Lancashire Cyber Crime Bulletin – Remote Access Scams Targeting Businesses

Action Fraud has received 31 crime reports since June 2023 relating to remote access scams targeting businesses. **Victims have reported losses totalling over £3.8M.**

Tactic used:

Contact the victim claiming to be a representative from their bank or from a financial services vendor used by the victim's business.

1. Convince the victim to install a piece of software that enables remote access to their computer, claiming that it's required to install an important software update.

2. At some point during the call, the victim is instructed to login to their online banking account. Once the victim has done this, the remote access software is used to blur the victim's screen whilst the scammer makes fraudulent transactions from the victim's account without their knowledge.

3. The victim is also asked to read out a series of numbers the scammer claims they have sent to the victim's mobile. In reality, the numbers are a one-time verification code from the victim's bank which, if shared with the scammer, will allow them to transfer money out of the victim's bank account.

How to protect your business from remote access scams

Your bank will never ask you to grant them remote access to your computer or smartphone. Never install any remote access software on your device. •The one-time verification codes sent to you by your bank to authorise transactions on your account should **never be shared with anyone, not even bank employees.**

If you believe your laptop, PC, tablet or phone has been infected with a virus, follow the National Cyber Security Centre's guidance on recovering an infected device –
https://www.ncsc.gov.uk/guidance/hacked-device-action-to-take

Received a suspicious call from someone claiming to be from your bank? Hang up, wait a few minutes, then call your bank using the contact number on the back of your debit card, or their website.

If your business has fallen victim to fraud or cybercrime, report it to Action Fraud at www.actionfraud.police.uk, or by calling 0300 123 2040.

ActionFraud
Report Fraud & Internet Crime
actionfraud.police.uk

National Cyber Security Centre
a part of GCHQ