Facebook Now Allows Users To Find You Using Your Cell Phone Number

March 5, 2019 - Facebook users who use the company's "two factor authentication", or 2FA, can now be looked up by anyone with who has their cell phone number. It's a giant step backwards for privacy and identity theft prevention. Ironically 2FA is used to enhance user privacy and security on most websites. But Facebook's move could make people think twice before they sign up for 2FA in the future.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

2FA is a simple concept that can help to prevent your online accounts from being hijacked. It works like this. When you setup an online account, you also provide a mobile phone number. When you go to log into that account a window pops up asking you for a verifications code. That code is sent to you via a text message and is usually a six or seven digit number. Once you enter the code, you're logged in as normal.

While simple, the concept is extremely effective at keeping hackers and identity thieves at bay. That's because in theory, it would be very unlikely for a hacker to get access to your password and have access to your cell phone.

The reason what Facebook is doing is so detrimental is also simple. Let's say that you're a determined hacker. You start entering random phone numbers into a Facebook search. Eventually, you get one right and a profile pops up. And on that profile there happens to be a lot of public information. Things like a birth date, a home town, a full name, place of work, etcâ€¦ After scrolling through some of the posts, you may even be able to find an address.

The bottom line is that now you're getting to the point that you might be able to commit identity theft. And you definitely have enough information to contact a cell phone carrier and do a SIM card swap. Essentially, you can steal the phone number and gain access to text messages and other information that may be available.

In essence, Facebook is weaponizing 2FA to work against anyone using it. And they are opting-in users automatically. Anyone who has been using 2FA on their site can now be searched for using their phone number. While the company will allow users to limit searches to friends, the default setting is "public" - meaning anyone can search for you if they have your number - and you can't completely opt out.

The bottom line here is that Facebook's 2FA isn't worth the security risk in our opinion. If you are going to use Facebook, just make sure that your user password is strong and that you're not using the same password on any other site. And if

you can, it may be best to find another way to stay in touch with friends and dump Facebook all together. That way you don't have to worry about the way the company disrespects user privacy
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS

.