Taking Down Tech Support Scams

Genevieve Bonan, Assistant Attorney General, Consumer Protection Division, Office of the Attorney General of Florida

Bonnie, a retiree in Florida, was going about her day when she received an alarming phone call from someone named Phillip, who said he was from Microsoft. Phillip told her that he detected several hackers in her computer and urgently needed to remotely access the computer to repair the damage. Frightened that her personal information was at risk and trusting that the call was from Microsoft, she followed Phillip’s instructions and gave him access to her computer. Phillip pulled up various windows and said he found 46,000 potential hackers trying to get into her computer. For only $299.00, Phillip offered to install security software and provide certified tech support for Bonnie. There was a discount if Bonnie was a senior citizen, which she is.

The Deceptive Tech Support Model

Tech support scams are a type of imposter scam that affects over 6 in 10 consumers\(^1\) in the United States. In this scheme, the perpetrator often poses as a representative of a well-known computer company such as Microsoft Corporation, and attempts to convince victims that their computer is in need of urgent repair. Common elements of this imposter scam include unsolicited calls, high-pressure tactics, threat of loss if the consumer does not act immediately, and requesting payment via wire transfer, credit card, or prepaid gift cards.

The scam often begins with an unsolicited phone call, as Bonnie encountered, or a pop-up advertisement disguised as a warning from Microsoft or a well-known antivirus program. The pop-up claims that the computer is infected and in need of urgent repair and the threat can be eliminated by calling the phone number on the ad. In both approaches, via phone call or pop-up, the consumer is connected to a scammer who attempts to remotely access the consumer’s computer. Once in control of the computer and with unfettered access to computer files, the scammer will pull up various programs, such as the Task Manager, and convincingly tell the consumer that there is evidence of viruses or hacker attempts. Inevitably, whether or not there is an actual threat, the scammer offers to remove the threat for a fee. This is all included in a predetermined script most tech-support fraudsters follow, which has been recycled and sold to countless boiler rooms. What so few consumers know is that these pop-ups are just advertisements (not detecting security

threats), and that Microsoft does not make unsolicited phone calls to offer computer repair services.²

Evolving Tech Scams

The tech support imposters are growing and evolving to avoid enforcement action. For example, Microsoft reported a growth of 24% in consumer complaints related to tech support scams in 2017.³ The Federal Trade Commission (FTC) received almost 143,000 reports about tech support scams in 2018.⁴ Although these scams often target senior citizens, millennials are also victimized. Consumers aged 25 to 34 were six times more likely to lose money to a tech support scam than consumers who were 66 and over.⁵

Fraudsters’ tactics continue to evolve. For example, some scammers are based in the United States but assist call centers in India to commit tech support fraud. These individuals are sometimes known as “money mules,” and collect victim payments through various means, keep a fee, and transmit profits to India-based call-center operators. Another method utilized by scammers to avoid investigation is when the scammer works with a software provider that sells its software to well-known retailers of personal computer devices, such as Home Shopping Network.⁶ In this scheme, the scammer acts as a purported tech support help desk for consumers who purchase a device; then, once a consumer calls the helpline, the same remote connection sales pitch is employed, fraught with fake security threats and claims of affiliation with Microsoft. Many fraudsters also pay to appear with online search terms, such as “Dell tech support” and “Microsoft support number.” Internet search engines, such as Google and Bing, often have their top search results polluted by paid scam results.⁷ Such deceptive advertising tactics are intended to make it difficult for consumers to distinguish legitimate support from scams.

Current Enforcement

Thousands of consumers like Bonnie are duped into purchasing unnecessary tech support products and services from fraudsters, but enforcement agencies are gaining ground in the effort to protect consumers from these scams. Over the last few years, the Department of Justice, FTC,

⁴ Figure based on 142,904 reports to Sentinel in 2018 that were classified as tech support scams. 105,676 of these reports were provided by Microsoft Corporation’s Cybercrime Center. https://www.ftc.gov/news-events/blogs/data-spotlight/2019/03/older-adults-hardest-hit-tech-support-scams, accessed May 4, 2019.
and state attorneys general have filed a number of enforcement actions intended to send shockwaves through this industry. Specifically, as part of a nationwide sweep on March 7, 2019, during National Consumer Protection Week, state and federal agencies took action against tech support scammers. Among others, the attorneys general of Florida, Minnesota, North Carolina, and Texas filed lawsuits seeking to stop tech support fraudsters in the United States and elsewhere. The complaints allege that the businesses misled consumers into paying thousands of dollars for unnecessary tech support services or software products using deceptive, high-pressure sales tactics.

Conclusion

The consumer injury of tech support scams reaches around the country and beyond. As assistant attorneys general, we play a critical role in effectively alerting consumers and the courts about trends and issues in the constantly changing tech support scam industry. Agency enforcement actions, as well as prevention through consumer education, are the best lines of defense against tech support predators.

---