Reporting Scams

Dear Surrey residents
We have had a few queries about how to report scams and what to do if you have been scammed. So this week we've set out below some suggestions.

Reporting
If you have suffered a fraud you can report it to Action Fraud on 0300 123 2040 or report it to Citizens Advice online at https://www.citizensadvice.org.uk/consumer/scams/reporting-a-scam/.

If you just want to report a scam email you can forward it to report@phishing.gov.uk.
You should delete the message once you have forwarded it. E-Mails tend to go to a deleted email folder so it's best to "hard" delete them (Shift + Del).

If you have a scam text you can forward it to 7726. The method for doing this varies between phones and also depending upon whether you have an android phone or an i-Phone. We've set out below some steps to get you started but if your phone does not quite match the procedure below then you might have to check the operating instructions for your individual phone. It can also be a good idea to save 'Report Scam' as a contact in your phone with the number 7726 to save you having to remember the number for next time.

i-Phone

- Open Messages. This is the app with the speech bubble icon found at the bottom of your Home Screen.
- Select a conversation. Chose the conversation that contains the message you want to forward. Scroll to the message in the conversation that you want to resend.
- Tap and hold the message. A menu will appear below the message that allows you to select "Copy," "Speak," or "More."
- You can forward one message or multiple messages. However, you are not able to forward an entire conversation.
- Tap More. A blue checkmark will appear next your selected message. You can tap other messages in the conversation to forward multiple messages.
- Tap Share. This is the curved arrow icon at the bottom of the screen. A new text message window will open.
- Enter 7726 or 'Report Scam' into the "To:" field. This will be the contact who will receive the message you are forwarding.
- You can also tap the blue Plus Sign next to the "To:" field to select a phone number from your list of contacts.
- Tap Send. This is the blue or green upward pointing arrow in the message box. The message you selected will be forwarded to the chosen recipient.

Android

- Open the Messages app on your Android. The Messages icon looks like a white speech bubble in a blue circle on your Apps list. Messages will open up to your inbox.
- Tap a conversation. This will open the chat in full-screen.
- Tap and hold the text message you want to forward. This will highlight the text message, and display a pop-up menu
- Tap Forward or it might be like an arrow icon at the top of your screen. This button will bring up your list of contacts in a new pop-up window.
- If you don't see a list of contacts, tap Contacts at the bottom of the screen.
- Type 7726 or 'Report Scam' where it says 'search contacts or enter number'
- Press '+' or enter and then tap 'Done'

- Tap the Send button. It looks like a paper plane icon in the lower-right corner of your screen. It will forward your text message.

Further guidance can be found on the National Cyber Security Centre website - https://www.ncsc.gov.uk/guidance/suspicious-email-actions.

Protecting

If you are unfortunate enough to have been scammed there are three things you should do:

1. Protect yourself from further risks
2. Check if you can get your money back
3. Report the scam (as above)

First, there are steps you can take to protect yourself from things getting worse. What you need to do depends on what's happened.

For example, if the scammer sends you a message, ignore them, but keep a record of what's happened so you can report it. If you've given the scammer access to your computer so that they can control it remotely, they might have infected your computer with a virus, or stolen passwords and financial information. To stay safe you should:

- reset your passwords
- let your bank know your financial information might have been stolen
- make sure you update your anti-virus software

You could also get an IT professional to check your computer.

If you transferred money to the scammer in the last 24 hours, tell the police immediately by calling 101 or report online at https://www.police.uk/pu/contact-the-police/report-a-crime-incident/.

If you think your account details or PIN have been stolen, contact your bank immediately so they can protect your account. After you've told your bank about the scam, keep an eye on your bank statements and look out for any unusual transactions. Also check your credit score to see if there are applications for credit you don't recognise.

If you think your password could have been stolen, change your password as soon as possible. If you've used the same password on any other accounts you should change it there too. Add 'two-factor authentication' if you can.

If you've lost money there may be ways in which you can get it back – check the Citizens Advice website for some ideas - https://www.citizensadvice.org.uk/consumer/scams/check-if-you-can-get-your-money-back-after-a-scam/

Finally if you are unsure about a website you can check whether it is genuine or not at https://bogusbuster.org/