

Don't Text Back

<http://www.onguardonline.gov/blog/dont-text-back>

By Aditi Jhavari

Consumer Education Specialist, FTC

You get a text message claiming your email account has been hacked. The message asks you to text back in order to reactivate your account. Has your account really been hacked, or is this a scam?

Here's an example of a spam text making the rounds:

User #25384: Your Gmail profile has been compromised. Text back SENDNOW in order to reactivate your account.

The scammers who sent that message want to take advantage of your computer security concerns in order to get your personal information. If you've received a text message like it, here's what to do:

- **Don't text back.** Legitimate companies won't ask you to verify your identity through unsecure channels, like text or email.
- **Don't click on any links within the message.** Links can install [malware](#) on your device, and take you to spoof sites to try to get your information.
- **Report the message to your cell phone carrier's spam text reporting number.** If you're an AT&T, T-Mobile, Verizon, Sprint or Bell customer, you can forward the text to 7726 (SPAM) free of charge.
- **File a complaint with the Federal Trade Commission.** Your complaint can help the FTC detect patterns of wrongdoing.
- **Check out Onguardonline's articles on [text message spam](#) and [computer security](#) for more tips.**

Cyberspace Training Initiative

Equipping the Cyber frontline defender at work, home and on travel.

Email questions/comments to: CTI@Stratcom.mil

Visit the Cyber Gateway (CAC required)

https://vela.stratcom.mil/sites/cyber_gateway/default.aspx

