



Jeremy Collins <bucklandnewtonwebmaster@gmail.com>

Broadband and Mobile Provider Account Takeover and Identity Fraud Alert

[#726659619]

1 message

Dorset Police via Neighbourhood Alert <alert@neighbourhoodalert.co.uk>

4 August 2026 at 09:31

Reply-To: reply@neighbourhoodalert.co.uk

To: bucklandnewtonwebmaster@gmail.com

A member of our community has reported a concerning scam that may affect customers of any broadband



Broadband and Mobile Provider Account Takeover and Identity Fraud Alert

A member of our community has reported a concerning scam that may affect customers of **any broadband or mobile phone provider**.

What Happened?

The victim discovered their broadband service had stopped working and contacted their provider's customer services.

During the call, they were informed that:

- A new mobile phone and accessories had been ordered on their account.
- A credit check had been completed in their name.
- Nobody in the household had placed the order.

Fortunately, the order was cancelled before the items were dispatched.

However, while reviewing their bank account, the victim also discovered that:

- A new Direct Debit had been set up for mobile services they had never requested.
- They had never had a mobile contract with that provider.

The provider advised that similar incidents are becoming increasingly common.

How Criminals May Be Operating

Fraudsters may be:

- Taking over existing customer accounts using stolen login details.
- Accessing personal information obtained through phishing emails, scam calls or data breaches.
- Using compromised email accounts to reset passwords and intercept security messages.
- Using stolen personal details to pass security checks and order devices on credit.

Their aim is often to obtain expensive phones, tablets, smart watches or accessories and then sell them on for profit while leaving the victim to deal with the consequences.

Warning Signs

Be alert if you notice:

- ✓ Unrecognised credit searches on your credit report.
- ✓ Emails or texts about orders you have not placed.
- ✓ New Direct Debits appearing on your bank account.
- ✓ Password reset notifications you did not request.
- ✓ Mobile devices, SIM cards or accessories arriving unexpectedly.
- ✓ Loss of access to your online account.

What to Do If You're Affected

- Contact your provider immediately and report the suspected fraud.
- Contact your bank on 159 and cancel any unauthorised Direct Debits.
- Change passwords for:
 - Your provider account
 - Email account
 - Banking apps
- Enable Two-Factor Authentication (2FA) where available.
- Check your credit file for unauthorised applications or searches.
- Report the incident to **Report Fraud**.
- Consider **CIFAS Protective Registration** if your personal information may have been compromised.

STOP! THINK FRAUD

If you receive an unexpected call claiming to be from your broadband or mobile provider:

- Never share passwords or one-time security codes.
- Never provide banking details unless you initiated the contact.
- Be cautious of offers for discounts, upgrades or free devices.
- Hang up and contact your provider using a trusted number from their official website or your bill.

If something doesn't feel right, trust your instincts and verify independently.

Get 24/7 fraud protect advice about any type of fraud call **Ask Damian** on 01202 144688

Please share this alert with family, friends and vulnerable relatives to help prevent others becoming victims of this type of fraud.

Reply

Share

Rate



Message Sent By
Damian Cranny
(Dorset Police, Fraud Protect Officer, Dorset)

Your Dorset Alert account...

[My Local Area](#)

[Message Preferences](#)

[System Support](#)

[Login](#)

[Unsubscribe](#)



You are receiving this message because you are registered on Dorset Alert. Various organisations are licensed to send messages via this system, we call these organisations "Information Providers". Please note that this message was sent by Dorset Police and that Dorset Police does not necessarily represent the views of Dorset Alert or other Information Providers who may send you messages via this system.

You can instantly review the messages you receive and configure which Information Providers can see your information by clicking [here](#), or you can unsubscribe completely, (you can also review our terms and conditions and Privacy Policy from these links). Alternatively, please email unsubscribe@neighbourhoodalert.co.uk and our team will action your request manually within ten working days.

This email communication makes use of a "Clear Image"(gif) to track results of the email campaign. If you wish to turn off this tracking for future emails, you can do so by not downloading the images in the e-mail itself. All links in the body of this email are shortened to allow click through monitoring.

VISAV Limited is the company which built and owns the Neighbourhood Alert platform that powers this system. VISAV's authorised staff can see your data and is registered with the Information Commissioner's Office as the national Data Controller for the entire database. VISAV needs to see your data in order to be able to manage the system and provide support; it cannot use it for commercial or promotional purposes unless you specifically opt-in to Membership benefits. Review the website terms.