# Authenticate what two factors are and why you should use it

Two-factor authentication (2FA) is a security method that requires two different ways to prove your identity. It is often used in everyday life.

Two-factor authentication (2FA) is a security method that requires two different ways to prove your identity. It is often used in everyday life. For example, credit card payments not only require a card but also a PIN, signature or ID. With the validation of a 1FA element becoming increasingly unreliable, two-factor authentication quickly achieved the importance of a security measure to log into online accounts.

By default, almost all online accounts use password authentication, ie one-factor authentication. But the password is very vulnerable to attack. Another problem is that many users still use one and the same password for all their accounts. Although there is a bit of trouble, 2FA significantly increases security by requiring an additional authentication element, thus making it difficult to hack an account.

## What are the two-factor authentication (2FA) exactly?

As mentioned in the introduction, 2FA is a 2-layer login method. Two authentication factors can be one of the following:

1. What you know, usually a password or an answer to a security question
2. What you have, for example, a security code sent to your mobile phone or an ATM card
3. Biometric data, such as your fingerprint

A daily example in which 2FA is used is to withdraw money from an ATM (card + PIN), pay with a credit card (card + signature OR card + PIN code or card + security code) or enter at foreign (passport + biometric data).

## Why should you use two-factor authentication?

Imagine someone breaking into your email account. What kind of information will they access?

Here are a few things that can be exploited from email accounts: user names of accounts, other passwords, personal data, personal photos, scanned documents, information about friends, family and other contacts, credit card numbers, bank account numbers, insurance numbers . and more.

1. Turn on 2-step verification for 2-layer security for Gmail, send the verification code to your phone when signing in
2. How to block Facebook account search via email

Can this information help them break into some of your other accounts, such as Facebook? And how many places have you logged in with Facebook or other social networking accounts?

1. Protect your Facebook account with 2-factor authentication


When thinking about this, you will find that most of your online accounts are linked together. Hacking one of these accounts can help intruders access some of your other accounts. In other words, if someone tries to hack into one of your main accounts, your identity has been stolen in practice and the potential consequences of this

are extremely large.

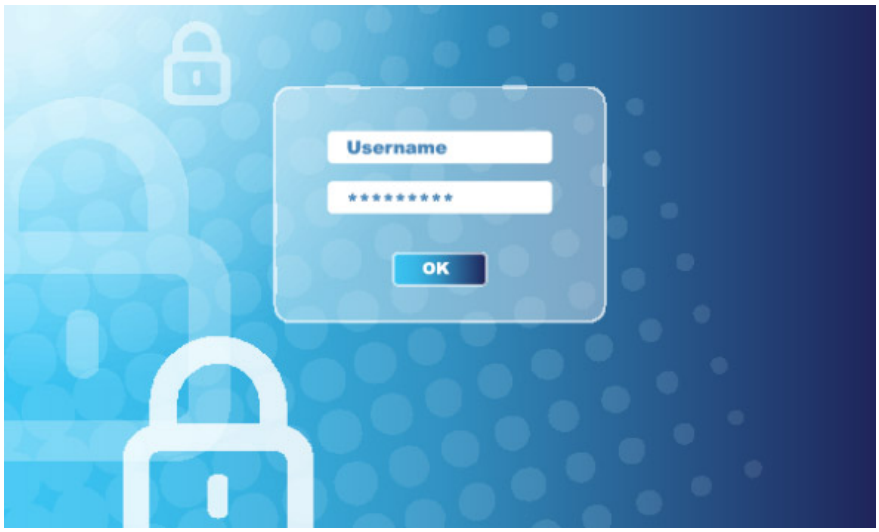
## Where should you use two-layer authentication?

Ideally, you should use 2FA for all accounts that you store any kind of personal information, as well as accounts with payment information associated with them. This includes, but is not limited to:

1. Email accounts
2. Facebook and similar social media accounts
3. Online banking
4. Online payment account
5. Online shopping account
6. Any kind of cloud storage service
7. Online gaming account

Unfortunately, not all online accounts or services provide 2FA or provide it explicitly. Usually, you have to search the web for additional security options.

The two main online services offer 2FA and you should definitely activate this service as Facebook (login approval) and Google (2-step verification).




2FA is an indispensable security measure for your main online accounts, such as email, bank or social network. Although two-factor authentication doesn't mean your account is immune to attacks. It only makes your account more flexible when hackers want to crack more than a simple password. Whether or not a second authentication element depends on the account and the type of information stored in it.

See more:

1. Activate 2-layer verification to secure your Apple ID account
2. How to secure Linux Ubuntu with two-factor authentication
3. More than 90% of Gmail users still don't use the two-factor authentication feature