**Why should I use two-factor authentication (2FA)?**

Imagine waking up on a fantastic morning, unlocking your phone or laptop only to realize that you have lost access to your online accounts. Someone has breached your email, your social networking account, your website, and your bank credit/debit card was used for suspicious transactions. The damage can be irreparable. The very thought of this situation can make anyone go a little bit paranoid about his online security. So this article gives you the solution to avoid the unfortunate situation and also tells why you should use it.

**Two-factor authentication (2FA) to the rescue**

**Two-factor authentication** (2FA), also known as dual-factor authentication or two-step verification, is an online security procedure where the user verifies themselves by providing two distinct authentication factors to secure better their user's credentials as well as the resources they have access to. **Two-factor authentication** adds an extra layer of security to the process of authentication. This additional layer is used to make sure the person trying to access an online account is who he says he is. Along with a username and password to an account (which constitutes single-factor authentication or SFA), another piece of information is required to log into the account. This additional information or factor is time-sensitive. Due to this, it becomes harder for an attacker to access a person's online account or device. Thus 2FA assures a high level of security. This is the reason that online service providers are using **two-factor authentication** successfully in protecting sensitive databases and systems.

The second factor we are referring here can be anyone of the following:

* Something you know: Also known as knowledge factor, this could be a PIN, an answer to a secret question, a password etc.
* Something you have: Also known as possession factor, this could be something a user would have in their possession, like a credit/debit card, a key fob, a smart card, a smartphone, an ID card etc.
* Something you are: Also known as inherence factor or biometric factor, this could include the input of a fingerprint, an iris scan, a voice or facial recognition. It also includes [behavioural biometrics](https://whatis.techtarget.com/definition/behavioral-biometrics), such as [keystroke dynamics](https://searchsecurity.techtarget.com/definition/keystroke-dynamics), speech patterns etc.
* Time factor: User authentication is restricted to a specific time window. Access to the system is limited outside of this time window.

Best of all, since [app-based **two-factor authentication** solutions](https://www.twilio.com/authy/features/totp) are available for mobile, wearables, or desktop platforms —user authentication is possible just about everywhere.

Currently, knowledge factors such as a password, whereas **the two-factor authentication** way adds either an inherence factor or a possession factor are relied upon. With two-factor authentication, if one of these chosen factors is missing the account cannot be accessed. So, chances of someone breaching into your online account, even if he has a password of it, are highly unlikely.

**Why should you switch to two-factor authentication?**

We opt to do everything on a laptop or smartphone, which makes it more evident that our digital accounts are always under the threat of attackers or hackers. Malicious cybercrimes against companies, governments and individuals have become more common. And such crimes are on the rise with no signs of slowing down, be it the hacks, data breaches, and other forms of cybercrime.

Even if it is durable and unique, it is still possible for hackers to steal or trick you into giving away your password. Using the second layer security key is the best and most secure way to make stealing impossible. This simply means adding just one step more to your logging in the process to protect your most sensitive accounts such as email or banking accounts. This one step can be as simple as an SMS code or a fingerprint pattern.

**What do people say about two-factor authentication?**

In a recent study conducted by the Johns Hopkins University and the University of Maryland, it was found that around 28% of people have never used **two-factor authentication** on their devices. Most of them said the inconvenience associated with using it as a reason for not opting in. While some stated that they did not have positive experiences with it in the past, others few said that in the security measure had no value to them. It was concluded in the study that it was the lack of information which was the root cause of this resistance in adoption. 64% of survey respondents had never used 2FA as agreed by them because they have never been prompted to use it or had never heard of it.

**Just ‘username and password’ not good option to authenticate**

Usernames and passwords are the most common way of user authentication. Using a password that is unique, strong and something only you know is the general rule of thumb which makes it difficult for someone to guess and use. But still, passwords are not foolproof no matter how strong are they. Here's why:

* A standard set: a recent report looked over 1.4 billion stolen passwords at, and it was found that most were simple. "111111," "123456," "123456789," "password" and "qwerty" were among the most commonly used. These are simple and easy to remember, and any decent attacker could crack these in no time.
* Too many accounts: With more digitalization, users are into creating more and more online accounts on different websites. Since it is difficult to remember so many passwords, password recycling becomes familiar with a growing number of accounts. It is easy for hacking software to test several stolen login username and passwords against a bank or shopping site. Hence other considerations are also at risk if a username and password pair is recycled.
* Security fatigue: Creating easy to crack passwords across multiple accounts.

Problem with 'username-password' authentication method is it requires to be remembered, and diligence is required to strong passwords. Passwords require security from several insider threats such as storing sticky notes with user login credentials carelessly, old hard drives etc. Passwords are exposed to external threats too. Hackers use brute-force, [rainbow table](https://whatis.techtarget.com/definition/rainbow-table) hacking attack etc.

With enough resources and time, a hacker can usually break into password-based online security systems. Though passwords remain popular because they are cheap and easy to implement, the rise in cybercrime has time to time encouraged to move to more sophisticated ways of verification and authentication.

**A rise in cyber-crime**

In recent years, it has been witnessed that there has been a massive rise in the number of service providers losing personal and sensitive data of their users. Cybercrime has become more sophisticated, modern threats and attacks are way ahead of the old security systems of the companies. Not only user trust is at stake, but organizations can suffer severe financial loss and reputation loss.

For consumers, targeted hack or identity theft can do them irreparable damage. A victim's credit rating can be affected due to stolen credit/debit card credentials. According to a recent study, in 2016, over $16 billion were stolen from 15.4 million U.S. consumers.

This clearly states that consumers must protect themselves with something stronger than just a password on these online websites. And thus, that extra level of protection is two-factor authentication.

### Mobile device authentication using two-factor authentication

Smartphones offer several various possibilities for **two-factor authentication**. This allows companies to utilize what is best. These devices are capable of fingerprint recognition; an installed camera is capable of acceptance of face or iris of user and voice recognition can be done using the microphone. [GPS](https://searchmobilecomputing.techtarget.com/definition/Global-Positioning-System) in smartphones can verify location which can be used as an additional factor.

Apple iOS, Windows 10, BlackBerry OS-10 and Google Android, all have applications that support **two-factor authentication**, which allows the phone to serve as the authenticating possession factor. Duo Security, purchased by Cisco for $2.35 billion in 2018, is a platform **two-factor authentication** vendor whose product customers can use with their trusted devices for **two-factor authentication**.

To access a web-based service or website which supports [Google Authenticator](https://searchsecurity.techtarget.com/definition/Google-Authenticator), takes the user's username, its password along with knowledge factor. The user is then prompted to enter a six-digit number. Authenticator automatically generates the number for authentication. These numbers are time-sensitive and are distinct for every login.

**How much secure is two-factor authentication?**

There is no denying that **two-factor authentication** improves security since the access to an account does not just depend on username and password strength. But the security of two-factor authentication mechanisms relies on the protection of their weakest component. To give an example, the security of the manufacturer or issuer decides the hardware tokens security. One such instance can be traced to 2011 when [RSA Security](https://whatis.techtarget.com/definition/RSA-Security)'s SecurID authentication tokens were reportedly hacked. Also, due to their size, the user often finds them vulnerable to get misplaced or lost.

The process of account-recovery when used to reset a user's current emails and password can be exposed to threat when the temporary password is allowed to the user to log again in. This process by-passes **two-factor authentication**. Such case occurred when the Gmail accounts of Cloudflare’s chief executive were hacked.

SMS-based **two-factor authentication** is vulnerable to a number of attacks, although being cheap, user-friendly and easy to implement. One-time passwords or OTP sent via text message/SMS are exposed to threats due to mobile number portability against the mobile phone network and malware such as Eurograbber which can be used to intercept or redirect SMS messages.

**How much difficult is it to use?**

**Two-step authentication** definitely adds an additional step to your process to access an online account, but the ease of its usage depends upon on how the service provider, such as Twitter, has implemented it. It can be a minor inconvenience or a significant pain. It also depends on one's patience and willingness to put extra time to ensure a higher degree of security. The process may seem to be more complicated, but it definitely saves you from the damage that can be done later.

**Conclusion**

According to a recent report, stolen, reused, and weak passwords remain a [leading cause of security breaches](http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/). Unfortunately, passwords are still the main (or only) way many companies protect their users. The good news is that cybercrime is in the news so much that 2FA awareness is quickly growing and users are demanding that the companies they do business with have improved security. We agree: “[Everybody Should Use](https://www.youtube.com/watch?time_continue=4&v=ds_TANz4n3U) **Two-Factor Authentication**."