State of Illinois
Department of Innovation & Technology

Division of Information Security

Smishing
SMS phishing

What is Smishing?

Mobile phones are a popular target of phishing scams. A recent trend in phishing is SMS phishing or smishing. Smishing is a scam sent to you via a text message. It is much easier to fall for these tricks on your mobile device because of its limited screen space and the "always on" nature of our mobile devices.

Most Phishing Scams Play on Your Fear of Things Such as:

- Fear of losing your money
- Fear of being accused of a crime that you did not commit
- Fear of harm to you or your family
- Fear of something embarrassing being revealed about you (whether it is true or not)

The Internet Crime Complaint Center (IC3) states that many banks don't send text messages because they don't want people to fall for smishing attacks. If it is really your bank texting you, then your bank should know exactly what you are talking about when you call them using their phone number on your latest bank statement. If they say there are no issues with your account, then the text was obviously bogus.

IC3 Tips to Protect Yourself From Cyber Scams

- Don't respond to text messages or automated voice messages from unknown or blocked numbers on your mobile phone.

- Treat your mobile phone like you would your computer…don't download anything unless you trust the source.

- When buying online, use a legitimate payment service and always use a credit card because charges can be disputed if you don't receive what you ordered or find unauthorized charges on your card.

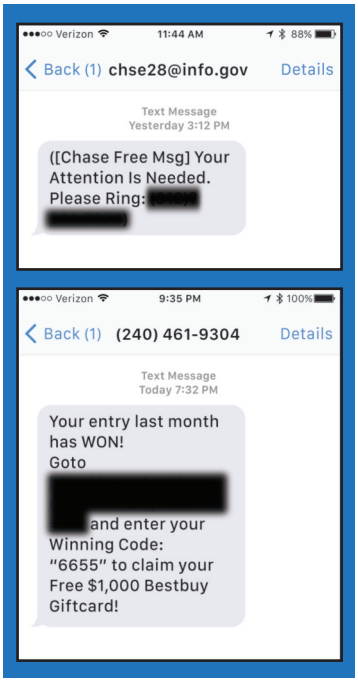
- Check each seller's rating and feedback along with the dates the feedback was posted. Be wary of a seller with a 100 percent positive feedback score, with a low number of feedback postings, or with all feedback posted around the same date.

- Don't respond to unsolicited e-mails (or texts or phone calls, for that matter) requesting personal information, and never click on links or attachments contained within unsolicited e-mails. If you want to go to a merchant's website, type their URL directly into your browser's address bar.

EXAMPLES OF SMISHING

Falling victim to these fraudulent texts could result in:

- Loss of personal information
- Installation of malware
- Exposing sensitive information
- Identity theft
- Financial loss



ENCRYPTION | SECURITY | AWARENESS | BEST PRACTICES

DoIT Illinois Department of Innovation & Technology

What do I do? You delete the fraudulent text.

Do NOT click on any links • Do NOT respond • Do NOT call any numbers listed

IOCI 17-240 Printed by Authority of the State of Illinois 11/16

www.DoIT.illinois.gov