Fuiripe(Filipe) Otsuka

Data Guardian

Are you ready to protect and store important data? Lets use iCloud

Data Guardian

Fuiripe(Filipe) Otsuka

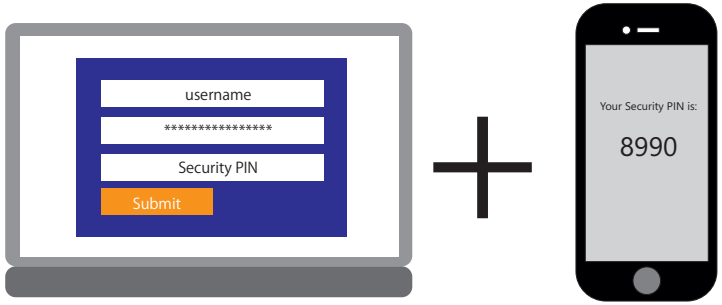
iCloud is a service that allows you to save information (data) in your iPhone to the Internet! If you compare your iPhone to your wallet and the data in your iPhone to the money in your wallet, iCloud is like a bank!

iCloud was launched in October 2011. Today, it has more than 782 million users. However, it has suffered from breaches in the past which may leave you wondering whether iCloud has become safer. We'll see below whether you can trust Apple's cloud security with your private data. iCloud provides users with cloud storage to host all kinds of data and more or less backs-up your iDevices.

Two-factor authentication represents a standard feature in iCloud service today. Using it, whenever you try to sign into iCloud on a new device for the first time, you'll be asked to provide your password and a six-digit code (a complex alphanumeric code, or a generated random code). If your device is 'trusted', the code is displayed automatically.

With two-factor authentication, you can access your account only on trusted devices such as iPhone, iPad, Apple Watch, and Mac. When you first sign in to a new device, you need to provide two pieces of information: a password and a six-digit verification code that automatically appears on trusted devices. By entering the code, you are confirming that you trust the new device. For example, if you have an iPhone and sign in to your account for the first time on a newly purchased Mac, you will be asked to enter your password and a verification code that automatically appears on your iPhone.

Two-factor authentication



Because passwords are not enough to access your account, two-factor authentication greatly increases the security of your Apple ID and all personal information stored on Apple.

Once you are logged in, you will not be prompted again for a verification code unless you need to log out completely, erase the device, or change your password for security reasons. You can choose to trust your browser when you log in to the web. As a result, you will not be prompted for a verification code the next time you log in from that computer.

iCloud secures your information by encrypting it when it's in transit, storing it in iCloud in an encrypted format, and using secure tokens for authentication.

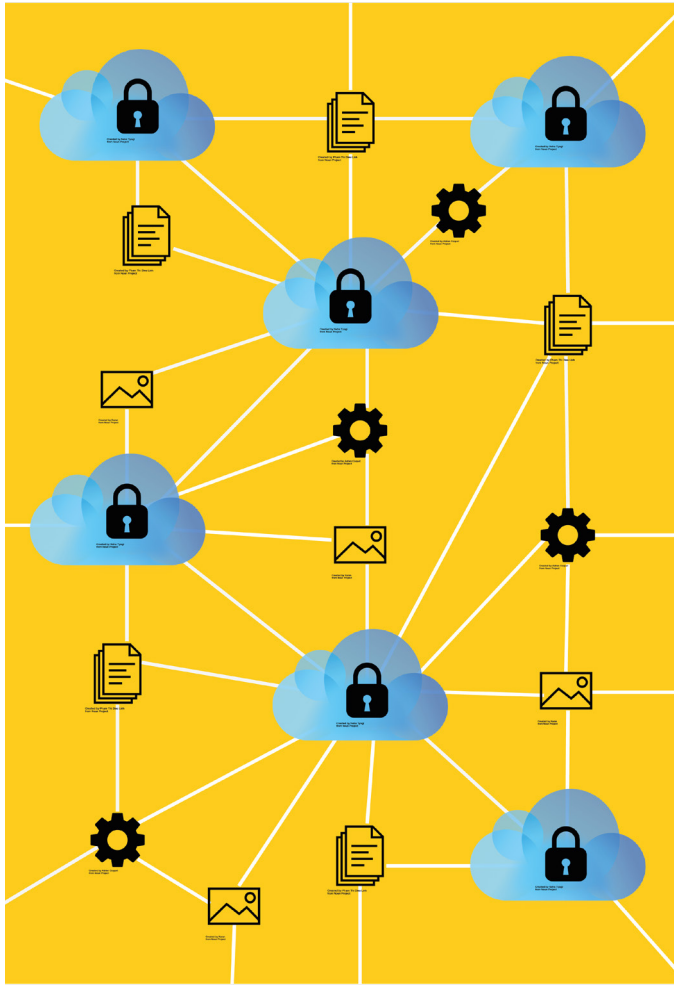
With end-to-end encryption (in this case, where there is only one party involved), the data is only ever decrypted on your device. This means that as long as data is encrypted on your device before being sent,

and can only be decrypted with a key only you have, you're the only individual that can access that data. Such encryption can be done rather seamlessly nowadays, and it provides the maximum security possible.

iCloud provides end-to-end encryption it is a type of encryption that's designed to prevent third parties from reading your data. Only those communicating directly have access. Home data, iCloud Keychain, payment information, Siri and WiFi network information are stored using end-to-end encryption. You need to have two-factor authentication enabled to be able to use it, though.

Messages in iCloud also use end-to-end encryption. If you turn iCloud backup on, you will have a copy of the key protecting your messages included in your backup. This enables you to recover your messages if you've lost access to iCloud Keychain and your trusted devices (iPhone, iPad, or iPod touch with iOS 9 and later). If you turn off iCloud Backup, a new key is generated on your device and it's not stored by Apple.

iCloud is safe, but not a little private. Everything is encrypted during transfer, and most of the data is encrypted at rest. However, in all cases that are not end-to-end encrypted, Apple can access it as needed. In all fairness they are not strictly worse than other similar services, but we expect Apple to take more steps to ensure that only you have access to your data. did.



References:

Elyse Betters. (2017 February 5). *What is Apple iCloud Drive and how does it work?*. Retrieved from https://www.pocket-lint.com/apps/news/apple/131058-what-is-apple-icloud-drive-and-how-does-it-work

(2019 January 8). *How does WhatsApp end-to-end encryption work*. Retrieved from https://www.businesstoday.in/buzztop/buzztop-feature/how-does-whatsapp-end-to-end-encryption-work/story/307998.html

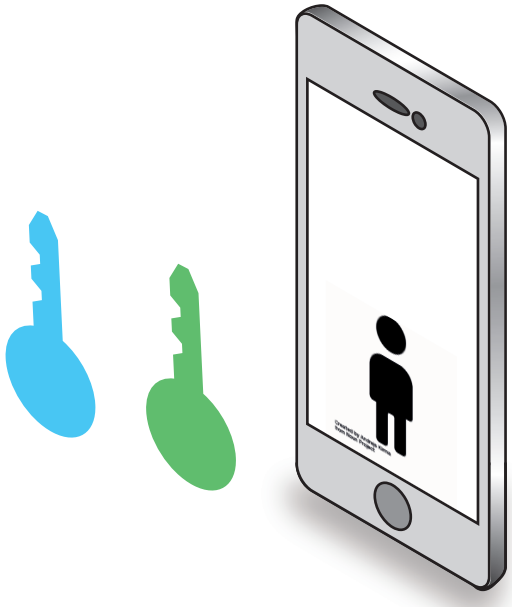
(2019 October 11). *Two-factor authentication for Apple ID*. Retrieved from https://support.apple.com/en-us/HT204915

Michael deAgonia. (2017 August 18). *iCloud security: How (and why) to enable two-factor authentication*. Retrieved from https://www.computerworld.com/article/3217007/icloud-security-how-and-why-to-enable-two-factor-authentication.html

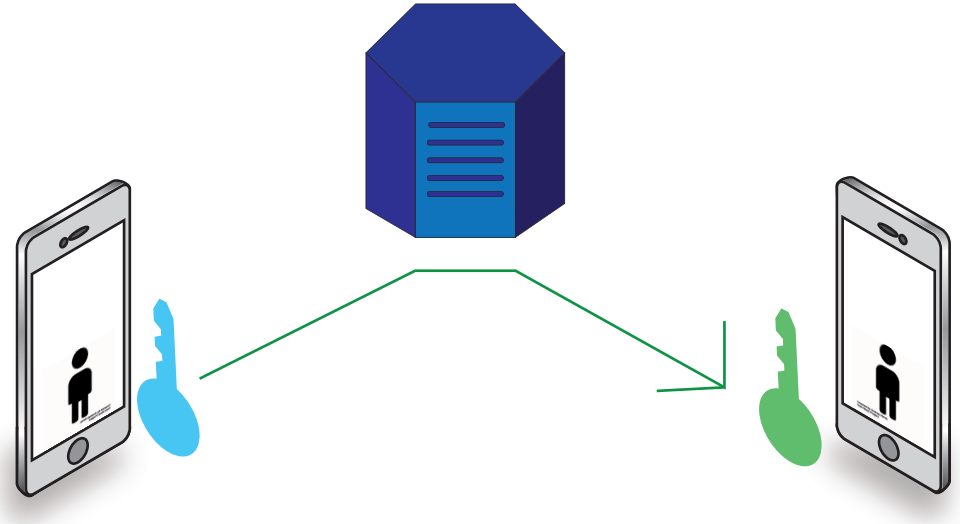
Bob Kfir. (July 5). *How Secure Is iCloud?*. Retrieved from https://medium.com/bob-kfir-tech/how-secure-is-icloud-d29f00286612#targetText=iCloud%20secures%20your%20information%20by,end%2Dto%2Dend%20encryption.

How end-to-end encryption works

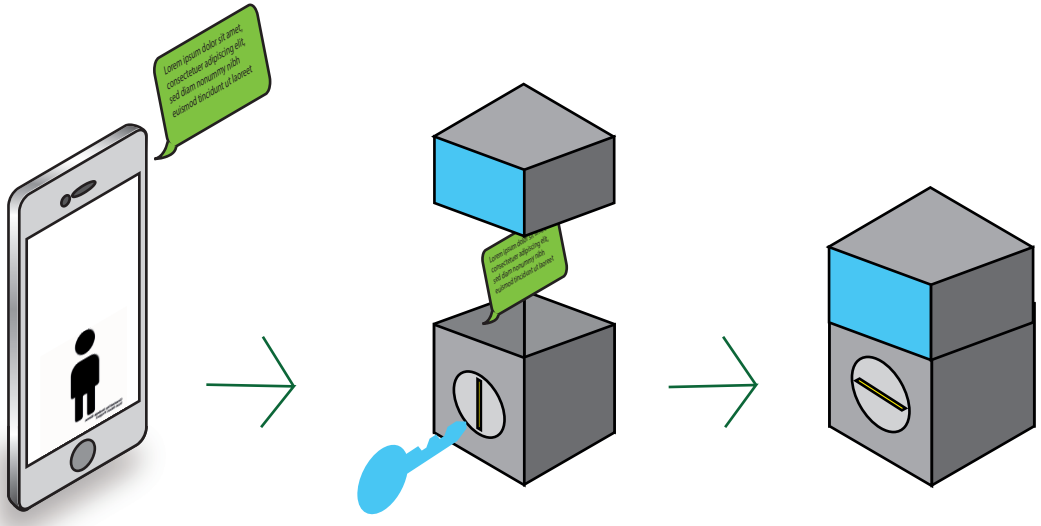
1 Two keys, public and private are generated when a user opens Whats App for the first time. The encryption process takes place on your phone.



2 The private key remains with the user on the phone. The public key is transmitted though the server to the receiver.



3 The public key encrypts the sender's message on the phone even before it reaches the server.



4 The server is only used to transmit the encrypted message. Only the receiver's private key can unlock the message. No third party including WhatsApp can read the message.