Issued 7/17/17

Facebook Users Pwnd by Phone with Account Recovery Vulnerability

Facebook account recovery using pre-registered mobile numbers is poorly implemented and open to abuse, according to critic James Martindale. Martindale wrote an article on Medium, titled I kinda hacked a few Facebook accounts using a vulnerability they won't fix, highlighting his concerns in a bid to push the social network into tightening up its system.

Old phone numbers no longer owned by a user but are still tied to their account can be assigned by a carrier to another person. If the number is still linked to a Facebook account, the new owner can subsequently log into the account without the password and either change it or leave it be (so someone doesn't know a breach has occurred). The loophole cannot target specific accounts but might be used to hijack an account before, for example, running scams against the account holder's friends and contacts.

Quizzed by The Register, Facebook said its practices mirrored those of other online services, adding that it already pushes alerts in cases where it detects suspicious password recovery attempts. Several online services allow people to use phone numbers to recover their accounts. We encourage people to only list current phone numbers, and if we detect the password recovery attempt as "suspicious" we may prompt the person for more information. Martindale responded that Facebook was missing the

point, adding that "several online services" also having account recovery via phone numbers isn't a very good defense.

Facebook is different from these other services because it allows users to have multiple mobile phone numbers. Martindale stumbled on the issue when his carrier assigned him a number previously linked to another Facebook user. He received a reminder text from Facebook and discovered that the associated account had five other phone numbers linked to it. "Many of my less tech- savvy friends never remove phone numbers, they just keep adding their new number when they switch carriers or move," Martindale noted. "I probably never would've stumbled across this exploit if it weren't for Facebook sending re-engagement SMS messages to the phone number I inherited," he added. "I understand sending a few texts to remind an inactive user of what they're missing out on, but after a while shouldn't Facebook decide they're just not interested? These text alerts make it incredibly easy to discover when a phone number is attached to a Facebook account (other than searching Facebook for the phone number)."

"When I started this experiment, I decided I would get to the point where Facebook forces a password reset, and then stop," Martindale explained. "Facebook surprised me by letting me log in without changing anything. I don't know of a single website other than Facebook that lets me recover an account with a phone number, and then not change the password." Martindale told El Reg he was glad to hear that Facebook has some sort of system to detect suspicious logins while arguing it needed it needed to be improved. "Once I discovered this exploit, I developed a habit whenever I get a new number to log into the associated Facebook account (if it exists) to see if the exploit still exists and to remove the phone number from the account," he said. "Never once have I been 'prompted for more information'. Facebook's suspicious login detection needs work." As well as improving detection of suspicious recovery attempts, Facebook should apply changes so that a user can't retrieve an account using the same

email address or phone number they used to log in. "Google, Microsoft, and a ton of other good online services make users use an alternate email address or phone number, and sometimes require the rest of the obfuscated number/email address in order to continue recovery," Martindale argued. "This alone would stop this exploit in its tracks." "When a user adds a new phone number to an account, Facebook should immediately ask them if they want to remove their old phone number," he added. "If Facebook encourages users to only list current phone numbers this would be the best way to do just that," Martindale concluded.