POLICE SCOTLAND
POILEAS ALBA

Cyber Security Alert

Remote Access - Scams

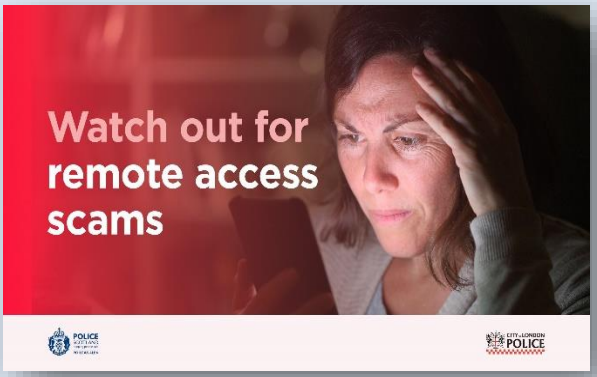
Police Scotland Cybercrime Harm Prevention Team.
29.01.2025

Remote Access – Scams

The use of remote access software in committing crime online is not very well known, let alone how easily criminals use this method to attack unassuming victims.

Remote access scams occur where online business and individual accounts are compromised by cyber criminals and Police Scotland wish to raise awareness of this.

Remote access software is a legitimate software used by businesses and individuals that allows a user to connect or control a computer that's in another location. It enables them to use one device to access another by downloading a smartphone app or installing a program. A simple passcode will then connect the two devices. However, criminals also use remote access for nefarious purposes to scam their victims.



Remote access scam criminals contact victims using very convincing emails or phone calls. By pretending to be electronics engineers from IT providers, bank staff, local authority staff and police for example, they offer to provide technical support to the victim but first request remote access to the victim's computer or other device.

Once they have been given access, they can freely access all the accounts stored on the device and begin stealing money, personal data and other useful information that can be used or sold.

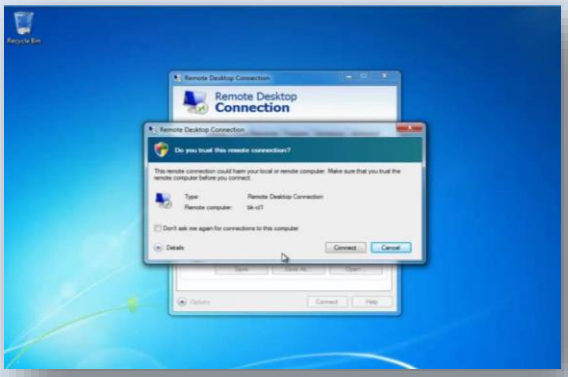
Other scammers are sneakier still, directing victims to websites, where clicking on various brand names or icons, downloads the software. Although they would still need the victim to enter a code to connect to their device, they are extremely influential in convincing victims to do this.

These criminals are not concerned for the impact their actions have on victims. Their intentions are to gain financially and move to the next victim.

If you are being asked to provide remote access to any of your devices or to download specific software, be aware, you risk becoming victim to a remote access scam.

Only install software or grant access to your devices if you are asked by someone you know and trust.

- Never trust requests from an email or call you weren't expecting
- Don't trust the "help" offered that you did not request
- No authority will ask for remote access to your device
- No bank or company will ask you over the phone to download software



What you can do.

Scammers are criminals after your money. If someone is remotely connected to your device and asks you to login to your bank account or to show any personal information or asks for your passwords to access a particular account, they are most likely a scammer.

Don't follow their instructions, even if they say you need to pay them because they allege to have solved a problem you were having, don't trust them. You didn't ask for their "help."

If you feel uncomfortable or insecure, stop the phone call just by hanging up. End any remote session by simply turning off your device.

We would also ask you to;

- Report the scam to your account provider
- Change any passwords to your accounts that may have been given away
- Have your device checked by an authorised IT specialist to ensure it is secure
- Report the scam to law enforcement

The following link will further assist you to Use a strong and separate password for your email - NCSC.GOV.UK

If you have been a victim of crime, and it is not an ongoing emergency, you can report this to Police Scotland on 101.

Police Scotland Cybercrime Harm Prevention Team

All information correct at time of distribution.