POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Computer Software Service Fraud

Fraudsters are cold calling victims, or using a 'pop up' windows on your web browser, purporting to be from well-known IT companies or broadband providers, claiming that the victim has problems with their computers, routers, or internet connection. The criminals persuades the victim to download software to their computer or laptop and connect via a Remote Access Tool (RAT), allowing the criminals to gain access to the victim's computer or mobile phone. Victims are persuaded to log into their online banking to receive a refund as a form of compensation, allowing the criminals access to the victim's bank account, and the ability to move funds out of the victims account.
There has also been an increase in the variety of service providers being impersonated to commit these scams.

Always remember

- Ensure you have effective and updated antivirus/antispyware software and firewall running whenever your computer or mobile device is switched on.
- Never install any software, or grant remote access to your computer, because of a cold call.
- Do not be tempted to download programs or apps that are not from a trusted source, as they could contain malware (malicious software).
- Genuine organisations would never contact you out of the blue to ask you for personal or financial details, such as your Bank card PIN or full banking password.
- Don't contact companies promoting technical support services via web browser pop-ups.
- Hang up on any callers who claim they can get your money back for you.
- Cover your webcam when not in use.
- Regularly back up your data.

If your device has been infected or you have been a victim

- If you have made a payment, contact your bank immediately. They can help you prevent any further losses.
- Disconnect your device from the network as soon as possible in order to prevent further malicious activity.
- If you granted remote access to your computer, seek technical support to remove any unwanted software. If you need technical advice, look for reviews online first or ask friends for recommendations.
- If you think the infection has been removed change the passwords of your online accounts and check your banking activity and report anything unusual to your bank.

For more information on how you can protect yourself online, visit www.cyberaware.gov.uk and www.takefive-stopfraud.org.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. For all emergency calls, dial 999.

This alert was sent out for your information by Police Scotland Safer Communities
Cybercrime Harm Prevention Unit - PPCWCyberHarmPrevention@scotland.pnn.police.uk
All information was correct at time of distribution. 06/01/2021