CYBER CRIME NEWS

ISSUE 1 • NOVEMBER 2022

WELCOME TO CYBER CRIME NEWS

WELCOME TO THE NEW BI-MONTHLY CYBER CRIME E-NEWSLETTER FROM DORSET POLICE TO KEEP YOU UP TO DATE WITH THE LATEST NEWS, CAMPAIGNS, CRIME PREVENTION GUIDANCE AND SUPPORT FOR BUSINESSES. PLEASE SHARE WITH YOUR NETWORKS.

THE BI-MONTHLY CYBER CRIME E-NEWSLETTER WILL:

- Introduce you to and explain some of the current threats
- Provide you with information on how to access available resources both locally and nationally to help keep you and your business safe
- Provide useful hints and tips.

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

PRODUCED BY DORSET OPCC AND DORSET POLICE

DORSET POLICE

WHAT IS CYBER CRIME

AND WHY IT IS A THREAT TO YOUR BUSINESS?

CYBER CRIME IS CRIMINAL ACTIVITY THAT EITHER TARGETS OR USES A COMPUTER, A COMPUTER NETWORK OR A NETWORKED DEVICE.

Most cyber crime is committed by cyber criminals who want to make money. However, occasionally cyber crime aims to damage computers or networks for reasons other than profit.

Cyber crime is a real threat, and the damage caused, results in financial or data loss and reputational harm. Cyber crime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud, and identity fraud, as well as attempts to steal financial accounts, credit card or other payment card information.

"IN THE LAST 12 MONTHS, 39% OF UK BUSINESSES IDENTIFIED A CYBER-ATTACK".

Fraud and cyber crime are undoubtedly among the largest threats facing businesses today. According to the Department for Digital, Culture, Media and Sport (DCMS) Cyber Security Breaches Survey 2022, in the last 12 months, 39% of UK businesses identified a cyber-attack.

The Cyber Security Breaches Survey is an influential research study for UK cyber resilience, aligning with the National Cyber Strategy. The survey found that of the 39% of UK businesses who identified an attack, the most common threat was phishing attempts (83%).

Of the 39%, around one in five identified a more sophisticated attack type such as a denial of service, malware, or ransomware attack.

Despite its low prevalence, organisations cited ransomware as a major threat, with 56% of businesses having a policy not to pay ransoms.

Across businesses of all sizes, cyber-attacks cost an average of £4,200 per attack. Collectively, in the last year, organisations in the UK lost £2.1 billion.

In Dorset, between October 2021 and September 2022, Action Fraud received 655 reports with total combined losses of £3.5m. The figures show that 5% of the reports are related to cyber dependent crime, and 95% linked to fraud. 80% of reported fraud is shown as being cyber enabled and classed as cyber crime. The figures for Dorset are in line with the trends seen nationally.

THE MOST COMMON TYPES OF CYBER CRIME IN DORSET ARE:

1 CHEQUE, PLASTIC CARD AND ONLINE BANK FRAUD

2 ONLINE SHOPPING AND AUCTION FRAUD

3 EMAIL/SOCIAL MEDIA HACKING

4 SERVER HACKING

5 DENIAL OF SERVICE ATTACK

6 HACKING WITH EXTORTION

Despite this clear threat, only 33% of businesses have carried out a cyber security risk assessment, 23% have a formal cyber security strategy, and just 17% carry out staff awareness training.

It doesn't have to be this way; businesses can do more to protect themselves against cyber attacks. There is a wide range of resources available for businesses, often for free with specialists on hand to help you through the steps to greater security.

FIND OUT MORE ONLINE

Dorset Police
cybercrimeprevention@dorset.pnn.police.uk

National Cyber Security Centre www.ncsc.gov.uk

South-West Cyber Resilience Centre
www.swcrc.co.uk

National Business Crime Centre
www.nbcc.police.uk

FREE CYBER AWARENESS TRAINING FOR BUSINESSES

FEWER THAN 1 IN 5 ORGANISATIONS IN THE UK CARRIED OUT CYBER AWARENESS TRAINING FOR THEIR STAFF IN THE LAST YEAR. WHETHER THIS IS DUE TO TIME CONSTRAINTS OR FINANCES, DORSET POLICE CAN HELP.

Dorset Police offer free and impartial cyber awareness sessions to businesses of all sizes – from a handful of staff to hundreds. The sessions provide organisations with National Cyber Security Centre backed advice and guidance, covering cyber security fundamentals, including how to spot and respond to various cyber threats.

Sessions can be delivered either in person, at a time and location that suits your needs, or virtually, via your chosen video conferencing platform.

If your business has a specific cyber security concern or you just don't know where to start, Dorset Police can tailor presentations to ensure your needs are met.

If you feel this would be of benefit to your company, please get in touch – we can then discuss your needs, and book in a cyber awareness training session at no cost to you.

To arrange a cyber awareness session, email us at:

cybercrimeprevention@dorset.pnn.police.uk

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

PRODUCED BY DORSET OPCC AND DORSET POLICE

DORSET POLICE

PICK OF THE MONTH

EACH MONTH WE WILL PROVIDE YOU WITH A COMMON TYPE OF CYBER CRIME AND EXPLAIN WHAT IT IS, WHY IT IS A THREAT AND WHAT YOU CAN DO TO PROTECT YOURSELF AGAINST IT. THIS MONTH WE WILL PROVIDE INFORMATION ABOUT MANDATE FRAUD AND PHISHING – THESE ARE LINKED, BUT DO YOU KNOW HOW?

MANDATE FRAUD & PHISHING

MANDATE FRAUD IS WHERE SOMEONE TRICKS YOU INTO CHANGING DETAILS OF A DIRECT DEBIT, STANDING ORDER OR BANK TRANSFER BY PRETENDING TO BE AN ORGANISATION YOU MAKE REGULAR PAYMENTS TO.

Examples include a business supplier or a subscription. It's a simple but effective fraud and is very common.

Phishing is when a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

The information is then used to access important accounts and can result in identity theft and financial loss. The email or text is likely to have an internet link which when clicked, will open a fake webpage. This is when information about you or your accounts can be obtained.

MANDATE FRAUD COSTS UK FIRMS OVER £145M

Generally considered to be one of the most common threats facing businesses in the UK, mandate fraud has cost UK businesses in excess of £145m in the last 12 months.

Mandate fraud involves the compromise of business email accounts. Criminals use techniques like phishing in order to gain access to company emails. This allows them to contact that companys' customers using their legitimate email address, adding credibility to their scam. They then use that address to send invoices with amended payment details. This results in the diversion of legitimate payments away from the supplier, and into the criminals' account.

In Dorset, 32 cases of mandate fraud were reported to Action Fraud in the last 12 months, collectively costing more than £430k. This is a significant threat to businesses. There are, however, some relatively simple things that can be done to mitigate it.

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

PRODUCED BY DORSET OPCC AND DORSET POLICE

DORSET POLICE

THINGS YOU CAN DO NOW TO STAY SAFE?

AS A SUPPLIER

Ensure your staff know how to spot the signs of a phishing email, as this is typically how criminals take control of business emails.

SPOT THE SIGNS OF PHISHING

- **Is the email addressed to you by name, or does it refer to 'valued customer', or 'friend' or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam.**
- **Others will try and create official looking emails by including logos and graphics. Is the design (and quality) what you'd expect?**
- **Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'.**
- **Look at the sender's name and email address. Does it sound legitimate, or is it trying to mimic someone you know?**
- **Your bank (or any other official source) should never ask you to supply personal information in an email. If you need to check, call them directly**
- **If it sounds too good to be true, it probably is.**

Ensure you have a robust password policy, making your email accounts harder to compromise, pets' names, dates of birth and football teams are not good for passwords as they are easy for criminals to guess. Use a combination of upper and lower-case letters, numbers and special characters. A passphrase, made up of three random words, is a good base to start with. Where possible, use Two Step Verification (2SV) to protect these accounts too. This acts as a safety net, requiring a second input (usually a six-digit code, sent to a trusted mobile device), which criminals would not have ready access to.

AS A CUSTOMER

Be sure to verify any changes to payment details. Typically, modified invoices are sent with a message advising of a change in payment details, but this isn't always the case. Should you receive an invoice with different payment details, contact the originating organisation to verify. Don't rely on email for this, as it may have been compromised. Instead, use a known and trusted telephone number from previous invoices or your contacts list.

HELPFUL ADVICE

For further advice about Mandate Fraud, and what you can do, head to **www.actionfraud.police.uk/a-z-of-fraud/mandate-fraud**

WATCH THE VIDEO

GENERAL TOP TIPS FOR CYBER SAFETY

1. Use strong, complex passwords
Use a combination of upper and lower-case letters, numbers and special characters. A passphrase, made up of three random words, is a good base to start with.

2. Install a reputable antivirus package
Antivirus programs are a safety net, protecting you against any malicious files that find their way on to your devices. Make sure it's always on, and always up to date.

3. Install updates
Make sure you install software updates as soon possible. They often contain important security fixes.

4. Be careful where you click
Take care with links and attachments in email. If it's unexpected, or suspicious, don't click. Double check the address of the website the link takes you to (by hovering your mouse over the link). Criminals often take advantage of spelling mistakes to direct you to a malicious site.

5. Beware of public Wi-Fi
Whilst it's absolutely fine for casual browsing, free Wi-Fi is not secure. Sensitive data, like passwords or banking details, can be spied upon. Use your mobile data, or a Virtual Private Network (VPN) instead.

6. Back it up
Make a second or third copy of everything you care about. If you suffer from a ransomware attack, restoring files from a removable hard drive is much easier, cheaper, and more reliable than paying a criminal for your files back.

7. Be careful what you share
Where you go to school, or work, or on holiday... this information is more valuable than some people think. Information shared on social media can be used by scammers to impersonate potential victims, or guess password reset questions, for example.

8. Keep your devices safe
Use passwords, pin codes or biometrics where available.

REPORTING CYBER CRIME

If you fall victim to fraud or cyber crime, you can report this to Action Fraud by visiting www.actionfraud.police.uk or by calling 0300 123 2040.

If you have received an email that you're not sure about, you can report this to the **National Cyber Security Centres Suspicious Email Reporting Service (SERS)**. Simply forward the email to **report@phishing.gov.uk**.

The SERS automatically analyses suspicious emails and, if it considers it to be malicious, can take steps to have email accounts and associated websites closed down, meaning each report can really make a difference.

DORSET POLICE

Dorset Police
Force Headquarters
Winfrith, Dorchester
Dorset DT2 8DZ

E cybercrimeprevention@dorset.pnn.police.uk
www.dorset.police.uk

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

Office of the Dorset Police & Crime Commissioner
Force Headquarters
Winfrith, Dorchester
Dorset DT2 8DZ

T 01202 229084
E pcc@dorset.pnn.police.uk
www.dorset.pcc.police.uk