



Police Beat

SCPD Crime Prevention Newsletter

Vol. 2 Issue 1

Feb. 2015

St. Charles is not immune to nationwide scams

For the better part of the last 18 months, local police departments across the country, including St. Charles, have responded to calls of residents falling victim to what has become known as the IRS scam. Nationwide, victims of this scam have lost close to \$10 million. The unfortunate part of it all is that our elderly residents are targeted more than any other age group; not just with this scam, but scams in general.

How it works

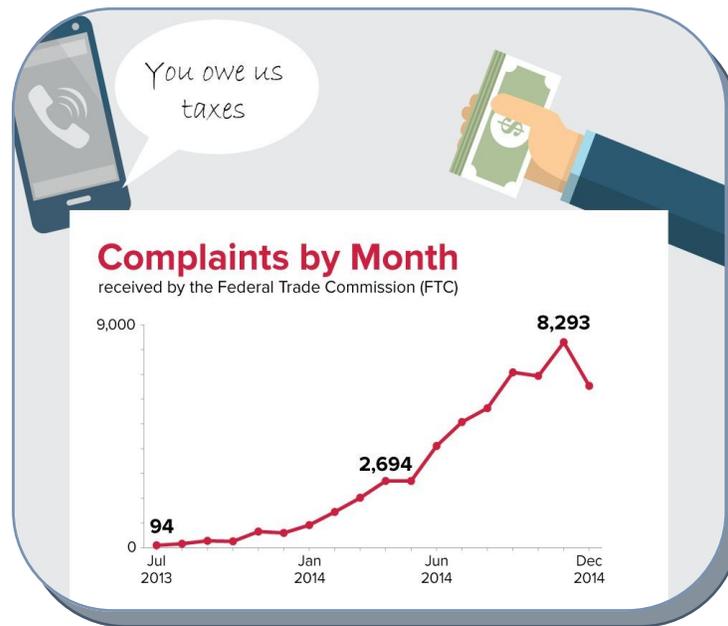
The IRS scam, as with other similar scams, uses scare tactics as a way to get people to comply with demands. Generally, the complaints say a male subject with an unknown accent randomly calls a resident. The offenders are able to “spoof” a phone number, that is, make it look like a legitimate number on Caller ID, but is not the actual number from which the offender is calling. In reported incidents, offenders have spoofed the IRS phone number in Washington, D.C. and the St. Charles Police Department’s main phone number. The offender then informs the homeowner that he is with the IRS, and the homeowner

owes thousands of dollars in back taxes. If the homeowner does not immediately pay the sum, threats of immediate seizure of a house and/or arrest are made. Initially, the calls sound completely legitimate, which causes homeowners to panic. This panic leads them to comply with demands that the homeowner rush out and put the sum owed onto multiple Green Dot or Reloadit cards. The victim is instructed to return

home with those cards, and re-contact the offender with the serial numbers on the back. That’s all the offenders need to take control of the money, and it’s at that point that victims realize they’ve been had.

Red flags

So how can you protect yourself? Always be on alert! Residents should



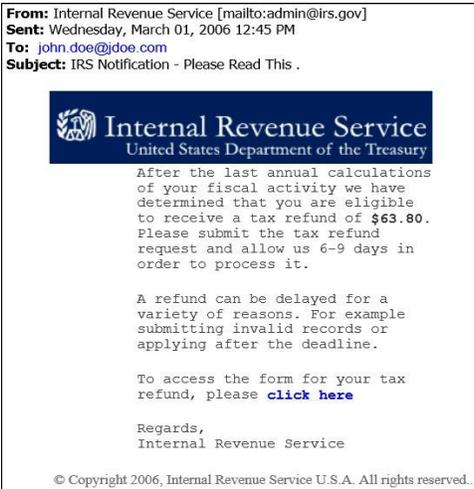
know that the IRS, or any other government entity, does not operate in this manner. Some type of mail correspondence would be sent first rather than a phone call. The IRS will never ask you to wire money, pay taxes with a prepaid debit card or share your credit card information over the phone.

See “Scam” on page 2

Tax season means prime time for email scams

While many people like to go fishing as a way to relax, during tax season, opportunistic scammers enjoy phishing as a way to steal your money.

Phishing is a way that scammers attempt to steal your personal information and/or money by sending bogus emails (as seen on this page). The emails look official and may state you have funds available, or that you may owe money. It's important to know that the Internal Revenue Service does not initiate contact with taxpayers via email, text messages or social me-



dia. Any requests for PIN numbers, passwords or access to bank information should be considered a scam. According to the IRS, if you receive an email claiming to be

from the IRS that contains a request for personal information, taxes associated with a large investment, inheritance or lottery, do not reply and certainly to do open any attachments. Those attachments contain malicious software that will infect your computer or phone.

Also, do not click on any embedded links. Forward the email to phishing@irs.gov, then delete the email. If you discover a web site that claims to be the IRS, forward the web address to the same email address.

"Scam" continued from page 1

Besides threatening, the scam artist is very convincing. The scammer usually is a male subject often with a foreign accent, usually described as Middle Eastern. He may give a bogus badge number, and may tell you the last four digits of your social security number. The scammer may also use a common name, such as Mr. Cruz, which was used in an incident in St. Charles. So what should you do if you get a call like this, but don't fall victim to the scam? A complaint can be filed with the Treasury Inspector General for Tax Administration (www.tigta.gov). You may also contact the IRS directly to confirm there are no issues calls at 800-829-1040. If you have fallen victim to the scam, a report should be made with the St. Charles Police Department. While the phone number the scammer used to call you doesn't help police much, the used Green Dot or Reloadit cards are useful, as the serial numbers can be used to track the money hopefully to the offender. However, it should be noted that odds of officials recouping your lost money are slim to none.



Data breaches becoming more common

Data breaches. We've all heard about them, and some of us have been affected by them. However, we usually only hear about the big ones: Target, Michaels, Albertsons. Did you know there were 784 data breaches in 2014 alone, resulting in more than 85 million records being exposed? You may guess that most breaches occur at businesses or retail establishments, but for the third year in a row, the majority of breaches—42.5—occurred in the healthcare sector.

Since the Identity Theft Resource Center (idtheftcenter.org) first began tracking reports of data breaches in 2005, there have been more than 5,000. Of these events, the highest percentage—34—have been in the business sector, while medical and healthcare breaches have made up about 26 percent.

The overwhelming majority of these data breaches were accomplished through hacking, in which criminals were able to access sensitive content through networks from outside the server. A concept known as "data on the move," which refers to sensitive information stored on portable technology like flash drives, laptops, and even

smartphones, accounted for the second highest number of breaches when that technology was lost or allowed to be compromised. Internal breaches, when an employee or third-party contractor accessed sensitive data without permission, were the third highest cause of leaks.

The year-end report was unveiled at nearly the same time that the [Obama administration announced its plan](#) for cybersecurity legislation that would alleviate some of the liability following an attack from companies who had voluntarily cooperated with the government's cybersecurity information sharing initiatives.

What do you do if your identity becomes compromised as a result of a data breach? The quicker you act, the less damage may be done. The first thing you should do is place an initial fraud alert on your information with all three credit bureaus (Equifax, Experian and TransUnion). Then, get copies of your credit reports through those same bureaus. You can get a free copy of your report at annualcreditreport.com.

You'll also want to create an identity theft report. This will allow you to have fraudulent information removed from your credit, stop companies from collecting debts, place an extended alert on your credit and allow you to gather information from companies about any accounts an identity thief may have opened in your name.

To create an ID theft report, submit a report about the theft to the Federal Trade Commission. When you finish writing all the details, print a copy of the report. It will be called an Identity Theft Affidavit. Bring that affidavit to the police department and file a police report. The police report and the affidavit combined will make up your ID theft report. Remember, these are just the first steps you should take if you become a victim. Contact the FTC and Illinois Attorney General's Office to determine what should be your next step.

 Identity Theft Resource Center 			
2014 Data Breach Category Summary			
How is this report produced? What are the rules? See last page of report for details.		Report Date: 1/5/2015	
		Page 1 of 1	
Totals for Category: Banking/Credit/Financial	# of Breaches: 43 % of Breaches: 5.5%	# of Records: 1,198,492 % of Records: 1.4%	
Totals for Category: Business	# of Breaches: 258 % of Breaches: 33.0	# of Records: 68,237,914 % of Records: 79.7%	
Totals for Category: Educational	# of Breaches: 57 % of Breaches: 7.3%	# of Records: 1,247,812 % of Records: 1.5%	
Totals for Category: Government/Military	# of Breaches: 92 % of Breaches: 11.7	# of Records: 6,649,319 % of Records: 7.8%	
Totals for Category: Medical/Healthcare	# of Breaches: 333 % of Breaches: 42.5	# of Records: 8,277,991 % of Records: 9.7%	
Totals for All Categories:	# of Breaches: 783 % of Breaches: 100.0	# of Records: 85,611,528 % of Records: 100.0%	

Report activity to keep STC safe

The SCPD consistently counts on residents to be the eyes and ears of the department. Crime prevention is everybody's business, and without the assistance from residents, officers could not do their job. So, how can you help?

If you see something, say something!

Most people are hesitant to call 911 to report what they saw or heard as suspicious. Yes, what you saw could have been nothing. But wouldn't it be better for a police officer to check and make sure? Police officers are never bothered or annoyed by suspicious activity calls. Investigating such things is a police officer's job. In St. Charles dial 9-1-1 to report any in progress incident. But what if you waited a couple hours, or even days, but you still want to re-

port it? You can still call 9-1-1 to meet with an officer or you can contact

the police department's anonymous tipline (866-DRUG-COP). Any crime tip can be called into this number, not just tips about drug activity. You can report suspicious activity online as well at stcharlesil.gov/report-crimedrug-tip.



Speed limits on state roads remain same

By Keith Goble, Land Line state legislative editor

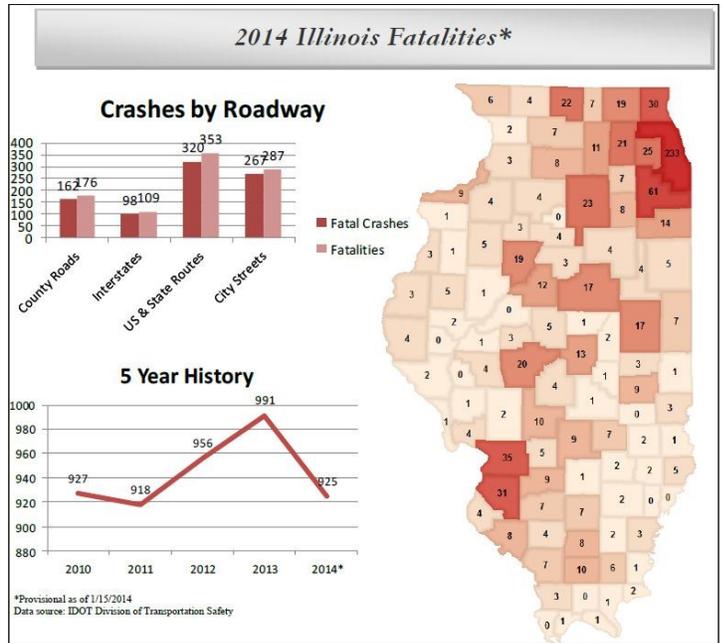
The speed differential between most cars and trucks on certain Chicago-area roadways will soon shrink. Since Jan. 1, 2014 the speed limit on rural interstate highways in Cook and the collar counties has been 70 mph for cars and 55 mph for trucks. Previously, car speeds were set at 65 mph.

The Illinois House voted 103-12 on Dec. 2, 2014 to overturn an August veto from Gov. Pat Quinn on a bill to permit trucks on affected roadways to drive 60 mph. The vote exceeded the three-fifths majority needed to over-

ride the governor's veto. The bill, SB930, now is law. At the time of his veto, Quinn cited concerns about allowing large trucks to drive faster. "Increased speeds on urban interstate highways for trucks will result in the increased loss of human life," Quinn wrote to lawmakers. He said speed also exacerbates the size and weight differences between large trucks and passenger vehicles, leading to more severe crashes.

Sen. Jim Oberweis, R-Sugar Grove, has said the interstates were designed for the higher rate of speed.

Others say since car



speeds were increased last year, the state should follow suit to update truck speeds. The Owner Operator Independent Drivers Association leadership says it's imperative for road safety that any changes made to driving speeds promote uniformity. Lawmakers also voted to override a separate veto on a bill to alter speeds for all vehicles on Illinois tollways. SB2015

will raise the speed limit from 65 to 70 mph on the 286-mile network of tollways. The governor previously said "the convenience of increased speeds for drivers on Illinois tollways does not outweigh the safety risks."

House lawmakers voted 100-11 in December to overturn the veto.

The Senate already voted 44-5 in favor of the override.

End of Year Fatalities

2014

Fatalities: 925*

Crashes: 847*

2013

Fatalities: 991

Crashes: 895

66 Under

*Provisional data as of 1/15/2015
Source: IDOT

New traffic-related laws implemented for 2015

SB 2583: Motorists will no longer be required to surrender drivers' licenses for minor traffic offenses. They may sign a ticket saying they will pay the ticket or take care of it in court and keep their license.

SB 3411: County and municipal law enforcement cannot implement ticket quotas.

HB 4745: Allows fines of up to \$2,000 for parents/guardians that allow those un-

der 21 to drink in their residence or owned/controlled vehicles, trailers, campers, or boats.

If a death occurs as a result, parents/guardians can be charged with a felony.

This law expands on the current law prohibiting parents or guardians from allowing those underage from drinking in their residence.

What to do before and during a winter storm

With the Super Bowl blizzard of 2015 behind us, one would hope the upper Midwest would be immune to any more large snowfalls this year. But, as Chicagoans, we know better than to assume anything like that. Were you prepared for survival during the storm? ComEd reported more than 54,000 customers were without power during the blizzard, and the frigid temperatures that followed. According to www.ready.gov, the following is how you can prepare and survive:

Before a winter storm

Add the following supplies to your [emergency kit](#):

- Rock salt or more environmentally safe products to melt ice on walkways. Visit the [Environmental Protection Agency](#) for a complete list of recommended products.
- Sand to improve traction.
- Shovels and other equipment.
- Sufficient heating fuel. You may become isolated in your home and regular fuel sources may be cut off. Store a good supply of dry, seasoned wood for your fireplace or wood-burning stove.
- Adequate clothing and blankets.

Make a [Family Communications Plan](#). Your family may not be together when disaster strikes, so it is important to know how you will contact one another. A NOAA weather radio broadcasts alerts and warnings directly from the NWS for all hazards. You may also sign up in advance to receive notifications from your local emergency services. Download FEMA's *Be Smart. Know Your Alerts and Warnings* for a summary of notifications at:

www.ready.gov/prepare. Free smart phone apps, such as those available from FEMA and the American Red Cross, provide information about finding shelters, providing first aid, and seeking assistance for recovery. Minimize travel. If travel is necessary, keep



a disaster supplies kit in your vehicle. Bring pets/companion animals inside during winter weather. Move other animals or livestock to sheltered areas with non-frozen drinking water.

During a winter storm

- Stay indoors during the storm.
- Walk carefully on affected walkways.
- Avoid overexertion when shoveling snow. Overexertion can bring on a heart attack—a major cause of death in the winter. Use caution, take breaks, push the snow instead of lifting it when possible, and lift lighter loads.
- Keep dry. Change wet clothing frequently to prevent a loss of body heat.
- Signs of frostbite: Loss of feeling and white or pale appearance in extremities, such as fingers, toes, earlobes, face and the tip of the nose. Cover exposed skin, but do not rub the affected area in an attempt to warm it up. Seek medical help immediately.
- Signs of hypothermia: Uncontrollable shivering, memory loss, disorientation, incoherence, slurred speech, drowsiness and apparent exhaustion. If symptoms are detected take the person's tempera-

ture. If it is below 95 degrees seek medical attention immediately.

Get the victim to a warm location. Remove wet clothing. Warm the center of the body first by wrapping the person in blankets or putting on dry clothing. Give warm, non-alcoholic beverages if the victim is conscious. Seek medical help immediately.

- Because frostbite and hypothermia both result from exposure, first determine whether the victim also shows signs of hypothermia. Hypothermia is a more serious medical condition and requires emergency medical assistance.
- Drive only if it is absolutely necessary. If you must drive travel in the day; don't travel alone; keep others informed of your schedule; stay on main roads and avoid back road shortcuts. Let someone know your destination, your route, and when you expect to arrive.
- If the pipes freeze, remove any insulation and wrap pipes in rags. Completely open all faucets and pour hot water over the pipes, starting where they were most exposed to the cold.
- Maintain ventilation when using kerosene heaters.

SCPD looking for a few good men and women

Have you ever wondered what it's like to be a part of the law enforcement profession? The St. Charles Police Department once again is hosting its annual Citizens Police Academy, from March 17 through May 14, 2015.

The CPA is meant to give residents and business owners a better understanding of how the police department operates. Participants will get to meet officers and discover what daily life is like for them. Some of the areas covered in the CPA are criminal and narcotics investigations, arrest and search procedures, courts, traffic stops, the K-9 unit, Taser, SWAT team and crime scene processing among many others.

When possible, the curriculum makes use of both classroom instruction and outside demonstrations. Students may get an opportunity to do the activity being demonstrated, such as processing a "crime scene" for fingerprints or getting a radar reading on a moving vehicle. The CPA has an added benefit of being a sounding board on how the police department is meeting the needs of its citizens.

The class meets from 7 p.m. to 9 p.m. Tuesdays and Thursdays. Most of the classes are held in the police department training room at 211 N. Riverside



Ave. Applications can be picked up at the front lobby of the PD, or downloaded from the city web site at www.stcharlesil.gov under "Crime Prevention." Completed applications can be dropped off, mailed or e-mailed to the police department in care of Officer Bill Tynan at btynan@stcharlesil.gov. All applications are subject to approval, and include a background check.

Fourth quarter crime stats

The following statistics represent the number of reports taken by the St. Charles Police Department for the period Oct. 1 through Dec. 31, 2014.

Commercial burglary—6

Residential burglary—8

Burglary from motor vehicle—19

Motor vehicle theft—3

Retail theft—37

Identity theft—5

Criminal damage to property—40

DUI (alcohol and drugs) - 28

The city of St. Charles is social!

Keep up to date with all that's happening in St. Charles by following the city on these sites:



facebook.com/cityofstcharles



twitter.com/cityofstcharles



vimeo.com/stcharlesil



www.stcharlesil.gov