Like many Minnesotans, I enjoy fishing. Regardless of the weather or the pace of the bite, fishing is a good time. The only thing that could ruin fishing for me is when it is phishing with a "ph." Phishing is the term used to describe scams perpetrated by criminals who attempt to trick you into giving them personal information, passwords, or access to your electronic devices. Most often, phishing attacks are carried out through either telephone calls or emails. Recently, there has been in increase in the frequency of phishing attacks coming to victims via text messages. This new method has been dubbed "smishing," a name derived from combining SMS (the name of the communication protocol for text messages) and phishing. Smishing attacks aim to trick victims by convincing them that someone they know is in trouble, that they have a prize or unclaimed money waiting for them, that a financial account or utility service is about to be interrupted and/or closed, or any number of other false premises. Smishing attacks may either ask a victim to call a phone number or click on a link in the message. Victims who call the telephone number are connected to a criminal who will work to steal personal information like social security numbers, banking information, and passwords. Victims who click on links in the text messages find they are brought to a website that is asking for personal information or have initiated a download of malware that may spy on them or steal personal information from their device. Most of these smishing attacks do their best to convince victims that the victim must act quickly to either help someone, claim their winnings, or avoid the loss of service.

Fortunately, it is quite easy to avoid the stormy waters of smishing attacks. Simply blocking the number and deleting the message will keep your device and personal information safe. If you feel the need to document the smishing attack, take a screenshot of the text message. Replying to a smishing attack is not recommended, even if the message says that a reply will stop future messages. By replying, you are letting a criminal know that your telephone number is an active number owned by a person that receives text messages. Armed with that information, criminals will mark your number as a potential target resulting in many subsequent such messages and phone calls.

So, in this modern world where everyone from our dentist to our closest friends send us text messages, how can you tell if a text message is coming from a legitimate business/government entity or a criminal? The first and most important rule is that if you were not expecting the text message, regardless of who the sender claims to be, you should automatically be very suspicious. If you think that there is a chance the unexpected message you received is from a legitimate source, find a telephone number on your own for that business or government agency and contact them independently to verify the source of the message. Next, if the message attempts to convey a sense of urgency for your actions, you should be wondering why this person or entity chose to send an urgent message to you via text. Take a moment and work independently to verify if the message is true. Finally, everyone should operate from the assumption that there is no free lunch. Any message you receive claiming that you are owed money or have won a prize should put you on alert, especially if you are being asked to either supply banking information or click on a link. Don't let your dream of free stuff turn into an identity theft nightmare.

The Minnesota Attorney General's Office offers the following advice on reporting smishing scams. "Forward smishing messages to short code 7726—which spells 'SPAM' on your keypad. Doing so allows cell phone carriers to identify the senders of smishing messages and take steps to limit messages

from them going forward." They also recommend those receiving smishing messages "file a complaint with the Federal Trade Commission and the Federal Communications Commission." If you believe you have been the victim of a smishing scam you should contact your local law enforcement agency. If you gave personal information you should consider contacting the three major credit reporting bureaus (Equifax, Experian, and Trans Union) and request they place a freeze on your credit to prevent criminals from opening accounts in your name. If you gave out banking information to a scammer, you should contact your bank or credit card companies to stop any illegal charges.

Play it smart to ensure you don't fall for a smishing scam hook, line, and sinker. For more crime prevention information and safety information visit the Benton County Sheriff's Office website at: https://www.co.benton.mn.us/211/Crime-Prevention. You can also like and follow us on Facebook and Twitter at @BentonMNSheriff for regular updates and crime prevention messages.