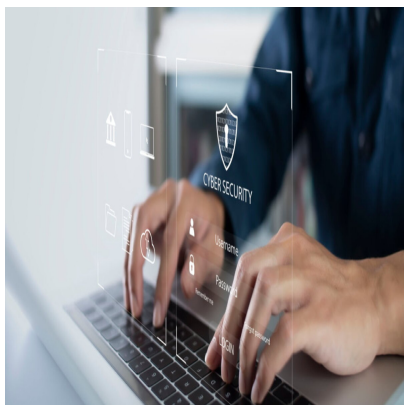




Microsoft Technical Support Scam: Stop the Remote-Access Sequence

Description

Microsoft does not make an unsolicited support call a reason to install remote-access software, reveal credentials or move money.

End the contact, disconnect the device if access was granted, secure financial and online accounts from a clean device, preserve evidence and report through the appropriate Singapore channel.

Recognise the pressure sequence

The scammer claims there is malware, a licence problem or suspicious activity, then pushes the victim to install remote-control software or reveal a code. Urgency and technical jargon are tools to remove independent verification. Do not continue the call while checking. ([CSA and SPF technical support scam advisory](#))

If remote control was granted, disconnect Wi-Fi and any network cable. Do not let the caller guide the cleanup. Use a separate trusted device to contact the bank, provider or security professional.

If banking credentials, card data or transactions are involved, call the financial institution through the number on its official site or card. Ask for account protection, transaction review and the bank incident reference. Speed matters more than explaining every technical detail first.

Situation	What changes
Only received a suspicious call	Hang up and verify independently
Installed remote-access software	Disconnect the device from networks
Shared bank or card information	Call the bank fraud line immediately
Credentials or files may be exposed	Reset from a clean device and report the incident

Related: [check a suspicious message](#)

Secure online identities

Change exposed passwords from a clean device, starting with email and financial accounts. Revoke unknown sessions and enable multi-factor authentication. Do not reuse the new password on another service. A compromised email account can reset many others. ([SingCERT Cyber Aid](#))

Save the caller number, messages, payment details, software name, screenshots and timeline without engaging the scammer again. Evidence helps the bank, Police and incident responders trace what happened.

Remote software removal alone may not prove the device is safe. Run trusted security checks and consider professional assessment or a clean rebuild where sensitive access occurred. Back up essential personal files carefully and avoid copying suspicious programs.

Example: A caller spends 12 minutes persuading a user to install remote software, but no password or bank detail has been entered. The priority is to end the session, disconnect the device, preserve the software name and obtain a trusted security check, rather than calling the number back.

Use the correct report channel

Police handle scams and crime reports; SingCERT Cyber Aid accepts Singapore-based cybersecurity incidents. Banks handle account and transaction protection. One report does not replace the others when both money and device compromise are involved.

Related: [handle another consumer warning](#)

Date Created

05/08/2026

Author

vanessakoh