Text Message Phishing — or "Smishing" — Scams

The Office of the
Minnesota Attorney General
helping people afford their lives and live with dignity, safety, and respect

ATTENTION:
Call back now to reactivate your credit card.

Be the first person to visit this link and win a free gaming system!

Text messages like these are quick to grab our attention. Studies show that the majority of incoming text messages are opened within 15 minutes of receipt. Scam artists know this and sometimes target consumers with "phishing" scams via text message or SMS (short message service).

Text message or SMS phishing—also called "smishing"—occurs when scam artists use deceptive text messages to lure consumers into providing their personal or financial information. The scam artists that send smishing messages often impersonate a government agency, bank, or other company to lend legitimacy to their claims. Smishing messages typically ask consumers to provide usernames and passwords, credit and debit card numbers, PINs, or other sensitive information that scam artists can use to commit fraud. It can happen like this:

"John" received a text message that appeared to be from his local credit union. The message stated that his debit card had been deactivated. The message instructed him to call a toll-free telephone number, which he did. When John received a recording that asked him to enter his debit card and PIN, he hung up. He then called his credit union and spoke to a representative who stated his debit card was working properly and the text message was a scam.

"Catherine" received a text message from a local telephone number that stated she could receive a free $1,000 shopping spree at a big discount store if she was one of the first 100 visitors to a website linked to the message. Catherine immediately opened the link and was asked to enter her email address and credit card number. Catherine noticed that the website had the same color scheme and a similar font as the store's website, but the store's name was spelled incorrectly and the URL did not start with "*https://*" like a secure website usually does. Catherine closed the link without providing any information and called her cell phone company to report the text message as a scam.

Avoid Smishing Scams

Don't be misled by smishing scams. Remember the following:

- Government agencies, banks, and other legitimate companies never ask for personal or financial information, like usernames, passwords, PINs, or credit or debit card numbers via text message.
- Don't be rushed. Smishing scams attempt to create a false sense of urgency by implying that an immediate response is required or that there is a limited time to respond.
- Don't "click" open links in unsolicited text messages. Clicking the link may infect your mobile device with a virus or malware designed to steal the personal or financial information stored on the device.
- Don't call a telephone number listed in an unsolicited text message. Scam artists often use email-to-text technology, short codes, or spoofed local numbers to hide their identity. You should contact any bank, government, agency, or company identified in the text message using the information listed in your records.
- Don't respond to smishing messages, even to ask the sender to stop contacting you. Responding to smishing messages verifies that your phone number is active and that you are willing to open

such messages, which may lead to an increase in the unsolicited text messages you receive.

- Use caution when providing your cell phone number or other information in response to pop-up advertisements and "free trial" offers. This personal information can be easily bought, sold, and traded, and make you a target for smishing scams.
- Never provide your personal or financial information in response to text messages from unknown senders. Verify the identity of the sender and take the time to ask yourself why the sender is asking for your information.
- Use the same safety and security practices on your cell phone as you do on your computer: be cautious of text messages from unknown senders, as well as unusual text messages from senders you *do* know, and keep your security software and applications up to date.

How to Report Smishing

Contact the bank, government agency, or company that the scam artist is impersonating so it can alert others and work with law enforcement to investigate the activity.

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.

File a complaint with the Federal Trade Commission ("FTC") and the Federal Communications Commission ("FCC"). These agencies enforce the laws regarding scam calls and text messages. You may contact the FTC and FCC as follows:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
(877) 382-4357
TTY: (866) 653-4261
www.reportfraud.ftc.gov

Federal Communications Commission
45 L Street NE
Washington, DC 20554
(888) 225-5322
www.fcc.gov/complaints

For more information, contact the Office of Minnesota Attorney General Keith Ellison as follows:

Office of Minnesota Attorney General Keith Ellison
445 Minnesota Street, Suite 1400
St. Paul, MN 55101
(651) 296-3353 (Twin Cities Calling Area)
(800) 657-3787 (Outside the Twin Cities)
(800) 627-3529 (Minnesota Relay)
www.ag.state.mn.us