Ramsey County Sheriff's Office **Neighborhood Watch**
Bob Fletcher, Sheriff

Public Safety Services Division – Crime Prevention Unit
1411 Paul Kirkwold Drive • Arden Hills, Minnesota 55112
Phone: 651-266-7339 • Fax: 651-266-7337
www.RamseyCountySheriff.us

Block Captain News – September 2020

Night to Unite – visits cancelled

COVID-19 pandemic prompts Sheriff's Office to cancel participation in 2020 Night to Unite events

In this issue:
Night to Unite cancelled
Back to School remote safety
Online shopping
Cyber security and tele working
Social media free money offers

In the interest of the health and safety of our citizens, the Ramsey County Sheriff's Office has canceled participation in the 2020 Night to Unite event. The event is traditionally celebrated the first Tuesday in August, was earlier postponed to October, and is now canceled.

It was a difficult decision to not participate in Night to Unite event visits by deputies this year, but one that needed to be made due to the safety concerns of the Covid-19 pandemic. Night to Unite has proven to be an effective, inexpensive, and enjoyable opportunity to promote neighborhood spirit and police-community partnerships in pursuit of safer communities. Community benefits often extend beyond this single evening event as neighbors get to know each other and public safety agencies that serve them.

Even though deputies will not be visiting neighborhoods (and enjoying great food and conversations with the "good guys") there are some activities that can happen in this time of social distancing and limited gatherings.

Neighbors can let criminals know they are committed to keeping the neighborhood safe:

- display outdoor lights
- hold front porch (or end of driveway) vigils
- calling 9-1-1 when they see criminal and suspicious activity
- update their contact information with their Block Captain
- stay informed when Block Captains share tips and information from the Sheriff's Office
- stay engaged by getting to know neighbors and neighborhood activity patterns

Night to Unite has provided a great opportunity for the messages and connections as we all work toward neighborhood safety.

We look to come back bigger and better next year when Night to Unite will be on Tuesday, August 3, 2021.

Ramsey County COVID-19 response, assistance and services

Ramsey County is responding to the COVID-19 pandemic with services across multiple departments working closely with federal, state and local government, health care and community partners. Learn more and find links to services at: https://www.ramseycounty.us/coronavirus-disease-2019-covid-19-information

What to do when you (and your kids) are online at home

Information from the Federal Trade Commission:

If you have kids in school, there's a good chance they're kicking off their school year…in your living room. All the while, you might be working away, yourself, in some carved out corner at home.

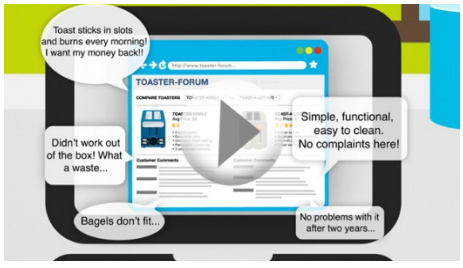
The start of a new school year is a good time to double-check your online set-up at home, since lots of people might depend on it. Here are a few things to check or consider.

- **Secure your router**. Does it still have the same default name and password that it came with? You'll want to change that (https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network) and be sure you've turned off remote management. Then log out as the administrator once the router is set up.
- **Update your software**. That means updating your browsers, operating systems, and apps. Then, set them to update automatically (https://www.consumer.ftc.gov/articles/0009-computer-security).
- **Use strong passwords** and two factor authentication when available. And while you're teaching your kids about the importance of a strong password (https://www.consumer.ftc.gov/articles/0009-computer-security#update), remind them NOT TO SHARE their password with their friends.
- **Update and protect your phone**. Make sure your phone's security is up to date (https://www.consumer.ftc.gov/articles/how-protect-your-phone-and-data-it) and you have your data backed up. (Backing up is good advice for your computer, too.)
- **Don't watch pirated content**. Hackers are using illegal pirated content as a way in to your devices and wireless network. So If you have content-hungry kids at home who have found free ways to stream content, learn more about what the pirates look like (https://www.consumer.ftc.gov/blog/2019/05/malware-illegal-video-streaming-apps-what-know), what the hackers can do, and what you can do to stop them.
- **Make use of privacy and security tools**. If you're hosting a video conference, or just participating in one, check out the privacy and security options your platform provides, including ways to keep unwanted visitors out of your conference (https://www.ftc.gov/news-events/blogs/business-blog/2020/04/video-conferencing-10-privacy-tips-your-business).
- **Don't open unexpected** video conferencing invitations or click on links. It might look real, but is it (https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams)? Check with whoever invited you to be sure (and not by replying to that message). Scammers are using fake invitations to load malware onto your computer or phone.

It's likely you're facing way bigger headaches than these right now. But taking a few minutes to check your systems now can save you from even bigger headaches later.

Shopping online? Watch this video from the FTC

Even as shops around the country open their doors again, buying online is still a great, useful tool for people to enjoy. It's nice to know that with a simple web search, you can find, buy, and ship almost any item right to your front door. But, while you're enjoying that convenience, you want to be sure that sharing your financial and personal data online is safe.



Before you click "Place Order," watch this video to learn some useful tips on how to keep your data secure and save money as you shop: https://www.youtube.com/watch?v=3w4t1dYCayM&feature=youtu.be

Beware of cyber criminals who take advantage of increased telework

Cyber criminals have been trying to take advantage of the COVID-19 pandemic and the increase in workers who are working remotely. In mid-July, cyber criminals started a vishing campaign at several companies and organizations. Vishing campaigns are attempts to gain unauthorized access to employee tools and technology, with the end goal of collecting information from private databases in order to sell that information or to use it for other nefarious purposes.

Tips to help keep your information safe:

- Verify web links do not have misspellings or contain the wrong domain.
- Be suspicious of unsolicited phone calls, visits or email messages from unknown individuals claiming to be from a legitimate organization. Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information. If possible, try to verify the caller's identity directly with the company.
- If you receive a vishing or phishing call, document the phone number of the caller as well as the domain that the actor tried to send you to and relay this information to law enforcement.
- Limit the amount of personal information you post on social networking sites. The internet is a public resource - only post information you are comfortable with anyone seeing.
- Bookmark the correct corporate VPN URL and do not visit alternative URLs on the sole basis of an inbound phone call.
- Evaluate your settings: sites may change their options periodically, so review your security and privacy settings regularly to make sure that your choices are still appropriate.

For more information on how to stay safe on social networking sites and avoid social engineering and phishing attacks, visit these Cybersecurity & Infrastructure Security Agency (CISA) Security Tips:

- Avoiding Social Engineering and Phishing Attacks - https://us-cert.cisa.gov/ncas/tips/ST04-014
- Staying Safe on Social Networking Sites - https://us-cert.cisa.gov/ncas/tips/ST06-003
- Keeping Children Safe Online - https://us-cert.cisa.gov/ncas/tips/ST05-002

The more things change - the more they remain the same

Unlocked vehicles remain easy targets for thieves

Thieves continued to find easy pickings in several of our neighborhoods this summer. Common themes in the reports are unlocked cars with valuables left inside parked on the street or driveway.

Even if you are parked in front of your house, in your driveway or inside your garage, lock your doors. Criminals like to walk down the street and see if a car is unlocked; if it is, they open the door and take whatever is visible and move on to the next target. However, if the door is locked, they are more likely to move on.

Reminder: Don't leave any valuables in your vehicle. Garage door remotes have provided access to burglars who have entered homes and stolen items, including cars.

Those free COVID-19 money offers on WhatsApp and Facebook are scams

Information from the Federal Trade Commission:

Have you seen a message on WhatsApp or Facebook offering you free help during the pandemic? People have reported seeing messages that seem to be from Pepsi, Walmart, Whole Foods, Target, and other big-name brands. These messages all offer money to people who need it — through grants, coupons for food support, or other giveaways. But they're all fake, and not from those companies at all.

You might get this kind of message, in English or Spanish, from a friend or contact. The message tells you to click a link to get your money. If you click, you might find a survey to take. Or they might ask you to enter your name, address, phone number, or other information. And they might ask you to forward the message to several friends to be eligible to collect.

But what these messages are really doing is running a phishing scam to collect your information (and your friends' info), and possibly putting malware on your phone, tablet, or computer if you click the link. There's no money to get, and no help to be had. Just scammers. It could have been a real (and hopeful) friend who forwarded that message to you – but it could have been a scammer who hacked your friend's account.

So: what do you do if you get one of these messages?

- Don't click on any links. That could download malware, expose you to even more scams, or add your phone number to lists sold to still other scammers.
- Delete the messages – and certainly don't share them.
- Call the friend who shared the message. Did they forward it to you? If not, tell them their account might have been hacked. If so, share this blog post with them.

If you already clicked or shared, run a security scan (https://www.consumer.ftc.gov/articles/0376-hacked-email) on your device to look for malware. And then share this blog post with the friends you forwarded the message to – and ask them to do the same.

And then tell the FTC: ftc.gov/complaint.

Neighborhood Watch is about Neighbors and Deputies working together

Involved neighbors are more likely to have open communication lines with each other, deputies, and the whole community. When neighbors know each other's names, normal patterns, and look out for each other, it is likely that they will report any activity that doesn't fit with regular schedules. Involved neighbors look out for each other.

Information sharing on crime prevention, crime trends, and law enforcement issues is a key element to the Neighborhood Watch program of the Sheriff's Office.

Neighborhood Watch program information and forms to help your block organization are available on the county website. **Please complete and return** the Block Captain registration form to ensure the Sheriff's Office has your most current contact information. THANKS!

Thank you for working for safer neighborhoods!

like us on facebook @RamseyCountySheriff

@RamseySheriff

@RamseySheriffMN

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

Randy Gustafson
Crime Prevention Coordinator
651-266-7315
website: www.RamseyCountySheriff.us

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