



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. At every turn, you can protect yourself by following one easy 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. Most often, fraudulent operators pose as a legitimate source, such as your bank or a government agency. Some may even pose as a trusted local business, or as a friend or family member. All of these actors 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 accounts. Some crooked actors make deceptive claims and try to scare you into giving up your banking information. A legitimate source should 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 to send new benefit cards and needing to "verify" private information. Other scam callers claim to be from "Card Services" or from a credit card company, asking to "verify" similar private account information. Even more troubling, many consumers report receiving calls from impostors who try to pose as a loved one, asking for banking information or an unsecure money transfer. All of these calls involve a scam artist who is trying to gain your trust and your private information in order to take your money.

Cell phone customers 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 very real and their need very urgent. Consumers must use caution whenever someone calls with a sense of urgency, needing their 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. Often the websites they visit collect personal information as they browse. Other sensitive information can be compromised in common email scams called "phishing." Similar to scam calls and text messages, a phishing email looks like it is from a legitimate source. The email 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 with buyers and sellers on classified websites. Beware of any unsolicited request for private information on the Internet, especially if you do not know the source. If you arrive at 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.**

In the mail. Some of the oldest and most destructive scams continue to be conducted via U.S. mail. These scams can involve fraudulent sweepstakes offers, fake checks, and other deceptive claims that seek to obtain private information or direct payment from your bank. Consumers have been led to believe they have prize winnings to collect, and many send away thousands

of dollars without seeing a dime. 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 money to receive any type of claim. When an offer seems too good to be true, it probably is. If you are ever asked to send private information or money to an unknown source, remember: **when in doubt, don't give it out.**

At your doorstep. Some deceptive 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 should actually require it. Some businesses such as banks, utility companies, and creditors do 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 be rushed 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

1400 Bremer Tower

445 Minnesota Street

St. Paul, MN 55101

651-296-3353 or 800-657-3787

TTY: 651-297-7206 or TTY: 800-366-4812