SHERIFF'S CORNER
Volume 28 / April 2025

This month we will give readers an update on recent frauds that we are seeing and have been reported. The fraudsters continue to work at scamming people in numerous ways and while the main content of the scam attempts stay the same we are constantly seeing new and revised methods that people are falling victim to, sometimes life-like and "real" looking schemes.

Scammers are sending fraudulent text messages and emails while impersonating MnDOT, E-ZPass or other tolling agencies. The messages falsely claim recipients have unpaid tolls, invoices or violations and urge people to verify personal information or submit a payment using a provided link. These messages claim you owe money and direct you to a payment link. This is a scam! MNDOT will never text or email you asking for payment or personal information. If you receive a suspicious text or email message, delete and do not respond. Do not set up an account due to a text or email scam. A few facts about this most recent scam as shared by MNDOT,

1. Minnesota E-ZPass (MnDOT) will never email or text you for payment or personal information.
2. Text numbers and email addresses are chosen at random, and they are targeting everyone—not just E-ZPass users. There is no data breach. This scheme has been more widespread and repetitive than others that we have seen and have been reported. The fraudsters continue to send the same message multiple times to almost every number in a prefix or area code.
3. Delete and don't click on anything that seems off or suspicious. Report as "junk" or "spam" if your device has this option. This helps your device recognize spam.
4. Do not set up a new or different E-ZPass account due to a text or email scam.
5. If you clicked on a link or provided information, take efforts to secure your personal information and financial accounts.
6. You can report fraud activity to the FBI's Internet Crime Complaint Center or the Federal Trade Commission – google search these organizations to get a link to make a report.

Annually with tax season we see an increase in reported scams and scam activity. The IRS publishes a list of known scam activities that are new for the tax preparation season. The commonly seen scams take place in a variety of formats like this:

Email phishing scams: The IRS continues to see a email and text scams targeting taxpayers and others. Taxpayers and tax professionals should be alert to fake communications from entities posing as legitimate organizations in the tax and financial community. These messages arrive in the form of unsolicited texts or emails to lure unsuspecting victims into providing valuable personal and financial information that can lead to identity theft. There are two main types:

- **Phishing:** An email sent by fraudsters claiming to come from the IRS. The email lures the victims into the scam with a variety of ruses such as enticing victims with a phony tax refund or threatening them with false legal or criminal charges for tax fraud.
- **Smishing:** A text or smartphone SMS message where scammers often use alarming language such as, "Your account has now been put on hold," or "Unusual Activity Report," with a bogus "Solutions" link to restore the recipient's account. The promise of unexpected tax refunds is another potential tactic used by scam artists.
- **Fake charities:** Bogus charities are a problem that can intensify whenever a crisis or natural disaster strikes. Scammers set up these fake organizations to take advantage of the public's generosity. They seek money and personal information, which can be used to further exploit victims through identity theft.
- Taxpayers who give money or goods to a charity might be able to claim a deduction on their federal tax return if they itemize deductions, but charitable donations only count if they go to a qualified tax-exempt organization recognized by the IRS.
- **The overstated withholding scam:** This is a recent scheme circulating on social media encouraging people to fill out Form W-2, Wage and Tax Statement, or other forms like

Form 1099-NEC and other 1099s with false income and withholding information. In this overstated withholding scheme, scam artists suggest people make up large income and withholding amounts as well as the fictional employer supplying those amounts. Scam artists then instruct people to file the bogus tax return electronically in hopes of getting a substantial refund due to the large amount of fraudulent withholding.

As always, if you feel that you are being scammed, stop the activity, communication or transaction immediately. Also, contact any financial institutions that you are affiliated with and report the incident. If you need additional help navigating through the process, feel free to contact our office to create a report and get some assistance and guidance on safeguarding yourself.

If you have specific questions that you would like answered in this column or in person, please feel free to contact me anytime using one of the following methods:

Email:
bryan.welk@casscountymn.gov
Phone:
218-547-1424 | 1-800-450-2677
By Mail/In Person:
Cass County Sheriff's Office
303 Minnesota Ave W
PO Box 1119
Walker MN 56484