QCS Quality Compliance Systems
an RLDatix company

Protect your business from £1M digital fraud

Digital banking has revolutionised business and transformed the world of finance from the days where any activity necessitated a trip to your local branch. However, this convenience brings a new range of risks.

A scam has arisen where cybercriminals phone people and trick them into downloading malicious software on to their computer which gives the attacker remote access. Through social engineering, they then coax the victim in to becoming an accomplice to the crime by divulging access codes enabling the attacker to make fund transfers seemingly legitimately. Two care homes have already been victims of the scam, costing one of them, £1.6m according to a national newspaper.

HOW TO PROTECT YOURSELF

If you respond to a phone call from your bank asking you to divulge any information about your account – refuse to do so. Instead, politely terminate the call, independently obtain the contact number for your bank and call them back to discuss the matter

Some banks will issue requests via text message (SMS) or authenticator app to approve purchases. They will never phone you to discuss these transactions. You are free to respond to these requests, but do not divulge any sensitive information. Merely confirm whether the transaction is legitimate or fraudulent

YOUR BANK WILL **NEVER** ASK YOU

- **** for your password in full
- to install any software on to your computer
- for remote access to your computer

Your bank will only ever ask for personal details or authentication codes for transactions that you are initiating, – i.e. if you are making an online purchase or have called via telephone banking to make a bank transfer

Your bank will never ask you to transfer money from one account to another

*If you are **ever** in any doubt about an incoming phone call from your bank – **terminate the call, obtain your bank's contact number independently and call them back.***

t: 0333 405 33 33 e: info@qcs.co.uk w: www.qcs.co.uk