Friends and Family: Beware of Imposter Scams

From the Office of Minnesota Attorney General Lori Swanson

In recent months, some Minnesotans have reported receiving phone calls or e-mails that appear to be from friends or family members in need of help. In reality, the e-mails and phone calls are from imposters posing as distressed family members. The scams take several different forms, but in all cases their goal is to dupe concerned family members into providing bank account information from which the imposter steals funds.

E-mail Imposters: A friend in trouble? Or an imposter?

Some Minnesotans report receiving e-mail messages from imposters who impersonate a friend or family member in sudden need of emergency funds. A typical imposter e-mail message is from a friend's e-mail address and describes the friend's sudden misfortune, which is often a lost or stolen wallet while traveling in a foreign country. The message asks the recipient to wire money immediately through Western Union or Money Gram. By claiming that the friend is stranded and utterly without means, the imposter friend implores the recipient to rescue the "friend" with money.

How to avoid the scam. The use of a friend's name, traveling abroad, and an urgent need for money are the hallmarks of this imposter scam. If you receive an e-mail from a friend or family member who claims to be stranded and needs thousands of dollars, be aware that an imposter may have hijacked an e-mail account or computer. A cautious recipient can avoid being scammed. Phone your friend or mutual acquaintances and investigate their story before you act.

What else to do. There are two ways this type of imposter e-mail is created. If the attack is from a webmail account, such as Yahoo, Gmail, Hotmail or the like, an attacker may have gained access to that webmail account. Or, it may be that you or your friend's computer is infected with a malicious program that found an address book on the computer and sent spam to every address, using one of the addresses as the "from" address. To stop this spam, make sure that your webmail account is secure. Change your password. If you can't change the password, or even log on, your webmail account has been hijacked. Contact your webmail provider for help. If you can log on and change your password, your webmail may not have been hijacked or, if it was, you've now taken it back. Next, malware on your computer could be spamming you and your friends. You can see if your computer is infected by running an online virus checker, available for free on the websites of most anti-virus vendors. If your computer is infected, disconnect from the Internet and have your computer cleaned. If you have financial or identity data on your computer, take steps to protect your financial accounts and your identity from theft and misuse. If your computer is clean, a friend's webmail or computer is the source.

Telephone Imposters: A grandchild in trouble? Or an imposter?

Some Minnesota grandparents report receiving telephone calls from what sounds like a grandchild in distress. The phone call starts with a phrase like, "Hi Grandma/Grandpa! Do you know who this is?," or something similar. If the consumer responds with a name, the imposter poses as that grandchild, describes urgent trouble, often in a foreign country, and begs the grandparent to wire money by Western Union or Money Gram to pay for medical care, bail money, auto repairs, or a ticket home. By claiming to be embarrassed or under urgent time constraints, the imposter "grandchild" tries to dissuade the grandparent from contacting the grandchild's parents or friends.

How to avoid the Grandparent Scam. You can avoid the Grandparent Scam by verifying a caller's identity and resisting pressure to act before the caller's identity is verified. To verify the caller's identity, contact a family member who could confirm the caller's story, call the real grandchild at a number you know is accurate, or ask questions of the caller that only the real grandchild would know. Do not give out names or information on other family members unless you are certain of the identity of the caller. Resist pressure to act quickly. This scam depends upon a grandparent's compassion for their grandchildren outweighing any concern about potential scams. The imposter always claims that there is an emergency and always asks for secrecy.

What else to do. If you receive a fraudulent phone call like the Grandparent Scam, try to trace the call. You can initiate call trace by immediately dialing *57 after you hang up from a fraudulent phone call. When you do that, the caller's phone number will be forwarded and recorded at the phone company's call identification center. You should then contact your local police department to file a complaint.

Overall Tips--Don't Become A Victim

When you receive an urgent request for help by phone or e-mail:

1. Verify that the person contacting you is who they claim to be, and not an imposter.
2. Resist pressure to send money quickly and secretly.
3. Refuse to send money through wire transfer or overnight delivery unless you are absolutely sure that you are sending money to a real friend or family member.

Additional Resources

For more information, contact your local law enforcement agency or the following:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, D.C. 20580
Toll free: 877-382-4357
www.ftc.gov

Federal Bureau of Investigation
Minneapolis Office
1501 Freeway Boulevard
Brooklyn Center, MN 55430
763-569-8000
www.fbi.gov

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