Using social media

Dear Surrey residents
Your email and social media accounts contain a wealth of personal information about you, which makes them a lucrative target for cyber criminals. Between February 2020 and February 2021, Action Fraud received 15,214 reports about email and social media account hacking. The majority of reports (88%) were made by individuals, with 12% of reports being made by businesses.

Analysis of the crime reports revealed that Facebook, Instagram and Snapchat were the most affected social media accounts, with phishing messages being the most common tactic used by cyber criminals to lure unsuspecting victims.
The motivation behind the hacks are varied and can range from financial gain, to revenge or personal amusement. Some victims are extorted for money, whilst others have their accounts used to send malicious links to their contacts. One victim who had multiple email and social media accounts hacked paid over £2,000 to regain access to them. Another victim reported that her hacked Facebook account was used to trick her friends into sending money into a PayPal account they thought belonged to her.

How to keep hackers out of your email and social media accounts

1: Secure your email accounts
If a hacker gets into your email, they could:
reset your other account passwords
access private information such as contacts, messages or photos.
Your email password should be strong and different to all your other passwords. This will make it harder to crack or guess. Using 3 random words is a good way to create a strong, unique password that you will remember. Enable Two-factor authentication (2FA) in your email account settings, it will help to stop hackers from getting into your account, even if they have your password.
How to change your email password:

Gmail (opens in a new tab)
Yahoo! Mail (opens in a new tab)
Outlook (opens in a new tab)
BT (opens in a new tab)
AOL Mail (opens in a new tab)

2: Enable two-factor authentication (2FA)
If a hacker gets into your social media account, they could:

- access private information such as contacts, messages or photos
- send messages containing malicious links to your followers
- trick friends or followers into sending them money by pretending to be you
- extort you for money in exchange for restoring access to your account.

Use three random words to create a strong, unique password for your social media accounts. Enable Two-factor authentication (2FA) in your account settings, it helps to stop hackers from getting into your accounts, even if they have your password.

How to turn on two-factor authentication (2FA)
For email accounts:

Gmail (opens in a new tab)
Yahoo (opens in a new tab)
Outlook (opens in a new tab)
AOL (opens in a new tab)

For social media accounts:

- Instagram (opens in a new tab)
- Facebook (opens in a new tab)
- Twitter (opens in a new tab)
- LinkedIn (opens in a new tab)

Watch out for suspicious messages.
Be cautious of social media messages that ask for your login details or authentication codes, even if the message appears to be from someone you know.