TEXT MESSAGE SCAMS: SMISHING

Consumer Alert

"Smishing"

Smishing is when scammers send text messages pretending to be from trusted sources. The goal is to get targets to respond with personal information like passwords and credit card details or to click on links that install malware. It is just like phishing that uses emails; instead smishing uses texts.

More than 20 billion text messages are sent every day in the United States.

A growing number of texts are from thieves trying to scam you. They can send millions of smishing texts at the same time. And because smartphone users are three times more likely to fall for fake text messages than computer users are to fall for fake email messages, text message scams are on the rise.

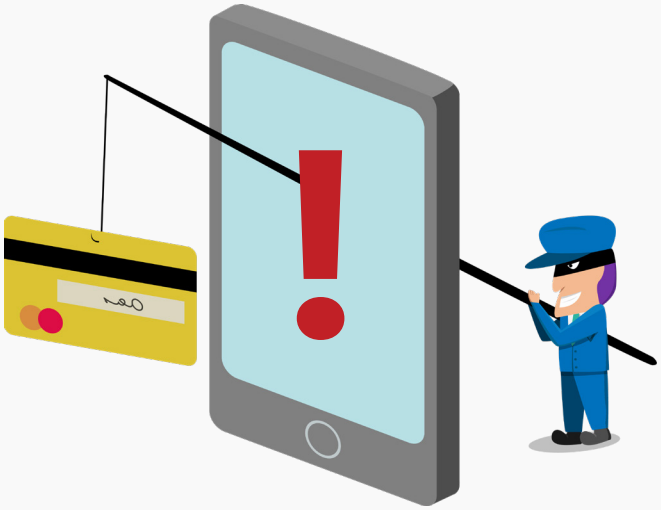
A common smishing tactic is to send a text warning about a fake problem with one of your accounts and ask for your information. Some scammers will pitch offers too good to be true or even promise free gift cards or trips. **Do NOT respond!** You may get malware or become an identity theft victim.

What you need to know

Federal law makes it illegal to send commercial text messages to a mobile device without first getting the consumer's permission.

This ban applies even if you have not placed your mobile number on the Do-Not-Call List, but there are two issues. First, you may unknowingly give your consent, and second, criminals don't follow the law.

Sharing the number for your device, buying apps, and using free or inexpensive ring tones or downloads put you at more risk.



Smartphone users are three times more likely to fall for fake text messages than computer users are to fall for fake email messages.

And those apps or free downloads often come with "terms of agreement," that if you don't read carefully, may allow your number to be shared or sold.

Forward smishing texts to 7726

If you are an AT&T, T-Mobile, Verizon, Sprint or Bell subscriber, you can report spam texts to your carrier by copying the original text and forwarding it to 7726 (SPAM), free of charge.

Report smishing texts

If you cannot use 7726, then report smishing texts to your mobile service provider and the Federal Communications Commission (FCC).

Dana Nessel
Attorney General

TEXT MESSAGE SCAMS: SMISHING

Consumer Alert

SPOT IT: Signs of a text scam

- A text message that looks like it is from your bank and is about a problem with your account. A phone number is listed for you to call immediately.
- A text message from an unknown sender that asks you to call a number or click on a link or respond with personal information.
- A text message that reads: "REAL ROLEX 90% OFF, click here."
- A text message that says, "click here," enter "x," or reply "stop" to opt out of future messages.

STOP IT: Protect your mobile phone number

- Don't share your phone number unless you know the person or organization well.
- Beware the fine print in user agreements for products or services that may use your phone number, like mobile apps and free ring-tone offers.
- **NEVER** follow a text's instructions to push a designated key to opt out of future messages. Instead, forward all questionable texts to 7726, so wireless carriers can investigate and block that sender.
- Report scam texts to the Federal Communications Commission online; by phone 888-225-5322; or by mail: FCC Consumer Complaints, 445 12th Street, S.W., Washington, DC 20554.

To file a consumer complaint or get additional information, contact the Michigan Department of Attorney General:

Consumer Protection Division
P.O. Box 30213
Lansing, MI 48909
517-335-7599
Fax: 517-241-3771
Toll free: 877-765-8388
Online complaint form

Dana Nessel
Attorney General