NOT REALLY TECH SUPPORT

BY JAY BORDEN

Tech support is an essential part of life today. With all the technology in use, something is bound to go wrong, and most users need help correcting it. Companies either have their own tech support groups or contract with a service.

For personal systems people may purchase support from third parties if they aren't able to do it themselves. Or they may get help from a friend.

Regardless of where it comes from, tech support is there to monitor our systems or at least repair them when something goes amiss.

The reliance on tech support hasn't escaped the notice of cybercriminals. According to the FBI's Internet Crime Report for 2023, fake tech support scams were reported 37,500 times and resulted in losses of over $924 million. These are only the ones reported to the FBI.

Why are they so pervasive? Because experience has made us expect problems and in some cases to be notified by tech support if there is a problem on one of our devices. For many people tech is either beyond their understanding past how to use it, or they just prefer to spend their time and energy on things they enjoy more. Even the language of tech is foreign to most people. This creates many opportunities for cybercriminals to take advantage by posing as tech support.

How does the scam work? Different ways.

It could be a phone call or text message or pop-up notification supposedly from a trusted source. Maybe an anti-malware company or a tech company like Microsoft or another well-known company claiming to have detected malware on your device. The message will create fear by saying you must allow them to remove it immediately before it becomes serious.

NOT REALLY TECH SUPPORT

CONTINUED

Some scammers use information about you that they acquired on the dark web to be more believable. It may be as simple as your name and the devices you use. But it can be enough to convince you the message is real.

Scammers even create fake websites or web pages to fool you into thinking you are on the website you wanted, before issuing the warning.

A social media presence is a must these days and cybercriminals know it. They create bogus social media accounts that imitate real ones. They put up ads on search engine pages hoping to attract people.

If their contact with you is through anything other than phone, they will make every effort to convince you to switch to a phone call. After all, it is harder to ignore a real person on the phone telling you they want to help and harder to get a credit card number and hook you.

The amount requested may be small to begin but grows quickly. In the FBI's list the average total amount was $25,000. People don't part with that amount easily so social engineering is widely employed to convince you there is a problem and that they can fix it for you. Delay will only make the problem worse.

The charges are usually not all for fixing the problem, but are run up by them putting numerous charges on the credit card number you give them.

What to do
As with so many other scams if the callers insist that action must be taken immediately it is a red flag. To put them off, say you must discuss this with someone first or that your phone is about to run out of battery. They will turn up the pressure to get you to act now but don't. Hang up on them if you need to but don't give them access to your computer or give a credit card number. Remember they are scammers. You do not need to be polite.

If a caller says they need you to install remote access software so they can fix the problem, that is another red flag. Once that software is installed they can do anything including load malware. Do not give them access to your computer. Never allow them to install anything! No matter have beneficial it sounds.

NOT REALLY TECH SUPPORT

CONTINUED

Be sure you have anti-malware on your devices from a reliable company. If something is detected it will issue the warning. Those warnings are more reliable.

The targets for these types of scams are rarely young people who tend to be more tech savvy. It is older people who are less familiar with technology even if they use it every day.

Always err on the side of caution.

Welcome to peace of mind.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.