# Offering Emergency Computer Help, Online Scammers Swindle About $1,800 from Darien Man

**Author :** David Gurliacci

**Categories :** Public Safety

**Tagged as :** Computer Scams 2016, Crime Prevention Advice, Crime Prevention Advice 2016, Internet Scams 2016, Online Scams 2016

**Date :** December 6, 2016

A 76-year-old Darien man told police last week he was repeatedly victimized by online scammers with bogus offers of help with computer problems.

Darien police gave this account of the incidents after the man contacted police last Tuesday, Nov. 29.

It appears that $1,837 was stolen by the scammers, but the man's credit card company may reimburse him for some of the charges. The scam took place over a period of months, beginning on Aug. 5.

While the man was online, an urgent, loud message appeared on his screen telling him to call a phone number because a virus had infected his computer. He called and was told he should pay a total of $939 for an anti-virus program. He paid with his credit card.

_____

*At the bottom of this article is some advice given last June about avoiding what the FBI calls the "Tech Support Scam" and a link to the FBI announcement.*

*See also these articles on other Internet-related to scams:*

- Scam Alert: Fake ‘Missed Delivery’ Scheme Unleashes Havoc on Your Computer (Dec. 5)
- Darien Police: How to Identify Someone Scamming You, Especially if You’re a Senior (Sept. 21)

- Darien Police: Don’t Fall for Overpayment Scam in Online Car Selling (April 29)

_____

On Nov. 14, he was contacted by what purported to be another another computer-assistance company which told him he had a problem with his I.P. [Internet protocol] address — the unique string of numbers that identifies each computer. He was told the company could fix the issue if he paid them $449. He paid with his credit card.

The company then double billed him, charging him $898.

They contacted him about the double billing. He was told by someone representing the company that the employee who made the double billing mistake was fired, and the company wanted to reimburse him. The victim was told he would be sent a check for the entire amount, but in order for the transaction to take place, he would have to authorize another payment. He did so.

Thinking about the matter the following day, he realized that he'd fallen for a scam.

_____

*Like this article? …*

- *Sign up for the* Darienite.com weekday newsletter.
- *Like Darienite.com* on Facebook.
- *Follow Darienite.com on Twitter.*

_____

At some point, he was contacted by what purported to be yet another computer company, which offered him a "firewall license" for $399. He bought it but cancelled the credit card payment, which his credit card company allowed.

After the man reported the swindle to Darien police, detectives began investigating. The credit card payments were made to "Studio S.O.S." and "Web Tech Craft Inc." The companies may be based in New York state, California or Hawaii.

_____

**FBI Advice About the 'Tech Support Scam'**

Here's an excerpt from an announcement on the FBI's Internet Crime Complaint Center. The announcement describes parts of the crime the Darien man experienced, along with other variations:

**Defense and Mitigation**

- Recognize the attempt and cease all communication with the subject.
- Resist the pressure to act quickly. The subjects will urge the victim to fast action in order to protect their device. The subjects create a sense of urgency to produce fear and lure the victim into immediate action.
- Do not give unknown, unverified persons remote access to devices or accounts. A legitimate software or security company will not directly contact individuals unless the contact is initiated by the customer.
- Ensure all computer anti-virus, security, and malware protection is up to date. Some victims report their anti-virus software provided warnings prior to the attempt.
- If a victim receives a pop-up or locked screen, shut down the device immediately. Victims report that shutting down the device and waiting a short time to restart usually removes the pop-up or screen lock.
- Should a subject gain access to a device or an account, victims should take precautions to protect their identity, immediately contact their financial institutions to place protection on their accounts, and monitor their accounts and personal information for suspicious activity.