Computer & Networking Technologies, LTD

September, 2018

Special Points of Interest:

- Tech-support Scammers
- Monster Deal
- Fall Into Savings

CNT

Tech-support Scammers Are Ramping Up Attacks

Windows 10 security or any anti-virus won't protect you from tech-support scammers' lies and trickery.

Microsoft says it received 153,000 reports in 2017 from customers who'd come in contact with tech-support scammers via a cold call, spam, or the web.

The reports from customers last year were up 24 percent on 2016, with filings coming from 183 countries.

Despite being a well-known fraud, some 15 percent of Microsoft customers who reported incidents lost money. Losses were typically between $200 and $400 each.

However, Microsoft received one report of a customer in the Netherlands, whose bank account was drained of €89,000 ($109,000) after contact with a tech-support scam.

The FBI in March reported it had received 11,000 tech-support fraud complaints in 2017 with claimed losses totaling nearly $15m, up 86 percent on reported losses in 2016. It received reports from victims in over 80 countries.

Part of the problem lies in the huge variety of hooks and techniques the scammers use. Besides masquerading as Microsoft staff, scammers also claim to represent GPS and printer companies, as well as ISPs.

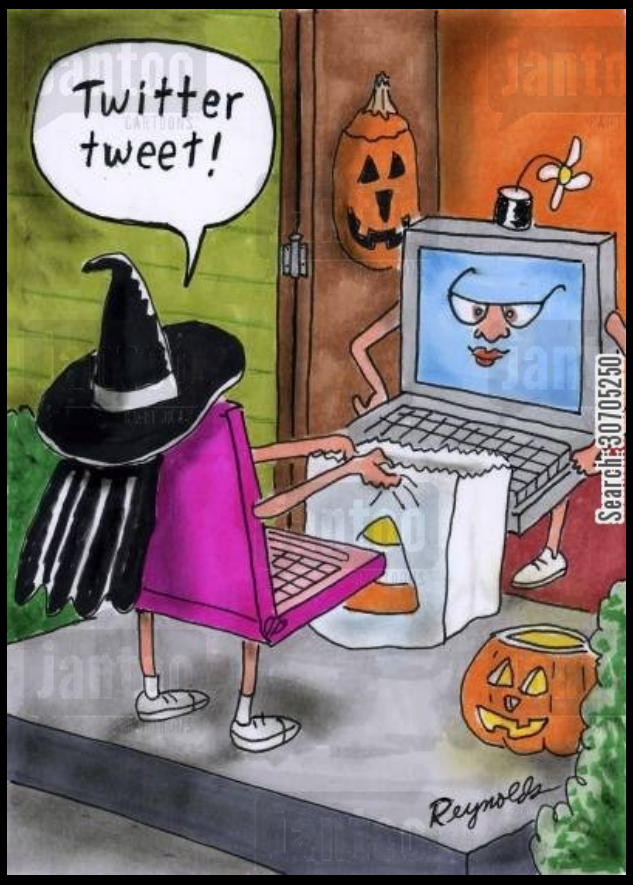
And along with phone calls, scammers reach victims through paid search results, pop-up messages, browser lockers, and phishing emails, with bogus warnings about fraudulent bank charges or fake refunds.

The FBI has recently seen a new trend emerging for scammers to retarget past tech-support victims by posing as government officials or law enforcement, and offering assistance recovering lost funds for further fees.

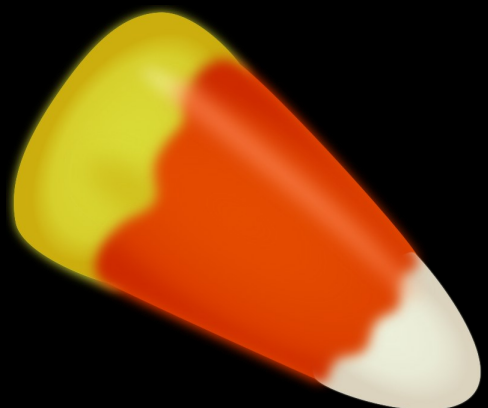
Some scammers also threaten legal action if victims don't pay to settle outstanding debts for tech-support services.

And once scammers have been granted remote access, they're not just presenting bogus security warnings, but increasingly downloading personal information and using it to request bank transfers or to open new accounts to make fraudulent payments.

Microsoft's advice for anyone who has given personal information to fake tech support or paid for bogus services is to uninstall any applications used to provide the fake support, run a scan with antivirus, change all passwords, and call the bank to reverse the charges.



CNT



MONSTER DEAL OF THE MONTH

Deals so big, they're scary!

- Intel Core i3 3.4GHz Processor
- 8Gb RAM
- 120GB SSD Hard Drive
- On Board Video
- DVD+/-RW Drive
- Integrated 10/100/1000 Ethernet
- Integrated Sound
- 6-USB Ports
- Microsoft Antivirus
- Mouse & Keyboard
- Microsoft Windows 10 Pro
- Mouse pad
- 20" LCD Flat Panel Monitor

One Year Manufacturer's Warranty

ONLY $869

*or $769 without Monitor!

**Prices good while supplies last!

CNT

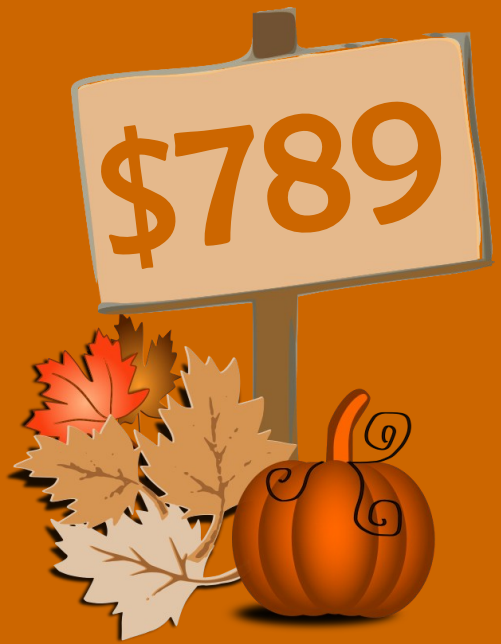
Fall Into savings

- Intel Pentium D 3.2GHz Dual Core Processor
- 8Gb RAM
- 120GB SSD Hard Drive
- DVD+/-RW Drive
- Micro-Tower Case
- Integrated Video
- Integrated Sound
- Integrated 10/100/1000 Ethernet
- Optical Scroll Mouse
- 104-Key Keyboard
- Microsoft Antivirus
- Microsoft Windows 10 Pro
- 20"" LCD Flat Panel Monitor

Windows 10

CNT

One Year Manufacturer's Warranty



Options:

- Upgrade to a 2GB Video Card - add $79
- MS Office Home/Student 2016 - add $159
- Add MS Office Home/Business 2016 - add $239

Upgrades:

- Wireless Optical Notebook Mouse - $30