

Five questions to ask your IT provider

If your provider connects remotely, looks around and reports they found nothing, that is not sufficient here. There is no virus to find — what installs is legitimate remote-access software.

Ask these five questions. Expect a clear answer to each.

1 Has the affected machine been properly assessed, not just scanned?

Why it matters: A scan alone will not settle this. What it needs depends on what is found, and rebuilding the machine is one possibility.

2 Have mailbox forwarding rules and filters been checked?

Why it matters: Hidden rules let an attacker keep reading mail after a password change.

3 Is two-step verification turned on across all accounts?

Why it matters: It is the single control that makes a stolen password much less useful.

4 Have all machines been checked for remote-access software nobody installed?

Why it matters: This attack installs a second copy elsewhere. Checking one is not enough.

5 Do our everyday accounts still have administrator rights?

Why it matters: This attack has to install software. A standard account cannot, so removing admin rights stops it.

If you cannot get a straight answer to all five, we will check for free.

Twenty minutes. No obligation. No disruption to clinic hours.