Scams

Supplement to the MKSSG Newsletter 11 includes a document from Trading Standards, MK Council, followed by information contributed by member Justine.

Advice on scams from Trading Standards Office, Milton Keynes Council

Covid-themed

Whilst most of society is law abiding, it is a sad fact that some individuals see the COVID-19 crisis as an opportunity to prey on the uncertainty which most of us are currently experiencing. We are all aware of the term 'scam' and may have even experienced a scam at one level or another, it is important now to recognise that these unscrupulous individuals have adapted their methods to exploit the current situation.

As a consumer protection authority, Milton Keynes Council Trading Standards is all too familiar with the latest scams brought about by COVID-19 and would like to bring some of the most recent to your attention and help you avoid falling victim to the perpetrators of these crimes.

As we look to keep ourselves safe and take protective measures during the pandemic, you may be looking to purchase **personal protective items** such as hand sanitisers or face masks which are known to be in short supply and fraudsters know this, so Trading Standards are warning the public to only make this type of purchase from reputable retailers as many fake hand sanitisers and untested face mask have already been found on sale. In addition to this, we have received reports that some online sellers have accepted payment for these products but in reality don't have the goods to send – it's all a scam.

Other types of scams which have been adapted by criminals are phone calls and email scams. Any **unsolicited phone calls and emails** that you receive should be treated with extra caution and if they are asking for personal details or payment for something, it is highly likely that it is a scam. If you receive a phone call and you are unsure whether the person calling is really from the organisation or business they claim, such as the police or bank for example, we recommend that you hang up and call the organisation or business on a known number to verify the caller is genuine – if it is genuine, the caller won't mind at all! With any suspicious emails you are advised not to download or click on anything until you can be absolutely certain of the sender – again check with the organisation. If you do receive a suspicious email it can be forwarded to report@phishing.gov.uk where they can check the legitimacy of the sender.

Scams are widespread and there have been reports of **cold-callers knocking at doors**, particularly the elderly, claiming to be from 'the health authority' selling virus testing or anti-virus kits; there are reports of 'charities' collecting donations for the NHS and cold-callers offering to do shopping for vulnerable people in self-isolation at their homes with the criminal claiming to represent a charity before taking their money and never returning with shopping – all of which are scams.

Christmas-themed

We all know about the 12 days of Christmas and who wouldn't like to have 5 gold rings as a present? Unfortunately we can't help you with the rings but we can give you some golden nuggets of wisdom about scams to be aware of this Christmas.

Dangerous E-cards – e-cards are a fun and inexpensive way of sending cards and you can get the whole family involved. Scammers can send fake versions that may include malware such as viruses. There is an easy way to protect your devices – do not open an e-card if it comes from someone you don't know.

Holiday SMishing – most of us have mobile phones or tablets these days and with them comes the risk of Smishing – phishing with text messages rather than emails in order to obtain sensitive information from you, like your bank account details! At Christmas we often buy gifts and food etc ready for the holiday. These scammers can pretend to be banks or other organisations requiring your details urgently for security purposes and often their texts come with a warning that your account may be closed if you do not respond. It is very unlikely that your bank will ask for this information by text message so don't panic into replying but call your bank instead to confirm that they have asked for your details.

Bogus Gift Cards – make sure your gift card is official. Adverts for deals on gift cards can appear on lots of social media sites. Our advice would be to buy them directly from the retailer, so that you avoid leaving the recipient of your card embarrassed, when the store in question won't accept the unofficial gift card.

Mobile App Scams – The festive season often prompts the launch of new mobile apps. Shoppers should think twice about downloading a new app as they can carry malware designed to steal personal data. The best advice is to stick to official app stores.

Phoney e-tailers – More and more we are shopping online for Christmas. If you do, beware of fake websites posing as legitimate retailers by checking the names and web addresses carefully for small differences, which might indicate you're dealing with someone other than that seller you thought you were dealing with. Try to stick to retailers that you know and trust and if the item you are buying is more than £100 use a credit card to pay for it, so that your bank will have to assist if anything goes wrong.

Investment opportunity scams – During the height of the lockdown, to June 2020, there was a 27% reported increase in investment scams, with innocent victims losing around £55m of their savings to unscrupulous scammers. Lockdown acted as extra incentive for these criminals as they could target savers who were anxious about the virus and the effect on the economy, so were more easily convinced to invest in an opportunity to increase their savings. The investments can range from wine to Bitcoin, but the forecast returns are never received, the scammers simply disappear with the money.

There is concern that we will see another spike of this type of scam in the lead up to Christmas, especially if the lockdown restrictions are increased again. If you are contacted

and offered a very lucrative investment opportunity which seems more favourable that your bank (where your savings rates may be very low at the moment), please seek advice before investing your hard-earned savings.

It is common for people aged 55+ to be targeted, as they are seen as a group that may be looking to increase their pension pot, but experts fear that, again, the vulnerable and the elderly will also become victims so if you know someone who might be caught out, please warn them about this type of scam or suggest a call blocker to prevent unsolicited phone calls.

Consumer advice: help and reporting

If you think that you have been caught out by any of these scams, or perhaps others, then for consumer advice you should call the Citizens Advice Consumer Helpline on 0808 223 1133 and you might also want to report the incident to Action Fraud on 0033 123 2040 or at https://www.actionfraud.police.uk/ Alternatively you can report any incident direct to Trading Standards by going online to the Milton Keynes Council website and searching for 'Form to report COVID-19 issues to Trading Standards'.

Additional note from MKSSG committee

We have a small number of 'Watch out for scams' booklets (published by National Trading Standards), which were given out in a 2018 MKSSG meeting so many of you will already have copies. Please contact us if you would like one.

Extracts from a document on scams contributed by member Justine

We have selected the following very useful points from Justine's document and listed them in a brief checklist format to make them easy to remember.

- **Avoid any unsolicited or unexpected contact.**
  If you have received any kind of contact, but particularly a phone call, out of the blue, it is best to avoid it. Do not engage in conversation. Be suspicious.
- **Never give out personal information.**
  No legitimate company will ask you for personal details, PIN codes and passwords.
- **Don't make any advanced payments** until you are sure the company you're dealing with is legitimate. [If you are worried or want to report on possible scams, see under 'Consumer advice: help and reporting' section above.]
- **Sign up for a call blocking service like the Telephone Preference Service.**
  This might not stop all scams but it will stop cold-callers. This means any suspicious or unexpected calls you do receive are almost certainly from people you don't want to deal with.
- **[Suspicious] texts: do not click on any links.**
  [See first note below on emails.]

Additional advice mostly for electronic media users

- **[Suspicious] emails: do not click on any links.**
  [For example:] you will receive a message stating your account (to a bank /account you're not even registered with!) has been restricted or suspended and to solve the issue, you need to click on the link within the text. Simply delete the [message].
  If you get an email, expand the pane at the top of the message and see exactly who it has come from. If it is a scam, the email address the message has come from will be filled in with random numbers, or be misspelled. The main body of the email will often have spelling mistakes, poor grammar, differences in font size and colour. Report it. [To do so, see note under 'Consumer advice: help and reporting' section above, and also suspicious emails can be forwarded to report@phishing.gov.uk]
- **Keep operating system and virus protection software up-to-date.**
  Don't ignore updates as these can often include patches to protect against new kinds of scans, viruses and ransomeware. This goes for mobile devices as well.
- **Make sure all accounts have a strong password.**
  Don't use the same password for multiple accounts and change them regularly.
- **Make sure any websites you are using are secure.**
  Check to see if the web address starts with **https**, not just **http**.

Our thanks to Justine for the document she prepared, which supplements the advice given above from Trading Standards.