



### **What's in the toolkit?**

Our monthly partner packs have a range of resources to help you support Take Five:

- Key messages and advice
- Assets
- Template social media posts

### **How can you help?**

There are a range of ways to get involved and support consumers, this might include:

- Posting on social media
- Including information in newsletters
- Sharing with internal colleagues

### **This month, we're focusing on:**

1. Purchase scams – January sales
2. Impersonation scams – deliveries and utility companies
3. New Year's Resolutions – get scam savvy

We will be sharing content across our channels throughout the month. You can re-post and share our content, or post your own content using the key messages and template posts below. If you need any support in using this partner pack, please contact us at: [takefive@ukfinance.org.uk](mailto:takefive@ukfinance.org.uk).

**[Download your January assets now](#)**



## **Key messages:**

Criminals are experts at impersonating people, organisations and the police. They spend hours researching you for their scams, hoping you'll let your guard down for just a moment. Stop and think. It could protect you and your money.

- **STOP:** Take a moment to stop and think before parting with your money or information
- **CHALLENGE:** Could it be fake? It's ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **PROTECT:** If you think you've been scammed, contact your bank immediately and report it to Action Fraud.

## **Advice this month:**

### **1. Purchase scams**

A purchase scam is where a person makes a payment for goods or services that never turn up. Criminals often advertise products such as phones, cars or computers at low prices to attract buyers, persuading them to make bank transfers, then disappearing once the payment is made.

Remember to:

- Do your research and read online reviews to check websites and sellers are genuine.
- Be suspicious of any 'too good to be true' offers or prices.
- Use secure payment methods recommended by reputable retailers and be wary of bank transfers.
- Pay by credit card for purchases over £100 if you can.
- Avoid clicking on any links from adverts on social media or email – always go to a trusted retail site directly.

Purchase scams are the most common type of Authorised Push Payment (APP) fraud. A total of £40.9 million was lost to purchase scams in the first half of 2023.<sup>1</sup>

---

<sup>1</sup> [UK Finance Half Year Fraud Report 2023](#)



## 2. Impersonation scams

An impersonation scam is where a criminal contacts you claiming to be from a trusted organisation such as: your bank, the police, a delivery or utility company, a communication service provider, or a government department such as HMRC. They may also pretend to be someone you trust such as a friend or family member.

They then convince you to share personal or financial details, or make a payment. Sometimes they will try to get 'remote access' to your computer by downloading software.

Remember:

- Be wary of unexpected requests for your personal or financial information.
- Don't give anyone remote access to your computer following an unexpected call or message.
- Avoid clicking on links in emails, messages and social media.
- Only criminals will try to rush and panic you.
- Take Five when faced with any requests for personal or financial information.

A total of £76.1 million was lost to impersonation scams during the first six months of 2023.<sup>2</sup>

## 3. New Year's Resolutions – get scam savvy

New Year, new you – set yourself a New Year's Resolution to get scam savvy for 2024!

Criminals will say and do anything to get your money, and scams are becoming more and more sophisticated. [Find out more](#) about different types of scams and how to protect yourself.

Test yourself on the [Take Five 'Get Scam Savvy' quiz](#) now.

---

<sup>2</sup> [UK Finance Half Year Fraud Report 2023](#)



## Template social media posts

Platform	Copy	Asset
Facebook, LinkedIn, Instagram (post 1 asset)	<p>Remember the #TakeFive advice to avoid purchase scams in the January Sales:</p> <p>⚠️ Be suspicious of any 'too good to be true' offers or prices</p> <p>⚠️ Use the secure payment method recommended by reputable online retailers and auction sites</p> <p>⚠️ Where possible, use a credit card when making purchases over £100 and up to £30,000 - as you receive extra protection</p> <p>⚠️ Do your research and read online reviews to check websites and sellers are genuine</p> <p>#StopChallengeProtect 🙌👍👍</p>	
Twitter (post 1 asset)	<p>Making purchases online? Beware of:</p> <p>⚠️ Offers that seem too good to be true</p> <p>⚠️ Requests for payment by bank transfer</p> <p>⚠️ Fake email receipts and email addresses that don't match the genuine sender's</p> <p>⚠️ Websites that are only days/weeks old</p> <p>#TakeFive</p>	

## Take Five to Stop Fraud

### January Partner Pack



Facebook, LinkedIn, Instagram (post 2 asset)	<p>Been told you missed a delivery?</p> <p>Be wary of clicking on links in emails and texts.</p> <p>STOP: Do you remember ordering anything? If you did, check the delivery company specified in the order confirmation.</p> <p>CHALLENGE: Is it the same? Does it have the correct email domain?</p> <p>PROTECT: If you think you've been scammed, contact your bank immediately and report it to Action Fraud.</p> <p>#TakeFive #StopChallengeProtect</p>	An advertisement on a yellow background. At the top, a black banner contains the text 'BEEN TOLD YOU'VE MISSED A DELIVERY?' in white. In the bottom left corner, there is a small black handprint logo with 'TAKE FIVE' and 'TO STOP FRAUD' below it. In the bottom right corner, there is a brown cardboard shipping box with a white label that has a red header and some illegible text.
Twitter (post 2 asset)	<p>Been told you missed a delivery?</p> <p>STOP: Do you remember ordering anything? If so, check the delivery company specified in the order confirmation.</p> <p>CHALLENGE: Does it have the correct email domain?</p> <p>PROTECT: If you think you've been scammed, report it to your bank &amp; Action Fraud.</p>	

## Take Five to Stop Fraud

### January Partner Pack



Facebook, LinkedIn, Instagram (post 3 asset)

#StopChallengeProtect when you receive a message requesting your personal or financial information. Remember criminals may impersonate utility companies hoping to trick you into handing over your personal or financial information.

⚠ Beware of suspicious links

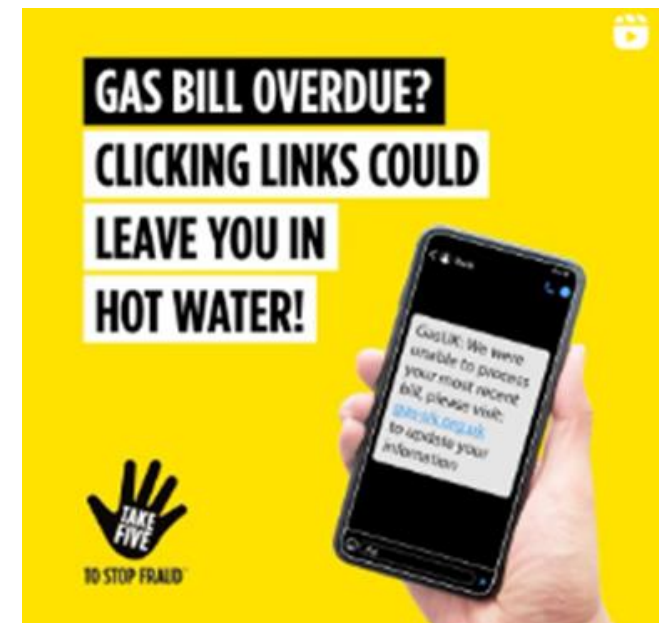
⚠ Just because someone knows your basic details doesn't mean they're genuine

⚠ Don't give anyone remote access to your computer following a cold call or unsolicited message

Report suspicious text messages by forwarding the message to SMS number 7726, which spells out SPAM on a phone keypad. You can also report suspicious phone numbers by texting 'CALL' to 7726 and following the prompts.

If you think you've been scammed, contact your bank immediately and report it to Action Fraud. If you're in Scotland, report to Police Scotland directly by calling 101.

#TakeFive



## Take Five to Stop Fraud

### January Partner Pack




Twitter (post 3 asset)	<p>#TakeFive if you receive a message requesting your personal/financial info.</p> <p>⚠️ Beware of suspicious links</p> <p>⚠️ Just because someone knows your basic details doesn't mean they're genuine</p> <p>⚠️ Don't give anyone remote access to your computer following an unsolicited message</p>	
Facebook, LinkedIn, Instagram (post 4 asset)	<p>Found a bargain on household bills such as WiFi or Broadband?</p> <p>Stop: Take a moment to stop and think.</p> <p>Challenge: Could it be fake? Do your research on the company and check online reviews.</p> <p>Protect: If you think you've been scammed, call your bank and report it to Action Fraud immediately.</p> <p>#TakeFive #StopChallengeProtect 🙅👍👏</p>	

## Take Five to Stop Fraud

### January Partner Pack



Twitter (post 4 asset)	<p>Found a bargain?</p> <p>Stop: #TakeFive to stop and think.</p> <p>Challenge: As yourself – could it be fake?</p> <p>Protect: If you think you've been scammed, contact your bank and report it to Action Fraud.</p> <p>#StopChallengeProtect 🙌👍👏</p>	
Facebook, LinkedIn, Instagram (post 5 asset)	<p>New Year, New You?</p> <p>Get Scam Savvy for your New Year's resolution and test your knowledge on the Take Five Quiz.</p> <p>Get your family and friends involved to see how much you know and how you can protect yourself from scammers by remembering to #TakeFive when faced with personal or financial information.</p> <p>#TakeFive #StopChallengeProtect</p> <p><a href="https://quiz.takefive-stopfraud.org.uk/">https://quiz.takefive-stopfraud.org.uk/</a></p>	



## Take Five to Stop Fraud

### January Partner Pack



Twitter (post 5 asset)	<p>New Year, New You?</p> <p>Get Scam Savvy for your New Years resolution and take the Take Five Quiz to test your knowledge.</p> <p>#TakeFive #StopChallengeProtect</p> <p><a href="https://quiz.takefive-stopfraud.org.uk/">https://quiz.takefive-stopfraud.org.uk/</a></p>	
------------------------	---	--