Woking Neighbourhood Watch column, November 2019

"Don't get caught out"

I was scammed over the phone a few years ago. The caller claimed to be from a company that I had recently done business with, and I was taken in easily because everything he said over the phone fitted with the recent transaction. Ultimately, no damage was done, as I realised something wasn't quite right and was able to prevent any money being moved.

We all hear how we need to be wary of fake telephone calls, suspicious emails, dodgy-looking blokes on the doorstep claiming to see a problem with your roof, for example, but the truth is these criminals are getting very clever. Do not assume these fake emails and calls always come from Nigeria and involve people who do not have a full grasp of English. My scam caller was from a known criminal gang in Manchester and was very polite, business-like and spoke "BBC English".

I reported the scam via ActionFraud, the national fraud and cyber crime reporting centre.

Knowing how good these people are, be aware of some basic rules:

- Never give bank or card details over the phone to anyone, unless you've called them about a purchase or service you are paying for. If they call you and you think it's legitimate, ask them to give you their number and call them back. No-one should ever require your full PIN.
- Never believe anyone on your doorstep about something wrong with your property. Thank them and close the door. You can get a second opinion later. If they are insistent, call 101, and if they are abusive, consider ringing 999.
- If you get an email you aren't expecting, never open the attachment or click the link. Check the spelling in the email and the address of the sender. If you're still not sure, hover over the link and see what the address is underneath. It will be obvious if the link takes you to a scam site. All legitimate download addresses should begin with "https://" – note the "s". Hard-delete all suspect emails by pressing the shift and delete keys together.
- If your bank or credit card has a chip and you can wave it at a reader to debit up to £30, then put it in an RFID holder in your wallet or purse. This means it cannot be scanned by a criminal passing their mobile phone close to the card. These holders are available very cheaply online.
- On the subject of chipped cards, never let the card out of your sight in a shop or restaurant.
- If paying for a service or product upfront, ideally pay by credit card as you will have more consumer protection with a credit card than a debit card.

Finally, some simple rules. If it looks too good to be true, it's probably a scam. If it looks suspicious, it's probably a scam. And always count to 20 before pressing "send" – think about what you are about to do. Following this advice could save you a lot of time, money and grief.

ActionFraud can be contacted by calling 0300 123 2040 or by visiting actionfraud.police.uk