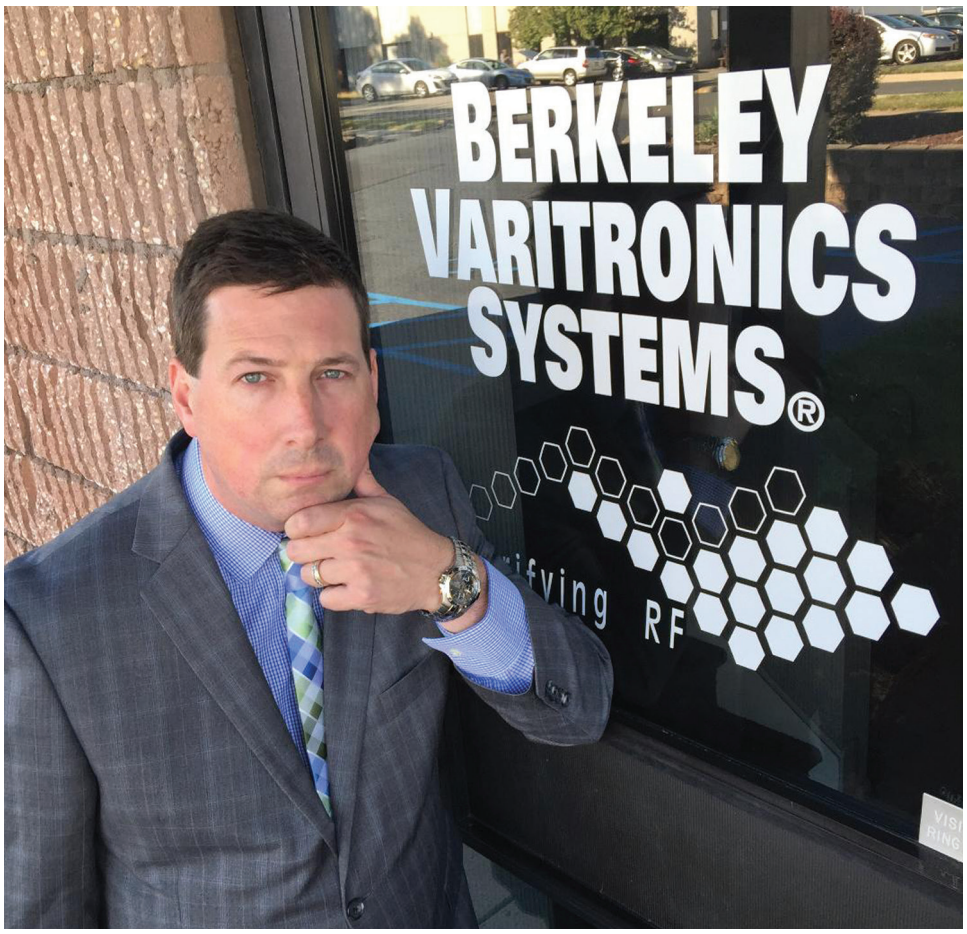
Scott Schober



Gas Pump Skimmers: High Tech Highway Robbery

Hackers do not discriminate between stolen data so whether you drive a Ferrari or a Ford, you are at risk of getting your credit card stolen at the gas pump. Cyber thieves are increasingly setting their sights on consumers fueling up at the gas ump so here's what you need to know to avoid high-tech highway robbery.

Why Are Gas Stations So Vulnerable?

Over the last few years, the retail sector has been barraged with attack after attack (from Target to Home Depot to Marriott Hotels) forcing retailers to spend money on more secure point of sale terminal upgrades using chip-in-pin technology. This technology is far more secure than traditional mag-stripe readers. However, since gas station pumps are technically located outside and are not a part of the retail footprint, they are not required to meet the same security protocols and deadlines. In fact, the petroleum industry is not required to upgrade their antiquated "mag-stripe" card readers that are built into most gas pumps until the end of 2020. Only then does the federal mandate go into affect shifting the liability down to gas station owners that do not comply with the recommended security upgrades. So, where does that leave more than 276 million vehicles in the United States and their drivers?

We need to exercise caution at the gas pump just as we would at an ATM, restaurant or retail space where our credit cards face exposure. I recommend using cash but that is not always possible nor is it convenient. Of the 150,000 gas stations across America, tens of thousands contain hidden Blue-tooth skimmers whicht are skillfully placed inside gas pumps just waiting for unsuspecting drivers to swipe their credit cards so cyber-thieves can immediately compromise their credit card credentials.

How Do Skimmers Get Into Gas Pumps?

Millions of gas pumps currently in use, utilize a universal lock and key system. While convenient for gas station attendants and maintenance workers the six generic key types that open the majority of all the gas pumps, are also quite favorable for any savvy cyber thief. For only $10 a complete set of keys can be purchased on eBay and it grants access. On the dark web (the underbelly of the Internet where cyber thieves buy and sell illicit goods anonymously) thieves can easily purchase a Bluetooth credit card skimmer unit including how-to installation videos and 24/7 customer support. This allows amateur cyber thieves to enter a whole new market of crime in no time. For only a few hundred bucks and the nerve to covertly install one, (it only takes about 15 seconds) the average Bluetooth skimmer rakes in $110,000 in stolen credit cards for cyber thieves before being discovered or removed. The same wireless technology that powers your AirPods also allows thieves to rest in their cars, up to 150 feet away from the scene of the crime, and collect stolen credit data at their convenience. They can then go home and use this stolen data to burn cloned credit cards that are no different from the one that was stolen. These cloned cards sell on the dark web for around $3 to $5 each. From there, the buyers begin a mad dash, a spending spree to accumulate as many purchases as they can with the card before it is shut off by the issuing bank.

How Big Is The Skimmer Problem?

Even though the skimmer problem is huge, very few individuals or organizations currently report the problem. Perhaps their resistence is because the root of the problem is too difficult for them to pin down. After all, we all have to gas up our vehicles once or twice every week in a hurry, and give little thought to a harmless looking gas pump. And when our banks shut down our credit cards for suspicious activity, the damage has already been done. But U.S. consumers typically enjoy a full refund for any fraudulent charges so there is little incentive for them to investigate further. To make matters even worse, many media outlets have misinformed the public by telling them to simply use their Smart phones to scan for suspicious Bluetooth devices in the area while they are fueling up at the gas pump. But how can the average consumer distinguish between a legitimate Bluetooth device and one that is suspicious—especially while looking through a list of 20 nearby devices? Surely, there is a better way.

A Better Mouse Trap

State inspectors have found Blue-tooth skimmers in over 1,000 gas pumps across the state of Florida alone in 2018. That is up from 650 skimmers discovered in the previous year and 220 in the year before that. It does not take a master detective to see the sharp rise in this problem, and we are just talking about known skimmers in Florida alone. This year, I was contacted by the National Weights and Measures division of the U.S. government as well as several law enforcement groups throughout the U.S. who were searching for a tool to combat this growing threat by accelerating searches and avoiding the false positives for hidden Bluetooth skimmers.

My answer to their challenge is the BlueSleuth Bluetooth locator which can wirelessly pinpoint known suspicious Bluetooth devices without the need for opening up and visually inspecting every gas pump first. The device goes further and can even locate cyber thieves as they connect to their skimmers. We have received great feedback from agents in the field so far, but security is a never-ending cat and mouse game, so I look forward to the next round of technical iteration and advancement in the business of illegal skimmer crime fighting. In the meantime, know that the next time you pay at the gas pump, those cyber thieves eager to skim your stolen data are just one step closer to paying for their crimes. ■

Scott Schober, President and CEO of Berkeley Varitronics Systems, Inc. is a Cyber Security Expert and the author of the best-seller, Hacked Again. Scott is the 'go to guy' for learning how to protect ourselves from cyber thieves by understanding security issues we can correct before it's too late. Check out his new book, CyberSecurity Is Everyone's Business. BVsystems.com Amazon.com ScottSchober.com