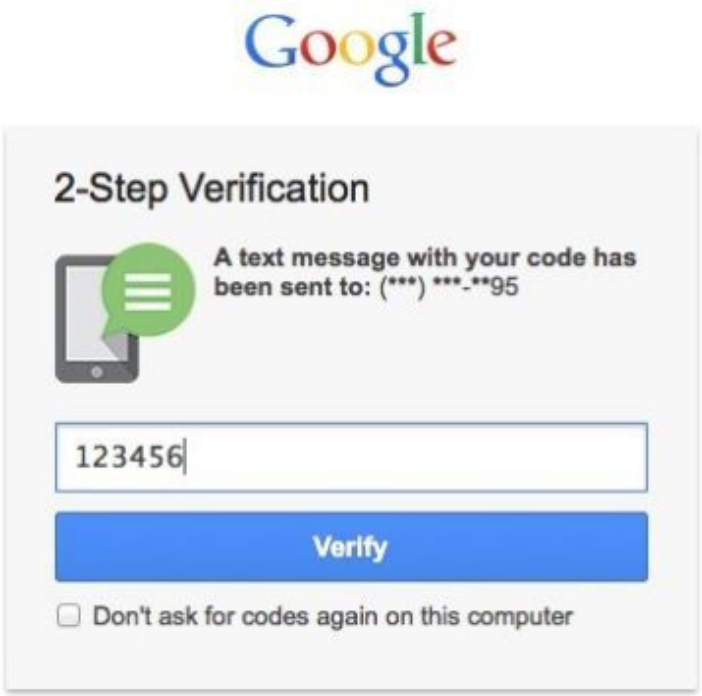
Two Factor Authentication (Simply) Explained

For many of us, a personal nightmare scenario begins with the wrong people getting hold of login credentials to our banking, email, retirement savings, or any other critical account. If you have been following the news, you know that passwords are hacked or stolen by the millions. What if there was a technology that would ensure that you are the only one who can log in to your account, even if an unauthorized person knows your password? One of the scariest things about technology is security, more specifically, the potential breach of security. Data breaches happen daily, but it doesn't have to happen to you. According to Verizon's 2016 DBIR report, 63% of confirmed data breaches involved weak, default or stolen passwords. Two Factor Authentication, also known as 2FA, is a way to add an extra layer of protection to your accounts.

Simply put, 2FA works by utilizing a combination of two factors such as:

- Something you know, such as a password, PIN number or pattern.
- Something you have, such as an ATM card, fob or phone.
- Something you are, such as a biometric feature like retina, iris, gait, voice print or fingerprint.



For example, if you have enabled Two Factor Authentication on your Google account, your account will work a little differently than before. With 2FA you will enter your password as

before, but there will be a second step before you get access into your account. You will be asked for a code that can be sent to you either via text message, mobile app or a voice call. This second step is what provides you with the extra layer of security.

Chances are that you are already using 2FA. When you enter your zip code at the gas station as you use your credit card to fill up your car, you are using Two Factor Authentication. When you enter your PIN at the ATM, you are using 2FA.

What are the critical elements of 2FA?

Knowledge Factor

Knowledge factor is a category of authentication credentials such as pin numbers, passcodes or patterns. The user provides the knowledge factor during the authentication process by either entering a password, a username, the answer to a secret question or a PIN number. Knowledge factors, when implemented alone, offer little security. The password-only authentication is no longer a sufficient method to keep your online accounts and data safe. Passwords are easily compromised or hacked. Therefore, it is better to move to the next level of security, Two Factor Authentication.

Possession Factor

The possession factor is the foundation of 2FA. The possession factor has to do with something that a user has such as a USB token, ATM card, hard token, smart card or mobile phone.

Inherence Factor

Inherence factors are unique to the user. They normally take the form of a biometric characteristic such as fingerprint, iris, retina, voice print, etc. Biometric authentication is commonplace in smartphones, laptops, healthcare, police, voter registration and security access points.

What are the benefits of 2FA?

- Extra layer or security. While there is no such thing as complete security, 2FA offers a simple way to improve security exponentially.
- No additional hardware required. One of the most significant benefits of 2FA is that it doesn't require additional equipment, devices, etc. We all have phones and emails to receive codes to be used with 2FA.
- 2FA is relatively fast. Usually, the code arrives instantly which makes the process convenient.
- It is transferable. If you ever lose your phone, you can transfer your number to a new device so you'll never be permanently locked out.
- Biometrics reduces your effort level. While biometrics are not 100% bulletproof, they are tough to hack.

What are the disadvantages of 2FA?

- Two Factor Authentication is slower. Even if 2FA only adds seconds to each login, the additional time required for each login is a source of frustration for many users.
- Extra steps. To enter a security code received through a text message is one too many steps for many people.
- Lack of trust. Some people don't feel comfortable giving their phone number to websites or apps.
- Dependence on other devices. If your phone is dead or lost, you can't log in.
- Reliance on mobile reception. If you are traveling your mobile phone might be unable to connect to a network, making it impossible to authenticate you.
- Biometrics isn't 100% hack-proof. The fundamental fear about this type of authentication method is that once your voice print, or some other biometric, is compromised, you can't change your voice print and start over.
- Extra support. Due to the added complexity, 2FA requires additional IT support.

Two Factor Authentication is one of the best ways to ensure that the only person who can log in to your account is you. It is the combination of a knowledge, possession or inherence factor that makes Two Factor Authentication a superior security measure. 2FA is a great way to prevent brute force attacks. By requiring a second form of authentication, you are introducing an extra layer of security in your life.