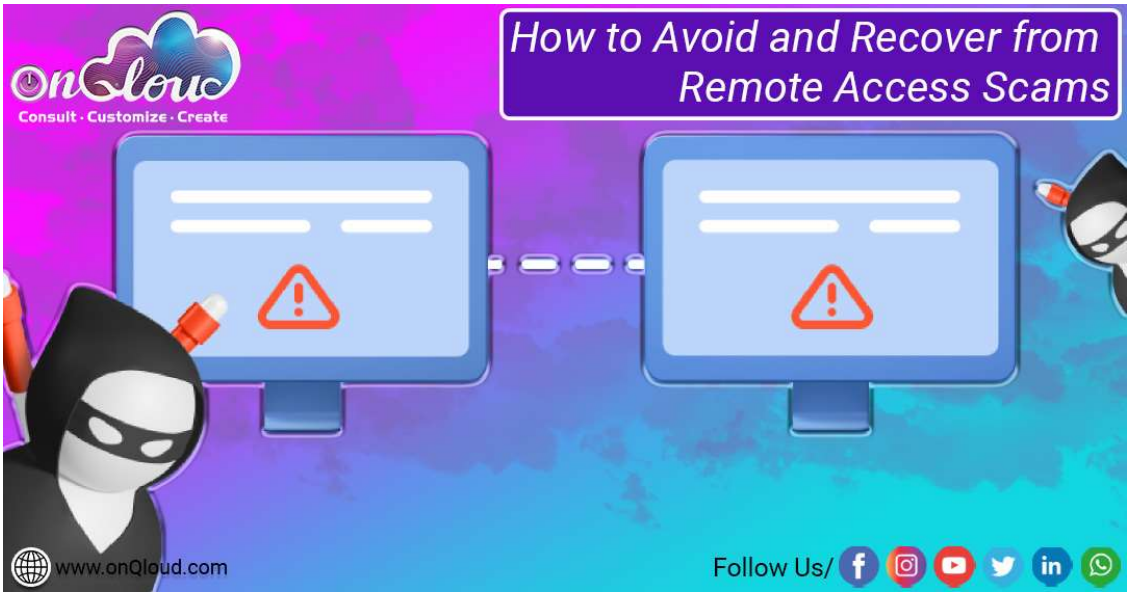

Recovering from a remote access scam

What to do if it happens to you

Every day, many people around the world become victims of cybercrime. Fraudsters use various methods to convince their victims to grant access to their computer in order to steal their confidential information, personal data, credentials and, of course, money. This type of attack is called “phishing”. Phishing is a form of social engineering attack in which an attacker tricks the victim into believing they have good intentions in order to convince them to grant access to their data. None of us can be fully protected from this. Fraudsters are excellent psychologists and professionals in their field. That’s why it’s so important to know how to spot a scam, in order to avoid it.

In general, here are the main tips on how to recognize a scam:

- Don’t trust strangers who call you and offer help you didn’t ask for. Be aware that it is quite common for scammers to spoof their caller ID information to falsify the phone number and/or name that is shown as caller ID information.
- When you see a scary-looking banner with a statement that something is wrong with your computer or data, and with contact details, it’s most likely a scam. It’s highly unlikely that companies will put their contact information on an online alert. Another distinguishing feature of these pop-ups is that they are hard to close.

- A bank's security service or the technical support of a company will not ask you to install any software over the phone, especially remote access software.
- If someone who is currently connected to your computer asks you to log into your bank account during a remote session or show one of your passwords, this person is most likely a scammer.

Book Your Demo

onQloud, USA, UAE, India, info@onqloud.com