THE LONDON BOROUGH
www.bromley.gov.uk

TRADING STANDARDS ALERT!

Remote Access fraud

Computer takeover scams

Alert 2.10

6 September 2021

Bromley Trading Standards is warning residents that criminals are tricking people into allowing remote access to computers, tablets, and smartphones to hack into accounts to steal money and sensitive information.

Remote access software enables one device to access another device from *any* location by installing a program onto a computer or downloading an app onto a smartphone or tablet. A passcode or 'click to accept' will link the two devices.

Residents have reported calls from scammers claiming to be calling to help fix a problem with their internet speed or falsely claiming to be from a bank saying they are concerned about fraudulent activity on their account.

Legitimate remote access software businesses, including AnyDesk and TeamViewer, have been misused by scammers and provide advice:

Avoiding Remote Access Scams (anydesk.com)

Report a scam - TeamViewer

Trading Standards advise residents to:

- ✓ Hang up if cold called by anyone they don't know or trust
- ✓ Contact the company/organisation scammers claim to be from directly, using a trusted number
- ✗ **Never allow anyone they don't know access to your devices**
- ✗ **Never share online banking login details, PINs, passwords or OTP (One Time Passcodes) with anyone, including banks and Police**.

If you would like to receive Trading Standards Alert! direct to your inbox please visit www.bromley.gov.uk/scams and complete the online form.

If you think you have given a scammer remote access to your device:

- Take back control of your device –
  - use the '**disconnect**' button to end the session
  - **turn off** the wifi at the router or **unplug** your network cable to fully disconnect your device
- **Don't open** anything you may have installed or downloaded and **remove** any software or apps installed by the scammer (check for recently installed programs/downloads)
- **Change passwords** to online accounts e.g. online banking, email (include any others that may have the same passwords)
- Run a full security scan, if you have security software
- To be extra safe you could do a factory reset of your device or ask an IT expert to confirm your device is safe to reuse.
- **Contact** your bank as soon as possible
- **Contact** the organisation you believed were contacting you
- **Report to** the remote access operator e.g. AnyDesk or TeamViewer
- **Tell** someone you trust so they can help you to get the help you need
- **Call** Citizens Advice if you need advice and guidance **0808 223 1133**
- **Report** to Action Fraud on 0300 123 2040 or www.actionfraud.police.uk

We are proud to be supporting Friends Against Scams –
make sure you are scam aware, take the online awareness session at
www.FriendsAgainstScams.org.uk/elearning/bromley

Please share with family, friends, neighbours, colleagues & clients

Read it. Share it. Prevent it

REPORT

Protect others by reporting incidents.

Report to Action Fraud on 0300 123 2040 or www.actionfraud.police.uk

If you have given out your bank details, contact your bank as soon as possible.

You can also visit www.Bromley.gov.uk/scams