5 ways to protect yourself from technology scams

(BPT) - “What’s your favorite scary movie?”

This famous line from the film “Scream” sent shivers down the spines of moviegoers everywhere and made us all think twice about answering the phone. But while Ghost Face and his creepy question are nothing more than fiction, the wrong call in the real world can also be dangerous.

Phone scams are nothing new, but today thieves are using the phone to perpetrate tech support scams that prey upon the non-tech savvy. The fraudsters will make calls to would-be victims purporting to be with a reputable company, alerting the victim that there is a problem with their computer. Once the fraudster has earned the victim’s trust, they may then offer a software solution that could ultimately steal from the victim. The fraudsters inform potential victims what it will cost and tell them to send an online money transfer or provide their credit card number over the phone to cover the fee.

Understanding the dangers of tech scams

For the victims of a tech scam, the best case scenario is to discover that the solution they purchased doesn’t work or that they could have gotten the software elsewhere for free. They’re out the money they paid the scammer but little else.

In more serious cases however, the scammer may ask for remote access to “fix the problem” and then use that access to install malicious software (malware) on the victim’s computer. This software enables the scammer to steal the personal information the machine holds, including the victim’s phone number, social security information, credit information and other sensitive data they can obtain. The results of this identity theft could be devastating.

Protecting your computer and your sensitive information

To protect yourself from ending up the victim of a tech support scam, Western Union offers these fraud awareness tips.

Just say no. Never send a money transfer or provide your personal or banking information to people or businesses you don't know personally. Scam artists can be very persuasive over the phone, so never turn over your information just because the person on the other line sounds legitimate.

Keep control. Never give control of your computer to someone that randomly calls you. Once you hand over control, you're at the mercy of that other person to get control back.

Don't be afraid to hang up. If you feel pressured or the caller mentions there is a subscription fee for the service they are offering, hang up. You can always call your software company on your own if you feel there is a problem with your computer.

Get professional help. If you suspect malware has been installed on your computer, take your device to a reputable computer repair service and have them run a diagnostics check on your machine to remove the suspicious software.

Act immediately. If you feel you've been the target of a scam, it's in your interest to act as quickly as possible. The longer you delay, the longer you leave your personal information vulnerable to outside threats. If you get one of these phone calls and you have sent a money transfer via Western Union, call the company's fraud hotline at (800) 448-1492 to report it. If the money has not been paid, then Western Union can stop the transaction and refund your money.

Unlike the characters in the movie "Scream," tech support scams are very real. However, if you apply the fraud prevention tips above, you can help protect your personal information and keep the terror out of your technology. For more information on common scams, visit Western Union's Fraud Awareness Center at wu.com/fraudawareness.