



Police Beat

SCPD Crime Prevention Newsletter

Vol. 2 Issue 3

Sept. 2015

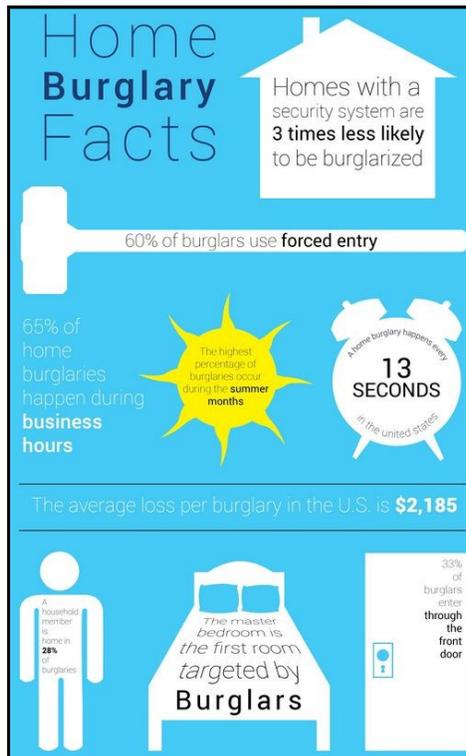
How to protect against property crime

We all know that St. Charles has a low violent-crime rate. So, what else do police officers deal with on a daily basis? A lot of crime that is reported falls under property crime. Everything from commercial and residential burglary, to vehicle burglary, to vehicle theft, to damage to property can take a considerable amount of time to investigate.

As discussed in last quarter's newsletter, preventing vehicle burglary may be as simple as locking doors. During the first quarter of 2015, 100 percent of those type of burglaries in St. Charles occurred to unlocked vehicles. That statistic is staggering. Recently, the Naperville Police Department reported a sharp increase in vehicle burglaries, and lo and behold, stated the vast majority of victims left their doors unlocked. This not only is an issue locally, but nationally as well, and it would seem that simply remembering to lock vehicle doors would be enough of a deterrent, which could lead to a significant drop in this crime.

But what about your house or your business? Often times a locked door will not stop offenders from finding a different way into the property. In more than half of residential burglaries nationwide, forced entry was made into the residence.

However, there are steps one can



Graphic by Joe Schwartz, Doyle Security (godoyle.com). Facts from FBI, alarm.org and the Alarm Industry Research and Educational Foundation.

take to fortify a property and reduce the likelihood of it becoming a target.

Crime prevention through environmental design is a much-respected technique in law enforcement used to reduce crime not only to homes and businesses, but to entire cities. The idea is that just creating the right environment around a property can act as a deterrent.

Lighting alone, both exteriorly and interiorly, can be the single-best deter-

rent. Think about the lighting in and around your home. Are all the doorways into your home lit at night with at least 60-watt bulbs? Are there dark corners around your property that would allow a burglar to enter through a window without anybody else observing? Is your home lit up inside at night when you are not home, or on vacation?

You probably never thought about the trees and shrubs on your property, but you should. Does the shrubbery cover windows and make it difficult to see out from the inside, and vice versa? If you can't see movement outside, how can you detect a threat? If neighbors can't see your property, how can they tell if something may be wrong?

When it comes to the physical security of the house, things to take into account include the type of construction of your entry door (it should be solid core), deadbolt locks should have at least a one-inch throw and strike plates should have at least 3-inch screws.

There are many more things to consider when it comes to home security. The police department has a downloadable home-security survey available online for residents to utilize so you can think about how to make your home more safe. The survey can be found at the address noted at the bottom of this page.

A home security survey can be found at www.stcharlesil.gov/public-safety/crime-prevention

That silent phone call may be trouble

by **Aarti Shahani**
NPR

Here's an experience some of us have had. The phone rings. You pick it up and say, "Hello. Hello. Helloooo," but nobody answers. It turns out there could be someone on the other end of the line, an automated computer system that's calling your number — and tens of thousands of others — to build a list of humans to target for theft.

Build a list

Vijay Balasubramaniyan, CEO of Pindrop Security, a company in Atlanta that detects phone fraud, says that in any number of ways, the criminal ring gets your 10 digits and loads them into an automated system. Maybe you gave your number to Target or some other big retailer that got hacked. Maybe you entered an online raffle to win a free iPhone. According to the Federal Trade Commission, these [robocalls are on the rise](#) because [Internet-powered phones make it cheap and easy](#) for scammers to make illegal calls from anywhere in the world.

That initial call you get, with silence on the other end, "[is] essentially the first of the reconnaissance calls that these fraudsters do," Balasubramaniyan says. "They're trying to see: Are they getting a human on the other end? You even cough and it knows you're there."

Gather account information

The next step is gathering information about your bank or credit card account. You get a call with a prerecorded voice that tells you, for example, "[we're] calling with an important message about your debit card. If you are the cardholder please stay on the line and press 1. Otherwise please have the cardholder call us at 1-877..."

If you're thinking about ignoring it, the message tries to scare you into paying attention with a warning: "A temporary hold may have been placed on your account and will be removed upon verification of activity."

That number leads to another automated system that prompts you to share personal details like your date of birth, your card number and secure PIN, the expiration

date, your Social Security number. It can be tricky because many real banks have a similar system. And, Balasubramaniyan says, fear does kick in. "They're like 'OK, if you want a moment to process this, we're going to send the law enforcement in front of your doorstep,'" he said.

Pindrop keeps a "honeypot" — about a quarter-million phone numbers that aren't being used by real people, which the company uses for research. Workers enter the numbers into sweepstakes and online databases, to see what kind of fraud hits. Company researchers estimate 1 in every 2,200 calls is a fraud attempt. And they've observed an interesting detail about the fraudulent 1-877 numbers.

If you call back from your phone — which the criminals dialed — you get the prompt to enter personal data. If you call back from somewhere else, you get "this number has been deactivated." So a regulator or police officer that's trying to crack down will think, incorrectly, it's out of commission.

Hijack account

Once the criminal ring scrapes enough information on you, it has humans call your financial institution. Banks and credit card companies hire Pindrop to help them detect fraud. In a real-life example, provided by one call center, the operator has a hard time hearing the caller and apologizes. The caller, who is pretending to be the account holder, wants to know his available credit — to make sure the account is

worth pursuing—and then changes the address on the account.

'Just hang up'

The FTC is trying to combat the rising number of illegal automated phone calls. "It is the No. 1 consumer complaint that we receive," says Patty Hsue, an attorney who leads the FTC's effort against robocalls. The agency receives an average of 170,000 complaints per month about robocalls. The FTC recommends that consumers "just hang up" on the robocalls.

"We don't want consumers to engage in any way with robocallers," Hsue said.



'Robocalls' continue to rise in frequency

FTC

If you answer the phone and hear a recorded message instead of a live person, it's a robocall.

You've probably gotten robocalls about candidates running for office, or charities asking for donations. These robocalls are allowed. But if the recording is a sales message and you haven't given your written permission to get calls from the company on the other end, the call is illegal. In addition to the phone calls being illegal, their pitch most likely is a scam.

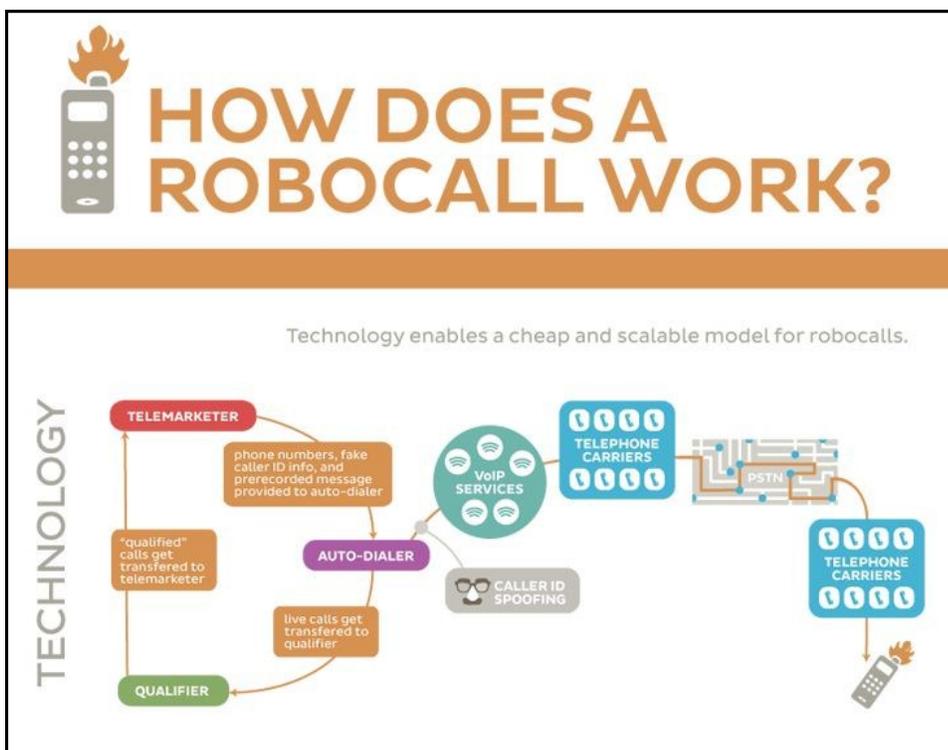
Why the spike in robocalls?

Technology is the answer. Companies are using auto dialers that can send out thousands of phone calls every minute for an incredibly low cost. The companies that use this technology don't bother to screen for numbers on the national [Do Not Call Registry](#). If a company doesn't care about obeying the law, you can be sure they're trying to scam you.

What's the FTC doing about it?

During the last few years, the FTC has stopped billions of robocalls that offer everything from fraudulent credit card services and so-called auto warranty protection to home security systems and grant procurement programs. Tracing these calls is a tough job. Many different companies use the same or very similar recorded messages. Robocallers fake the caller ID information that you see on your phone. That's called caller ID spoofing — and new technology makes it very easy to do.

In some cases, the fraudulent telemarketer may want you to think the call is from your bank, or another entity you've done business with. Sometimes, the telephone number may show up as "unknown." Other



times, the number is a real one belonging to someone who has no idea his or her number is being misused. Robocallers often place the calls through internet technology that hides their location.

What to do if you get called

If you get a robocall:

- Hang up the phone. Don't press 1 to speak to a live operator and don't press any other number to get your number off the list. If you respond by pressing any number, it will probably just lead to more robocalls.
- Consider contacting your phone provider and asking them to block the number, and whether it charges for that service. Remember that telemarketers change Caller ID information easily and often, so it might not be worth paying a fee to block a number that will change.

[Report your experience to the FTC online](#) or call 1-888-382-1222.

What calls are allowed?

Some prerecorded messages are permitted — messages that are purely informational. That means you may receive calls to let you know your flight's been cancelled, reminders about an appointment, or messages about a delayed school opening. But the business doing the calling isn't allowed to promote the sale of any goods or services. Prerecorded messages from a business that is contacting you to collect a debt also are permitted, but messages offering to sell you services to reduce your debt are barred. Other exceptions include political calls and calls from certain health care providers—pharmacies are permitted to use messages to provide prescription refill reminders. Prerecorded messages from banks, telephone carriers and charities also are exempt from these rules if the banks, carriers or charities make the calls themselves.

Annual most stolen vehicle list released

The National Insurance Crime Bureau (NICB) recently released its annual “Hot Wheels” report which identifies the 10 most stolen vehicles in the United States. The report examines vehicle theft data submitted by law enforcement to the National Crime Information Center and determines the vehicle make, model and model year most reported stolen in 2014.

Although vehicle theft has been on a long downward trajectory, it is still a severe economic hardship for many to lose their vehicle to theft—especially if a vehicle is uninsured. That is why NICB continues to advise all drivers to review our four “Layers of Protection”:

- **Common sense:** Lock your car and take your keys. It’s simple enough, but many thefts occur because owners make it easy for thieves to steal their cars.
- **Warning device:** Having and using a visible or audible warning device is another item that can ensure that your car remains where you left it.
- **Immobilizing device:** Generally speaking, if your vehicle can’t be started, it can’t be stolen. “Kill” switches, fuel cut-offs and smart keys are among the devices that are extremely effective.

MOST STOLEN VEHICLES — 2014

1. Honda Accord
2. Honda Civic
3. Ford pickup (full size)
4. Chevrolet pickup (full size)
5. Toyota Camry
6. Dodge pickup (full size)
7. Dodge Caravan
8. Nissan Altima
9. Acura Integra
10. Nissan Maxima

- **Tracking device:** A tracking device emits a signal to the police or to a monitoring station when the vehicle is stolen. Tracking devices are very effective in helping authorities recover stolen vehicles. Some systems employ “telematics,” which combine GPS and wireless technologies to allow remote monitoring of a vehicle. If the vehicle is moved, the system will alert the owner and the vehicle can be tracked via computer.

Do you know what state law says about phones and driving?

Since January 2014, most use of electronic devices, including cell phones, while driving has been outlawed in Illinois. However, you probably see it continue day in and day out, and you may even be guilty of using a phone while driving yourself. Do you know the law? The following is taken directly from the Illinois Compiled Statutes: **Sec. 12-610.2. Electronic communication devices.** "Electronic communication device" means an electronic device, including but

not limited to a hand-held wireless telephone, hand-held PDA, or a portable or mobile computer, but does not include a GPS or navigation system or a device that is physically or electronically integrated into the motor vehicle.

(b) A person may not operate a motor vehicle on a roadway while using an electronic communication device.

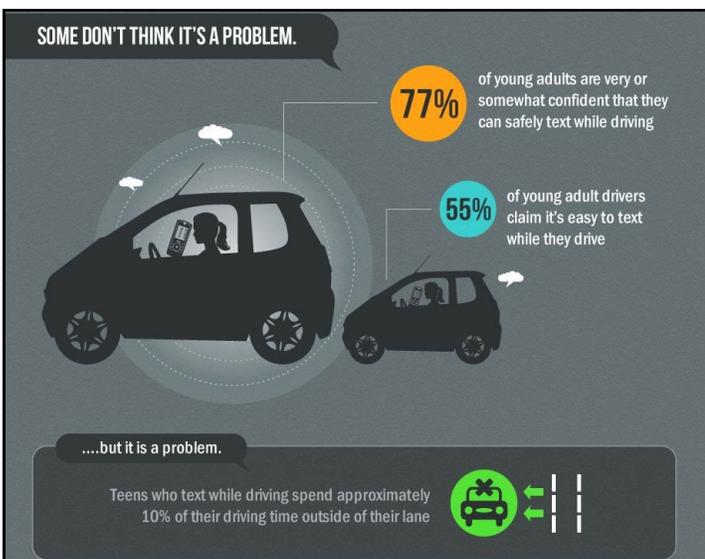
(b-5) A person commits aggravated use of an electronic communication device when he or she violates subsection (b) and in committing the violation he or she was involved in a motor vehicle accident that results in great bodily harm, permanent disability, disfigurement, or death to another and the violation was a proximate cause of the injury or death.

(c) A second or subsequent violation of this Section is an offense against traffic regulations governing the movement of vehicles. A person who violates this Section shall be fined a maximum of \$75 for a first offense, \$100 for a second offense, \$125 for a third offense, and \$150 for a fourth or subsequent offense.

(e) A person convicted of violating subsection (b-5) commits a Class A misdemeanor if the violation resulted in great bodily harm, permanent disability, or disfigurement to another. A person convicted of violating subsection (b-5) commits a Class 4 felony if the violation resulted in the death of another person.

There are several exemptions to the law, including:

- Police officers performing official duties
- Any driver reporting an emergency
- Any driver while parked on a roadway shoulder
- Any driver stopped in traffic while in neutral or park
- Two-way citizen-band radios
- FCC licensed amateur radio operators



Does that email look fishy? It's probably a scam

When Internet fraudsters impersonate a business to trick you into giving out your personal information, it's called phishing. Don't reply to email, text, or pop-up messages that ask for your personal or financial information. Don't click on links within them either – even if the message seems to be from an organization you trust. It isn't. Legitimate businesses don't ask you to send sensitive information through insecure channels.

Examples of phishing

You open an email or text, and see a message like this: "We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."

"Our records indicate that your account was over-charged. You must call us within 7 days to receive your refund." The senders are phishing for your information so they can use it to commit fraud.

How to deal with phishing scams

Delete email and text messages that ask you to confirm

or provide personal information (credit card and bank account numbers, Social Security numbers, passwords, etc.). Legitimate companies don't ask for this information via email or text. The messages may appear to be from organizations with which you

do business. They might threaten to close your account or take other action if you don't respond. Don't reply, and don't click on links or call phone numbers provided in the message, either. These messages direct you to spoof sites – sites that look real but whose purpose is to

steal your information so a scammer can run up bills or commit crimes in your name. Area codes can mislead, too.

Some scammers ask you to call a phone number to update your account or access a "refund." But a local area code doesn't guarantee that the caller is local.

If you're concerned about your account or need to reach an organization you do business with, call the number on your financial statements or on the back of your credit card.

HOW TO REPORT PHISHING EMAILS

- ◆ Forward phishing emails to spam@uce.gov – and to the company, bank, or organization impersonated in the email.
- ◆ Report phishing email to reportphishing@antiphishing.org
- ◆ If you might have been tricked by a phishing email: File a report with the Federal Trade Commission at www.ftc.gov/complaint.
- ◆ Visit the FTC's identity theft website at www.identitytheft.gov. Victims of phishing could become victims of identity theft; there are steps you can take to minimize your risk.

Second quarter police reports

The following information represents the number of reports taken by the St. Charles Police Department for the period April 1 through June 30, 2015.

Commercial burglary - 4

Residential burglary - 4

Burglary from motor vehicle - 22

Motor vehicle theft - 2

Retail theft - 38

Identity theft - 22

Criminal damage to property - 46

DUI (alcohol and drugs) - 19

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