Facebook Breach: What to do Next

October 3, 2018
by Lisa Weintraub Schifferle
Attorney, FTC, Division of Consumer and Business Education

Facebook recently announced the largest breach in the company's history. The breach affected about 50 million users, allowing hackers to take over their accounts. If you use Facebook, you may be wondering what to do next. Here are a few steps you can take.

First, you probably want to know more about the breach. According to Facebook, the attackers took advantage of a weakness in the "View As" feature, which lets people see what their profile looks like to others. The hackers stole digital keys that keep you logged in to Facebook so you don't need to re-enter your password every time. Facebook says they've fixed the vulnerabilities and reset digital keys on 50 million affected accounts, plus an additional 40 million accounts that used the "View As" function.

To better protect yourself after this breach:

- Watch out for imposter scams. With access to your Facebook account, hackers can get a lot of information about you. That information could be used to impersonate people you know or companies you do business with. If someone calls you out of the blue, asking for money or personal information, hang up. Then, if you want to know for sure if the person calling you was really your family member or was really from a company you know and trust, call them back at a number you know to be correct before you give any information or money. And remember: anyone who demands that you pay by gift card or by wiring money is scamming you. Always.

- Consider changing your password. Facebook says that it fixed the vulnerability, so there's no need to change your password. But, to be safe, log in and change your password anyway. If you use the same password other places, change it there, too. Don't forget to change your security questions, as well – especially if the answers include information that could be found in your Facebook account.

For more information about what to do after a data breach, visit IdentityTheft.gov/databreach and watch the FTC's video on What to Do After a Data Breach.

If you learn that someone has misused your personal information, go to IdentityTheft.gov to report identity theft and get a personal recovery plan. Because recovering from identity theft – and data breaches – is easier with a plan.