ForReel Pictures

The Situation Report
"Honest Reporting"

CONFRONTING AND PREVENTING "TECH SUPPORT SCAMS:" WHAT YOU NEED TO KNOW

Written by: Mackenzie Kram

June 5, 2017

In May of 2017, Florida's Attorney General Pam Bondi, along with numerous government officials, including the Federal Trade Commission (FTC), have announced the launch of "Operation Tech Trap." The goal of Operation Tech Trap is to shut down companies associated with tech support scams and punish all individuals responsible for deceiving consumers, identity theft, and large scale fraud.

WHAT IS A TECH SUPPORT SCAM?

Tech Support Scams are when fraudsters "run ads that resemble pop-up security alerts from Microsoft, Apple, or other companies." (Fair, 2017). These pop-ups block a victim's computer and urge them to call "tech support" via a toll-free number on the screen or their computer would be permanently disabled. Tech Support Scams are also launched via phone calls, where scammers will call their would-be victims at random.

Once a scammer picks up the phone, he/she will claim to be from a legitimate company, like Microsoft, and inform the victim that his/her computer is seriously damaged and needs to be fixed immediately. Next, the scammer will ask you a series of questions to establish a “claim” that your computer is corrupt. By doing so, victims give up their names and addresses to the scammers for further criminal activity.

With that, the scammer “[claims] to need remote access to consumers’ computers so they can run ‘diagnostic tests.’ Those tests purport to reveal [serious] problems that can only be solved by one of their ‘certified technicians’ – for a hefty fee….” (Fair, 2017). However, the scammers are forcing their victims to grant them remote access to worsen a falsified claim.

As a result, scammers use high-stakes tactics to push victims into paying hundreds, if not thousands, of dollars for unnecessary software. The FTC “estimates that more than $24.6 million has been lost to tech-support scams alone in the last two years. On average, a typical consumer can lose about $280.” (Tompor, 2017). USA Today reported that one woman “got caught…twice...to the tune of $800. (Tompor, 2017) To make matters worse, some scammers will force you to send checks or money orders because they claim your credit cards are “susceptible to hackers,” when they are attempting to steal your bank account information, credit cards, and identity. Worst of all, if victims refuse to give up any money or try to stop the scammers in their tracks, the scammers will threaten their victims with force. One scammer even threatened “to kill a man who pointed out that the scammer was trying to steal money.” (Brodkin, 2015).

Legitimate companies, like Microsoft, Apple, etc., never force you to call tech support or threaten to disable your computer. In addition, they will never call you to uncover “computer problems” and/or demand remote access to one’s computer to perform “diagnostic tests.” These companies “shouldn’t have to compete against outfits that use phony-baloney pitches to fix…” (Fair, 2017) nonexistent computer problems, nor use high-stakes tactics to scare their customers.

With tech support scams worsening every year, the FTC and several law enforcement agencies are pursuing 16 civil and criminal actions through “Operation Tech Trap.” Their goal: target all tech support scams, pop-up and cold-call, and high-stakes tactics used by scammers that defraud consumers for millions and potentially steal their identity. “In three of those cases, federal judges have entered temporary restraining orders to halt the practices, freeze assets, and appoint temporary receivers to take control of the businesses.” (Fair, 2017). Closer to home, Florida’s Attorney General Pam Bondi and the FTC “have shut down an operation that ran a tech support boiler room in Boynton Beach, Florida. The defendants in that manner are banned for life from providing tech support products or services and [must] turn over $700,000 in assets.” (Fair, 2017).

If you do get a pop up that resembles Microsoft, Apple, etc. that urges you to call tech support and/or threatens to disable your computer, DO NOT CALL THE PHONE NUMBER LISTED ON YOUR SCREEN. “The fake Tech Support pages are…malicious websites…used by cybercriminals to promote their remote support services.” (Malware Tips.)

Instead, click on Task View, or Task manager to close the page, and close it immediately. If the pop-up is a full screen pop-up, press ESC before clicking on the task view. Then, restart your computer. If you have an option that has update and restart, click on that. Once you’ve rebooted your computer, you can fully access the internet. If you come across a page that says “Restore previous session,” DO NOT RESTORE IT. Instead, go to your history and you’ll find the cause of the pop-up scam: a malicious web link. DO NOT CLICK ON THAT LINK. Instead, clear your history, and refresh your internet browser.

TIPS TO PROTECT YOURSELF FROM TECH SUPPORT SCAMS

1. Use caution when surfing the internet
2. Keep your computer updated and free of viruses and malware
3. Do not give anyone remote access to your computer and/or electronic devices
4. Do not give your bank account and/or credit card information to anyone you do not know or trust
5. If you do lose money, call your credit card company, bank, etc. and ask them to reverse the charges
6. If you do encounter a pop-up or a cold-call, even if you didn’t fall for the scam, report it to the Federal Trade Commission and/or local law-enforcement agencies.

Sources

1. Brodkin, Jon: Tech support scammer threatened to kill man when scam call backfired. *https://arstechnica.com/information-technology/2015/03/tech-support-scammer-threatened-to-kill-man-when-scam-call-backfired/* Ars Technica. Published: March 4, 2015. Retrieved: June 5, 2017
2. Fair, Lesley: Operation Tech Trap targets tech support scams – and offers insights for businesses. *https://www.ftc.gov/news-events/blogs/business-blog/2017/05/operation-tech-trap-targets-tech-support-scams-offers* Federal Trade Commission. Published: May 12, 2017. Retrieved: May 26, 2017

3. Malware Tips: Remove Tech Support Scam pop-up virus (Call For Support – Scam). *https://malwaretips.com/blogs/remove-tech-support-scam-popups/* Retrieved: June 3, 2017

4. Tompor, Susan: Beware of tech-support scams. *https://www.usatoday.com/story/money/business/2017/05/21/tompor-ftc-declares-war-tech-support-scams/101953542/* USA Today. Published: May 21, 2017. Retrieved: June 5, 2017