User accounts and systems are further protected by the security technique known as two-factor authentication (2FA). Making it significantly more difficult for attackers to get unauthorized access, 2FA requires the user to provide two separate forms of identity before giving access.

Something the person has and something they know are the two factors that are generally employed in 2FA. A mobile phone, for instance, may serve as the second factor and a password as the first. The second factor, which can be a code produced by a mobile app, text message, or email, will be requested from the user when they enter their password to log in.

By requesting two different factors, the security of the account is significantly increased because an attacker would need to know both the user's password and the second factor in order to get access. Even if an attacker has succeeded to steal the user's password via techniques like phishing or brute force attacks, it will now be considerably harder for them to access user accounts or systems.

Overall, 2FA is a quick and easy technique to increase the security of online accounts and systems, and it is being used as a standard security procedure in many businesses. Today, many well-known online services, including Google, Facebook, and Amazon, give their consumers the option of 2FA. The usage of 2FA is also required by many sectors, including finance and healthcare, as a security measure for their online systems and apps.

“Microsoft.” *Microsoft Support*, https://support.microsoft.com/en-us/account-billing/how-to-use-two-step-verification-with-your-microsoft-account-c7910146-672f-01e9-50a0-93b4585e7eb4.