Issued 4/26/18

Tech Support Scams Ramping Up, Microsoft Warns

Microsoft said it received 153,000 reports in 2017 from customers who dealt with tech support scams. That's a 24 percent increase from 2016. Such incidents happened in 183 countries, and around 15 percent of them involved the victim losing money—usually between $200 and $400—to the scammer. Reports detailed multiple ways users encountered these scams, including email campaigns that use phishing techniques, scam websites that give fake error messages, malware and cold-calls from fake technicians. The ease of fooling people is partially why the problem has become so widespread. "Cybercriminals want to bilk users' money. They can spend a great deal of time and energy attacking the security of a device—brute-force passwords, develop custom and sophisticated malware, and hunt down vulnerabilities to exploit," Erik Wahlstrom, Microsoft's Windows Defender Research project manager, wrote on the company's site. "Or they can save themselves the trouble and convince users to freely give up access to their devices and sensitive information."

The FBI announced in March that it had received 11,000 reports of tech-support fraud in 2017, with monetary losses amounting to almost $15 million. So how do you protect yourself from this common scheme? Never give your password or account information over email or over the phone. A legitimate tech support operation wouldn't ask for this sensitive information in these ways. In general, don't trust any unsolicited calls with personal information. Microsoft recommends only downloading software from official vendor sites instead of third-parties. They also recommend keeping all of their software updated and reporting any scams if you encounter them.