Pop-Ups and Impostors

A Better Business Bureau Study of the Growing Worldwide Problem of Computer Tech Support Scams

BBB International Investigations Initiative:
BBB Chicago | bbbinfo@chicago.bbb.org
BBB Dallas | info@nctx.bbb.org
BBB Omaha | info@bbbinc.org
BBB San Francisco | info@bbbemail.org
BBB St. Louis | bbb@stlouisbbb.org

BBB International Investigations Specialist
C. Steven Baker stbaker@bbbinc.org

December 2017

COMPUTER SCAMS

Imagine your computer freezes, with a full-screen warning and the speakers blaring a voice. The voice tells you that all your personal data, including credit card information, email passwords, and social media logins have been compromised. To make matters worse, your personal data is being sent to hackers — how frightening would that be?

Growing numbers of people are being victimized by networks of thieves posing as skilled computer technicians who operate from the shadows, using sophisticated advertising and carefully crafted sales techniques to scare consumers into buying phony fixes for their home and business computers.

Simply put, these tech support scammers depend on their ability to convince people that their computers have a virus, malware or have "crashed" when in fact there is nothing wrong with the devices.

Consumers are most often brought into the scheme through a sudden and persistent **pop-up warning that appears on their computer screen or by an unsolicited phone call from a "technician" claiming to have detected problems with the user's computer.** Some consumers have described high-pitched squeals or alarms; several have said their computers have suddenly locked up or frozen. In many cases these warnings are not the pop-up ads that are fairly common; rather, they look like error messages generated from the computer itself or even the "blue screen of death" that appears when a computer crashes completely. The screens provide a telephone number for the victim to call. Several consumers have said the pop-ups make it appear that the phone number is connected to a reputable tech company, such as Microsoft, HP, Apple or Dell.

Once connected to the toll-free number, a "sales technician" (often from India) offers to repair any issues and asks for payment. In each case, the "technician" on the phone offers to take remote access of the computer, scan the device for issues and take any necessary measures to protect it from future problems. The price tag is often around $500, but the cost can be even higher.

The sales technicians often pretend to be from Microsoft, Apple, Dell, or other trusted companies. When the payment is made and the consumer grants remote access to their computer, the representative begins running through what they describe as a series of diagnostics and "fixes" to the machine. Consumers have described sitting in front of their screens – sometimes for more than an hour – watching as a remote operator controls their computers.

Although there are tens of thousands of complaints, this tech support scam may be seriously underreported because many victims do not even know that they have been defrauded. Others learn only later that there was nothing wrong with their computers and they were duped.

This fraud has become so common that anyone with an internet connected device is at risk. In a **2016 global survey**, Microsoft found that **two out of three people experienced a tech support scam in the previous 12 months.** Unfortunately, for most of us it isn't a question of if we will become targets of these thieves, but when.

The computer scams also may capture the victim's account information during this process, and use it later to gain online access to the victim's bank accounts. In at least some cases the scammers may actually install spyware on the victim's computer.

Therefore, anyone who has been a victim of a tech support scam should have their computers checked to be sure no unwanted software has been installed.

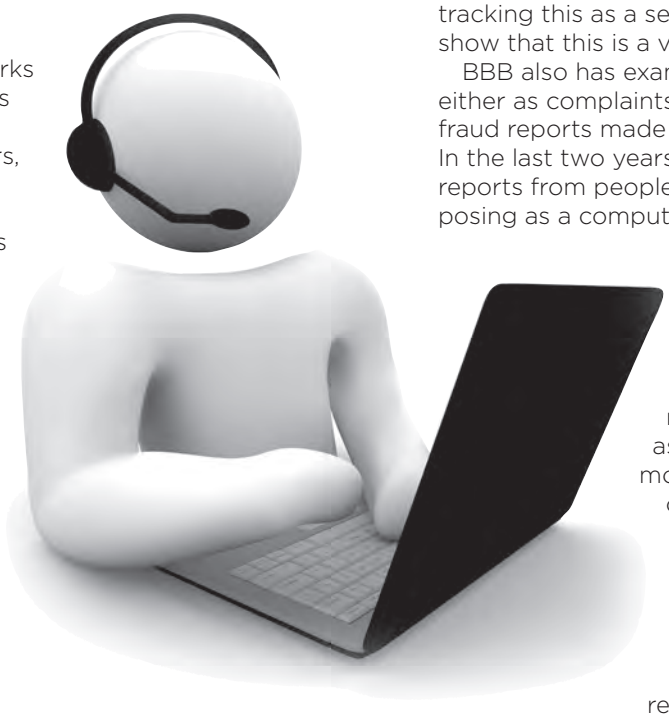
Victims also need to be alert to follow-up contacts claiming to offer them a "refund," at times even from impersonators of Better Business Bureau (BBB). The fraudsters have gotten access to online bank accounts of some victims, moved money from the victim's savings to their checking accounts, and then pretended that they have gave victims a refund. The fraudster claims to have accidentally provided a larger refund than was owed, and asks victims to take the "overpayment" and send it back to them. Often the fraudsters will claim that they will lose their jobs unless the victim helps them out by "returning" money.

Courtney Gregoire, Assistant General Counsel with Microsoft's Digital Crimes Unit, calls tech support scams "pervasive global cybercrime that needs to be addressed through expanded enforcement, technology disruption, and consumer education." Microsoft has referred cases directly to law enforcement globally, and works across industry to combat fraud with working group members including Dell, HP, Intuit, and others.

The evidence shows that the majority of tech support scams take place from call centers in India, a country that has recently become the source of IRS impersonator calls and other types of fraud. Many companies have outsourced their customer service functions to call centers in India over the years, and it seems likely that some scammers have used their skills to move into fraud efforts.

This study is an effort to identify the scope of the problem, explain how it works and offer recommendations on what can be done to reduce its toll on consumers, both financially and emotionally.

This tech support scam is distinct from ransomware frauds, which use malware to encrypt all the data on the victim's computer system and then demand payment by bitcoin to unlock it. With tech support frauds, simply powering off the system and rebooting it will normally eliminate the warning screens and return the computer to working order.



The scope of the problem:

Consumer reports of computer tech support scams have exploded in recent years. Virtually anyone who owns or uses a computer is a potential target – from the college student researching a history project on their laptops, to senior citizens searching out a holiday cookie recipe on their computers.

Statistics gathered from a variety of reporting sites are staggering. **Microsoft** – whose corporate name is dropped regularly by thieves hoping to gain the trust of skeptical consumers – **reports receiving 12,000 complaints worldwide every month.**

The Federal Trade Commission (FTC) maintains the national Consumer Sentinel Network complaint system, which includes complaints not only to the FTC, but also those made to BBB, the U.S. Postal Inspection Service, about half the country's State Attorneys General, the Consumer Financial Protection Bureau, and many other organizations. The FBI's Internet Crime Complaint center (IC3) also receives and tracks complaints.

YEAR	2014	2015	2016	2017	(1/1 – 9/30)
FTC	134	40,004	45,319	33,132	(losses $13,177,470)
IC3			10,850	8,303	(losses $7,865,585)
TOTAL	134	40,004	56,169	41,435	(losses $21,043,055)

Although there may be some overlap with people complaining to both the FTC and IC3, and IC3 only began tracking this as a separate crime in 2016, these numbers show that this is a very large and serious problem.

BBB also has examined the reports that it has received, either as complaints filed about specific companies or fraud reports made by consumers to BBB Scam Tracker. In the last two years, BBB received about 7,000 total reports from people claiming that a company fraudulently posing as a computer repair or security service contacted them to fix a real or alleged malware/virus.

Outside the U.S., the United Kingdom recently reported more than 34,000 complaints of tech support scams in the past year, making what that country refers to as "computer fixing fraud" the second most common source of consumer complaints.

But the reported numbers tell only a part of the story. An FTC study indicates that less than 10 percent of consumers victimized by fraud actually complain to law enforcement or to BBB. In addition, research from Nielsen Inc. estimates that for every one complaint or report that the BBB receives, there are at least 50 more cases of serious consumer dissatisfaction that never reach BBB.

This problem is compounded in the tech support area by the fact that many people believe they are working with legitimate businesses, never realizing they have been defrauded, and thus do not file complaints. **William Tsing** of Malwaybytes confirms this, stating that "It's quite common for tech support scam victims to not realize they've been scammed, which is something our Customer Success team encounters on a regular basis."

While the ages of potential and actual victims run the gamut, **Microsoft's 2016 survey revealed that millennials between the ages of 18 to 34 were more likely to continue with a fraudulent tech offer than other age groups.** On the other hand, scam reports received by Microsoft tend to be from older consumers.

The U.S. states with the highest per capita numbers of

complaints and scams of this pattern reported to BBB are (in descending order): Idaho; Hawaii; Wisconsin; Minnesota; Alaska; Ohio; and Washington. BBB found that approximately equal numbers of males and females have become victims of tech support fraud.

Sherry Thomas from the St. Louis suburb of **Hazelwood, Missouri**, was viewing an online cosmetics product on her three-month-old computer when a warning suddenly appeared on her screen, joined by an automated message over her speakers alerting her to a dangerous situation with her device. The pop-up warning instructed her to call a number on the screen to address the issue.

The person who answered told Thomas he worked for a subsidiary of Microsoft. He told her that her computer had been infected by a virus.

The technician, who said he represented a business called Cromshield, took remote control of her computer and charged $179 to her debit card to "fix the problem." Suspecting she had been victimized, she took her machine to a Best Buy store where she was told there was nothing wrong with her computer and she had been scammed.

Thomas said the story didn't end there.

A year later, a representative claiming to be from the same company called again, this time saying it was refunding her initial payment. But, instead of returning her original $179, the company said it inadvertently had deposited $2000 into her checking account. They asked her to buy $1821 in iTunes gift cards to return the overpayment. Thomas realized it was another scam and immediately declined. She says she felt violated by the incident. Her advice: Call BBB and make sure to keep any supporting documentation from the scheme.

Using the right bait: How consumers get hooked

Tech support scammers use a number of ways to contact potential victims. In addition to pop-up ads many consumers say they have received unsolicited phone calls claiming to be from a reputable tech company or Internet Service Provider, claiming to have detected a virus or malware problem with their machines.

Some thieves have gone so far as to send emails to potential victims that trigger pop-ups when they are opened encouraging calls to tech support numbers. Scammers are always trying new ways to operate. Though the information below is built on experience in dealing with these schemes, it is entirely possible that they will develop additional methods of reaching potential victims.

Some tech support scams also have taken advantage of the publicity surrounding recent ransomware attacks around the world. Because many of these pop-up viruses freeze consumers' computers, the thieves tell them they are victims of a ransomware scam and the company can help them through the attack.

Ransomware. Admittedly a growing and dangerous problem, operates very differently in that victims typically open an email attachment that contains malware. The program inadvertently installed on a computer system encrypts all the data, making it unreadable. Ransomware frauds then contact victims, offering to decrypt the files. These frauds almost always demand payment by Bitcoin.

Among the thousands of incidents reported to BBB Scam Tracker, approximately 45% describe being hooked by a pop-up warning message, 45% describe being hooked by an unsolicited telephone call, and 10% by other means or unspecified.

There are actually several roads that can lead potential victims to a tech support fraud including through: pop-ups; sponsored links; internet searches; cold calls; and even emails.

Warning screens. Nearly half of these computer scams begin with a full screen alert message appearing on a user's computer screen stating that a problem has been detected, directing the user to a legitimate-looking technical support phone number. Many of these full screen messages freeze the browser window — and do not allow consumers to close the browser or switch to other programs. Thus victims often believe that their computer has crashed, potentially losing of all data on the computer. These screens sometimes warn that powering down the computer will mean that data on the system will be destroyed. Some of these alerts include audio messages.

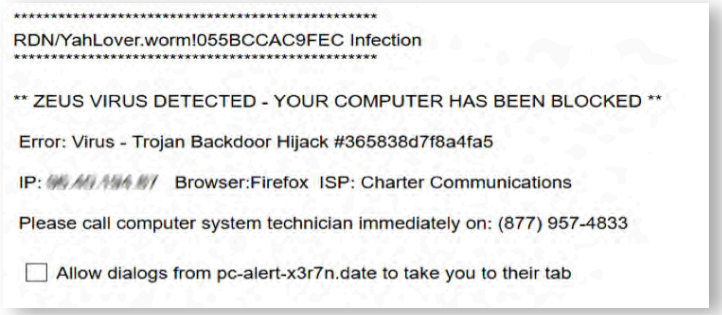
A **recent academic study** of the tech support industry at Stony Brook University in New York found that in many cases victims end up with a pop-up after mistyping the web address of a popular website. If a user accidentally types in "twwitter.

com", with an extra "w," a pop-up (along with obscene content) may suddenly freeze the computer browser. The academic study located 22,000 of these "typo squatting" domain names.

They also found that 88% of these malicious sites are hosted, or have their data actually located on computer servers, in the U.S. Usually the same pop-up will not appear if you try the same mistyped web address again from the same computer. Microsoft recently has introduced a new feature in its Windows Defender that warns consumers if they are going to a website that may trigger a pop-up for this fraud.

Note that in most cases these pop-ups simply appear without the victim clicking on any links or taking any affirmative action. Thus victims often conclude that these are messages their computer has generated or that they come from their Internet Service Provider.

This pop-up recently appeared on the author's computer:



Note that the warning specifically refers to the author's browser (Firefox) and cable company (Charter). The on-screen message was accompanied by a repeated warning coming through the computer speakers:

"Error number 268d3. Cripple alert from Microsoft. Your computer has alerted us that it is infected with virus and spyware. This virus is sending your credit card details, Facebook log and personal emails to hackers remotely. Please call us immediately at the toll-free number listed so that our support engineers can walk you through the removal process over the phone. If you close this page before calling us we will be forced to disable your computer to prevent further damage to our network."

In most cases, the best way to clear the warnings is simply to close the browser or reboot the computer.

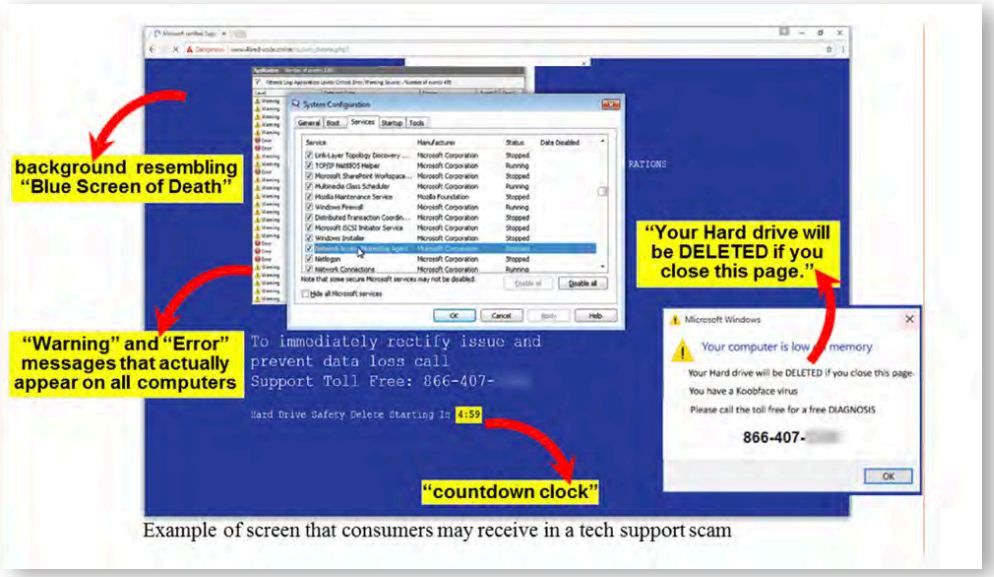
The FTC has also provided this example of another screen that can appear on a victim's computer:

Cold calls. In almost half of the cases reported to BBB, consumers receive calls from people claiming to be from Comcast, Norton, Dell, or other technical-sounding companies saying that their central servers have detected signals that the consumers' computers have viruses, spyware, or other security problems and the company needs to remotely access the computer to determine whether there is a problem. Inevitably they find problems and offer to fix them – for a price.

Recently the scammers have begun to use robocalls to reach potential victims. **BBB has reported** that some tech support frauds are using robocalls with caller ID numbers, making it appear the call is from Apple. They tell victims that their iCloud account has been hacked, and offer to remotely access their machines and make repairs. Because the purpose of these robocalls is to sell goods or services the calls themselves are illegal.

Like other telemarketing frauds, the Caller ID will almost never reveal the true location of the person calling. Some fraudsters buy cell phones with US area codes, and those that call through the internet, using Voice Over Internet Protocol (VOIP), can easily obtain special software that "spoofs" the telephone number and again makes it appear that the call is coming from somewhere in the United States.

Sponsored links. When a consumer uses a search engine, the first search items appearing in the queue are paid advertisements. If consumers search for "tech support" or for a specific computer problem, they will receive a list of paid ads, often claiming to be associated with Microsoft or approved by the company. Microsoft warns that many of these links go directly to businesses set up specifically to scam consumers. In fact, in 2016 **Microsoft announced that it no longer allows online tech support advertising from third parties,** due to the high rates of fraud and the need to protect users and industry partners from scammers. In fact, Microsoft says it blocked 17 million fraudulent tech support ads from



Example of screen that consumers may receive in a tech support scam

reaching consumers January through December 2016.

Internet searches for technical support/non-sponsored ads. Some people searching for help for computer issues come across other sites that do not have paid advertising but are nonetheless simply meant to attract potential victims. For example, some legitimate online businesses, such as antivirus providers, may not have customer support telephone numbers or they are difficult to find. Frauds may have online ads claiming that they are affiliated with Microsoft or another legitimate company, when they really are not. Thus consumers seeing these sites and calling for assistance may find themselves talking to a tech support scammer.

Emails. Microsoft **recently reported** that these tech support scammers also have begun using email to reach potential victims. The emails, appearing to be from well-known companies like LinkedIn, Amazon, or Alibaba, are disguised as invoices, cancelled orders or social media messages. If consumers click on the link, they are sent to a compromised website that redirects them to sites operated by tech support scammers. The sites then signal pop-up warnings instructing the consumer to call a phone number for technical support.

Marissa Evans, a college student living in **Commerce, Texas**, was on a movie website when she abruptly received a pop-up message warning her that she was at risk of having her passwords and credit card information stolen. Her computer screen froze and, unable to operate the device, she called the phone number on the screen. The representative on the other end of the phone instructed her to download software to allow him remote access to her laptop. Evans was told the "company" had discovered a virus in the system. She used a debit card to pay $250 to fix the problem.

When the computer stopped working entirely, Evans tried to get a refund. Although promised a refund she never received one. She registered a complaint with BBB. Ultimately, she had to buy a new computer.

Who are behind these pop-up viruses?

Tech support businesses hoping to steal your money usually hire other businesses to direct pop-up ads to a consumer's computer. Because the pop-ups contain deceptive claims, those responsible for them are also liable for false claims made in them. In fact, in the FTC's **lawsuit against tech support Help Desk National** the FTC also sued a third party company that was responsible for the pop-up.

What happens to those who call the phone number provided?

A call to a pop-up phone number often will direct a consumer to a business claiming to be associated with Microsoft or another familiar company. These "salespeople" will tell potential targets that their computer has to be infected with a virus or they would not have received the pop-up (or phone call).

In FTC's press release on a recent enforcement effort the FTC has even posted a **two minute clip of the conversation** with one elderly victim in the right margin.

Microsoft tech support scammers will offer to look at the consumer's computer to investigate. They tell victims to download free software from legitimate companies like Logmeinrescue.com or Citrix GoToAssist. Victims download the programs and the scammer gives the consumers a code over the phone to activate the service.

At this point, the scammer has full control over the victim's computer and can explore files, change settings, or do almost anything else that the consumer could do with their own system.

With the victim still on the telephone, the scammer proceeds to pull up completely normal files and tell victims that these are the result of malicious programs such as Zeus or Koobface, and that the victim has a very serious problem with their computer, which the scammer then offers to fix.

In the **Stony Brook University study**, researchers located phone numbers of several fraudulent tech support businesses, made sure their computers were free of viruses or other problems, and called the businesses posing as potential customers. They found that those they called were extremely patient, typically spending a full eleven minutes on the phone with the victim and highlighting alleged "problems" before asking for money. If researchers asked why this problem was not addressed by the victim's antivirus program, they were often told that the safeguards were ineffective or out of date.

The researchers reported that the average amount of money requested was $290, though some bogus tech support operations asked for as much as $1000 for multiyear continuing support. This average loss is consistent with complaints received by BBB. If the researchers asked about taking their computer to a local store for repairs, the bogus technicians often claimed that those companies would charge up to $500, and the consumer likely would be without their computer for several days. The thieves typically complimented the callers on the quality of their computers, apparently in an attempt to convince them that the remote fixes would be sufficient to correct their problems.

The Stony Brook researchers did not pay money for the services, so they did not complete the process. However, in FTC cases where undercover purchases were made, the FTC found that the scammers did a full scan of the consumer's computer, which could take several hours, and usually sold them an additional antivirus program as well – for even more money.

Sally Komrofske of **Omaha, Nebraska** was reading an article on Facebook, when she clicked a "read more" link and was confronted with a blinking alert on her computer screen. A voice announced that the computer had been compromised by a serious virus, and asked her to call the telephone number on the screen. She said she ultimately spoke with a man who identified himself as a representative of Micra Tech, supposedly a subsidiary of Microsoft. After allowing him remote access, she was told a virus had infected her computer and she was offered three options: $200 for one year of support, $300 for three years; and $500 for five years. Suspicious, Komofsky hung up the phone, saying she had to first speak to her son-in-law. Because her computer had stopped working, she had to pay $88 to a local technician for repairs. She reported the scheme to the Omaha BBB. Since then, she said she has experienced similar pop-ups and has also heard from friends who have been similarly victimized. Luckily, the friends did not pay for repairs. Komofsky's advice: "Don't listen to (the thieves); just hang up."

How do people pay?

There is no reason for scammers to run a fraud if they can't collect the money, so this is a key part of any scam investigation. It is critical for law enforcement to understand how payment was made, so that authorities can "follow the money" in such transactions.

Stony Brook University researchers found that they were consistently asked to pay by credit card. Additionally, in one FTC case the scammers sent the consumers to a separate website at click4support to enter credit card information.

According to a study of BBB complaints, payment types requested or arranged by scammers overall are as follows:

Payment Type	%
Credit/debit card	55%
Check	36%
Invoice	4%
Gift card	3%
Money order	3%

BBB also looked at the payment types requested for each of the last three years. This shows that although credit cards are still the main payment types, the use is declining and payment through checks is increasing.

Scammers who can't get access to the credit card system may ask for payment though Western Union, MoneyGram, a stored value card, or a remotely created check. The **FTC's telemarketing sales rule** makes it illegal in any telephone transaction to require payment by those methods.

With remotely created checks, scammers ask victims to provide their checking account information over the phone and agree to have money withdrawn from their account. With this information the scammer can create a check, although it of course does not contain the signature of the victim. Again, use of this payment method when a telephone call is involved **is now illegal**. Victims that have paid for tech support services with this method should contact their bank.

Victims that are defrauded in a credit card transaction should be able to get their money back. **Disputing a charge because it is a result of fraud is called a charge back.** MasterCard and Visa generally require that victims dispute the charge within 120 days (four months), but if the victim does not discover the fraud immediately these companies may extend this period. In addition, victims that have paid with a debit card may have similar protection if their debit card operates through the Visa or MasterCard system.

Complaining about a fraudulent charge is also important because it alerts credit card companies to potential scams. Credit card companies that discover an unusual number of charge backs can trigger the closing of an account — leaving the thieves without this convenient method to get paid.

Recently, many bogus tech support operations (and other types of computer scams) have begun asking victims to buy gift cards to pay, similar to the previously mentioned case of Ms. Schwab who was directed to pay for her tech support service with iTunes gift cards. If victims read the card number over the telephone, scammers can get access to the funds on the cards. BBB is not aware of any legitimate business taking payment through iTunes or any other type of gift card.

Where are the victims?

This is a worldwide problem. In the Stony Brook University study researchers found that the top five countries with the most victims were: U.S. — 33.6%; Australia — 25.36%; Singapore — 22.4%; Canada — 7%; and New Zealand — 4.8%. The researchers reported to BBB that thieves also have hit the UK hard. This is one of the top two complaints to the London Metro Police.

Who are the thieves?

The Stony Brook University study looked at the Internet Protocol addresses of the scammers and concluded that 85.4% of them are in India; 9.7% are in the U.S., and 4.9% are in Costa Rica. There are a variety of these operations located in Florida, and a number of these have been the subject of lawsuits by the FTC or the Florida Attorney General.

Note that consumers cannot determine the actual location of the scammers from the Caller ID on their phones. The major telephone carriers are reportedly working with the Federal Communications Commission in an effort to deal with this problem, as well as to attack robo (or automated) telephone calls.

Some tech support scammers may have a physical presence in the U.S. The FTC **recently sued and settled** with a tech support company that was incorporated in St. Louis – a case that was initially brought to the agency's attention by BBB St. Louis. While the head of the company was an Indian national living in the St. Louis County community of Creve Coeur, Mo., the FTC found that the bogus technicians were operating out of a call center in India. There are most likely additional operations that have people in the U.S. fronting for the frauds. We believe this is done because it is difficult to obtain a credit card account from outside the U.S.

While some operations have locations in both the U.S. and India, others are based entirely in India. India is known for performing outsourced work on behalf of U.S. companies – both legitimate and illegitimate. India-based telemarketing frauds have erupted in the last few years – not just in the area of tech support, but also in cases involving Internal Revenue Service (IRS) impersonators, government grant schemes and thieves claiming to be U.S. immigration agents.

In **Durand, Illinois, Jeannie Schwab's** husband got a phone call claiming the couple's Windows license was expiring. He thought they were dealing with Microsoft support and let the caller take remote control of their laptop computer. The caller said the Schwabs needed to buy a "new license key" for $400, instructing them to make payment through iTunes gift cards. Schwab said she bought the cards and read the activation codes on the back of the cards to the caller. However, the caller claimed that two of the cards were no good, and instructed her to buy another $150 in gift cards. He also wanted additional money for ongoing tech support.

She hung up and took her laptop to a local computer store, which quickly cleaned the machine. She notified BBB, and then the local police. She also called Apple to tell them about her issues with the iTunes cards. She advises those getting similar calls to "just hang up."

Should I worry about my computer being compromised by someone with remote access to my computer?

There is very troubling evidence that at least some tech support scammers are taking advantage of their access to victims' computers and stealing the information needed to get into online bank accounts. In some cases thieves have moved money from an online savings account into a checking account, and then phoned the victim, advising them that a refund has been deposited into their bank account. The potential victim is then told that the business mistakenly sent too much money and asks that some of the money be "returned" through Western Union, MoneyGram, or a gift card. The caller often pleads that they will lose their job over this "error" if the victim does not help and send funds.

IC3 reports of this type of "refund" fraud are on the rise. Jonathon Frost, a Programme Director with the UK's National Fraud Intelligence Bureau (NFIB) operated by the City of London Police confirms that this practice is happening from operations in India. He also says that in some cases the frauds simply take money directly from the victim's online bank account.

National Fraud Intelligence Bureau

IC3 also warns that scammers have at times locked victims out of their computers if they decline to pay for the tech support "services," and have become threatening or abusive to those who do not want to pay.

If you believe your bank account may have been compromised in a tech support scam, and especially if you have provided checking account information over the phone, contact your bank immediately. BBB also recommends that anyone who believes they have been victimized should take their computer to a trusted local business to have it checked out thoroughly.

What is law enforcement doing?

The FTC has brought a number of civil cases against phony tech support operators over the last several years. The FTC has no criminal authority, so it seeks injunctions and attempts to return money back to victims. In the

ICE tech support case the FTC alleged that the company took consumers for over $120 million. That company had 550 sales personnel working from a sales boiler room in Tampa, Fla.

In May 2017 the FTC and six State Attorneys General announced 16 new enforcement actions against tech support operations as part of Operation Tech Trap.

To date, there have been only a few criminal cases brought against tech support thieves. In one, a **guilty plea was announced in federal court in South Carolina** against Linda B. Massey, 70, alleging that she collected the money from consumer victims on behalf of a coconspirator in India. This investigation was conducted with assistance from the Better Business Bureau of Upstate South Carolina.

On May 17, 2017, seven telemarketers running a tech support operation in Florida were **indicted in the Southern District of Illinois**. The defendants are the first tech support phone operators to be charged criminally in the U.S. The charges allege that the company paid for pop-up ads to solicit potential victims, that the enterprise charged $650 for "repairs," and that this business stole more than $25 million from some 40,000 consumers. The alleged victims were from the US, all Canadian provinces, the UK, and several other countries.

On November 16, 2017, **six individuals were charged** by the United States Attorney for the Southern District of Illinois with running a tech support scam with victims nationwide.

On June 28, 2017, it was reported that **four people were arrested in England** for their involvement in tech support fraud.

Police in India have also begun to do more to attack the problem. On July 21, 2017 **five people were arrested in Kolkata** for tech support fraud. In September 2016, **six people were arrested** for making fraudulent tech support calls to the U.S. In another case **police in India arrested three people** who were making such calls to Germany and Denmark.

Official-sounding calls about an email hack

SHARE THIS PAGE

April 5, 2016
by Andrew Johnson
Division of Consumer and Business Education, FTC

There's a new twist on tech-support scams — you know, the one where crooks try to get access to your computer or sensitive information by offering to "fix" a computer problem that doesn't actually exist. Lately, we've heard reports that people are getting calls from someone claiming to be from the Global Privacy Enforcement Network. Their claim? That your email account has been hacked and is sending fraudulent messages. They say they'll have to take legal action against you, unless you let them fix the problem right away.

What if my computer does have a virus?

Experts advise against doing any online tech support, and suggest that consumers take their computers with a problem to a local "brick and mortar" store to get an assessment. BBB recommends checking out a company at bbb.org.

What steps should tech support victims take?

There are several steps victims of tech support scams should take. First, they should have the software removed that authorized remote access to their computers and have the device checked to make sure malicious software was not installed by scammers.

Second, they should change the passwords of any online access to financial institutions. Frost with the NFIB in the UK also recommends that consumers use two factor authentication, something many banks and other financial institutions already offer for online accounts. With two factor authentication more than just a password is required to log in. In some cases consumers must put in a number that is sent to their phone by a text message in order to confirm their identity and log in. Most internet service providers and financial institutions now offer this authentication as an option for customers.

Also, consumers should understand that once victimized they may be victimized again, as thieves are likely to contact them to "renew" the tech support services or offer them a bogus "refund," as outlined in this report.

Brian Collard, a computer security specialist from **Dublin, California**, had recently installed advanced antivirus software on his 90-year-old mother's computer when she received a pop-up alert claiming the computer was infected with a virus. Collard's mother, a resident of Colorado, said she was unable to navigate or turn off her computer so she called a phone number for a business called giltedgesolutions.com. Collard says the business took remote control of her computer and, after assuring her she had viruses, charged her $287 for repairs. She signed an online contract but, after speaking with her son, refused to pay for the service and closed her bank account. Her son later found that the business had removed the antivirus he had installed for his mother and replaced it with something that was not nearly as effective. Collard then called BBB.

Where to go with complaints:

If you are victimized, it is critical that you file a complaint with BBB and law enforcement authorities, such as the FTC. Complaint filings can uncover patterns that assist law enforcement agencies taking action against these scams.

BBB is always receptive and can provide guidance in the event of a tech support scam. If a company has a presence in the U.S., Canada, or Mexico, it will sometimes make refunds to complaining consumers. Complaints can be filed against specific businesses at BBB. Consumers that do not know the specific name of the business can still report the experience through **BBB Scam Tracker**.

Consumers also can **complain to Microsoft** through its

online form. Microsoft looks for patterns in complaints and works with law enforcement to combat the fraud.

How can we stop this fraud?

As always, BBB and law enforcement agencies strongly encourage consumers to talk to friends and family about the fraud and how to react if you find yourself victimized. Senior citizen organizations can be critical in getting warnings out to older consumers. IT personnel on staff at senior living facilities can also play a part in fighting this fraud. Simply put, no one should allow a stranger to have remote access to their computer.

Consumer education materials:

BBB has **tips on tech support scams**.

Brochures and similar materials from the FTC are available for free and in bulk. **Here is their alert on tech support**.

Note also that the FTC has no copyright on its materials, so those in consumer protection should feel free to adapt them to their own use.

IC3 issued an **alert on tech support fraud** on June 2, 2016.

Microsoft has **more tips here**.

In Canada, call the **Canadian Antifraud Centre**:
Toll Free 1-888-495-8501.

Consumer tips:

• Do not purchase any software or services from an unsolicited call, email, bogus website, or online ad.

Never give control of your computer to a third party unless you can confirm that it is a legitimate representative of a computer support team with whom you are already a customer.

• Do not be fooled if a phony tech support scammer knows your name, address or even some facts about how your computer operates. Cybercriminals trade information about customers and often claim to have specific information about your computer that is very generic.

• Do not rely solely on monthly statements from your bank or credit card companies; check account activity online or by phone at least weekly for quick indicators of fraud. If you have been defrauded, contact your bank or credit card company.

• Do NOT contact the fraudulent company or respond to a fraudster claiming to need your financial information to address overpayment or provide a refund.

Recommendations:

BBB suggests several key recommendations to address this massive fraud problem.

• **Tougher and more coordinated law enforcement action**, including the filing of both civil and criminal cases against the perpetrators of this computer scam.

• It is crucial that **law enforcement officials in India and other countries make computer tech fraud a higher priority.**

• **Search engine companies should carefully vet**, set strict standards and consider eliminating sponsored links for tech support not meeting such standards. (Microsoft has taken steps to stop pop-up viruses.) They should also create new safeguards to prevent pop-ups from appearing (such as those introduced by Microsoft against MIcrosoft tech support scams).

• **Banks, credit card companies and other payment platforms should do more** to eliminate tech support frauds from their systems. Also, customer educational efforts should be made to those already victimized by tech support scams that they are at risk of being targeted again, and to take steps to protect their bank account and other financial information.

• Finally — and perhaps most importantly — **increased consumer education** is vitally important if we are to make true progress in combating this problem.