

YOUR MONEY

A Two-Step Plan to Stop Hackers

By Ron Lieber

Aug. 8, 2014

There are a number of ways that consumers could react to the news this week that Russian hackers got their hands on 1.2 billion username and password combinations.

We could pass it off as just another theft — one that has become public, among many others that we may never know about. If we haven't been hacked by now, maybe there's no need to worry, and our banks and brokerage firms are protecting us. Another possibility is to assume that the hackers are smarter than the banks, opt out of online access altogether and go back to using the phone or showing up in person for help.

But the developments pushed me in a third direction: To seek out all of the crucial accounts in my life, including every financial one, and try to add another level of security to the login process for each one. Sadly, not many of the companies involved were able to do it.

I was seeking to opt into something called multifactor authentication. There are three basic factors that a company can generally use to identify you. There's something that you *know*, like a username, password or the name of your school mascot. There's something that you *have*, like a code that you pull from an app, a text message or a SecurID plastic doodad that you have to carry around with you. The third factor is something that you *are*, which usually refers to biometric credentials like a fingerprint or an iris scan.

Companies have gone back and forth about whether to even allow their customers to sign up for that second factor and require the company to generate a one-time code to be entered in addition to a username and password. While such precautions add to the consumer's security, they can also increase the company's tech support needs.

But at this point on Planet Breach, you ought to be entitled to ask for the ability to make your logins more secure, beyond creating a different, airtight password for all of your most important accounts (which everyone should do). Here's what I learned as I tried to get a bit more protection.

HOW TO ASK Phone representatives don't always have the right answers to questions about adding a factor to a login. Websites may not have the relevant information either, which may mean both calling and burrowing five layers deep into company sites.

There is one excellent web resource where you can start, though: twofactorauth.org, which is a growing directory of companies that do and don't allow multifactor authentication. For companies that don't, you can push one button and send them a Twitter message urging them to adopt it, which I encourage you to do (please include me @ronlieber). A recent Iowa State University graduate named Josh Davis created the site earlier this year. He recently started working for Amazon, and his site says that just one of the three Amazon services he lists uses multifactor authentication.

RECOGNIZING YOUR MACHINE Upon login, many companies ask you if you want their site to remember your machine. If you say yes, this makes logging in easier, as you may not even need to enter your username again. But I'm with my friend Bob Sullivan, an author and consumer advocate, on the wisdom of saying no here, as he suggested in a blog post this week. He figures that anything he can do to force thieves to take an extra step or two might just cause them to give up and move on to an easier mark on their list of stolen credentials.

Some companies, like American Express and Vanguard, tell you to say yes and say that doing so adds to security. I discussed their arguments for doing so with them and didn't find them persuasive, especially the notion that having a site remember me will help keep me from accidentally ending up at a fake site, since I'd supposedly notice and remember that it hadn't asked for my username. However, Capital One notes quite plainly that "Selecting the 'Remember Me' feature on a computer or mobile device may put your personal information at risk," even on a machine that only you or your family members use.

UNIQUE CODES I'd hoped to be able to ask every company I do business with to simply send me a code by text message each time I successfully entered my username and password. It's a fairly simple arrangement (unless you're abroad, or somewhere else where receiving a text is a challenge), and I already do something similar with Gmail. But not one company was able to do this, though Vanguard intends to start a similar service before the end of the year. American Express has no such plans for its card customers for now. "We understand why some customers would want this, but it's not something we've heard overwhelmingly," said Amelia Woltering, a spokeswoman.

The best that Charles Schwab could offer was one of those plastic things that hangs on your key chain with numbers that continuously change. TD Ameritrade used to send those out but stopped two years ago. A low percentage of customers requested them, and of those who did, a low percentage actually used them.

The Wells Fargo customer representative I spoke to couldn't help me on this front either, though he took the opportunity to try to cross-sell me on a paid identity theft protection service. Good man! Later, after I logged in for the second time that day, the company's website wished me a happy birthday. It wasn't my birthday, which made me fear for a moment that I'd been hacked.

NOTHING FOOLPROOF The single best change I was able to make was at Vanguard's site, though it took some back-and-forth by both email and phone with a company spokeswoman to find the feature. Vanguard will allow people to declare

certain machines known and then instruct the site not to let any other person (including the account holder) using any other machine get past the initial login page.

I made that change, though it might be trickier to use a feature like that with an online banking site, where most people need more frequent (and occasionally emergency) access.

And there's the danger of leaning too hard on one piece of hardware. "What happens when that computer has an issue and is unavailable to you?" said Steve Adegbite, a Wells Fargo security executive, adding that we've all been in a spot where, say, a Windows upgrade causes our main machine to refuse to boot up at all.

Indeed, nothing is truly foolproof. If more companies adopt that Vanguard off switch, some hacker will find a way around it. People have already found ways around multifactor authentication. Bruce Schneier, chief technology officer of Co3 Systems, which helps companies respond to breaches, points to the existence of something called man-in-the-middle attacks. There, someone intercepts your one-time use code and then turns around and uses it at a bank's site in combination with other stolen credentials.

Panic is not necessary, though. The hackers or people who buy your data from them need to go through many steps before they can harm you. First, they have to acquire your login credentials successfully. Then they have to decide to use them; they don't always use all of the data they have. Finally, they have to be successful in gaining access to your accounts; perhaps you change your credentials regularly for crucial accounts. Then they need to successfully steal once they have access, but banks and brokerage firms have all sorts of security measures that kick in after a login to keep money transfers from going to the wrong place. Some thieves may also use stolen credentials for spam only.

Still, in a world where so many usernames and passwords are floating around in the hacker ether, it probably won't hurt to demand and then use every reasonable bit of protection available. Having a security freeze on all three credit files with the

credit bureaus, for example, makes it very hard for people to open new credit accounts in your name. Those of us who take such precautions and change our most important passwords often stand a good chance of making life harder for all but the most determined hackers.

Twitter: @ronlieber

Make the most of your money. Every Monday get articles about retirement, saving for college, investing, new online financial services and much more. Sign up for the Your Money newsletter [here](#).

A version of this article appears in print on , Section B, Page 1 of the New York edition with the headline: A Two-Step Plan to Stop Hackers