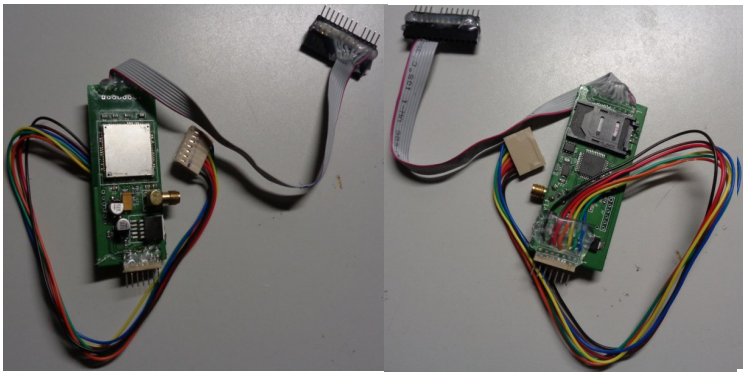
HAFER EQUIPMENT

Customer Newsletter

Issue 02: October 2017

Gas Pump Skimmer Devices Now Sending Data Via Text

Often skimming devices that crooks are installing inside fuel station gas pumps are relying on an embedded Bluetooth component allowing the thieves to collect stolen credit card data from the pumps wirelessly with any mobile device. However, they found the downside to this is that anyone with a mobile device can detect the skimmer. To determine if the dispenser has a Bluetooth skimming device inside, while standing next to the pump, try connecting to Bluetooth. If you see a long string of numbers trying to connect, that's a sign that there's a Bluetooth skimming device inside the dispenser. The newest type of skimmer has been created using cannibalized cell phone components to send stolen card data via text message. The thieves have found using the GSM based skimmers enable stolen card data to be transmitted wirelessly anywhere in the world. This data is then used to create physical counterfeit copies of the cards. Skimming devices are now being hooked up to the pumps internal power, allowing it to operate without using separate batteries.



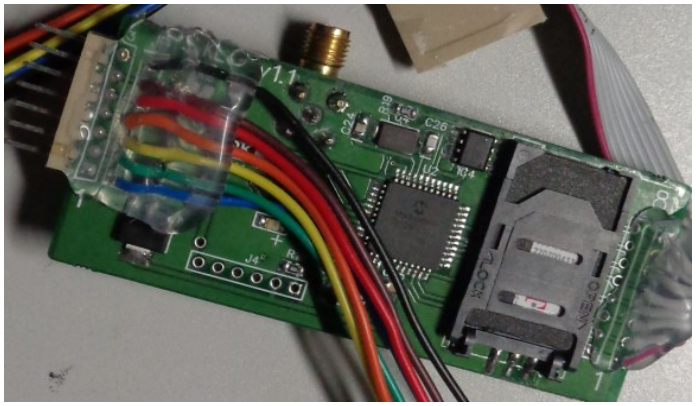
Upcoming Training Schedule:

• Passport	October 23-27
• Veeder Root	November 13-16
• Dispenser	November 27–December 1
• Passport	December 18-22

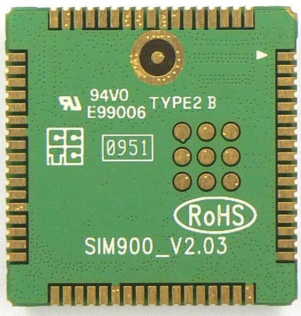
Concerned About Possible Credit Card Theft?

See Hafer's For Your Secure Transaction In The Forecourt

Fraud patterns are showing that the fuel theft gangs tend to target stations that are close to major highway arteries; those with older dispensers, and those without security cameras, as well as stations that do not do a regular scheduled inspection with security tape placed on the dispensers. EMV Serves as a substantial barrier to prevent thieves from successfully cloning credit cards.



New skimmers are using chips, like the SIM900, a quad-band GSM/GPRS module with a very powerful single-chip processor as the backbone of the newest generation skimmers. Skimmers are not a new problem, but the technology that powers them has markedly improved over time. Previous incarnations were easy to spot with the naked eye, but newer versions are all but invisible.



Credit Card Data Theft Prevention Tips

- **Use a credit card, not debit card, when you pay.** If a credit card number is skimmed, you're more protected than if you were to pay with debit.
- **Pay inside, with cash or a credit card, rather than at the pump.** Chances are good that thieves have not entered the physical building to tamper with the pump.
- **Pay attention when fueling and if it feels weird, don't do it.** Sometimes, thieves also swap out the card readers attached to the skimmers. In those cases, they can deliver an unusual feeling to the inserted card – it may stick or otherwise feel not quite right. If that happens, cancel the transaction and pay inside.
- **Be suspicious if the gas pump has a broken security seal, or the word "void" appears on it.** These are part of a voluntary program by the industry to thwart gas pump tampering.
- **Choose pumps closest to the physical building,** not the ones hidden around the corner.

Contact us to learn more!

(800) 422-8135

sales@hafers.com