CYBERCRIME NEWS

ISSUE 19 • FEBRUARY 2026

"IT'S NOT TOO LATE"

SELF-ASSESSMENT TAX SCAMS

ALTHOUGH THE SELF-ASSESSMENT DEADLINE PASSED ON THE 31ST OF JANUARY, IT IS LIKELY BUSINESSES AND SOLE TRADERS WILL STILL BE TARGETED BY SCAMS IN THE COMING MONTHS.

CRIMINALS KNOW THAT

- Some people submit their taxes late
- Others are worried about incurring penalties
- Many businesses are catching up on admin following January

Fraudsters will try and exploit this by sending messages that create urgency and fear, pressuring people to click links or offer information. Examples include emails or texts offering a tax rebate and asking you to verify details or provide banking information or, messages claiming there is a warrant out for your arrest because you owe HMRC money.

HOW THESE SCAMS OPERATE

- Fake tax demands or refund offers sent via email, text, or phone calls
- Creating a sense or urgency or pressure to respond
- Threatening legal action or arrest if you do not comply or respond
- Using official-looking logos and branding to appear genuine
- Email or number spoofing to make it appear that the message has been sent from HMRC
- Directing victims to fake websites that closely copy the real HRMC pages to steal information or spread malware
- Attempting to steal banking passcodes or one-time verification codes

DORSET POLICE & CRIME COMMISSIONER DAVID SIDWICK

DORSET POLICE

PRODUCED BY DORSET OPCC AND DORSET POLICE

HOW TO PROTECT YOURSELF

Avoid clicking on unexpected links or opening attachments, even if they appear to come from HMRC or another trusted organisation. Instead access services by going to the official website address.

Never share personal information, bank details, passwords, or security codes with anyone. HRMC and other legitimate organisations will never ask for this information.

Be cautious of messages or phone calls that pressure you to act quickly or create urgency. If something feels pressured, slow down, take your time and hang up the phone before contacting the organisation directly on trusted and verified contact details.

Crucially, ensure multi-factor authentication is enabled on your emails and other important accounts. This adds an extra layer of security if your login details become compromised.

Finally, ensure suspicious communications are reported and delete them once you have done so.

WHERE TO REPORT A SCAM

Forward emails to: **report@phishing.gov.uk**

Forward text messages (SMS) to: **7726**

Report Fraud at: **https://www.reportfraud.police.uk/** or by calling **0300 123 2040**

Report suspicious websites at:
https://www.ncsc.gov.uk/section/about-this-website/report-scam-website

Report scam adverts to:
https://www.asa.org.uk/make-a-complaint/report-an-online-scam-ad.html

While this article focusses on Self-Assessment tax scams, the warning signs and protective measures apply to most scams affecting businesses.

Criminals rely on urgency, authority, and pressure to persuade people into acting quickly without checking. By slowing down, questioning unexpected messages, and verifying information through trusted and verified communication channels, businesses can reduce the risk of falling victim to tax scams and other forms of fraud throughout the year.

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