Secure use of remote support

Remote support is a technology enabling you to obtain third party help on your own device without the need to have an engineer on site. Financial institutions and software manufacturers also use this option in the context of their support/help desk facilities. However, to use remote support securely, you have to take certain measures.

The most important points to remember:

- Only establish connections with trustworthy people. You should be particularly cautious if it is not you initiating the connection (e. g. if you receive an unexpected phone call).
- Use an encrypted connection.
- Use a session password or a meeting ID.
- Don't grant full access to your system. The person helping you should only ever be able to view your screen passively.
- Consider that everything shown on your screen can be seen and also recorded by the other side.
- Enter as few passwords during the session as possible.
- Don't surf to any Internet pages which have nothing to do with the session - even if you are asked to do so.
- Make sure that the remote support connection is terminated after availing yourself of any help, to stop any further access to your device.

Many companies use remote support software to enable their support staff to have a quick look at a user's machine without the need of someone having to go visit them on site straight away.

Unfortunately, this technology is also abused by criminals to obtain access to Internet user devices by fraudulent means, for instance to capture passwords, install malware or trigger an e-banking remittance, by purporting to be support staff of a certain company. You should therefore be careful who you trust!

Please also consider our info sheet "How to protect yourself against fraudulent support calls".

(https://www.ebas.ch/wp-content/uploads/2019/09/supportSKP_en.pdf)

Remote support software enables remote access to a third party system via a local network (LAN) or the Internet. In the process, the remote device desktop is displayed on the local system and sometimes also allows for it to be remotely controlled.

Further information for all those interested

Invitation

Only establish connections with trustworthy people. You should be particularly cautious if it is not you initiating the connection (e. g. if you receive an unexpected phone call). Currently, a common method by attackers trying to scam you is to ring you purporting to be support staff, for instance working for Microsoft, Apple, an IT support company or a financial institution, to obtain access to your device. Any session should only be initiated after your explicit invitation to do so. Before you accept any connection via their software, you should expressly have to agree to do so.

Encryption

When choosing a product, you should ensure that there is a sufficient level of encryption to guarantee data cannot be transferred in plain text. The key should be at least 128 bit in size.

Authentification

Any person establishing a connection to your device must authenticate him- or herself via a meeting ID and/or a password. Depending on the software used, there are different ways to do so. To make sure that this sensitive information is only received by the right person, it is best to advise the password or meeting ID beforehand, by telephone.

Access rights

Don’t grant full access to your system. The person helping you should strictly only ever be able to passively view your screen and give you instructions. This ensures that you still have exclusive control over your system and that no unintended changes can be implemented.

Screen capture

Please note that support sessions can be recorded. Anything appearing on your screen during this session can be viewed and captured by the other party.

Session

Enter as few passwords as possible during the session (ideally none at all), and don’t surf to any Internet pages which have nothing to do with the session. If for instance it is a financial institution providing you with support, make sure you only ever remain on the website of the financial institution involved.

Termination

Make sure that the remote support connection is terminated after availing yourself of any help, to stop any further access to your device. While the connection is still active, a remote support information screen which cannot be hidden should permanently be displayed on your screen. Please follow the instructions in the software documentation.