CYBERCRIME NEWS

ISSUE 17 • OCTOBER 2025

CYBER PREPAREDNESS

CYBER THREATS CONTINUE TO BE ONE OF THE GREATEST THREATS UK BUSINESSES FACE, WITH SMALL AND MEDIUM SIZED ORGANISATIONS OFTEN TARGETED DUE TO LIMITED CYBER DEFENCES.

The run-up to Christmas often sees a marked increase in cybercrime, as criminals take advantage of heightened online activity and seasonal pressures. It is therefore vital businesses strengthen their preparedness and resilience during this high-risk period. Being prepared can make the difference between quick recovery from an incident to suffering serious financial and reputational damage.

WHY PREPAREDNESS MATTERS

Just over one in four national businesses (43%) and three in ten charities (30%) reported having experienced a cyber breach or attack in the last 12 months. This equates to approximately 612,000 businesses and 61,000 charities being impacted in the previous year.

Cyber breaches in Dorset typically cost businesses thousands of pounds, with ransomware, phishing, and business email compromise being the most common threats. Cyber attached are not a matter of 'if' but 'when' – Preparedness reduces downtime and loss.

KEY STEPS BUSINESSES CAN TAKE

1. STRONG ACCOUNT SECURITY

ENSURE USER ACCOUNTS HAVE STRONG AND COMPLEX PASSWORDS.

Passwords should not be repeated, and passwords should never be used for both personal and business accounts. Unique passwords ensure that if one password is compromised, it cannot be used to access further accounts.

Additionally, ensure Two-Step Verification (2SV) is enabled on all user and business accounts, especially email, payroll, social media, and banking. Two-Step Verification adds an extra layer of security by requiring a numerical code before access to an account is provided. This way, even if a password is compromised, the account remains secure.

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

DORSET POLICE

PRODUCED BY DORSET OPCC AND DORSET POLICE

2. REGULAR UPDATES & BACKUPS

Keep systems, software, and devices updated. If regular updates are not installed, this leaves devices susceptible to vulnerabilities. Critical and business data must also be regularly backed up. Backing up data ensures that if a cyber attack occurs, systems and data can be quickly restored from the backups.

USE THE 3-2-1 RULE:

- **3 Copies of Data:** Ensure there are 3 backups of critical data.
- **2 Storage Mediums:** To further protect yourself, save backups on two different storage mediums. For example, one copy on a computer or hard drive, and one copy in the cloud.
- **1 Copy Off-Site:** One copy of data should always be stored off-site. This backup will be offline, therefore, if the business experiences a cyber-attack which compromises the network and on-site backups, the business can still recover using the off-site backup, as this will remain unaffected.

3. INCIDENT RESPONSE PLAN

It is crucial to develop an Incident Response Plan in the case of an emergency. This will detail the steps to take when a cyber attack occurs, such as who to contact, and how to isolate affected systems. Important steps to document are:

- Who to contact – For example, IT support, your cyber insurer, and the Police
- How to isolate infected devices and systems, and preserve evidence
- How to communicate with staff and customers during downtime
- How to recover, such as by restoring using data backups

4. STAFF AWARENESS & TRAINING

Finally, ensuring staff are aware of how to recognise phishing emails and suspicious requests for information, money, or data is essential. Dorset Police offer free Cyber Awareness sessions covering important topics such as ransomware, business email compromise, data protection, phishing scams, and account security. To find out more, or request a free session, please email: **cybercrimeprevention@dorset.pnn.police.uk**

WHERE TO GET FURTHER HELP

NCSC Small Business Guide - Offers practical steps to strengthen your cyber defences: https://www.ncsc.gov.uk/collection/small-business-guide

Action Fraud – The national service for reporting cybercrime and fraud: https://www.actionfraud.police.uk/

South West Cyber Resilience Centre – Provides free local support and guidance: https://www.swcrc.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
Dorset DT2 8DZ

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