CYBER CRIME NEWS

ISSUE 18 • DECEMBER 2025

THREAT LANDSCAPE

STAY VIGILANT FOR CYBER CRIME & FRAUD

IN THE LAST 13 MONTHS, NATIONALLY, THERE HAVE BEEN £4 BILLION REPORTED LOSSES TO CYBER CRIME AND FRAUD, £3 BILLION OF WHICH ARE FROM INDIVIDUAL VICTIMS.

With regards to cyber crime reports, 67% of all reports were in relation to social media and email hacking.

EMAIL COMPROMISE

EMAIL ACCOUNTS ARE OFTEN TARGETED BECAUSE OF THEIR VALUE.

Once compromised, emails can be used to defraud others, for example by sending out requests for money or gift cards to friends, family, or business contacts.

In addition, often when resetting a password on an account, the password reset link is sent via email. Therefore, criminals are attempting to compromise email accounts with the hope they can then compromise further accounts.

WE HAVE ALSO SEEN AN INCREASE IN SIM SWAPPING:

Once criminals have access to an email account, they may contact the victim's phone provider to request a PAC code to transfer the victim's number into their possession.

It is therefore important that if you receive any of the following you immediately contact your phone provider:

- An unexpected PAC code
- Emails or texts about your number being migrated
- Sudden loss of service not tied to an expected outage

However, the biggest protection from Sim Swapping and account compromise is for accounts to have unique passwords and Two Step Verification enabled.

It is important to stay vigilant for cyber crime and fraud, as attacks will increase during the festive period.

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

DORSET POLICE

PRODUCED BY DORSET OPCC AND DORSET POLICE

CURRENT CYBER CRIME THREATS

1. ACCOUNT COMPROMISE

Account Compromise remains a substantial risk to individuals and businesses. It is therefore crucial to use strong, unique passwords for important accounts, and ensure Two Step Verification is enabled.

2. PHISHING SCAMS

Phishing scams via phone, SMS, email, and QR codes, remain a significant cyber crime threat. Any unexpected communications must be treated with care by taking time to verify the sender before giving over any personal or financial information.

3. RANSOMWARE

The biggest cyber crime threat businesses' face is Ransomware. We have discussed this threat in a previous edition.

During the festive period we see a sharp increase in ransomware attacks as criminals are aware businesses close early for that well deserved holiday break. As such, make sure to brush up on your knowledge of ransomware so you are prepared and know how to respond to an attack.

4. BUSINESS EMAIL COMPROMISE (BEC)

Another large threat for businesses' is BEC whereby compromised email accounts or spoofed email addresses, are used to trick employees into transferring money or sensitive information. Always verify all requests for money and information via another communication method, especially if there has been a change to payee details.

5. UNPATCHED SOFTWARE

Unpatched software and devices that are not regularly updated continue to pose threats to network security.

Manufacturers and developers will put out updates (or patches) to fix potential security vulnerabilities, therefore, if you are not regularly updating your devices and software there is a chance you are suspectable to security threats.

WE ARE HERE TO HELP!

Dorset Police are here to take the stress away and ensure you can enjoy your well-deserved Christmas break.

Dorset Police offer free Cyber Crime sessions covering a range of topics that are tailored to your needs. As such, if something in this edition has brought to light potential weaknesses in your cyber security, please do get in touch.

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