Some Help With

Abuse management

TABLE OF CONTENT

Best practices for using remote access software

Currently executed schemes

Authorities and abuse management

This article outlines simple best practices to follow when using Remote Access software, highlights common misuse scenarios, and explains how to spot and report suspicious activity. Following these guidelines ensures a safer and more reliable Remote Desktop experience.

Best practices for using remote access software

1. **Verify website authenticity**
   Always ensure the websites you visit are authentic. Be cautious of phishing pages and malicious downloads that can compromise your data.
2. **Be skeptical of remote access offers**
   Legitimate officials will never ask to remote access your device unsolicited. Always be wary of such requests.
3. **Protect your access codes**
   Never share access codes to your devices with anyone. This is crucial to maintain your security.
4. **Ignore cold call attempts**
   Do not respond to cold call attempts. Scammers often use this tactic to gain unauthorized access.
5. **Restrict access to trusted parties only**
   Only grant remote access to trusted parties. Be particularly cautious of individuals claiming to be from legitimate companies.

6. **Request identity verification**
   Always ask for identity credentials from anyone requesting access to your device. Verify their legitimacy before proceeding.

7. **Beware of unsolicited calls**

   Do not engage with or provide information to callers from unknown origins. Scammers may attempt to extract sensitive information this way.

8. **Protect sensitive information**
   Never reveal sensitive information, including banking credentials, to unknown or unverified parties.

9. **Recognize legitimate company practices**Legitimate companies will never cold call you to solve a problem. Always initiate contact yourself if you need assistance.

10. **Report scammer activity**
    If you encounter scammers, record all details and report the incident to local authorities immediately.

By following these best practices, you can help protect yourself from potential security threats and ensure a safer remote desktop experience.

Currently executed schemes

1. Money theft via mobile sessions in India:
   - Scammers extract data during mobile sessions to steal money. For more details, refer to RBI Warning.
2. Fake Microsoft technicians:
   - Scammers pose as Microsoft technicians, claiming they need to clean your device of malicious software. Remember, Microsoft will never cold call you for such issues.
3. Impersonation of legitimate companies:
   - Scammers often try to gain your trust by pretending to represent legitimate companies. Always be skeptical of unsolicited contact.
4. Fake AnyDesk support claims:

- Scammers may pose as AnyDesk support, claiming to solve bugs in Windows, even if you are using a macOS device.

> 🚨 **IMPORTANT**
>
> AnyDesk will only respond to support tickets that you initiate. Furthermore, we exclusively provide support for issues related to AnyDesk software and do not support any third-party software or products.

Authorities and abuse management

At AnyDesk, we take abuse seriously and cooperate closely with law enforcement authorities to combat fraudulent activities. Users found violating our terms of use will be banned upon identification.

By working together, we can help ensure a safer and more secure environment for all users.

Related articles:

- Microsoft Report Scam
- Google Report Scam

The ability to access and control a device from a different location using AnyDesk, facilitating remote support and work.

The ability to access and control a device from a different location using AnyDesk, facilitating remote support and work.