**The Economist explainsWhere are the flaws in two-factor authentication?**

One of the main tools for keeping hackers at bay offers no guarantee of security



### [The Economist explains](https://www.economist.com/blogs/economist-explains)

Sep 13th 2017

by G.F. | SEATTLE

TWO-FACTOR authentication (2FA) is becoming ever more popular as companies deal with growing concerns over cyber-insecurity. With 2FA, account-holders validate their identity online by entering a password and then adding a countersign that is generated by something to which they have physical access. This “second factor” is not fool-proof, though. DeRay Mckesson, an activist with Black Lives Matter, had his 2FA-protected Twitter account hacked last year. Banking customers in Germany had their 2FA accounts hijacked in May. And in August a bitcoin entrepreneur had the equivalent of $150,000 drained from his virtual wallet. How did a second factor fail them?

Security factors can be something you know (a password), something you own (a phone or a smart dongle) or something you are (like a fingerprint). The idea is that whereas a ne’er-do-well might crack your password, that action is futile without access to a piece of hardware you keep close, or a piece of your body. The test often takes the form of a text message (SMS) sent to a mobile phone. Many modern phones are unlocked by fingerprint, which ostensibly adds a biometric layer of protection on top. In theory, these second factors deflect attempts to crack accounts made by thieves, governments and jilted partners, while also defusing mass breaches of online accounts. Without a second factor, passwords are just so much dross. But even with them, accounts continue to be cracked.

The flaw lies largely with the weakest link: the phone system and the humans who run it. Mr Mckesson and the bitcoin victim, for example, suffered at the hands of attackers who fooled phone-company employees into re-routing the victim’s phone number to a device in the attacker’s possession. Such a move should require either private, personal details or the customer’s PIN. But even if a customer-service rep ignores the scammer’s entreaties, the scammer will just try calling again, to another rep, and may eventually succeed. Another flaw, used in the German attack, is found in a system known as Signaling System 7 (SS7), which routes calls on networks worldwide and dates back to 1975. Vulnerabilities abound, and though mobile operators claim to be monitoring for abuses, access to an SS7 system allows hackers to intercept voice calls and SMS messages.

The move away from SMS has been under way for some time. Many websites offer a time-based, one-time password system, popularized by Google. With this, account-holders log in using a password. The website then generates an access code unique to the account and displays it as a 2D code (a square full of dots), which can be scanned into an app like Google Authenticator. The app then spits out a new code, valid for a very short time, which is used to complete the account login. For each subsequent login, the user must return to the app for a new access code. Apple's current 2FA system, which replaced a weaker version two years ago, sends an alert to all of a user's registered Apple devices when a new login is in progress. It then issues a code that must be entered in order to complete the login. And the Fast Identity Online Alliance, a group with broad support across the industry, developed a public-key cryptographic token system called Universal Second Factor that uses a USB dongle to prove a user’s identity to a site and also to prove a site’s identity to a user. However, nearly all accounts that offer these superior 2FA options also use text-messaging as a required backup, undermining their efficacy. Many security experts would like to see SMS removed from the system entirely, or to let advanced users disable it. But some warn that SMS is better than nothing, for users who cannot navigate more complicated systems. Giving up on SMS could cause users to revert to password-only logins. The proper solution, yet to appear, is some second factor that would be as easy to find as a text message and as persistent as the possession of a smartphone.

Source: <https://www.economist.com/blogs/economist-explains/2017/09/economist-explains-9>