CYBERCRIME NEWS

ISSUE 15 • JUNE 2025

BUSINESS EMAIL COMPROMISE: A COSTLY CYBER THREAT

BUSINESS EMAIL COMPROMISE (BEC) IS A GROWING THREAT TO BUSINESSES ACROSS THE UK – AND IT'S SOMETHING WE'RE INCREASINGLY SEEING HERE IN DORSET.

BEC is a form of cyber-enabled fraud where attackers impersonate a legitimate contact - often a senior staff member, supplier, or partner - to trick employees into making unauthorised payments or sharing sensitive information.

Unlike phishing, BEC attacks are highly targeted and rarely rely on suspicious links or malware. Instead, they exploit trust, urgency, and human error.

HOW DOES IT WORK?

A TYPICAL BEC ATTACK MIGHT LOOK LIKE:

"Hi Jo, I'm tied up in meetings all day. Please make an urgent payment of £5800 to the new supplier account - We can't afford delays on this project. I'll explain later. Thanks!"

This tactic is often used during busy periods (like the end of the financial year) and can involve:

- Spoofed email addresses that look nearly identical to a real one
- Compromised email inboxes where fraudsters monitor communications
- Fake invoices with altered bank details
- Impersonation of CEOs, finance officers, or known suppliers

WHY IS BEC DANGEROUS?

1. Low-tech but high impact – There is no need for sophisticated malware
2. Hard to detect - Emails often appear legitimate
3. Expensive - Globally BEC causes more financial loss than ransomware

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

DORSET POLICE

PRODUCED BY DORSET OPCC AND DORSET POLICE

HOW TO STAY SAFE!

- Verify all changes to bank details with a different form of communication, using a trusted contact number
- Use dual authorisation for payments
- Introduce a 'pause and check' policy for urgent requests involving money or data
- Review your email security - ensure strong & unique passwords are used and enable 2 Step Verifications
- Don't rely on email alone - confirm unusual requests through a secondary communication method

RED FLAGS TO WATCH OUT FOR:

- Sudden pressure to act quickly or urgently
- Changes to known payment instructions and details
- Requests to keep the action or payment confidential

WHAT TO DO IF IT HAPPENS

1. Act fast - contact your bank immediately an recall the payment

2. Report to Action Fraud

3. Preserve evidence - Do not delete emails or internal communications

4. Review and strengthen your internal processes

The OPCC are interested to know what you think about the Cyber Crime newsletter – the answers you provide will be used to inform the development of future issues.

Please complete our quick survey via this link:

CLICK HERE

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
Dorset DT2 8DZ

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