I'm not a bot

Example of two factor authentication

With two-factor authentication, you protect your account using a pair of authentication methods. Each method is different, with 2FA making it harder for hackers to get into your account. The first stage of 2FA is typically a password. After entering your password, you're asked for a second type of authentication. These usually come in the following forms: Something you have, such as mobile devices, that you can use to access online accounts. A knowledge factor, which is something that you know that nobody else should know. A possession factor that is unique to your body, such as your fingerprint. The idea is to provide you with more than just a password for the protection of your online accounts. After all, passwords aren't perfect. They can be hacked by malicious individuals. By adding a second authentication factor, you may be able to stop hackers in their tracks. Examples of Two-Factor Authentication There are several types of 2FA that websites and apps can use to confirm user authentication and prevent data breaches. While all add an extra layer of protection, some examples are far more effective than others. Example No. 1 – Security Questions What's your mother's maiden name? What was the name of your first pet? What street did you grow up on? Almost everybody who has set up an online account somewhere has likely encountered this form of 2FA. It may be the most common example. The theory is that security questions are effective because they ask for information that only the user should know. So, how do they work? When you set up an account, a website asks you to create a password and answer a security question. From then on, you're asked for both the password and answer to your question when you try to log in. Failure to provide the right answer can lead to you getting locked out of your account. Sounds simple enough. And that simplicity can be a problem. Security questions often relate to basic information about you, such as the examples we shared above. If that information is floating around the web somewhere, the question becomes less effective. For example, let's say you want to commemorate the passing of your first pet on social media. You share a picture and a little bit of text that happens to contain the pet's name. If one of your security questions asks for that name, you've just shared information that a hacker could use to bypass this form of two-factor authentication. The Pros of Security Questions Super easy to set up. Simple to remember the answer. Questions generally relate to information that's memorable enough that you don't need to write it down. They can be used across multiple devices. The Cons of Security Questions Hackers can dig up the answers to your security questions if they look hard enough. Public records can often show the answers to these questions. Sharing information on social media could compromise this example of 2FA. Example No. 2 – SMS Messages If you're asked for a phone number when creating your login credentials, the odds are that the site uses SMS messages for 2FA. This type of authentication is really simple. You log in to your account with your username and password. But before you get full access, you're asked to enter a unique code that's sent to your mobile phone via text message. Once the code reaches the user's mobile device, there's usually a time limit in place for its use. For example, a site may give you a minute to enter the code before you need to request another one. Just pop the code in and you're good to go. This type of two-step verification assumes that only you have access to your mobile device. Text messages aren't easily accessible to hackers unless they find a way to hack into a user's phone. Still, the possibility of hacking exists. If somebody manages to access your phone, SMS security measures may not work. The hacker could just read the SMS and enter the code you receive. Of course, they also need to have your password to get the SMS sent in the first place. The Pros of SMS Messages Extremely convenient because you'll almost always have access to your phone. Usually provides an option to change the phone number linked to your account if you lose your device or get a new number. Your code should arrive instantly. The Cons of SMS Messages If you don't trust the service you've created the account with, you may not want to share your phone number with it. You have to be wary that the account providers won't use your number for advertising. A lack of cellular service may make it impossible to receive your code. Some hackers can intercept SMS messages, though this isn't a simple process. Example No. 3 – Email Messages Email messages work similarly to SMS messages with one key difference: You don't need a specific physical device to access them. Instead of sending a verification code via text message, the account provider sends it to your email address. You can then access this email using any device that connects to the internet, giving you more options for getting your hands on the code. That's the good news. The bad news is that email is easier to hack than SMS. A hacker only needs your email address and password to get into your account. After that, they don't need to change anything within your inbox. They just need to get a verification code sent to the email address so they can access whatever account they're trying to get into. Worst of all, you likely won't know that a hacker has bypassed this type of identity verification until the email with the code lands in your inbox. And by that point, it's probably too late to do anything about it. For this reason, most providers that offer two-factor authentication don't use email to transmit any sort of sensitive information. The Pros of Email Messages Extremely convenient due to the ability to access the sent email on multiple devices. Allows you to gain access to your account with no complications. As long as you have an internet connection, you can access your code. The Cons of Email Messages A stolen password for your email account gives hackers access to any codes sent to your email. You may not notice somebody has hacked your email account until the email with the authentication code lands in your inbox. You're relying on a non-secure method of communication. Example No. 4 – Push Notification Again, push notification works similarly to SMS messages as it relies on you having access to your phone. But the key difference here is that no type of personal identification number gets sent to your device. That means no sensitive data inside an email or text message. Instead, you get a notification on your phone that tells you somebody is trying to access your account. Typically, this notification comes with the option to accept or decline the access attempt. If you know that you're the one making the attempt, you tap accept. But if you're not trying to access your account, you can hit decline and stop whoever's trying to get in. But what if you and a hacker try to access your account at the same time? Most push notifications solve that problem by providing general details about the device being used to log in. For example, they may give you a location, IP address, and device type, which you can use to confirm the login attempt comes from you. Finally, this authentication method is tied directly to your phone, rather than the SMS or email services your phone users. If you don't click accept when the notification comes in, the person attempting to access your account can't get in. The Pros of Push Notifications Provides information about the person trying to log in to your account. Doesn't transmit any sensitive data that a hacker could use to bypass authentication requests. Requires you to directly approve authentication requests before access to an account is provided. The Cons of Push Notifications The user's mobile phone needs to be connected to the internet for this security process. If you're not online, you won't receive a notification. A single tap provides access, which could lead to you accidentally approving a request. Example No. 5 – One-Time Passwords This method usually involves using a smartphone app to confirm the user's identity. After entering your standard password into your account, you'll see a QR code. You have to use your mobile device to scan the QR code, which contains a secret key. Once the secret key gets loaded into your smartphone app, it generates a one-time password. You enter this password into your account to gain access. It's a method that relies on you having access to a mobile device, the related app, and an internet connection. However, the passwords are time-limited. They usually expire within a minute of being generated. That makes it very hard for anybody who doesn't have access to your mobile device to get around this second type of authentication. The Pros of One-Time Passwords Though you're using an app to access your one-time password, your phone doesn't need mobile service. Secret keys are stored on your device, meaning they can't get intercepted. Some apps allow you to sync codes between different devices. The Cons of One-Time Passwords You can't access your one-time password if you lose internet connection or your phone runs out of battery. Codes may be unusable if your phone's clock isn't synced with the account you're trying to access. Hackers might be able to force their way into your account if the service doesn't limit login attempts. One-time passwords often rely on the use of authenticator apps. You may need to download several of these for all of your accounts. Example No. 6 – Universal Second Factor (U2F) Keys Simplicity is the name of the game with U2F keys. This authentication method uses an open standard that is placed on an NFC or USB device. It can also be loaded into a smart card. When you attempt to log in, you enter your password and then use the appropriate device to complete secondary authentication. For example, let's say you're using a USB. All you need to do is keep that USB device plugged into your computer when logging in. Your online account picks up on the data in the USB and uses it to verify that you are who you say you are. In the case of NFC devices and smart cards, you'll usually scan them over a reader to provide secondary authentication. U2F relies on a physical factor that grants access. That means there's no chance of a password or secret key getting intercepted online. Of course, losing the physical factor locks you out of your account. The Pros of U2F Keys As a physical factor, these keys can't be intercepted digitally. That means hackers can't see your secondary authentication, even if they have access to your device. They only work for the site you've registered them for, making them phishing-proof. The Cons of U2F Keys You have to keep hold of physical security keys to use this method. If you lose the device, you might lose access to your account. Relying on physical devices can create compatibility issues. For example, your U2F key may have a USB-A connector, which can make it incompatible with newer devices that use more modern USB standards. As a new technology, U2F is not as widely supported as other two-factor authentication methods. Example No. 7 – Phone Calls It's good to talk. With phone calls providing your two-factor authentication, your conversations can also stop hackers from getting access to your online accounts. Phone calls are simple. You give the account provider your phone number when setting up your account. When you try to log in, you get a call from the provider after you've entered your password. They deliver a unique code, which you enter to gain access to your account. It's convenient, simple, and makes use of a device that almost everybody owns. However, phone call verification requires you to trust the incoming call enough to answer security questions or provide a unique password if the account provider needs them. The Pros of Phone Calls They're simple, easy, and effective. You're the only person on the call, which means you're the only person who gets to hear the security code you need to use. Almost everybody has access to a phone. You don't even need a smartphone. Landlines work just as well with this authentication method. The Cons of Phone Calls If you're using a smartphone, cell reception plays a big role. If you lose reception, you can't take a call. Losing your phone or sim card means you can't use this authentication method. In rare cases, hackers can clone sim cards and gain access to accounts using phone calls. Example No. 8 – Biometric Authentication What could be safer than something that is part of your own body? That's the philosophy behind using biometric factors for 2FA. A biometric factor is anything that's both unique and a part of your body. Fingerprints are excellent examples. Nobody else has your exact fingerprint, meaning nobody else can access an account that requires a scan of your fingerprint for access. The same goes for the iris in your eye. Many forms of two-factor authentication use iris scanners to confirm the right person is gaining access. This method is most commonly used in buildings, though some smartphones now have the ability to take iris scans. Facial and voice recognition also fall under this umbrella. Nobody else has your exact face and voice. As long as the technique used to scan these elements of you is detailed enough, you can use your voice or face to gain access to your account. The Pros of Biometric Factors Biometric authentication uses parts of you to provide access. That makes it incredibly difficult to hack because a hacker needs to have you physically present to gain access. Even biometric factors that can be copied, such as fingerprints, require physical access to you first. Voice recognition needs a recording of your voice, which is also not easy to obtain. The Cons of Biometric Factors Special equipment is needed to scan the biometric factor to provide access. A compromised biometric factor is unusable for life. After all, you can't change your fingerprints or face without extensive surgery. Many people feel uncomfortable with the idea of providing their biometric identifiers to companies. They create some serious privacy concerns. Regaining Access Two-factor authentication is great in the sense that it provides an extra layer of protection to your online accounts. But it isn't perfect. There are all sorts of things that can go wrong with 2FA that could leave you locked out of your account. Do you want some examples? Let's say you're using physical security keys as secondary authentication. You lose the key and poof! You lose access to your account. There's also the issue of hackers to consider. Skilled hackers can gain access to smartphones, email accounts, and SMS messages. If you're relying on these methods for two-factor authentication, a hacker might take advantage. They only need to get access once so they can change your account and, potentially, change your method of 2FA. So, what can you do about these problems? You rely on the last resort that accounts using two-factor authentication usually offer – the recovery code. Think of recovery codes as your safety net. They're static codes that you usually receive when you're setting up two-factor authentication. You have to write the code down and keep it somewhere safe so you can use it if you ever lose access to your means of providing secondary authentication. Consider Using Several Types of 2FA What happens if the account doesn't offer a recovery code? You're not completely out of luck. Some providers let you use several two-factor authentication methods. For example, your local banking app may provide biometric access, security questions, and SMS codes. If you can't use one, for whatever reason, you may be able to use another to gain access to your account. Leverage Two-Factor Authentication Single-factor authentication, such as user passwords, only protects your account as long as you're the only person who knows the password. If somebody else gets their hands on it, your account is compromised. Multi-factor authentication techniques create more protection for user accounts. They address security concerns directly by using a separate authentication process to confirm that the person attempting to gain access is actually the right person. But the secondary methods providers use to authenticate users aren't perfect. Some are vulnerable to hacking. Others require you to have access to a physical device, cell phone signal, or internet connection. Still, two-factor authentication provides much more security than single-factor authentication.