CYBERCRIME NEWS

ISSUE 14 • APRIL 2025

£16.9 MILLION STOLEN IN DORSET

IN THE LAST 13 MONTHS, OVER 400,000 INCIDENTS OF FRAUD AND CYBERCRIME HAVE BEEN REPORTED TO ACTION FRAUD.

In Dorset alone, over 4,400 reports were made, with losses totalling £16.9 million. Additionally, in Dorset, 80% of reports originated from limited companies, showing that businesses are prime targets. These figures highlight the growing threat of cybercrime across the UK and the urgent need for businesses to stay vigilant.

The most common categories of reported fraud were Consumer Fraud (122,000 incidents), Cyber-Dependent Crime (59,000 cases), Advance Fee Fraud (48,000 reports, and Banking Fraud (34,000 incidents). The most common reported cybercrime is social media and email hacking which accounts for 67% of reports.

IMPACT ON BUSINESSES & CHARITIES

CYBERCRIME CONTINUES TO RISE SHARPLY. IN 2023, THERE WERE 745,000 REPORTED INCIDENTS, INCREASING TO 1,022,000 IN 2024.

Cybercrime is a major risk for organisations. 50% of businesses, and 32% of charities faced a cyber security incident or breach in the past year. The most common types of attacks are:

- Phishing: 84% of businesses, 83% of charities
- Impersonation attempts: 35% of businesses, 37% of charities
- Malware infections: 17% of businesses, 14% of charities

The most targeted sectors include education, arts/ entertainment and recreation, manufacturing, and retail/ trade.

Manufacturing industries are prime targets for ransomware attacks due to their dependence on physical operations—disruptions from an attack can halt production and cause significant financial losses.

So, with this increase in cybercrime and fraud, how can you protect yourself from cyber threats?

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

DORSET POLICE

PRODUCED BY DORSET OPCC AND DORSET POLICE

REDUCE YOUR RISK!

- Verify the identity of the person or organisation requesting financial or personal details, on another form of communication
- Never click on unsolicited links, or open suspicious email attachments
- Avoid sharing personal information unless absolutely necessary
- Use trusted download sources
- Keep software and operating systems updated
- Ensure you have backups of important data, in case of loss or disruption

We have also seen a rise in Invoice Fraud, a common type of Business Email Compromise, whereby criminals pose as suppliers or executives to divert payments. Therefore, we recommend being wary of the following:

- Unusual requests from executives
- Requests for confidentiality, such as keeping transactions private
- Attempts to bypass normal procedures
- Language and formatting inconsistencies
- Mismatched email addresses

By staying informed and adopting strong cyber security practices, businesses and individuals can reduce their vulnerability to cybercrime and fraud.

REPORTING CYBERCRIME

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 offer free Cyber Awareness sessions, tailored to your businesses' needs. For more information on the sessions we offer, please contact Hannah Bird, Cyber Crime Protect and Prevention Officer at **cybercrimeprevention@dorset.pnn.police.uk**

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

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