

Two factor authentication

Two factor authentication (2FA) is a security process in which users provide two forms of authentication to verify their identity. The first form is typically a password or PIN, and the second form is a one-time code generated by a mobile app or hardware device. This process significantly reduces the risk of unauthorized access to accounts, even if the password is compromised. 2FA is supported by many major services and is highly recommended for protecting sensitive information.

1. Two factor authentication can be enabled in Settings > Security and Logon > Two factor authentication. Once enabled, you will receive a QR code to scan with your mobile device. After scanning, you will receive a one-time code that you must enter along with your password to log in.

2. You can also enable 2FA by scanning the QR code with your mobile device. Once scanned, you will receive a one-time code that you must enter along with your password to log in.

3. You can also enable 2FA by scanning the QR code with your mobile device.

4. You can also enable 2FA by scanning the QR code with your mobile device. Once scanned, you will receive a one-time code that you must enter along with your password to log in. The one-time code is valid for a short period of time, typically 30 seconds. After the code expires, you will need to scan the QR code again to receive a new code.

5. You can also enable 2FA by scanning the QR code with your mobile device. Once scanned, you will receive a one-time code that you must enter along with your password to log in.

6. You can also enable 2FA by scanning the QR code with your mobile device. Once scanned, you will receive a one-time code that you must enter along with your password to log in. The one-time code is valid for a short period of time, typically 30 seconds. After the code expires, you will need to scan the QR code again to receive a new code.

□□□□

□. Settings □ □□□ Security and Logon-□ WHERE YOU'RE LOGGED ON
□□□□□ □□□□□□ □□□□ □□□□□ □□□□ □□□□ □□□□ □□□□ □□□□ □□□□
□□□□ □□□□ □□□□□ □□□ □□□□□ □□□ □□□□□□□□□□ □□□□□ □□□□□

□. □□□□□ Settings □ □□□□ Security and Logon-□ SETTING UP EXTRA
SECURITY □□ □/□ □□ □□□□□□□□□□ contact □□□□ □□□□□

□. □□ □□□□ □□□□ □□□□ □□□□□□□□ □□□□□□ □□□□□ □□□□□□□□□□
□□□ □□□□□ □□□ □□□□ □□□□□□ □□□□□ □□□□□ □□□□□ □□ □□□□□□□□□□
□□□□□□□□□□ □□□□ □□□□□ □□□□ □□□□□ Yahoo □□□□ □□□□ □□□□□□□□□□
□□□□ □□□□□ □□□□□ Yahoo □□□□□□ □□□□□□□□ □□□□ Gmail □□ □□□□
□□□□□□ □□□□ □□□□□□ □□□□□ Yahoo □□□□□□ □□□□□□ □□□□□ □□□□□□□□□□
□□□□□ □□□□ Yahoo-□□ □□□□ □□□□□□□□□□

□□. □□□□□□□□ □□□□□□ □□□□ □□□□□□ □□□□□□□□□□ □ □□□□□ □□□□□□□□
□□□□□□□□□□□□□□ □□ □□□□□ □□□□□□□□□□ □□□□□ □□ □□□□□- Cyber
Security & Crime Division, CTTC, DMP.