# When in Doubt, Don't Give it Out

From the Office of Minnesota Attorney General Lori Swanson

Scams and crooked deals are everywhere today, often where we least expect it. When you're home answering the phone, browsing the Internet, checking the mail, or opening your door, scam artists and fraudulent operators look for ways to get your Social Security number and other private information. You can protect yourself in many situations by following one simple principle—if someone contacts you and claims to need your private information, think twice and remember: **when in doubt, don't give it out**.

## How it Happens

Private information can be compromised in a number of ways. Fraudulent operators may pose as a legitimate entity, such as your bank or a government agency. Some may even pretend to be a trusted local business, or a friend or family member. These swindlers will try to get you to provide private information, such as your Social Security number, a bank account number, or a credit card number. Once you give it out, however, a scam artist may steal your identity and your money, opening lines of credit in your name or draining your bank accounts. A legitimate source will not contact you to ask for private information up front. If you are unsure of who is contacting you, remember: **when in doubt, don't give it out**.

## Over the Phone

Consumers report receiving calls from individuals who claim to be many things they are not. Some scam operators pose as Medicare, Social Security, or an insurance company, claiming they need to "verify" private information in order to send new benefit cards. Other scam callers claim to be from "Card Services" or credit card company, asking to "verify" similar private account information. Even more troubling, many consumers report receiving calls from impostors who pose as a loved one—for example, a grandchild—asking for banking information or an unsecure money transfer. Scam callers may even pretend to be the IRS and claim that you owe tax debt to the government as a reason to demand sensitive information. All of these calls involve a con artist who is trying to gain your trust and learn your private information in order to take your money.

Cell phone users also experience scams. Consumers report receiving text messages from scam artists and fake organizations claiming a need to "verify" their bank account, credit card, or other private information.

Telephone scams can be some of the most difficult to detect, because callers can seem legitimate and their need very urgent. Consumers must use caution whenever someone calls or sends a text message asking for private information. Take time to verify the call with the help of a friend and through a trusted line of communication. Before providing any private information, remember: **when in doubt, don't give it out.**

## On the Internet

Consumers increasingly face uncertainty when they shop or communicate online. The websites they visit often collect personal information in the background as they browse. Other sensitive information can be compromised in common email scams called "phishing." Similar to fraudulent calls and text messages, a phishing email looks like it is from a legitimate source and presents an urgent need for your private information. Once you provide it, however, a scam artist on the other end will use it to commit fraud or identity theft.

Some consumers also report fraudulent activity on marketplace or social media websites. Beware of any unsolicited request for private information on the Internet, especially if you do not know the source. If you encounter an unfamiliar website or email, or if you are unsure of who is behind a request for information, remember: **when in doubt, don't give it out.**

**MINNESOTA ATTORNEY GENERAL'S OFFICE • 445 MINNESOTA STREET, SUITE 1400, ST. PAUL, MN 55101**
(651) 296-3353 (Twin Cities Calling Area) • (800) 657-3787 (Outside the Twin Cities)
TTY: (651) 297-7206 • TTY: (800) 366-4812 • *www.ag.state.mn.us*

## In the Mail

Some of the oldest and most destructive scams continue to be conducted via U.S. mail. Fraudulent sweepstakes offers, fake checks, and other deceptive mail may seek to obtain private information or ask for a direct payment from your bank. Consumers have been led to believe they have prize winnings to collect, and many transfer thousands of dollars without seeing a dime in return. A scam offer can be difficult to detect and nearly impossible to stop once anything is sent to an unknown source. The scammer usually works from outside the country, making it very difficult and expensive for law enforcement to investigate the crime. Beware of any mail that says you must provide private information or pay money to receive any type of benefit. When an offer seems too good to be true, it probably is. If you are ever asked to send private information or pay money to an unknown source, remember: **when in doubt, don't give it out**.

## At Your Doorstep

Some bad actors may try to get your private information by visiting you in person. These individuals may use deception and fear, hoping you will give up private information or agree to a quick sale on the spot. Regardless of the offer, don't be afraid to say "no," and shut the door when you feel unsafe. If a salesperson wishes to do business with you, he or she should be willing to leave the company's information or contract behind for you to review. Rather than release private information on the spot, remember: **when in doubt, don't give it out**.

Honest businesses are often aware of the danger customers face with giving out private information, and few actually require it. Some companies, such as banks, utility companies, and creditors may require certain information to do business. When this is the case, these organizations generally will not contact you in order to get it. Don't rush into doing business with any company before you have a chance to check it out.

For more information, contact the Office of Minnesota Attorney General Lori Swanson:

**Office of Minnesota Attorney General**
**Lori Swanson**
445 Minnesota Street, Suite 1400
St. Paul, MN 55101
(651) 296-3353 (Twin Cities Calling Area)
(800) 657-3787 (Outside the Twin Cities)
TTY: (651) 297-7206 or (800) 366-4812
*www.ag.state.mn.us*