REMOTE ACCESS SCAM

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

What is a remote access scam?

A remote access scam is when a criminal convinces you to install software on your computer to "fix" a problem, only to then take control of your computer and steal money from your online bank account. It's also known as a *'computer takeover scam'*.

There are variations of this types of scam, for example:

- You are prompted to call the scammer through a pop-up notice on your computer. The pop-up notice warns you that there is a problem with your computer and encourages you to contact a phone number for technical support. DO NOT CALL. If you call the number, the scammer tries to convince you to allow them to remotely access your computer. When the scammer has access to your computer, they will usually tell you there's a serious problem they can fix for a fee.
- You receive a call from someone pretending to be from your phone/mobile phone provider, or a technology/computer company or similar.

The criminal tells you that you have a problem with your account and that, to "fix the issue", they need to install software on your computer; which, once installed, provides the criminal remote access and control of your computer.

At some point, the criminal will try to convince you to log into your Internet banking – perhaps to pay a nominal sum of money for the "fix". Shortly after, the criminal will then take control of your online account and transfer larger amounts of money. In some cases, the screen goes blank so you can't see what's going on.

The scam is then over in a matter of minutes and you're left out of pocket.

How to avoid a remote access scam.

Remote access scams can come in different guises. No matter what the story is, this is how you can avoid remote access scams:

- **Look out for a phone call out of the blue.** Particularly from someone claiming to be from a telecommunications or technology company claiming to be able to fix your computer or WiFi router.

- **Hang up on persistent callers.** Especially if they become angrier if you don't do what they say.
- **Never share your PIN or One Time Passcode.** These are essential security features and private and personal to you.
- **Don't be persuaded to download remote access software (such as TeamViewer) by a stranger and never share access to your computer with anyone you don't trust.** Without access, a criminal can't directly control your computer
- **Never share online banking login details or passwords with anyone**. Not even if they claim to be from your bank or any other company
- **Know that numbers can be spoofed**. Just because a text or caller ID says it's from your bank or another company, it doesn't mean that it is. If you're unsure, call the company on a number from a trusted website - not a number provided in an email, text or via a call
- **Look out for viruses – even fake ones**. As soon as you've given the criminal access to your computer, they may manipulate it in a way to seemingly show you loads of viruses. The criminals then try to convince you that they'll help you clear the viruses for a fee.
- **Keep software and systems up to date** - Make sure your computer is protected with regularly updated anti-virus and anti-spyware software, and a good firewall.

What to do if you think you're a victim of a remote access scam.

If you think you're a victim of a remote access scam and you've given remote access to your computer, or you fear that your computer has been hacked, **turn it off right away** and seek help or advice from a qualified and reputable computer technician.

Contact your bank immediately. Your bank may be able to stop the money from leaving your account or they may be able to contact the scammer's bank to freeze their bank account.

*You should also **contact Police Scotland on 101** to report the incident*