THE BENEFITS OF TWO-FACTOR-AUTHENTIACTION (2FA)

Two Factor Authentication (2FA) is an extra layer of security used when logging into websites or apps, also known as two-step verification, and is an additional security measure that can be used to protect your account.

A form of authentication could be:

- **Something you know, e.g** personal identification number (PIN), a password, etc.
- **Something you have, e.g** credit card, a smartphone, or a small hardware token.
- **Something you are, e.g** biometric pattern of a fingerprint, an iris scan, or a voice print.

2FA is the usage of a combination of any of these 2 forms of authentication. 2FA protects your accounts and ensures that if the passwords are compromised, there is a reduced chance of the account being hijacked by an attacker.

Common 2FA types include:

- Hardware tokens that produce a numeric code that change every 30 seconds.
- SMS or Email message containing a One Time Password (OTP) that the user must enter after putting in the correct username and password.
- A push notification sent to the user on a login attempt asking the user to accept or deny access to their account

Two Factor Authentication is available on most of the social media platforms and websites we use on the internet. It is of great importance to use strong password and also enable these settings to better protect your accounts.