TECH CORNER

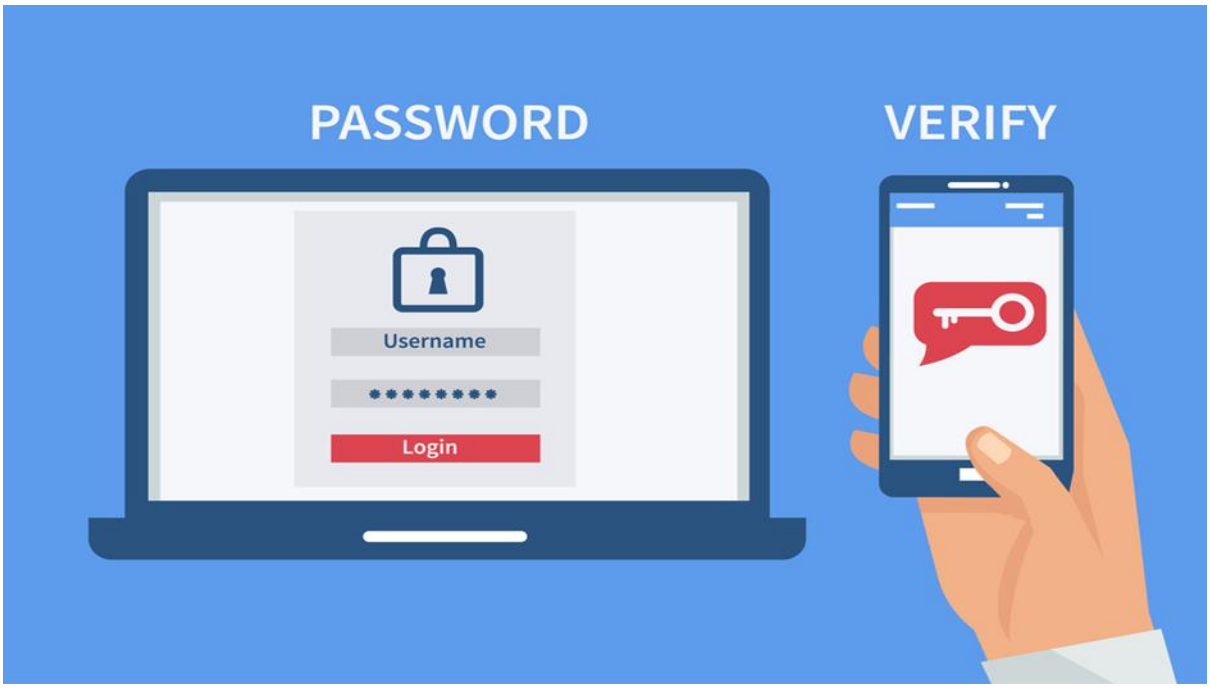
Dear Member

Two-factor authentication (2FA) helps to stop hackers from getting into your accounts, even if they have your password.

Hackers and cybercriminals often send fraudulent emails through phishing attacks, develop fraudulent websites and perform many other kinds of social engineering to steal a person's username and password. Without additional authentication methods, those basic credentials could grant criminals easy access to highly sensitive information.

The goal of two-factor authentication is to make information and accounts more secure by restricting access unless the administrator's security criteria have been met. This can help prevent stolen laptops from being used to steal information and prevent bank accounts from being accessed with a stolen card.

Some online banking uses 2FA automatically. It does this by asking for more information to prove your identity.



What is 2FA?

Two-factor authentication (2FA) is the requirement of additional verification beyond a username and password. Common examples of 2FA verification include security questions, SMS (short messaging service) messages, and push notifications.

Examples of two-factor authentication

These are a few examples of two-factor authentication commonly used to secure accounts on websites, applications and networks:

SMS text: SMS texts are sent to a mobile device associated with an account when the account is accessed from a new location or device, or when individuals request to reset their passwords. The individual receives a code they must enter online to reset their password.

Security questions: Users might be asked to set and answer security questions when initially setting up an account. They are typically personal questions only the individual can answer. Some may be easier to guess than others, but examples include their mother's maiden name, the street they grew up on or the first car they owned.

FaceID/Face Unlock: FaceID is used to log into Apple iOS devices, Face Unlock is the Android equivalent. The biometric factor is completed through a facial scan. If the facial scan fails to verify an individual's identity, the device will require a passcode of some kind to verify the user.

How does 2FA work?

The components of 2FA are typically categorised into five factors of authentication: knowledge, possession, inherence, location and time.

Knowledge: Knowledge factors refer to information an individual knows. They are most commonly demonstrated in the form of a username and password. With this single factor of authentication, the user knows their access ID and the passcode associated with their account.

Possession: Possession factors refer to something physical that an individual has with them. This can be in the form of a device that generates security tokens, a smartphone, or a banking card. Most of the time, possession factors are used as a complement to knowledge factors, rather than granting access directly.

Inherent: An inherent factor is something you are as an individual. Inherent factors are typically evaluated through a form of biometric authentication such as a fingerprint, face scan, or voice recognition.

Location: Location factors are becoming more commonly used in multi-factor authentication solutions. They are used to identify individuals hoping to access sensitive information from a new or unusual physical location. For example, if someone tries to log into an account from another country when they are typically in their home country, systems may prompt additional authentication requirements.

Time: Much like location factors, time factors consider the time of day an individual is requesting access. If someone always logs in at 9.00am but attempts to access an account at 11.00pm or 2.00am, additional authentication methods may be prompted.

How to turn on two-factor authentication (2FA)

You will need to manually turn on 2FA for most of your accounts. Not all accounts will offer 2FA. Most online banking uses 2FA automatically.

2FA is also known as two-step verification or multi-factor authentication.

Click the relevant link below.

Turn on 2FA for email

- Gmail (opens in a new tab and log in to account required)
- Yahoo (opens in a new tab)
- Outlook (opens in a new tab)
- AOL (opens in a new tab)

Turn on 2FA for social media

- Instagram (opens in a new tab)
- Facebook (opens in a new tab)
- Twitter (opens in a new tab)
- LinkedIn (opens in a new tab)

Kind regards

Nicholas Spike
Assistant Secretary