Community Cyber Ambassador Newsletter (Vol 4. July 2017)

Creating a safer Cambridgeshire

In a (slight) change to the previously advertised topic, this month's newsletter will be giving you advice on how to spot and protect yourself from online scams and frauds.

This July the Citizen's Advice Bureau CAB has declared it to be Scams Awareness Month, giving consumers the skills they need to understand how scammers operate (both online and in the real world) and how to identify a scam before they potentially become victims.

Every day people and businesses are targeted by those trying to extort money or information or even gain access to computers or devices. Some of these approaches can clearly be identified as scams but many others are more subtle in their approach, adopting sophisticated social engineering techniques to manipulate innocent people into taking various actions which lead to them being defrauded. With the increasing use of the internet and technology it is now possible for scammers to contact a larger number of victims than ever before. The most common of these methods are:

1. **Phishing –** Scammers will often use emails, messaging services or even traditional mail as an initial approach to contact their victims. This can be unwanted material which is at best, annoying and at worst, malicious – causing considerable harm to your computer and yourself.
2. **Smishing –**commonly-used name for SMS (text message) phishing – is an activity which

How to protect yourself from Auto fraud

As previously advertised this month's little blue box is dedicated to Auto Fraud.

Technology and the internet has transformed the autotrade business and people's experience of viewing, buying & selling new and used vehicles. It has also made it easier for dishonest buyers and sellers to defraud larger numbers of people, so before you go online consider the following:

- When **buying**, always view the vehicle & check its authenticity against documentation, before parting with any payment & if in doubt, ask an expert. While paying by cash or bank transfer might be cheaper it offers no protection to getting your money back from a fraud. Where possible pay by debit or credit card to give you added protection.
- When **selling**, do not pay any advance 'shipping' fees, and always receive cleared payment in full before handing over the vehicle and paperwork.
- If you receive an email which you believe to be from a fraudster, do not respond. Forward it to the abuse department of the sender's email provider and use your email filter software to block further emails from the sender. Never click on links or download attachments in an unsolicited email.
- If you are asked to phone a premium rate number via SMS or email, check it first with the number checker on Phone-paid Services Authority (PSA) website or via their helpline on 0300 30 300 20 or online at http://psauthority.org.uk.
- If you think you have been a victim of vehicle fraud report it to Action Fraud, the UK's national fraud reporting centre, on 0300 123 20 40 or at www.actionfraud.police.uk. You can also report it to the trading website's team so they can remove an advert and prevent others from being defrauded.
- During July Get Safe Online and VSTAG (Vehicle Safe Trading Advisory Group) will launch a new buyers and sellers checklist and have advice on their websites while Cambridgeshire Constabulary will have further updates through our social media.

enables criminals to steal victims' money or identity, or both as a result of a response to a text message. Fraudsters can target both smartphones or traditional non-internet connected mobile handsets and have even been known to fake (also known as spoofing) legitimate telephone numbers of companies so that it can appear in a string of messages.

3. **Vishing** – a combination word for voice and phishing, fraudsters use the telephone to scam their victims. Telephone Banking Fraud is an increasingly commonplace scam. As with Smishing fraudsters can 'spoof' (fake) telephone numbers so that when displayed it looks like one used by a legitimate company. One way to cut down on the number of nuisance calls you receive is to register your number with the Telephone Preference Service (www.tpsonline.org.uk). Your phone company may also have a blocking service or you may also wish to purchase a call blocking device to limit the number of nuisance calls you receive.

It's important to highlight how professional these approaches have become and that many of us will fall victim to a scam at some point. The Financial Fraud Action UK's **Take 5** campaign has 5 steps you can take to protect yourself from fraudsters:

1. **Never disclose security details, such as your PIN or a full password - it's never okay to reveal these details.**
2. **Don't assume an email request or caller is genuine – no matter how sincere people are not always who they say they are.**
3. **Don't be rushed – a genuine bank or organisation won't mind waiting to give you time to stop and think.**
4. **Listen to your instincts – if something feels wrong then it is usually right to pause and question it.**
5. **Stay in control – have the confidence to refuse any unusual requests for information. Don't be afraid to end a call by hanging up if you feel uncomfortable.**

More information can be found at https://takefive-stopfraud.org.uk/

What else can I do:

- **Get advice** from Citizens Advice consumer service **03454 04 05 06** or get online consumer advice and information at www.citizensadvice.org.uk. The Little Book of Big Scams, the Little Book of Big Scams business edition and the Little Book of Cyberscams cover some of the most widespread scams that fraudsters use. All three are available to download electronically from the Cambridgeshire Constabulary website on the Crimes and Support page under Fraud and Cybercrime.
- **Report** scams and suspected scams to Action Fraud, the UK's national reporting centre for fraud and internet crime **0300 123 2040** www.actionfraud.police.uk. Where debit cards, online banking or cheques are involved in the scam the victim should contact their bank or credit card company immediately as they have the ability to block or freeze payments. Never be afraid or ashamed to report or ask for advice if you think you have been a victim of a scam.
- **Tell** family, friends and neighbours. Some people are embarrassed about sharing this information but you could prevent others from becoming a victim. National Trading Standards **Friends Against Scams** offer free online training at www.friendsagainstscams.org.uk to help raise awareness among communities in the UK or join their Facebook group and post a pledge.

Trading standards also protect consumers and the community against rogue and unfair traders. Report a problem to Trading Standards via the Citizens Advice consumer service.

Next month's newsletter will focus on Safe Social Media