How can Two-Factor Authentication help you increase cybersecurity?

By Elina Toufexi – Business Development Officer

In the recent years, cyber-attacks against government, companies and individuals have rapidly increased. Currently, since more and more individuals are now online due to the coronavirus pandemic, cybercriminals took this advantage to breach sensitive information. Cyber criminals manage to do so by carrying out phishing campaigns, spread malware especially with remote working, ransomware and malicious domains that infect and endanger corporates' networks.

According to Cisco's research, "at least 75% of all domains with 'COVID' or 'Corona' are malicious". Hence, the global events have demonstrated the urgent need to combat these cyberattacks.

So as to protect user accounts in your business, it is highly recommended to use multi-factor authentication. IBSCY's IT experts can enable 2FA to your emails, file access or any other application or data that is important for you. Two-factor authentication, will safeguard your work and your data and you will be able to continue your operations problem-free.

What is a two-factor authentication?

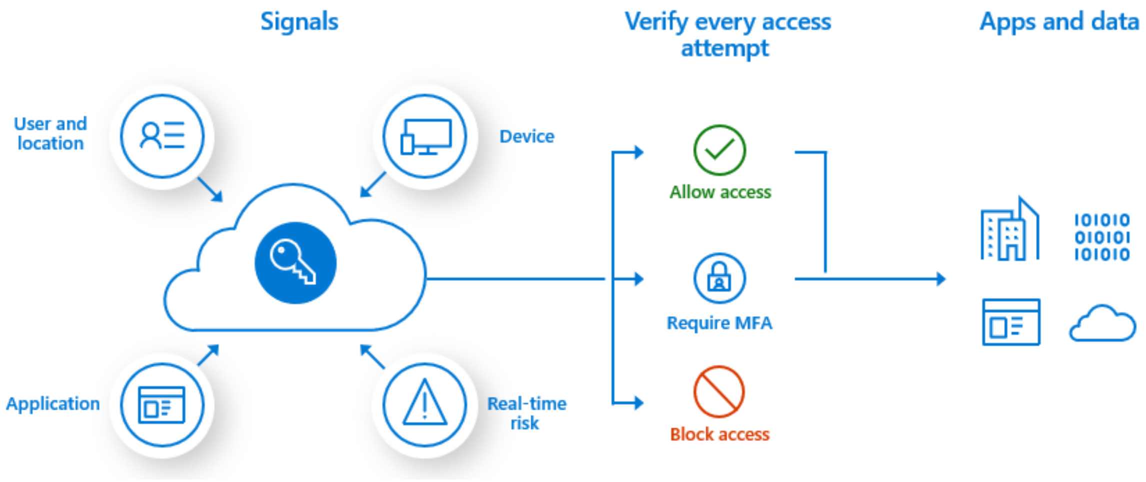
Two-factor authentication is an extra layer of security for your corporate account (i.e. Microsoft, Apple, Fortinet, Synology and more) intended to ensure that you are the only person who can access your account, even if someone finds your password. It uses two different forms of identity: a password, and a contact method (a.k.a. security information, SMS, email or a fingerprint).

How does it work?

Firstly, a user will sign-in into their account normally by entering their username and a password. Then, instead of instantly gaining access, they will be required to provide another piece of information. 2FA works by requiring two or more of the following authentication methods:

- Something you know - typically a password/code received as SMS or generated from a mobile app.
- Something you have - a trusted device that is not easily duplicated, like a cell phone.
- Something you are - biometrics like a fingerprint or face scan.

A security code will be sent to your email, phone or authenticator app every time you sign-in on a device that isn't trusted. To better understand the concept of dual-factor authentication, see the picture below.



Why do you need it?

Two-Factor Authentication helps safeguard access to data and applications while maintaining simplicity for users. When you require a second form of authentication, security is increased as this additional factor isn't something easy (almost impossible) for an attacker to obtain or duplicate.

Two-Factor Authentication Features include:

- ✓ Protects every point of access, from on-premises, to web-based, to cloud-based applications
- ✓ Safeguard access by mobile apps, phone calls and SMS
- ✓ Receive real-time fraud alerts and 2FA reports
- ✓ Increase cybersecurity