Cheshire East Age UK

ISSUE 9 DECEMBER 2020

SCAMS AWARENESS UPDATE

Older Persons Scams Awareness & Aftercare Project

In this update:

The Good The Bad and The Ugly!

Let's beat the scammers and use social media for good.

Social media has been part of our lives for around twenty years. Once the domain of the younger generation, older people are exploring its benefits more and more. With the wide range of smartphones, tablets and computers available there's ample opportunity to connect with friends, family and the wider world from the comfort of your sofa or local coffee shop. This has been the case even more this year, with online social interaction replacing face to face contact during the COVID-19 pandemic.

Unfortunately, though, just like on the doorstep, over the phone or through the post, scammers use social media too. However, with the information and top tips in this bulletin we hope you will be more confident to enjoy social media safely, and avoid being scammed.

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

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

SOCIAL MEDIA SCAMS

Cheshire East Age UK

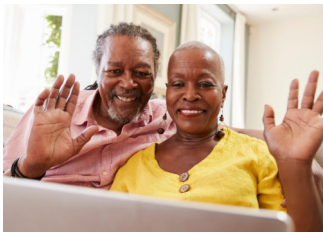
Social media is computer-based electronic technology. It is a way of sharing of ideas, thoughts, and information by building virtual/online networks and communities. Examples include Facebook, Twitter, Instagram, Tik-Tok, WhatsApp and Zoom. However, this is not an exhaustive list, and there are new social media networks developing all the time.

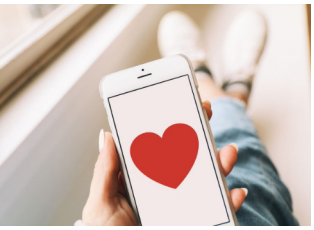
When it comes to scams, social media fraudsters have the same objective as all scammers - their mission is to get you to part with your money, your personal or bank details, or to infect your device so they can steal information from it.

Our mission is to fight back. Here are some social media scams to avoid:

Quizzes have kept the nation going through lockdowns and self-isolation. However, fraudsters sometimes set these up across social media and online to gain personal information, or get people to click on a link which may be full of scams and computer viruses. They can even make it look like it's been sent from one of your contacts.

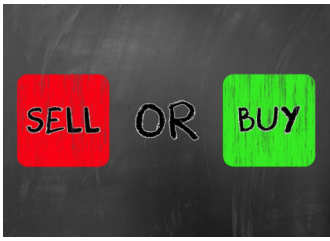
Video conferencing apps such as Zoom, WhatsApp, Facetime and MS Teams have been a wonderful way for families to keep in touch throughout the pandemic. However, scammers are making the most of this by sending fraudulent emails stating there is an issue with your account, and encouraging you to click on a link to rectify it. The link takes you to a fake website asking for personal details or installs malware on your device to extract information.





Facebook, Twitter and Instagram are great for keeping in touch with people. Unfortunately, social media is also a great way for romance fraudsters to befriend their victims, pretend to strike up a relationship and then ask for money. In 2019, £27million was lost to romance fraud and 2 out of 3 romance scams started on social media.

Using social media is a great way to sell items you no longer want. This could be through Facebook groups. Be aware that fraudsters may pretend to be interested in buying an item to get you to direct message them. If your security settings are not tight, this could lead to them having access to your social media profile, which they could use fraudulently.



You may see great offers, promotions by celebrities, or a chance to win a prize on social media such as Facebook, Instagram, Gumtree and WhatsApp. Remember, though, if an offer is too good to be true, it usually is! Fraudsters use these adverts to get you to click on links that send you to fake websites or ask for personal or banking details. You may also unknowingly be signing up for a monthly subscription.

HEALTHY SOCIAL MEDIA HABITS

Keeping safe on social media is the same as keeping safe in your own home. There's lots you can do to lock people out and invite only trusted people in.

Here are some top tips for enjoying social media safely:

Secure your social media profile information. Set your privacy settings so only invited friends and contacts can see information you share.

Be wary of accepting friends requests from people you don't know. Check their social media profile to see if they're genuine, and never send money to social media friends you haven't met in person.

If someone contacts you to buy something you're selling on social media, check out their social media profile, location etc. to see if they are genuine.

Clear your internet search history regularly. Social media adverts are based on this, so you may be tempted to click on an offer for something you want.

Take care when using public WiFi e.g. in cafes and libraries. Scammers can hack these networks to steal your information.

Always log out of your social media account. Closing your internet browser or just returning to your device's home screen may not log you out.

Don't overshare! Avoid posting personal details such as pets and family names, where you live etc. Scammers can use this information to guess passwords or befriend you for romance fraud.

Don't click on links for special offers or to fix a problem with your social media accounts. Always search deals independently online and log in to social media accounts separately.

You can report social media scams to Citizens Advice, either at Report a Scam or by calling 0808 223 1133. They will pass the information on to the right agency, for example, Trading Standards.

If you have been scammed, you are encouraged to report it to Action Fraud on 0300 123 2040 or at www.actionfraud.police.uk.

As always, contact your bank immediately if you have transferred money to the scammer in the last 24 hours or you think your account details or PIN have been stolen.

CURRENT SCAMS

Each month our volunteers let us know about current scams. Here are a few to be aware of:

COVID-19 vaccine scams

It's great news that the COVID-19 vaccine rollout has begun. However, we have already had reports of scam recorded phone messages and emails asking you to press a number or click a link to make an vaccine appointment. You are then asked for financial and personal details.

Remember, the vaccine is free. If you're unsure after receiving a call or email, check with your medical provider.

Premium rate numbers scams

You may receive a call and your mobile phone tells you on the screen its a premium rate number. These can be scams, wanting you to answer or to let it go to voicemail, so the call connects. You're then charged an inflated price for a few seconds phone call (equivalent to £160 per minute).

To avoid incurring a cost from these scams, make sure you reject the call rather than ignoring it and letting it go to voicemail.

DPD delivery scam emails

After mentioning these in our last bulletin, we've had reports of very plausible emails being received locally, pretending to be from DPD, and asking for information in order to deliver a parcel. However, the email address was from a hotmail account, not @dpd.co.uk.

Always check the email address of any communication, as it helps to see if it's genuine.

Shark Attack!

After lots of spending at Christmas, money may be tight in January. Loan sharks will take advantage of this.

Always check with the Financial Conduct Authority that your loan provider is authorised to loan money, before you borrow. Visit www.register.fca.org.uk or call 0800 111 6768.

COMING NEXT TIME...

- **Current scams**
- **Focus on identity theft scams**

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