Time to dump passwords for good?

Diggers, 2014-15-12

The more news we get about this latest Sony hack, the more depressing it seems to get. Among the latest revelations, it was revealed that the entertainment giant was keeping passwords to internal systems as well as social network accounts in plain text. Not only that, but they were kept in a folder called 'password.'

Here's how Buzzfeed described it: "Included in the newest data dump is a file directory titled "Password," which includes 139 Word documents, Excel spreadsheets, zip files, and PDFs containing thousands of passwords to Sony Pictures' internal computers, social media accounts, and web services accounts. Most of the files are plainly labeled with titles like 'password list.xls' or 'YouTube login passwords.xlsx.'"

For anyone with a passing interest in security, which really should be all of us, that is a pretty shocking thing to read. Basic security advice is to try to avoid writing passwords down, and particularly to avoid keeping them somewhere so easily identifiable. Avoiding easy to guess words, such as anything from the dictionary, is also good advice, as is never repeating passwords; make sure each one is unique to that service.

But while passwords remain the primary way to access so many services, all of that is easier said than done. And so maybe that is what needs to change. Maybe it's time to get rid of passwords for good. Are they fit for purpose these days? Many would argue they are not. They can be hacked, they can be guessed, they can be forgotten.

For those still wedded to passwords, using a password manager can help, as can using two factor authentication where it's available.

But the industry is beginning to offer alternatives to passwords. The launch of Apple's TouchID has brought fingerprint recognition technology to a wider audience. And as we know, where Apple leads the rest of the industry tends to follow: Samsung and HTC have both released devices with fingerprint scanners.

Biometrics such as TouchID or eye scanners are a good alternative and the technology is becoming more convenient and easier to use (which is key for widespread adoption). Someone looking over your shoulder can copy your password; they cannot copy your fingerprint.

At the moment Apple's TouchID can be used to unlock iPhones and iPads and make purchases from Apple's online stores such as the AppStore and iTunes as well as its Apple Pay NFC technology. But it's conceivable that one day biometrics may replace passwords completely, across many different services.

It's not just mobile apps that could benefit from biometrics. Imagine accessing work emails - or any other work-related application - on your home PC and, instead of entering a password on your computer, you authenticate yourself via a fingerprint reader on your mobile device that is connected to your office back-end systems.

But those days are not here just yet, so maybe it isn't time to dump passwords. As well as following the advice above, it is wise to make sure passwords are just one layer in the security infrastructure.

This involves adding more context to security. Instead of just using a password for authentication, businesses can look at the device being used and its location, what the user is attempting to access and other details to give a clearer picture of the authentication request. Context in security is something we've talked about recently, in fact.

So it seems to me that we are moving beyond passwords as the primary method of authentication. But they will be around for a while yet; at least until the alternatives become more convenient. Until the industry does standardise on a replacement, it is wise to ensure that passwords are just one layer of your security infrastructure.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.	F5 Networks	F5 Networks Ltd.	F5 Networks
Corporate Headquarters	Asia-Pacific	Europe/Middle-East/Africa	Japan K.K.
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	f5j-info@f5.com