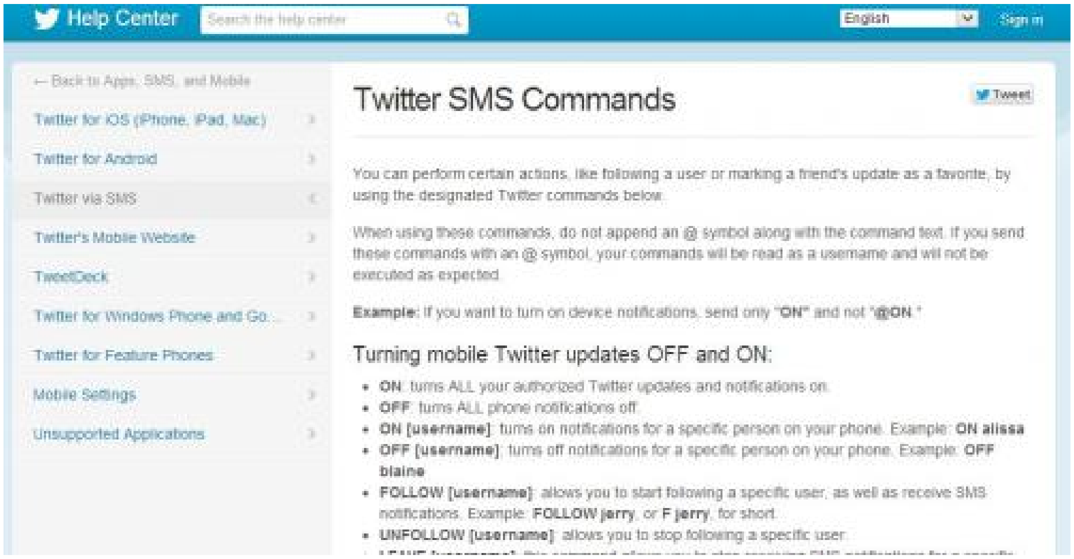
Security researcher finds SMS vulnerability in social media sites

December 5 2012, by Bob Yirka



Twitter SMS Commands

You can perform certain actions, like following a user or marking a friend's update as a favorite, by using the designated Twitter commands below.

When using these commands, do not append an @ symbol along with the command text. If you send these commands with an @ symbol, your commands will be read as a username and will not be executed as expected.

Example: If you want to turn on device notifications, send only "**ON**" and not "**@ON**."

Turning mobile Twitter updates OFF and ON:

- **ON**: turns ALL your authorized Twitter updates and notifications on.
- **OFF**: turns ALL phone notifications off.
- **ON [username]**: turns on notifications for a specific person on your phone. Example: **ON alissa**
- **OFF [username]**: turns off notifications for a specific person on your phone. Example: **OFF blaine**
- **FOLLOW [username]**: allows you to start following a specific user, as well as receive SMS notifications. Example: **FOLLOW jerry**, or **F jerry**, for short.
- **UNFOLLOW [username]**: allows you to stop following a specific user.

(Phys.org)—Jonathan Rudenberg a self described security consultant, developer and researcher has been heavily involved in stamping out an SMS messaging vulnerability he found in Facebook, Venmo and Twitter. He has been posting his efforts on his blog and says that all three companies have finally fixed the problem.

Rudenberg says the vulnerability allowed hackers to spoof messages from the services if they obtained the phone number associated with an account. Spoofing is where hackers send messages that appear to be from the true account holder – most users of email have seen examples of spoofed messages in their spam folders. He apparently became aware of the vulnerability in all three services sometime last summer and has been trying to get all three to fix the problem. Twitter was the last to do so, having only notified him that the problem had been fixed December 4.

With Twitter the problem came about when users configured their account to accept SMS messages and also didn't have a personal identification number set up for the account. To spoof a message, hackers would only need to know the phone number that had been associated with the account. Also because of the way Twitter accounts are set up, knowing the phone number would also allow hackers to change profile account information.

Rudenberg says he notified Twitter and Facebook that he had found the vulnerability last August and Venmo in November. He was only able to get through to Facebook, he says because he has a friend working with the company. Facebook let him know they'd fixed the problem in November, and Rudenberg will be receiving a bounty check from the company for his efforts. He says Venmo, (an Internet payment system similar to Paypal) responded very quickly and fixed the problem by disabling SMS payments. Twitter however, took longer.

Rudenberg says he notified the company about the problem on August 12, and received a response three days later letting him know his concern had been routed to a security team. In September he was asked by the company to not publish what he'd found till they'd fixed the problem. In October, having not heard from the company he requested an update and received no response. By the end of November he'd become frustrated and sent the company a message indicating he was going to go public with the issue. Six days later he received a message from the company saying the issue had been resolved.

Citation: Security researcher finds SMS vulnerability in social media sites (2012, December 5) retrieved 25 April 2024 from https://phys.org/news/2012-12-sms-vulnerability-social-media-sites.html