**A logo for a company

Description automatically generatedA blue text on a white background

Description automatically generatedA black text on a white background

Description automatically generated**

**Paul Fox – Regional Manager SW**

**Money and Pensions Service**

**October 2024**

**Fraud and Scams Awareness**

Fraud and scams can be known by many different names, but let us not forget exactly what it is – it is theft, pure and simple. No one thinks tends to think they be a victim of fraud or caught out by a scam, but it happens far more than you might think. This article is designed to help you understand some of the different ways you might be scammed, and how to recognise them so you can be more confident you can spot one. If the worst does happen, we can help you understand what to do next and who you need to contact to report a scam.

**  **

**Different Types of Scams**

Phishing - Vishing - Authorised Push Payment – Pharming – Smishing … Do any of these sound familiar?

**Phishing** **-** This is an email scam where it appears you have a message from a legitimate source, such as HMRC, PayPal, Apple or Amazon. You will encouraged you to click a link and log into your account, often by telling you your account has been locked or frozen or there has been a suspicious transaction. In reality, the link in the email takes you to a fake website which gathers your information.

* **Action** - Look at how you are addressed in the email. Scammers tend to use a general greeting such as Dear Sir/Madam or Dear Customer, whereas legitimate emails will use your name.
* **Action** - Check the email address the message has been sent from. If it is a real message, it will come from a recognisable address – such as ‘noreply@bank.com’. Scammers won’t be able to send messages from a real domain name, so the email addresses might be filled in with random letters or numbers, such as ‘noreply@1234.bank.com’, or have deliberate spelling mistakes.
* **Action** - Never click the link in an email if you are even remotely suspicious

**Vishing -** Vishing is when scammers call and pretend to be from your bank, building society or even a government agency. During the call, fraudsters will try to get you to reveal personal details, or to transfer money out of your account. Scammers may use ‘number spoofing’ which usually involves changing their caller ID when making a phone call. It can be very difficult to spot vishing. The big clue is that the caller will be desperately to get you to reveal your information, which no legitimate caller would ask you to do.

* **Action** - If you think the call is fraudulent, just hang up the phone.
* **Action** - If you’re not sure, hang up the phone and call your bank/building society on the number on your debit or credit card. This means you can be sure you’re going to the right people. And if there is a problem, they can tell you about it
* **Action** - Be careful. Scammers can hijack your phone line. So when you hang up, wait a few minutes before calling your bank or building society or use a different phone.

**Authorised Push Payment -** The aim of this scam is to get you to voluntarily send, or authorise, a payment to the scammers. This scam can often occur when you’re in the process of buying a house, having building work done on your home or booking a holiday. The scammer intercepts a company’s email and sends you a message asking for payment. Because you’re expecting to have to pay a bill, it can be difficult to spot that this is a scam. There’s a new common scam where you might get a text or WhatsApp from a new number, telling you that they are a friend or relative that needs money. The messages can be worryingly convincing. If in doubt, call or message the person they’re pretending to be on their old number to double check.

* **Action** - If you are paying by bank transfer, you need to be 100% confident that you know who the recipient is, as it can be hard to get the money back.
* **Action** - Check the company you expect to be paying sent you the email, and that the bank details match.
* **Action** – Stop and give yourself time to think before you make any transaction

**Pharming -** This is similar to phishing, but instead of sending you an email directly, the scammers target the website you’re visiting. You type in the correct website address, but you then get directed to a fake version, where you inadvertently put in your login details and secure information.

* **Action** - Be observant when you’re logging into or visiting websites and look out for suspicious website addresses.
* **Action** - It’s also important to keep your operating system and anti-virus software up to date.

**Smishing -** These are text message-based scams. Scammers will contact you claiming to be from your bank, saying you need to update your personal details or that there’s an issue. The text might contain a link, like a phishing scam or a phone number to call. The phone number is fake and when you call the fraudsters will attempt to get you to reveal your details.

* **Action -** If in doubt, call the number on your card and find out if they have tried to contact you.
* **Action** - Don’t click any links in text messages. Always go directly to the website and log in as normal.

**What to do if you have been defrauded or scammed**

If you think you’ve been scammed there are some steps you should follow.

* Contact your bank or card provider immediately if you've lost money, so they can start trying to get it back.
* Stop sending money straight away. If the payment has been set up as a Direct Debit, get in touch with your bank to stop this immediately.
* If you’ve been targeted, even if you’re not a victim of it, report the scam to Action Fraud on 0300 123 2040, use the Action Fraud online reporting tool ([www.actionfraud.police.uk](http://www.actionfraud.police.uk))
* Beware of follow-up scams. Sometimes after reporting a scam you might get targeted again by a fraudster who says they can get your money back.
* Regularly check your credit report for applications or activity you don’t recognise.

Finally - it is some very valuable time spent to become more fraud aware. MoneyHelper has some fantastic free resources to help you, and don’t forget to share far and wide with family and friends.

Visit www.moneyhelper.org.uk/en/money-troubles/scams



You can access further independent, impartial and free guidance and support around money and pensions at [www.moneyhelper.org.uk](http://www.moneyhelper.org.uk) or speak to us free in confidence on 0800 138 7777.