08 September 2021

The danger of Banking Apps

POLICE are warning people to beware of a new form of highway robbery in which people are being mugged in the street and being forced to transfer money via their digital banking Apps. Scotland Yard has investigated a spate of offences which have left victims deeply shaken and traumatised.
In one recent case a man in his 20s was attacked as he walked home from a pub in north London and was dragged into an alleyway and threatened by two men. The victim, who asked not to be identified for fear of reprisals, said his ordeal lasted for 15 minutes and left him extremely shaken.
He said that while one of the pair threatened him, the other one made a phone call and appeared to be taking instructions. After forcing him to open his smart phone banking app they then checked his bank balance before instructing him to transfer £10,000 into another account.
Once the transaction had gone through the victim was released and contacted the police and his bank. Fortunately, the transaction was stopped, and he did not lose any money.

If your smart phone is your only means of accessing and managing your bank account, it may be wise to keep it out of sight whilst you are out and about, using it to access your bank only from the privacy of your own home.

Paying for parking

The Daily Mail reported today that when a well-dressed man came to the assistance of Ray Bradbury and wife Plum after the payment machine they were trying to use refused their card, they assumed he was a friendly local resident or a parking machine engineer who worked for the council.
The helpful stranger took them to an alternative payment machine just down the road, but, after putting her debit card into the slot and entering her Pin, the machine swallowed her card.
At this point, the helpful stranger made a phone call to someone she believed to be a colleague who looked after parking in the area and handed the mobile to Plum. The 'colleague' advised her to wait by the car for 20 minutes until someone came to help retrieve her card.

This is called a Lebanese Loop and involves fraudsters inserting devices into the cash machine's card slot to stop your card being ejected.

Instead it is sucked back in, leaving the victim to believe the bank has retained their card. Someone may then appear to offer help which involves the victim re-entering their Pin. When you walk away, they recover your card and use the Pin they saw you type.