Dear,

**RE: SCAMS and Fraud**

We have recently experienced an increase in reports concerning scams and financial frauds, most notably those originating from online transactions. One of the drivers for this has been the effect of the global pandemic and restrictions arising as a result. Most people now have access to the internet in their home but also via their smartphones and tablets; and are increasingly reliant on it. Scammers are organised criminals who are increasingly using text messages or social media as part of their scams.

Scams can come in all varieties and can look genuine and convincing. The tactic of the scammer is to trick you into providing personal or sensitive information, obtain money directly from you, or access your finances.

We have provided some further information below, that you may find useful.

*On the following pages there is also a form that you may be able to complete and return to us that will provide us with further information on the seller or trader that you dealt with. We will review any information received and assess if any further actions can be taken.*

**Rental Fraud**

**Rental fraud happens when would-be tenants are tricked into paying an upfront fee to rent a property.** In reality, the property does not exist, has already been rented out, or has been rented to multiple victims at the same time. Rental fraud is a type of advance fee fraud.

To protect yourself from rental fraud:

* Do not send money to anyone advertising rental properties online until you are certain the advertiser is genuine.
* If you need to secure accommodation in the UK from overseas, seek the help of the employer or university you are coming to, or get a friend, contact or relative to check the property exists and is available.
* Do not pay any money until you or a reliable contact has visited the property with an agent or the landlord.
* Ask for copies of tenancy agreements and any safety certificates such as Gas Electricity or HMO Licence.
* Do not be pressurised into transferring large sums of money. Transfer funds to a bank account having obtained the details by contacting the landlord or agent directly after the above steps have been followed. Be sceptical if you’re asked to transfer any money via a money transfer service like Western Union.

**Scams**

There is a scam for virtually anything and fraudsters tend to exploit the latest trends. The increase in online shopping has led to more scams happening on social media sites such as Facebook and Instagram; where people are tricked into paying for goods or services that don’t turn up or do not exist. There have also been many cases of people buying from websites that do not supply to correct goods or do not supply items at all.

So how can you avoid being scammed?

1. Be careful when buying online. Follow this guidance:

(a) Make sure your online payments are secure, look for the padlock symbol in the address bar;

(b) Double check you are using an authentic website; check reviews, get information from legitimate sources;

(c) Don’t buy from social media platforms until you’ve researched the company or seller;

(d) Don’t accept “friend requests” from people you don’t know;

(e) Avoid bank transfer as a method of payment because it is unsecure. It’s the same as giving cash to someone you’ve just met in the street and never seeing them again;

(f) If the price for something you want to buy seems to be an unbelievable bargain, then stop and think. It’s likely that it’s fake and therefore inferior or even unsafe. It may not even be available;

(g) When buying from private sellers via e-commerce sites such as Gumtree or eBay, check and follow the safety guidance before completing a purchase.

2. Never give out your personal or banking details in response to a phone call, text, email or any other message that has come out of the blue from what appears to be a legitimate source. If you’re unsure, don’t respond. They make the message urgent and they want you to respond immediately. Stop, think and take your time to check it out. Don’t respond out of impulse;

3. If it sounds too good to be true, then it is. You have not won a lottery that has notified you of a win. No lottery will do that. The onus is on the winner to contact the lottery company to claim their prize. Also, do not fall for the “you can’t lose” investment opportunities that are sent to you (e.g. cryptocurrency). If you want to invest, then it is best to do so legitimately and safely by contacting the Financial Conduct Authority (FCA) for guidance;

4. Don’t give your money to Mr or Mrs Right. Romance scams are cruel and sadistic. If you have encountered someone online with whom you have developed a relationship but who has started to ask for money, then this is a big warning sign. Again, stop and think!

5. Be wary of tradespeople knocking on your door offering to do the work because they are in the area or are just passing and noticed a problem with your property. They are likely to demand high upfront costs, inflate prices and may not complete the work.

**How do they get my information?**

These days, the sharing of information is so much easier with so much technology at our fingertips. It is quite possible that you have shared your personal details without being aware of it. Your information is obtained by various means, such as:

(a) Using automated software to generate phone numbers and email addresses;

(b) Enticing people to enter their details on fraudulent websites;

(c) Fake social media accounts;

(d) Hacking into legitimate websites to gather users’ details;

(e) Buying lists from other scammers.

If you respond to a suspicious message, then the scammer knows that your contact details exist, and this leads to them sending many more messages. No matter how tempted you may be to reply, DON’T DO IT! Simply delete the message or report the any e-mails to the National Cyber Security Centre (details at the end of this letter).

**Covid 19**

Fraudsters are using the Covid vaccine to trick people into handing over money and their banking details. The scammers are using convincing text messages, emails or phone calls to claim that they are contacting you from the NHS or your pharmacy to try and convince you that you are eligible for the vaccine. In light of this, be aware of the following:

(a) The vaccine is free. The NHS will never ask for payment;

(b) The NHS would never ask for your bank details;

(c) The NHS would never send someone to your home unannounced to administer the vaccine;

(d) The NHS would never ask you to send them copies of your personal documents such as a passport or driving license to prove your identity. The main Covid vaccine scams to be aware of are:

(e) Text Messages – the message asks you to press a number on your phone keypad or to reply with a message to confirm that you wish to receive the vaccine, which is likely to result in a charge being applied to your phone bill and fraudsters colleting your personal information to be used again;

(f) Phone Calls – the caller offers the vaccine for a fee or asks for your bank details;

(g) Websites – fake links to convincing-looking NHS vaccine booking forms, which look like official NHS forms and may contain some of your basic personal information already but, at the end of the form, you will be asked for your bank details;

(h) In Person – fraudsters are knocking on doors unannounced pretending to be from the NHS to administer the vaccine there and then, in exchange for a cash payment.

**Helpful Links**

More information about online scams can be found by visiting the National Cyber Security Centre (NCSC) at <https://www.ncsc.gov.uk/section/information-for/individuals-families> and phishing e-mails can be forwarded directly to them using this e-mail address [report@phishing.gov.uk](mailto:report@phishing.gov.uk) The NCSC will analyse the suspect email and any websites it may be linked to; they will use any additional information you’ve provided to look for and monitor suspicious activity.

Help with identifying scams and knowing how to warn you family and friends can be found by visiting <https://www.friendsagainstscams.org.uk/>

More general information regarding scam can be found on our website <https://www.srs.wales/en/Consumer-Advice-Safeguarding/Scams.aspx>

If you or someone you know has been affected by loan sharks in person or online, please visit <https://www.srs.wales/en/Wales-Illegal-Money-Lending-Unit/Wales-Illegal-Money-Lending-Unit-WIMLU.aspx>

Yours faithfully

**TRADING STANDARDS TEAM, SHARED REGULATORY SERVICES**

Mae’r Cyngor yn croesawu gohebiaeth yn Gymraeg a Saesneg a byddwn yn sicrhau ein bod yn cyfathrebu â chi yn yr iaith o’ch dewis, boed yn Saesneg, yn Gymraeg neu’n ddwyieithog cyhyd â’n bod yn ymwybodol o’ch dewis. Cysylltwch â [safonaucymraeg@bromorgannwg.gov.uk](mailto:safonaucymraeg@bromorgannwg.gov.uk) i nodi dewis iaith. Os na fyddwn yn derbyn eich dewis iaith, byddwn yn parhau i gyfathrebu â chi yn unol â’r weithdrefn bresennol. Ni fydd gohebu yn Gymraeg yn creu unrhyw oedi.

The Council welcomes correspondence in English or Welsh and we will ensure that we communicate with you in the language of your choice, whether that's English, Welsh or in Bilingual format as long as we know which you prefer. Please contact [welshstandards@valeofglamorgan.gov.uk](mailto:welshstandards@valeofglamorgan.gov.uk) to register your language choice. If we do not receive your language choice, we will continue to correspond with you in accordance with current procedure. Corresponding in Welsh will not lead to any delay.

|  |  |  |  |
| --- | --- | --- | --- |
| **For Office use** | Your Ref: | S/R Ref: | Officer: |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SCAM / FRAUD REPORTING FORM** | | | | |
| **CONSUMER DETAILS** - details of the person who purchased the goods/service below | | | | |
| **Name:** |  | **Telephone Number:** | |  |
| **Address:** |  | | | |
| **E-mail:** |  | | **Postcode:** |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| If you are reporting this matter on behalf of somebody else, please provide your details below | | | | |
| **Name:** |  | **Telephone Number:** | |  |
| **Address:** |  | | | |
| **E-mail:** |  | | **Postcode:** |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **BUSINESS / SELLER DETAILS** - details of the business/ seller of the goods services (if known) | | | | |
| **Name:** |  | **Telephone Number:** | |  |
| **Address:** |  | | | |
| **E-mail:** |  | | **Postcode:** |  |
| **Website Address:** |  | | | |

|  |  |
| --- | --- |
| **Facebook Username:** |  |
| **Facebook URL/web address:** |  |

|  |  |
| --- | --- |
| **Instagram Username:** |  |
| **Instagram URL/web address:** |  |

|  |  |
| --- | --- |
| **eBay ID or Username:** |  |
| **eBay URL/web address:** |  |

Example of a URL/ web address (normally located towards the top-left of a web page)

|  |
| --- |
|  |

|  |  |  |  |
| --- | --- | --- | --- |
| **For Office use** | Your Ref: | S/R Ref: | Officer: |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **TRANSACTION / COMPLAINT DETAILS** | | | | | | |
| **Date of Payment:** | |  | | **Amount Paid:** | |  |
| **Method of Payment:**  ***(i.e. Bank Transfer, PayPal, Debit Card, Credit Card)*** | | |  | | | |
| Sellers bank details *(if known)* | | | | | | |
| **Sort Code:** |  | | **Account Number:** | |  | |

|  |
| --- |
| **Your account of events**  Provide in the space below as much information about what has happened as possible.  Include any relevant dates and communications you have had with the seller.  **Where applicable, include the exact website address (URL) of any website advert on which the goods/services you purchased were being advertised.**  Please attach any relevant screenshots you may have taken and any emails or receipts you may have been provided with during the transaction.  ***Please continue overleaf and on additional pages if required.*** |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |  |  |  |
| --- | --- | --- | --- |
| **For Office use** | Your Ref: | S/R Ref: | Officer: |

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |  |  |
| --- | --- | --- |
| Are you willing to provide a written witness statement?  Note - If formal action is taken any witness statement you have provided may be used as evidence in court proceedings and you may be asked to attend court to give evidence in person? | **YES** | **NO** |
| Do you consent to the Shared Regulatory Services sharing the information you have supplied in this form with other Trading Standards departments?  Note - The Information will only be shared for the purposes of providing intelligence, investigating or taking enforcement action. | **YES** | **NO** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Consumer Declaration** – I confirm that, to the best of my knowledge, the information I have provided in this form is true: | | | |
| **Signed:** |  | **Date:** |  |

|  |
| --- |
| Please return the completed form to:  [TradingStandards-SRSWales@valeofglamorgan.gov.uk](mailto:TradingStandards-SRSWales@valeofglamorgan.gov.uk)  or  Trading standards Team, Shared Regulatory Services,  Room 116, County Hall, Atlantic Wharf, Cardiff, CF10 4UW |