BEWARE OF REMOTE ACCESS SCAMS

To conduct business, real estate practitioners rely on computers, mobile devices, transaction management systems and web apps. Since just about anyone that uses technology faces cyber risk, real estate brokerages are not immune from on-line scams, privacy breaches, and cyber-attacks.

Recent scams using a software application by the name of AnyDesk target bank accounts, including business accounts such as broker trust accounts. Unfortunately, the scam is perpetrated in such a way that anyone can be easily fooled.

AnyDesk is a software application used to remotely connect two different workstations. Once installed, the application allows access to that device from anywhere in the world. Although the product is used legitimately by IT professionals to connect remotely to their clients in order to help resolve technical issues, scammers misuse AnyDesk in an effort to connect to the victim's device and steal data, access codes, and even money.

Scammers begin the process by contacting individuals by phone claiming to be from well-known companies such as Amazon, Apple, and Microsoft. They explain that fraud or an unauthorized purchase has been detected on the victim's account.

To resolve the issue, the fraudster asks the victim to download AnyDesk from the Google Play Store or Apple App Store. One or two permission requests will be sent to the victim as is generally the case when new applications are installed. However, once the victim grants permission to these requests, their device is fully accessible to the fraudster.

With complete access to the device, the fraudster will have access to the PIN and passwords of the victim's mobile banking apps, along with other Private Personal Information (PPI). Once in possession of that information, the fraudster can remotely perform banking transactions without the victim's knowledge. And while fraudsters often target an individual's bank account, this scam is just as easily used to access business accounts, including broker trust accounts.

If someone you don't know asks you to install a third-party app, you should always refrain from doing so. Hackers frequently try to install remote control apps that enable a gateway to the victim's device. Hence, you should avoid installing any app based on the caller's recommendation.

Furthermore, no bank or company should ask you over the phone to download software.

If you think there may be a problem with one of your accounts, contact the company using a phone number or website that you have independently verified and know is accurate. Do not call the phone number provided to you by the scammer and do not give out your personal information.

If someone you don't know is asking to access any of your devices and wants you to download specific software, be careful! You're at risk of becoming a victim of a remote access scam.

For more information on the AnyDesk remote access scam, go to AnyDesk: **How to Avoid Remote Access Scams**.

This article is of a general nature and reflects only the opinion of the author at the time it was drafted. It is not intended as definitive legal advice, and you should not act upon it without seeking independent legal counsel

ABOUT THE AUTHOR

Scott M. Drucker, Esq.
A licensed Arizona attorney, Scott is General Counsel & Assistant CEO for the Arizona REALTORS® serving as the primary legal advisor to the association.