Scam Warning - Amazon Prime

Criminals are targeting members of the public with automated calls stating that the recipient has been charged for an Amazon Prime subscription. The callers use this lure as a way to gain access to the recipient's online banking account.

HOW DOES IT WORK?

1.The victim receives an automated call stating that they've been charged for an Amazon Prime subscription. They're asked to press 1 to cancel the charge, this connects them directly to the fraudster.
2.A fraudster, posing as an Amazon customer service representative, then tells the victim that the Prime subscription was purchased fraudulently and that they need remote access to the victim's computer in order to fix a security flaw that will prevent it from happening again.
3.The victim is asked to download an application called Team Viewer, which grants the fraudster remote access to the victim's computer.
4.The victim is then asked to log onto their online banking account whilst the criminals are able to monitor everything via Team Viewer.

Other variants of the crime involve fraudsters stating the recipient is due a refund for an unauthorised transition on their Amazon account.

WHAT YOU NEED TO DO:
Personal information: Always question uninvited approaches in case it's a scam. Instead, contact the company directly using a known email or phone number.
Stay in control: Have the confidence to refuse unusual requests for personal or financial information. It's easy to feel embarrassed when faced with unexpected or complex conversations. But it's okay to stop the discussion if you do not feel in control of it.
Remote access: Never install any software or visit a website as a result of a cold call. Unsolicited requests for remote access to your computer should always raise a red flag.