Keep Your Money Safe

Surrey Police and Sussex Police Fraud Newsletter

In this issue:

Each month we see many incidents of fraudsters targeting our residents in an attempt to defraud them. We're working hard to prevent this and support vulnerable victims of fraud or scams. By following our tips and encouraging family, friends and colleagues to do so too, you can reduce the risk of becoming a victim.

T/Detective Chief Inspector Antony Leadbeatter, Surrey Police & Sussex Police Economic Crime Unit

DOORSTEP CALLERS

Over the past few weeks in both Surrey and Sussex we have received multiple reports from residents reporting that they have been approached by unwanted cold callers offering to jet wash their property.

Reports involve one or more men visiting would be victims with a jet washer, offering to clean either their driveway or their roof with some victims parting with large amounts of money for unnecessary work.

In a recent example, an elderly female resident was handed a leaflet and asked if she wanted her roof cleaned for £1400-£1600. She declined and went inside.

The next minute the male was seen standing by the front door, jet washing a 2x1 metre square of her roof tiles above the front door . The male then showed her how clean it was, however despite emphasising she didn't want it cleaned she is now left with a small patch on her tiles that is clean, and the rest of the roof with moss on it .

Other reports claim the males were intimidating and aggressive in their approach and left residents feeling shaken and unsafe.

Please be aware that callers posing as builders and gardeners may pressurise or intimidate you to let them do work.

- You may not really need the work done
- They may do a poor job
- They may charge you far more than the job is worth
- They may provide false names, addresses and telephone numbers so you are unable to contact them again.
- Look out for your elderly relatives, friends and neighbours and please report any suspicious activity to Police.

SOUTHERN WATER SCAM

Recently across both counties we have received multiple reports about communications received from Southern Water.

Southern Water has confirmed that they were the target of a recent cyber attack and they have been in contact with affected parties via email and letter.

This is to make affected parties aware that:

- Their details may have been compromised,
- The details that have potentially been compromised
- The steps to take to protect themselves. A copy of which is shown in the link below.

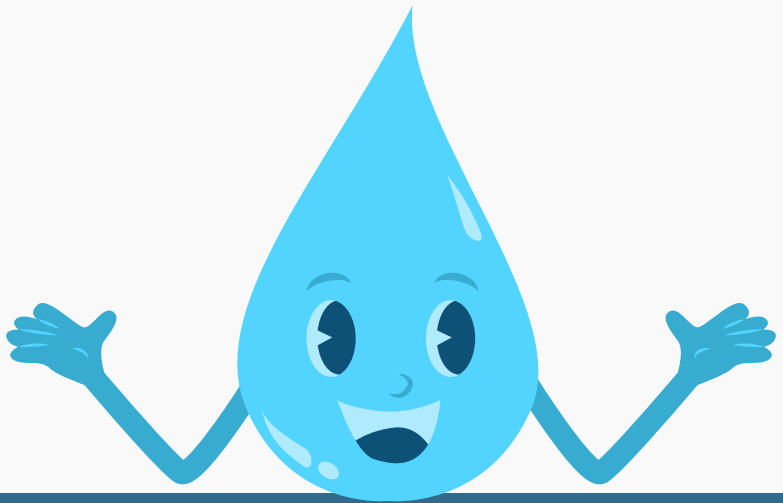
Cyber Notification – Southern Water

Southern Water has said:

> *We continue to work with our expert technical advisers to confirm whose data is at risk. Our initial assessment is that this is the case for some of our customers and current and former employees. We take data protection and information security very seriously and, in accordance with our regulatory obligations, we are making contact with anyone whose personal data may be at risk.*

The official Southern Water **website** also holds further information around the Cyber Attack and the process it has taken to protect its customers.

If you have any concerns, please contact southern water on **0330 303 0025**, which is a dedicated team that will be able to answer your questions.

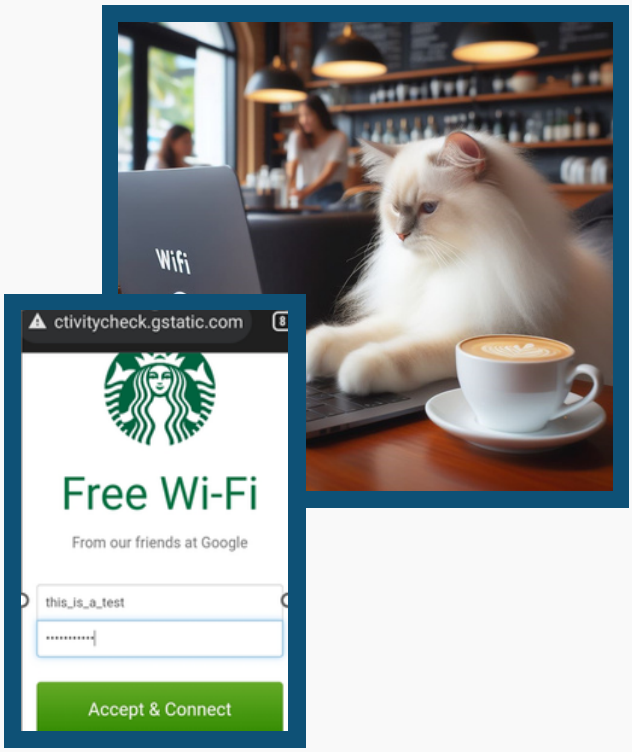


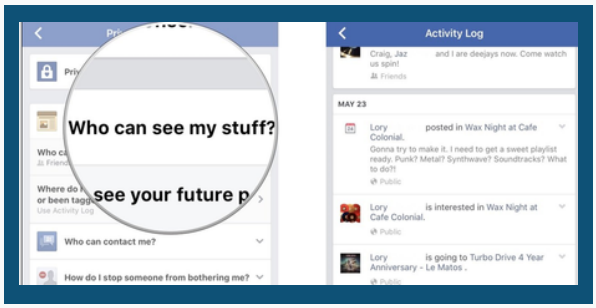
BEWARE OF THE RISKS OF PUBLIC WI-FI

Easy Target: Imagine public Wi-Fi as a busy street with lots of people. Just like pickpockets target crowded areas, hackers target public Wi-Fi because there are many potential victims.

Data Eavesdropping: It's like someone listening in on your conversation in a crowded room. Hackers can intercept your personal information, like passwords or credit card numbers, while you're using public Wi-Fi. Use a VPN if possible and never access sensitive data using public Wi-Fi.

Fake Hotspots: Think of fake Wi-Fi networks like traps set by thieves. They look real, but they're actually created by hackers to steal your data when you connect to them. It may look very similar to “Starbucks” but it could be a fake site. Never input your password or data on a site that does not have HTTPS in the URL (bar at the top).





DIGITAL FOOTPRINTS & PRIVACY INFORMATION

Control Over Information: Privacy settings on social media are like locks on doors. They help you control who can see the things you share, like your photos, posts, and personal details. Also, avoid those “Quiz” things on Facebook, sometimes they ask for very private information which overlaps with bank security questions such as “Who was your first childhood pet?” always think, can what I’m posting ever be used against me?

Protection from Strangers: Imagine your social media profile as your home. Privacy settings act like fences, keeping strangers out and only letting in people you trust. Don’t accept friend invites from people you don’t know and trust.

Avoiding Unwanted Attention: Just like you might not want everyone knowing where you live, privacy settings help you avoid unwanted attention by limiting who can find and contact you on social media.