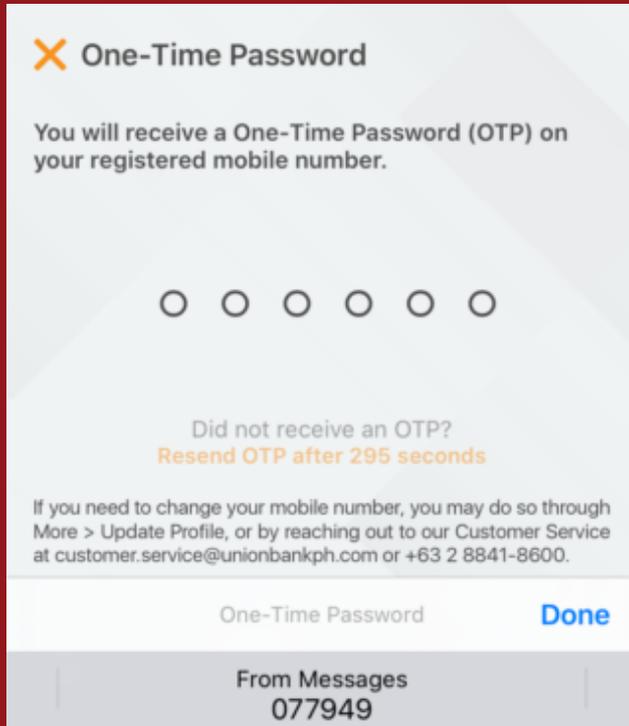




# TARIAN

## MONTHLY FRAUD ALERT

FEBRUARY 2024



### ACCOUNT TAKEOVERS

Account takeover fraud is a form of identity theft that involves unauthorised access to a victim's online accounts to enable financial crimes.

Fraudsters have made efforts to gain control of mobile or email accounts so they can intercept one-time passwords or password change instructions to retain control of the account. **Never repeat a one-time password to anyone online, or on the phone.**

Once fraudsters have control of one account, they can use it to access other personal information to breach additional accounts.

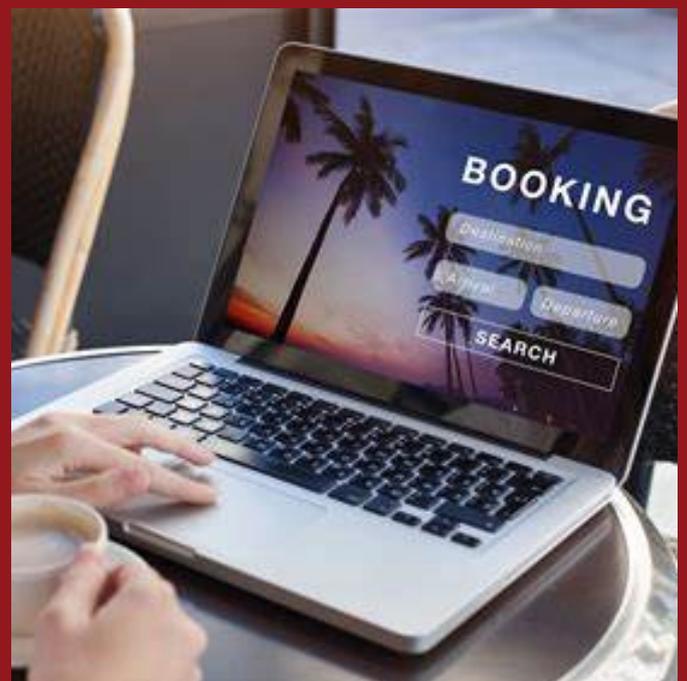
### HOLIDAY FRAUD

Last year, there were 255 recorded reports of Holiday Fraud in the South Wales region. These reports amounted to a loss of over £457,041.

Holiday makers are encouraged to take precautions and do their research online to ensure holidays are booked safely, without a hitch. The four main ways that holiday frauds circulate are through:

- Fake accommodation deals
- Cloned holiday booking websites
- Fake cancellation refunds
- Scam giveaways

If they're a member of the **Association of British Travel Agents**, report them.



If you think you've uncovered a fraud, been targeted by a fraud or fallen victim to fraudsters, contact Action Fraud on [0300 123 2040](tel:03001232040) or via the Action Fraud website.



# TARIAN

## MONTHLY FRAUD ALERT

FEBRUARY 2024



### COURIER FRAUD

We have had several reports of courier fraud this month, specifically from fraudsters posing as Police Officers. They will claim that someone has either been arrested with the victim's card or that they have arrested a family member with their card.

Victims are then asked visit their bank to withdraw their money, withdraw foreign currency from an exchange or to purchase an expensive item to hand over to a courier for examination who will also be a fraudster.

The Police will **never** contact you like this.

### HOME IMPROVEMENT SCAMS

Recently we've been made aware of victims receiving unsolicited calls from individuals claiming to work for a loft insulation company or an "energy hub". It is important to be aware of anyone trying to contact you to carry out home improvements at a low cost.

These scammers can contact you in many ways:

- By a knock at your door.
- By phone call.
- Via social media.
- By email.
- By text message.



If you think you've uncovered a fraud, been targeted by a fraud or fallen victim to fraudsters, contact Action Fraud on [0300 123 2040](tel:03001232040) or via the Action Fraud website.

## **Advice**

Always remember: if something seems too good to be true, it probably is.

Never give anyone your bank PIN or National Insurance number.

Shred or tear up any letters that include your personal details.

Always log on to a website directly rather than clicking on links in an email.

Never send money to anyone you don't know or trust, whether in the UK or abroad, or use methods of payment that you're not comfortable with.

Create strong passwords.

Never use the same password for everything.

Never tell anyone answers to your security questions.

## **Reporting**

If you think you've uncovered a fraud, been targeted by a fraud or fallen victim to fraudsters, contact Action Fraud on 0300 123 2040 or via the Action Fraud website.

If you have been a victim of Fraud, contact your bank immediately.

## **Support**

Take 5 - <https://www.takefive-stopfraud.org.uk/>

Citizens Advice - <https://www.citizensadvice.org.uk/wales/>

Crime Stoppers - Call [0800 555 111](tel:0800555111)

Age UK - Call 0800 678 1602

Victim Advice Line - Call [0800 952 3000](tel:08009523000)