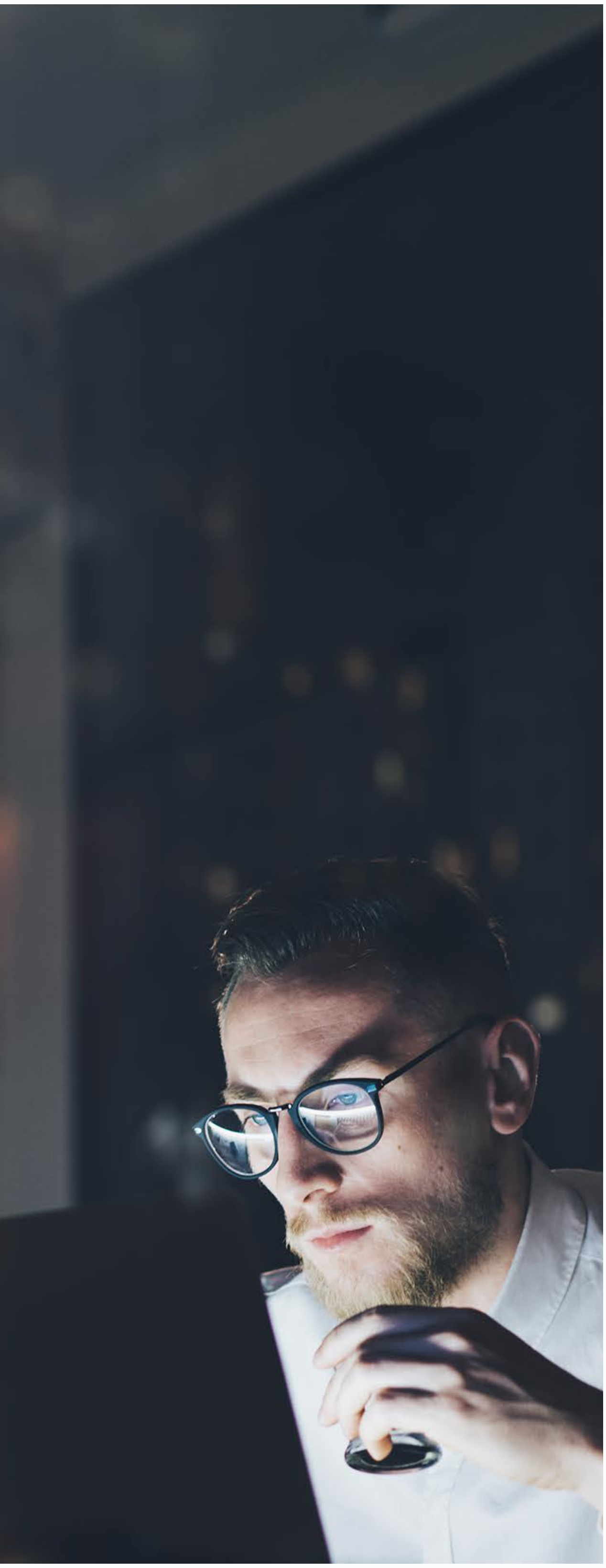
After the payment was made, nothing happened. The computers were still locked. When we came in for work the next morning and saw that the computers still weren’t working, that’s when we realised that we’d been scammed. We gave them the money, but they weren’t going to unlock our computers.

It’s been almost a week since it happened and we’ve only just managed to fix about half of the computers. We had backups of some files but my team tells me that we’ve lost most of the data stored on our main computers.

Reported by a school in London.

6 in 10 malware payloads were ransomware in Q1 2017.

www.malwarebytes.com/



Protect your business against cyber crime

Backups

Backup all of your important data to a storage device that won't be left connected to your computer or network, such as an external hard drive, or an online storage service.

Anti-virus

Anti-virus software - which is often included for free within popular operating systems - should be used on all computers and laptops.

Updates

Install the latest software and app updates on all of your devices. They often include important security fixes which will protect your devices from viruses and hackers.

Emails

Don't check emails using an administrator account. Look for obvious signs of phishing such as poor grammar & spelling, or low quality versions of recognisable logos.

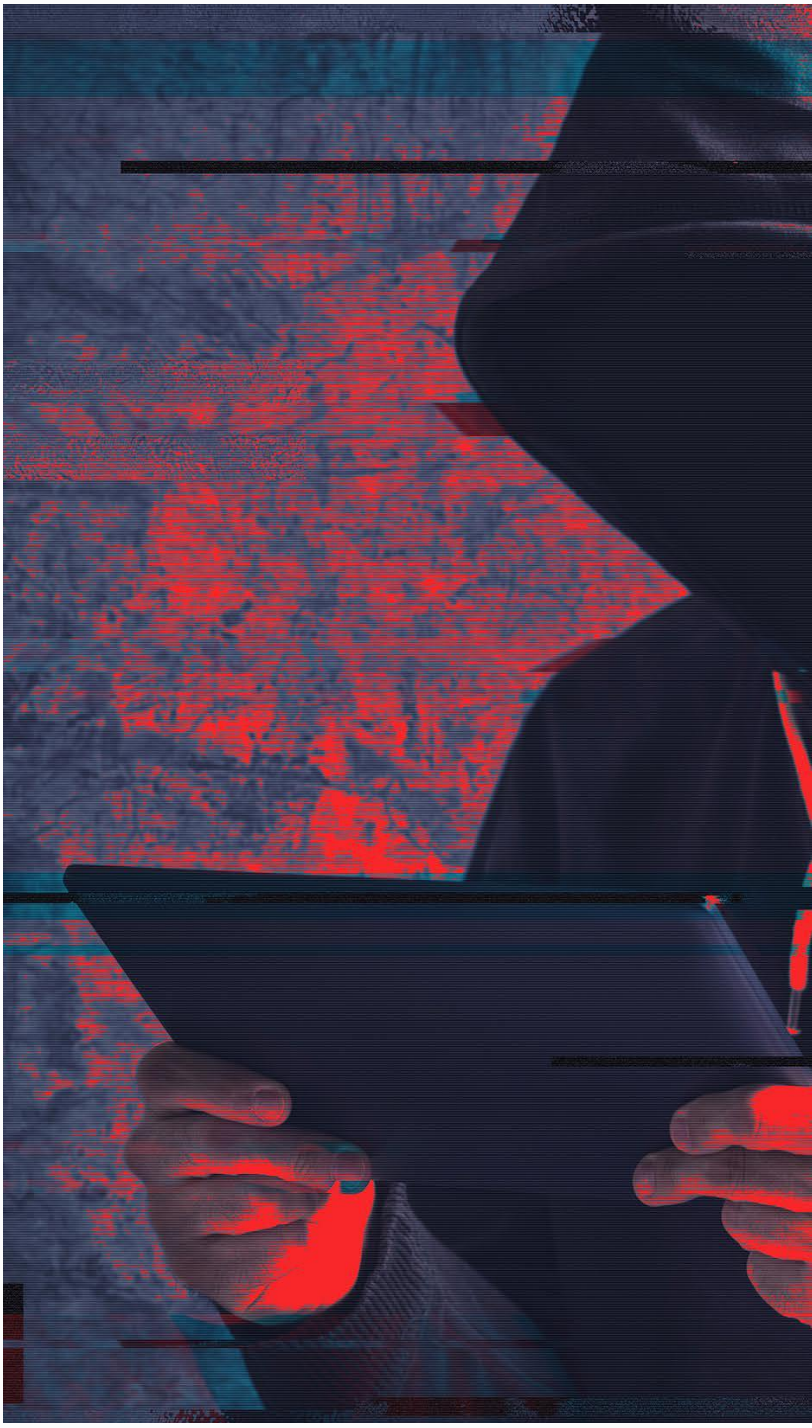
For more information on how to protect your business from cyber crime, visit www.ncsc.gov.uk/smallbusiness

ActionFraud 0300 123 2040 CYBER AWARE @CyberProtectUK

Don’t pay the ransom

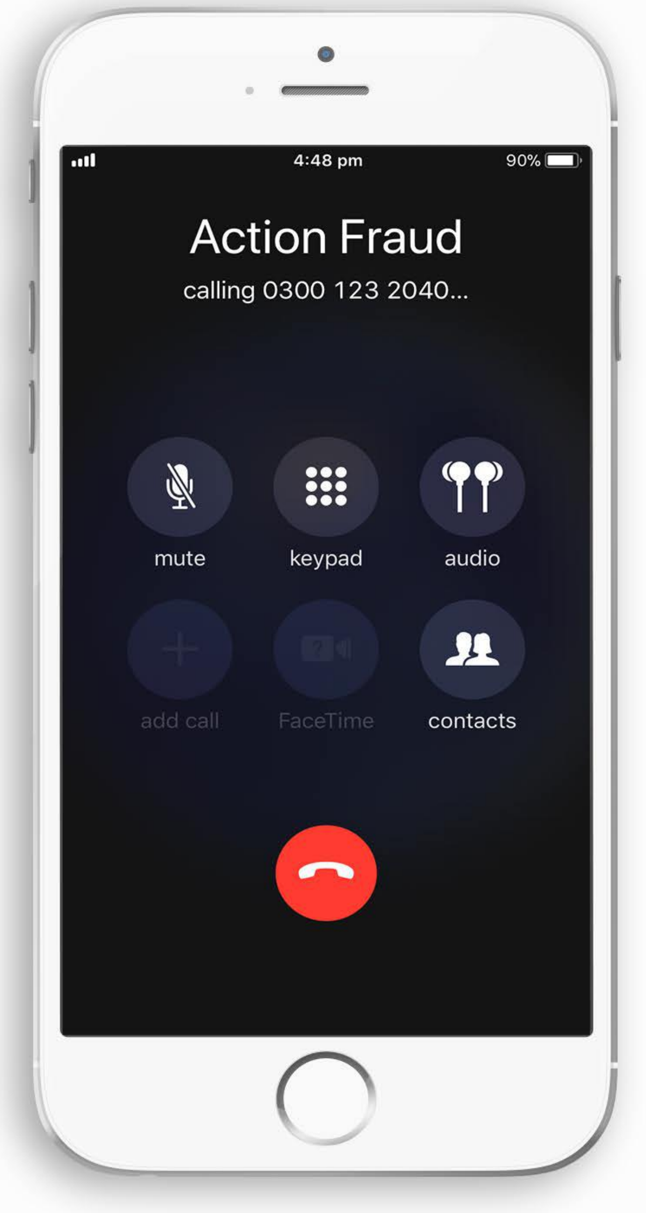
Access to your files may not be restored

When considering whether or not you should pay the ransom, bear in mind that you’re dealing with criminals. You could end up in a situation where you’ve paid the ransom but access to your files hasn’t been restored. Criminals have also been known to re-target victims that have already paid a ransom once; paying a ransom only highlights to criminals that you’re vulnerable to a ransomware attack. Even after you’ve paid the ransom, and access to your files is restored, it’s possible for criminals to leave a “backdoor” installed on your device which can later be used to re-infect it.



You’re funding organised criminals

By paying the ransom, you’re putting money into the hands of criminals who will use it to commit further crimes. As long as this type of attack remains lucrative, criminals will continue using it against people and businesses.



Is your business under a live cyber attack?

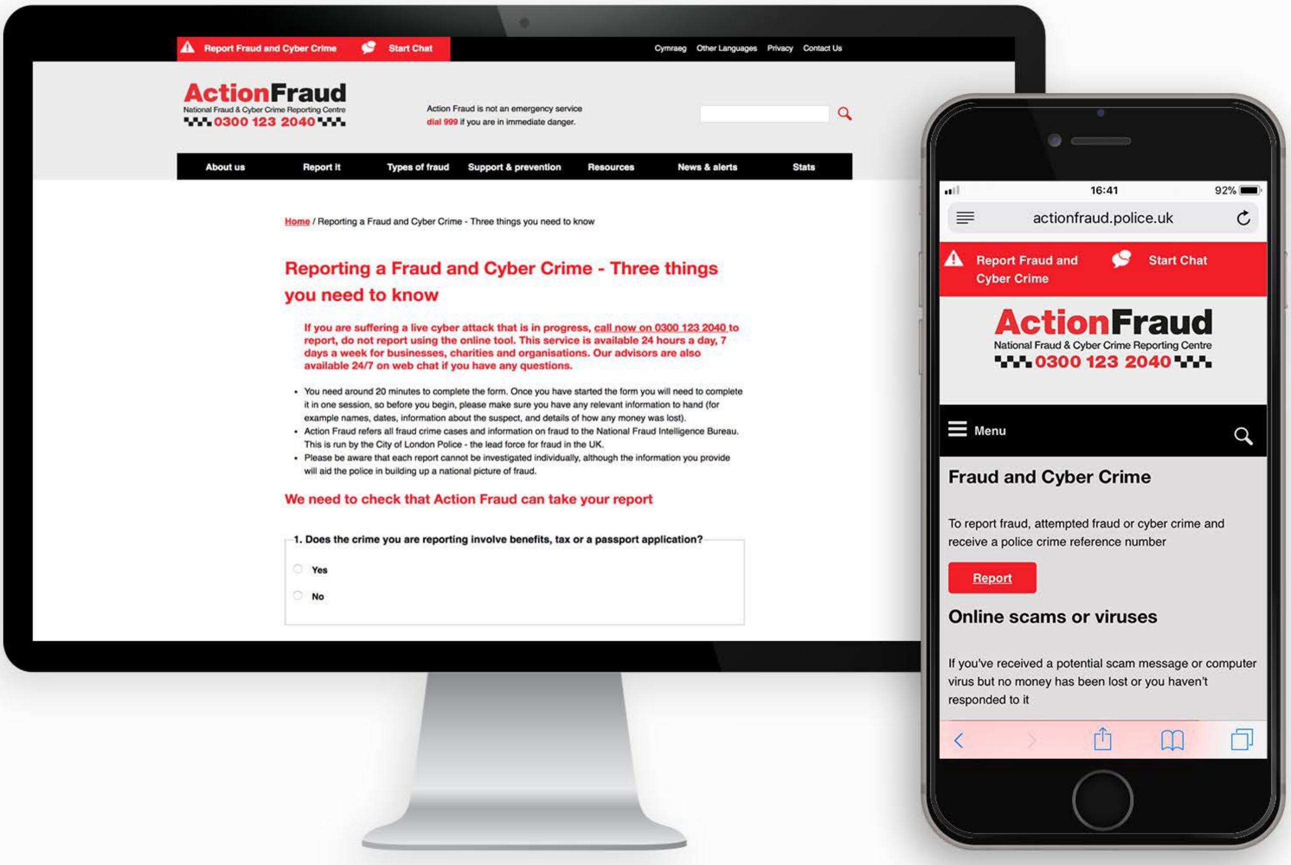
24/7 Reporting for Businesses

If you are a business, charity or other organisation that is currently experiencing a live cyber attack (an attack in progress), please call Action Fraud immediately on **0300 123 2040** to speak with one of our specialist advisors.

You should keep a timeline of events and save any information that is relevant to the attack.

Every report matters

Victim of fraud or cyber crime?



Action Fraud is not an emergency service
dial 999 if you are in immediate danger.

Home / Reporting a Fraud and Cyber Crime - Three things you need to know

Reporting a Fraud and Cyber Crime - Three things you need to know

If you are suffering a live cyber attack that is in progress, call now on 0300 123 2040 to report, do not report using the online tool. This service is available 24 hours a day, 7 days a week for businesses, charities and organisations. Our advisors are also available 24/7 on web chat if you have any questions.

- You need around 20 minutes to complete the form. Once you have started the form you will need to complete it in one session, so before you begin, please make sure you have any relevant information to hand (for example names, dates, information about the suspect, and details of how any money was lost).
- Action Fraud refers all fraud crime cases and information on fraud to the National Fraud Intelligence Bureau. This is run by the City of London Police - the lead force for fraud in the UK.
- Please be aware that each report cannot be investigated individually, although the information you provide will aid the police in building up a national picture of fraud.

We need to check that Action Fraud can take your report

1. Does the crime you are reporting involve benefits, tax or a passport application?

○ Yes

○ No

Fraud and Cyber Crime

To report fraud, attempted fraud or cyber crime and receive a police crime reference number

Online scams or viruses

If you've received a potential scam message or computer virus but no money has been lost or you haven't responded to it

Report it to Action Fraud

If you have been a victim of ransomware, please report it to Action Fraud at **actionfraud.police.uk.** Every report you make helps us to build a clearer picture of the threat from ransomware and allows us to direct the focus of our investigations. Even if you have removed the ransomware from your device, details such as when your device first became infected or what operating system you're using, can still be useful to our investigations.