(Approx. 984 words)

Do You Use Two-Factor Authentication?

By Phil Sorrentino, Secretary & Newsletter Contributor

Sun City Center Computer Club

<https://scccomputerclub.org/>

philsorr (at) yahoo.com

If not, you might want to consider it for specific accounts if it is offered. Two-factor authentication is a way of adding an additional level of privacy to a computer account. When you set up an account, typically on a computer server, you assign a "User Name," which is not private, and a Password, which you are advised to keep private. This provides a certain level of privacy because to access your account, you must provide the User Name, which is not private, and the password, which is, hopefully, known only to you. This is probably all you need to do for most of your accounts. However, adding another level of privacy would be prudent to guarantee that you can access the account only for specific accounts. These accounts would be those that you would be very unhappy if someone else, or some other computer, could access and download or manipulate its contents. An account that contains very personal information or an account at a financial institution might be just this type of account.



Client-Server Architecture

Keep in mind the internet employs a Client-Server Architecture. Using this architecture, your account is on a server computer, not your home computer, tablet, or phone. These (client) devices only provide the ability to connect to the server and manipulate the account contents. So if someone else knew your User Name, which is not protected, and knew or stole or guessed your Password, which is hopefully protected, they could access the account and manipulate the contents. If it's a financial account, they could probably manipulate its value. Unfortunately, no matter how diligent you are in protecting your password, sometimes passwords become known to the bad guys, such as "hackers." If hackers get into your financial account, they can possibly use it for fraudulent financial transfers or payments, or worse, a password alone may not be enough. Even many services that don't offer two-factor authentication have instituted various checks on the computer attempting to use a particular server account, like sending an email to the email of record indicating a new computer is trying to access the account and asking, "Is this you?". If you are concerned about this, google "What happens if someone accesses my account" and see the possibilities. Nowadays, many services employ two-factor authentication to help guarantee that only the account owner can access a particular account.

Two-factor authentication is not a new concept. Banks have used a second form of identification for years, using ATMs to secure access to safe deposit boxes. When a bank customer visits a local automated teller machine (ATM), one authentication factor is the physical ATM card that the customer slides into the machine ("what you have"). A second factor is the PIN the customer enters through the keypad ("what you know"). When you want to get into your safe deposit box, you have to provide the account number ("what you know") and a key ("what you have") before they will let you into the box.

Fortunately, many, if not all, financial institution servers provide the ability to use two-factor authentication. Two-factor authentication requires a second form of identification, which you typically have. Two-factor authentication increases the probability that the requester is who he says he is. The more factors used, the higher the likelihood that the requester is the account owner. Two-factor authentication is sometimes confused with "strong authentication," but these are different strategies. Soliciting multiple answers to challenge questions may be considered strong authentication. However, unless the process also requires "what the user has" or "what the user is," it would not be regarded as two-factor authentication.



What you know **+** What you have **=** Positive Authentication

In general, authentication can be done by "what you know," like a password or pin, or "what you have, "like a badge or a smartphone, or "what you are," like a fingerprint or iris eye-print. (Some highly classified systems may require all three for authentication, which would involve possessing a password and a physical token used in conjunction with biometric data, such as a fingerprint, a voiceprint, or a retina scan.)

For most typical internet servers, the second form of identification is "what you have." The "what you have" can be a code sent to you by text, email, or phone; the account owner usually makes the choice. The code is typically a one-time-use series of six or so digits. Once the code is sent, you will have enough time to enter it into the screen that starts the authentication process. If email is selected, the server will send an email with the code to your email address of record on that server. Once you provide the correct code, you will be granted access to the account. If a voice phone call is selected, the call is made to the phone number on the record on that server. Once the phone call is answered, the digits are announced, and you can enter them on the screen that starts the process. If a text is selected, the text will be sent to the phone number of record on that server (ensure the phone number can receive texts). The code in the text can then be entered into the screen that starts the process.

Two-factor authentication adds an extra step to your login process, and depending on how the service has implemented it, it can be a minor inconvenience or a major annoyance. (And it also depends on your patience and willingness to spend the extra time to ensure higher security.) However, in the long run, using two-factor authentication improves the security of your private information, which is undoubtedly something we all want. So, take the time to set up two-factor authentication on at least all of your financial and very private accounts.