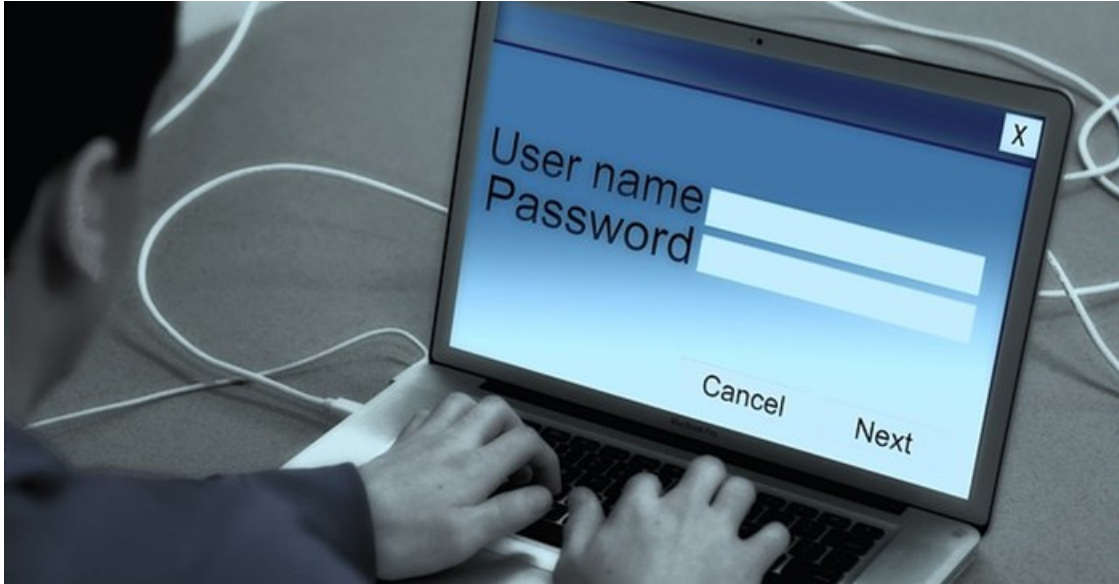


Mobile ID can make passwords obsolete

Our phones are always on hand and our mobile numbers are unique, so could mobile provide a secure alternative to the password? Vice president of mobile security at Gemalto, Jean-Francois Ouillet outlines the potential of mobile ID.



geralt via pixabay.com

How many passwords do you have? Are they complicated enough to resist a hacker attack? Can you remember them all?

Two-factor authentication

In a world where portable devices can connect to millions of sites and apps, passwords are just not up to the job. Our research found people have an average of 25 usernames and password combinations each. We need a trusted and simple way to bypass this unsatisfactory system. Such a solution does exist. It's called Mobile ID.

Here's how it works: when you want to log in to a website, you select 'log with Mobile ID' and type your mobile number. Your phone instantly displays a pop-up screen asking you to enter your Mobile ID personal code in order to connect to that website. That's it: just a few seconds to log in.

Mobile ID is secure because it identifies you not only by what you know (your Mobile ID personal code), but also by what you have (your phone). In other words: Two-factor authentication. This makes it virtually impossible for any criminal to pretend to be you. It's a great way to move us away from using insecure passwords. Of course, it's not the only form of login available. There's also Facebook and Twitter. But there's no guarantee their processes are secure, end to end. They still depend on login/password combinations.

One sign-in to rule them all

Another advantage of Mobile ID is its ubiquity (or its potential to be). In 2014, the telco trade body, the GSMA, created Mobile Connect to unify all MNOs behind one Mobile ID standard. Dozens of operators have pledged to support it. In time, this could make Mobile Connect a universal way to sign in. You don't need a username and password to make a phone call, you just click on the green button. In the digital world, you need a username and password for every service you access. This is a problem and it's something that the mobile operators have the assets to resolve, whether it's through the SIM or mechanisms like USSD.

Building the backbone

MNOs can't do this alone. They need partners to furnish service providers with one connection to all telcos. This is where Gemalto comes in. We helped the GSMA draft the specs for Mobile Connect and we already manage live Mobile ID services in individual countries. In time, these services will sync to Mobile Connect.

In Norway, for example, hundreds of thousands of bank customers use BankID to sign in to services. Traditionally, they would use a PIN Pad, which they would often forget to take with them. Now they sign in securely with mobiles instead: the BankID is stored on the SIM card. Participating banks include DnB, Skandiabanken, Eika, Nordea and Sparebank1. Overall, Gemalto connects more than 500 service providers to Mobile ID worldwide.

Another great benefit of Mobile ID is flexibility. People can use basic security for simple access to sites. But when payment is involved, they can use stronger authentication. Mobile ID can even go as far as providing users with a legally binding digital signature, thanks to an enhanced technology of the kind currently used in Finland. But no matter the level of security behind the scenes, the essential user experience will always remain the same.

Speedier form filling

Mobile ID is not only used for signing in securely. It could also speed up form-filling. In this scenario, a user would store personal data with the mobile operator. Then, when faced with a complex registration form, he or she could log in with Mobile ID and grant permission to fill in the missing details. This would be excellent for eGovernment services, such as applying for a passport.

For more, visit: <https://www.bizcommunity.com>