Cheshire East Age UK

ISSUE 10 JANUARY 2021

SCAMS AWARENESS UPDATE

Older Persons Scams Awareness & Aftercare Project

In this update:

There'll Never be Another You...

...or will there?

Once again, we find ourselves in a national lockdown. Being at home more, we may hear the phone ring or a knock at the door. Whilst we hope it's a friend calling or a delivery we've ordered, these are two ways scammers will try to contact us. We can all familiarise ourselves with top tips to avoid such scams by reading previous bulletins from September and October.

This month, we're focusing on identity theft. This not only leads to many people being scammed out of their hard earned money, but often happens without the victim knowing. There can be long-term, devastating effects on a victim's financial, emotional and mental health prospects. However, by becoming aware, informed and following some top tips, there's lots we can do to keep our information safe from identity thieves.

Remember, information about our Scams Awareness and Aftercare Project, along with further scams awareness resources, is always available on our Age UK Cheshire East website or by contacting Sally Wilson at sally.wilson@ageukce.org or on 07932 999902.

Printing costs funded by David Keane Police & Crime Commissioner for Cheshire

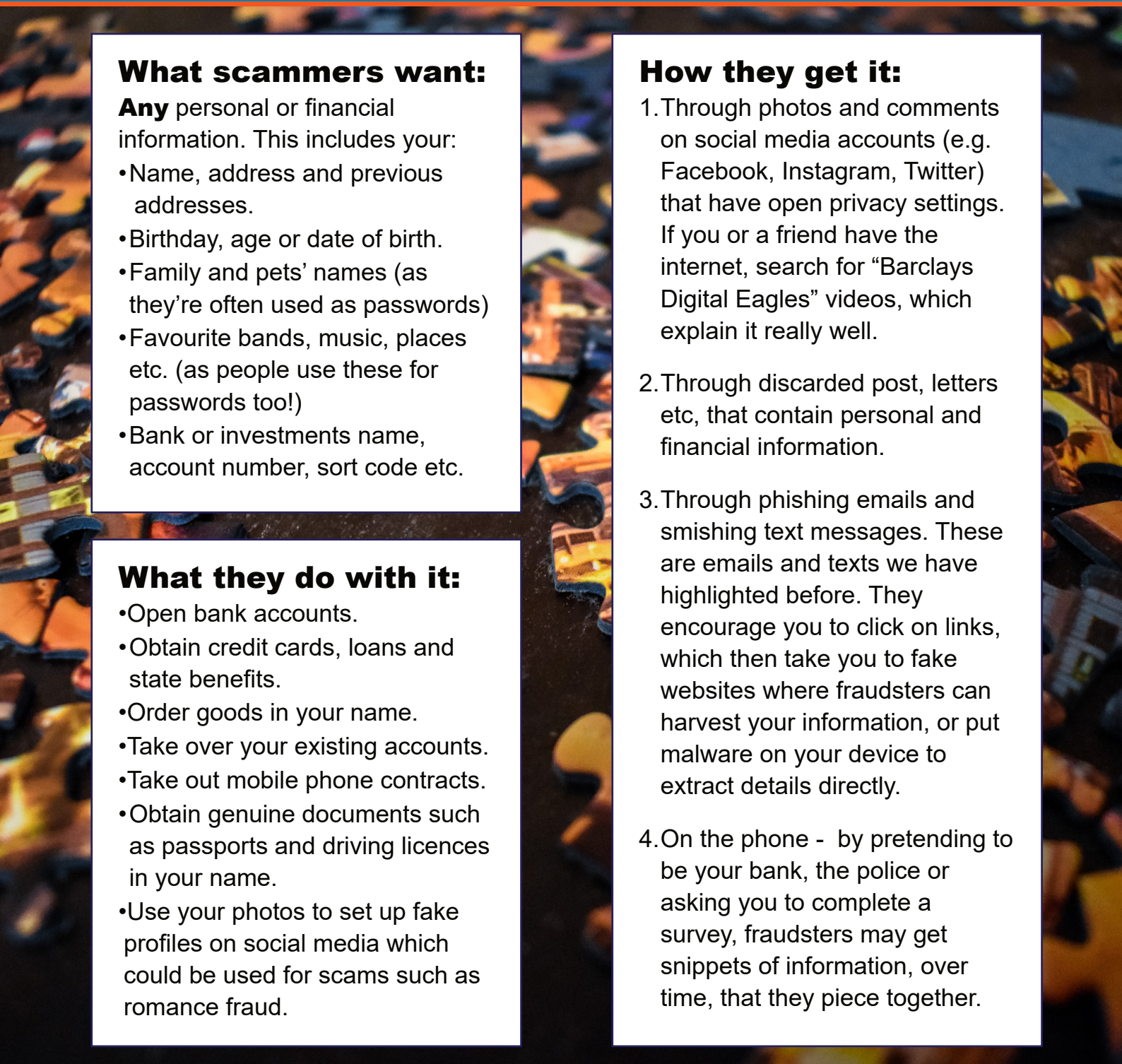
Cheshire East Age UK in partnership with Cheshire East Council Trading Standards funded by Garfield Weston Foundation and Community Fund

IDENTITY THEFT

Identity theft is when your personal details are stolen. Fraudsters are good at jigsaws and piece together the information they've stolen to create another "you". They will collect the information from a range of places, so you don't suspect. Then they use the stolen identity to commit identity fraud.

Cases of identity fraud rose by 18% in 2019 to 223,163, compared to 2018, and accounted for 61% of the cases recorded to the National Fraud Database. There was a 22% rise in victims aged 61+ within the year.

Source: CIFAS Fraudscape 2020



What scammers want:

Any personal or financial information. This includes your:

- Name, address and previous addresses.
- Birthday, age or date of birth.
- Family and pets' names (as they're often used as passwords)
- Favourite bands, music, places etc. (as people use these for passwords too!)
- Bank or investments name, account number, sort code etc.

What they do with it:

- Open bank accounts.
- Obtain credit cards, loans and state benefits.
- Order goods in your name.
- Take over your existing accounts.
- Take out mobile phone contracts.
- Obtain genuine documents such as passports and driving licences in your name.
- Use your photos to set up fake profiles on social media which could be used for scams such as romance fraud.

How they get it:

1. Through photos and comments on social media accounts (e.g. Facebook, Instagram, Twitter) that have open privacy settings. If you or a friend have the internet, search for "Barclays Digital Eagles" videos, which explain it really well.

2. Through discarded post, letters etc, that contain personal and financial information.

3. Through phishing emails and smishing text messages. These are emails and texts we have highlighted before. They encourage you to click on links, which then take you to fake websites where fraudsters can harvest your information, or put malware on your device to extract details directly.

4. On the phone - by pretending to be your bank, the police or asking you to complete a survey, fraudsters may get snippets of information, over time, that they piece together.

AVOIDING BEING AN IDENTITY FRAUD VICTIM

Cheshire East Age UK

Thinking about the information identity thieves are looking for and how they get it, here are some practical things we can do to avoid our information being stolen and used for fraud:

File documents away quickly or shred them. If you don't have a shredder, soak them in a bit of water and screw them up before putting them in the bin.

If you move house, ask Royal Mail to redirect your post for at least a year.

Opt out of the electoral open register. This is the version of the register that's available to anyone who wants to buy a copy. By opting out, your details are less likely to fall into the hands of criminals.

Go paper free - Get receipts, insurance documents, bank and credit statements online.

Check your privacy settings on social media are not set to "public". If you're not sure how to do this, ask a friend or relative to help.

Be careful what you put on social media, even for your friends to see, as you can't guarantee where it will end up. Remember, information can be gathered from several posts and comments to piece together your identity.

Regularly search for your name on the internet and use the reverse picture look up facility on Google. It will show where your name and photos have been used online.

If you receive a call, text or email out of the blue, never share your personal details.

Check all your financial statements carefully. Report anything suspicious to the bank or financial service provider concerned.

If you're expecting a bank or credit card statement and it doesn't arrive, tell your bank or card company. Cancel lost bank, store and loyalty cards or documents right away.

Use a trusted credit agency such as Experian or ClearScore. They'll tell you if a credit check is made in your name.

If you think you have been a victim of identity fraud (e.g. you may have been refused credit, spotted suspicious transactions, or you get bills for goods you never ordered.)
ACT QUICKLY:

Check your bank account - Look for any odd transactions or other changes you didn't make. If you spot anything strange, contact the bank right away.

Change your security questions, user names and passwords on every account you have e.g. bank accounts, online shopping, social media, email etc.

Contact Action Fraud - They can help you to report a crime or give general advice.

Contact Royal Mail - If you think your mail has been stolen or redirected.

Consider registering with **CIFAS**. This could help to protect you and stop fraudsters using your details to apply for products or services in your name.

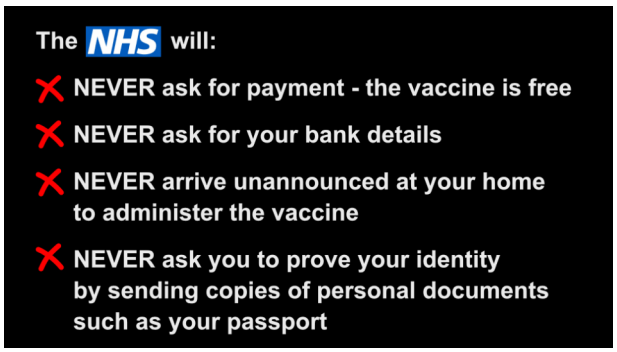
CURRENT SCAMS

Each month we like to alert you to current scams. Here are a few to be aware of:

COVID-19 vaccine scams continue

The mass vaccination is well underway across the country. However, scammers are still taking advantage, as we warned against last month.

Remember:



HMRC Scams as self assessment deadline looms

Fraudsters will be ramping up their activity, claiming to be HMRC, in the run up to the 31 January Self Assessment deadline.

If you receive a text, email or call claiming to be from HMRC that tells you about a tax rebate or penalty or asks for your personal or financial info, it's a scam.

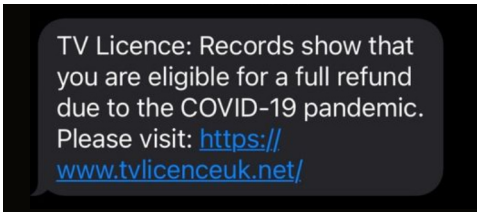
HMRC have examples on their website, along with a list of legitimate reasons they may contact you.

Investment and pension scams

From celebrity endorsed Bitcoin investments, to offers of high returns on bamboo and wine; scammers are taking advantage of the current economic situation to entice people to invest in (non-existent) investments.

If you are approached with an investment or pension opportunity, always check its legitimacy with the Financial Conduct Authority, along with the company's credentials too.

TV licence refund scam returns



As the country has moved in to lockdown #3, this text message scam has returned, offering a refund due to COVID-19. One of the signs it's a scam is that the link is not www.tvlicen**s**ing.**co.uk**.

TV licensing will never send a text message offering a refund of your licence.

COMING NEXT TIME...

- **Current scams**
- **Focus on reporting scams to fight back**

Though we don't like to see you leave, you can unsubscribe from these bulletins by emailing sally.wilson@ageukce.org

The Older Persons Scams Awareness & Aftercare Project is brought to you by

Cheshire East age UK *in partnership with* Cheshire East Council Trading Standards *funded by* Garfield Weston Foundation *and* Community Fund