Ramsey County Sheriff's Office **Neighborhood Watch**
Jack Serier, Sheriff

Public Safety Services Division – Crime Prevention Unit
1411 Paul Kirkwold Drive • Arden Hills, Minnesota 55112
Phone: 651-266-7339 • Fax: 651-266-7306
www.RamseyCountySheriff.us

Neighbors and Deputies working together for safer communities

Block Captain News – November 2017

Next Meeting Tuesday, November 14 – 6:30 pm

Ramsey County Public Works Building - Marsden Room
1425 Paul Kirkwold Drive, Arden Hills MN 55112
Near intersection of Highway 96 and Hamline

In this issue:

Internet & Cyber Safety top November agenda

Safety and security have been the subject matter focus of Block Captain meetings in 2017. October was National Cybersecurity Awareness Month, and the fourth quarter meeting will feature an in-depth discussion of internet and cyber safety.

Technology advances continue to open our world providing tools to help us communicate, collect information, share ideas and more. The internet offers access to goods, services, people, and more. Internet users are also concerned about the safety of their personal information, bank accounts, and online activities.

Join us at the Marsden Room on Tuesday, November 14 at 6:30 pm to discuss this topic to better understand cyber security and the simple steps you can take to protect yourself and your family.

Coffee with a Cop – Thursday, November 30

Join local deputies to chat over a cup of coffee. There is no agenda or speeches, just a chance to ask questions, voice concerns, and get to know the officers in the neighborhood.

Thursday, November 30, 2017
7:30 a.m. - 9:00 a.m.

Holiday Stationstore
1150 County Road J (at Centerville Rd)
White Bear Township, MN 55110

Thieves use ATM skimming devices to steal in Shoreview

In September thieves installed skimming devices on ATMs in Shoreview and Dakota County to collect card information and then commit fraud - stealing more than ten thousand dollars. Investigators shared photos on social media asking for assistance in identifying the thieves, and the story was picked up by local news media. (*If you recognize the crooks please call 911.*)

How Card Skimming Works: (source FTC.gov)

Victims of credit card skimming are completely blindsided by the theft. They notice fraudulent charges on their accounts or money withdrawn from their accounts, but their credit and debit cards never left their possession. How did the theft happen?

Credit card skimming is a type of credit card theft where crooks use a small device to steal credit card information in an otherwise legitimate credit or debit card transaction.

How Card Skimming Works, continued

When a credit or debit card is swiped through a skimmer, the device captures and stores all the details stored in the card's magnetic strip. Thieves use the stolen data to make fraudulent charges either online or with a counterfeit credit card.

Credit card skimmers are often placed over the card swipe mechanism on ATMs and gas stations. With ATMs, the crooks may place a small, undetectable camera nearby to record you entering your PIN. This gives the thief all the information needed to make fake cards and withdraw cash from the cardholder's checking account.

Occasionally, certain retail and restaurant workers who handle credit cards are recruited to be part of a skimming ring. These workers use a handheld device to skim your credit card during a normal transaction. For example, we routinely hand our cards over to waiters to cover the check for a restaurant. The waiter walks away with our credit cards and, for a dishonest waiter, this is the perfect opportunity to swipe the credit card through a skimmer undetected.

Once the victim's credit card information is stolen, thieves will either create a cloned credit card to make purchases in store, use the account to make online purchases, or sell the information on the internet.

Victims of credit card skimming are often unaware of the theft until they receive a billing statement or overdraft notices in the mail.

How to Prevent and Detect Credit Card Skimming

Simply using your credit card puts you at risk of becoming a credit card skimming victim. Credit card skimming incidents can be difficult to detect. Unless you know what you're looking for, it can be extremely difficult to detect skimming devices. When in doubt don't use the device and call law enforcement.

Catching fraudulent charges related to a skimming incident requires you to watch your accounts frequently. Monitor your checking and credit card accounts online at least weekly and immediately report any suspicious activity to your bank or credit card issuer.

Here are a few more tips for avoiding credit card skimming.

- **Watch where you shop**. Restaurants, bars, and gas stations seem to be the places where credit card incidents happen most frequently. Retail store self-checkouts and ATMs, especially standalone ATMs (those that aren't at the bank) are also places that skimmers can be found.
- **Know how a credit card skimmer looks**. Krebs on Security has a well-documented page on credit card skimming and several pictures of credit card skimmers that demonstrate how difficult it is to detect the devices, which have become smaller and more difficult to detect over the years.
- **Check ATMs before using them**. At ATMs, skimmers often place a camera within view of the keypad to steal your PIN. Or, they place a fake keypad on top of the real one to record your keystrokes. When you're using an ATM, cover your hand as you type your PIN to keep a camera from catching a view of what you're typing. If the keys seem hard to push, eject your card and use another ATM. Use a bank-operated ATM, which is less likely to have a skimmer, rather than an ATM at a store or gas station.
- **Don't become a victim of "credit card cleaning" scams**, where thieves claim to clean the magnetic strip on your credit card to help it work better. These thieves simply swipe your credit card through a credit card skimmer and take your credit card information.

How to Report a Credit Card Skimming Loss

Contact your bank or credit card issuer to let them know that your credit card information has been compromised. Call first, then follow up in writing. If only your credit card information has been stolen, you won't be liable for any fraudulent charges. Call 911 and have a deputy take a report.

Winter Parking – ordinances in effect November 1 to April 30

The weather on the last Friday in October brought home the thought of snow as a wet blanket. Winter, snow and ice are part of what makes Minnesota a great place to live, work and play.

The winter parking regulations are in effect in all seven contract communities, and there is no on street, overnight parking from November 1st through April 1, 2017. In White Bear Township, please remember the following:

- No parking on any highways, streets, boulevards and alleys between the hours of 2:00 am to 6:00 am
- No Parking after a snowfall of 1" (one inch) or more
    - No vehicles shall be parked on the highways, streets, boulevards and alleys until plowing and snow removal is complete
- On trash & recycling days, place garbage cans at the end of the driveway, not in the street
- Keep your mailbox area clear of snow
- Keep a clear a path to the fire hydrants in your neighborhood

Though similar, each community does have separate ordinances regarding snow emergencies, snow depth and parking. Here's a list of ordinances which can be found on the community's website.

Arden Hills:	City Code Chapter 8, Section 800.03
Gem Lake:	Ordinance #86, Section 6.4.2
Little Canada:	Municipal Code 403
North Oaks:	Ordinance 07 Title VII 71.12
Shoreview:	City Code 901.030, 901.040
Vadnais Heights:	City Code Chapter 77
White Bear Township:	Ordinance 17 1.6

Beware that each community requests that Deputies issue citations for illegally parked vehicles.

Sheriff's Office Citizen Academy scheduled for January

The Ramsey County Sheriff's Office is hosting a Citizen Academy in January 2018. This three-week-six-session course will take participants on a behind the scenes journey of the work and activities of the Sheriff's Office. The course will begin Tuesday, January 9 and continue through Thursday, January 25, 2017. Sessions will run each Tuesday and Thursday for three and a half hours per night, from 6:00 PM – 9:30 PM.

The course is designed to give citizens a better understanding of the duties, responsibilities, equipment, training and facilities of the Sheriff's Office. Topics include patrol procedures, K-9, criminal investigations, crime scene processing, narcotics, crime prevention and the communication center (911 system). The academy will also include the topics of court orders, civil process, criminal history, and warrants. In addition to classroom training, participants will receive tours of the patrol station, the adult detention center (jail), and other Sheriff's Office facilities.

There is no fee, the only commitment is that participants are asked to attend all six sessions. At the conclusion of the academy, graduates will receive a certificate of completion. Participants will also be offered volunteer opportunities to continue their partnership with law enforcement.

Applicants must be 18 years of age, pass a criminal history background check, and be available to attend all of the sessions. Academy size is limited.

Download the application (pdf fillable form). To request an application via email send your request to CrimePrevention@co.ramsey.mn.us Via US Mail or for additional information, call 651-266-7315.

Applications must be received by Tuesday, December 12, 2017.

A scam-free vacation

Heading out of town? Make sure you come back with a nice post-vacation glow and not a case of identity theft. Here are some things you can do to lessen the chances you'll be a victim.

Limit what you carry. Take only the ID, credit cards, and debit cards you need. Leave your Social Security card at home. If you've got a Medicare card, make a copy to carry and blot out all but the last four digits on it.

Know the deal with public Wi-Fi. Many cafés, hotels, airports, and other public places offer wireless networks — or Wi-Fi — you can use to get online. Two things to remember:

- **Wi-Fi hotspots often aren't secure**. If you connect to a public Wi-Fi network and send information through websites or mobile apps, the info might be accessed by someone it's not meant for. If you use a public Wi-Fi network, send information only to sites that are fully encrypted, and avoid using apps that require personal or financial information.
- **That Wi-Fi network might not belong to the hotel or airport**. Scammers sometimes set up their own "free networks" with names similar to or the same as the real ones. Check to make sure you're using the authorized network before you connect.

Protect your smartphone. Use a password or pin, and report a stolen smartphone — first to local law enforcement authorities, and then to your wireless provider. In coordination with the Federal Communications Commission (FCC), the major wireless service providers have a stolen phone database that lets them know a phone was stolen and allows remote "bricking" so the phone can't be activated on a wireless network without your permission. Find tips specific to your operating system with the FCC Smartphone Security Checker at fcc.gov.

ATMs and gas stations — especially in tourist areas — may have skimming devices. Scammers use cameras, keypad overlays, and skimming devices — like a realistic-looking card reader placed over the factory-installed card reader on an ATM or gas pump — to capture the information from your card's magnetic strip without your knowledge and get your PIN.

Watch that laptop. If you travel with a laptop, keep a close eye on it — especially through the shuffle of airport security — and consider carrying it in something less obvious than a laptop case. A minor distraction in an airport or hotel is all it takes for a laptop to vanish. At the hotel, store your laptop in the safe in your room. If that's not an option, keep your laptop attached to a security cable in your room and consider hanging the "do not disturb" sign on your door.

Still, despite your best efforts to protect it, your identity may be stolen while you're traveling. Here's a link for information on what you can do: https://www.identitytheft.gov/#what-to-do-right-away

Mark your calendars for 2017 & 2018 events:

Tuesday, November 14 – 6:30 pm – Captains Meeting, 1425 Paul Kirkwold Drive, Arden Hills

Topic: Internet & Online Security

Tuesday, February 6, 2018 – 6:30 pm – Captains Meeting, 1425 Paul Kirkwold Drive, Arden Hills

Saturday, February 18, 2018 – 9 am-Noon – Scouting Day, Public Works campus, Arden Hills

Tuesday, May 1 – 6:30 pm – Captains Meeting, 1425 Paul Kirkwold Drive, Arden Hills

To be determined – 6:00 pm – Night to Unite Hosts / Captains Appreciation Dinner

Tuesday, August 7 – Night to Unite events in neighborhoods throughout the community

Tuesday, November 13 – 6:30 pm – Captains Meeting

Thank you for working for safer neighborhoods!

like us on facebook

Deputy Mike Servatka
Crime Prevention Specialist
651-266-7339
email address: CrimePrevention@co.ramsey.mn.us

Randy Gustafson
Public Communications Coordinator
651-266-7315
website: www.RamseyCountySheriff.us

Remember – when you See Something, Say Something, Call 9-1-1