

HANG UP. CHECK FIRST.

Before trusting a support call

Hang up. Check independently. Then decide.

FICTIONAL CALLER

“I am from IT. Install this so I can fix it.”

| Unexpected contact

| Caller ID can be faked

| Remote access gives control

-  **Treat the call as unverified**
Knowing your name or workplace does not establish that an unexpected caller is genuine.
-  **Call your usual IT team**
Caller ID is not proof. Contact IT or the organisation using a number you already trust.
-  **Verify before granting access**
Do not install software, share your screen or grant control until independently verified and approved.
-  **Keep secrets private**
Never give passwords, banking codes or recovery codes. Do not approve unexpected MFA requests.
-  **Reject payment pressure**
Do not transfer money to “protect” it or call numbers displayed in suspicious popups.

| Legitimate remote-support tools can be misused. Independently confirm the person and purpose before allowing access.

Already allowed remote access?

- End the remote session and disconnect the internet. Contact IT using another device or phone.
- If you paid or exposed banking information, contact your bank immediately.
- With IT help, change exposed passwords from a trusted device.

osmicro.com.au/printable-guides/phone-remote-support-scam-checklist/

Follow your organisation's security and payment procedures. These checks reduce risk; they do not guarantee a message or transaction is safe.

Checked October 2026 • Sources: [Scamwatch](#) [1] [Microsoft](#) [2] [ACSC](#) [3] • More detail and accessible text at the URL above.