Multifactor Authentication

By Trey Peacock, Winning Cases Based On Science & Data For Over 25 Years
Originally published on LinkedIn.com

In this series of articles, I've discussed strategies the modern-day tech user can employ to fortify online and cyber security. Yet, apart from using a password manager, none of the techniques I've previously discussed are quite as effective, easy, and readily available as multi-factor authentication. This mouthful-of-a-term is the name for a secondary layer of security a user can add to online accounts, applications, and devices. Multi-factor authentication will drastically decrease the likelihood that information can be accessed by a hostile or unwanted party.

What Is It?

The operation of multi-factor authentication (MFA) is simple but varied. The most standard configuration is as follows: Upon setting up an account or enabling the feature, the program prompts the user to add a second form of contact, like an email or phone number. The next time the user logs in, in addition to supplying a username and password (which, if you've been

following these articles, should be unique, long, alphanumeric, and complicated), the user will need to input a unique numeric code, which will be sent automatically by the app to the user's second form of contact. Once the user enters the code that was delivered to the second form of contact, access to the account is permitted. In the case of an unauthorized login attempt, the person attempting to log in will lack the code and entry to the account will be denied. Easy peasy.

How Do I Use It?

In its most basic form, MFA is quite simple to use. Simply set up MFA, login to your accounts as usual, and at certain times, such as when you are logging in from an unfamiliar device, location, or after a significant amount of time, you will be prompted to enter a code sent to one of your registered devices. Review the code, enter it into the website or login, and boom, you're in. However, don't forget to delete the message containing the code just in case.

In recent years, a few apps have emerged to add yet another layer of insulation from hackers and to defend the viability and integrity of code-based Two-Factor Authentication (2FA). These apps, called "authenticators," take the place of a confirmation code sent to a phone or email address, and thus eliminate the possibility of a hostile code interception and subsequent login. Some prominent and effective apps in this class include Google Authenticator and Authy, which supports authentication across multiple devices. Additionally, the password manager software Dashlane, which I have previously recommended to readers, also comes enabled with a built-in authenticator for users of its premium version.

Overall, use of an authenticator app is more secure than a simple confirmation code, as a code can be intercepted by a hacker or thief who has gained access, either physically or virtually, to your secondary device. After all, we lose phones sometimes, and if one of your passwords is vulnerable, others may be also. Having said that, 2FA will greatly increase your network and cyber security. It can be a bit tedious to always enter essentially two passwords, but the added layer of security is vital for those concerned about the integrity of their online and technological information.

Where Can I Use It?

Dozens of popular companies and websites have integrated MFA into their login portals and accounts in order to keep pace with the growing demand for sturdier online security measures. Online marketplaces such as Amazon and eBay have readily available MFA features. These websites offer users the ability to confirm their identity via a one-time code sent via text, or through an automated phone call directly to the number associated with the user's profile. Additionally, both websites require MFA in order to reset a password, preventing would-be thieves from eluding security measures by using the "Forgot my password" feature. Google's online tools and products such as Gmail, Google Drive, and Google Scholar, all operate from the user's Google account which offers the protection of MFA. Users should enable this service on Google accounts, as the elaborate integration of Google's web-app ecosystem allows many services and applications to be accessed with a single user login. Google also allows users to list "back-up" phone numbers

and email addresses. This feature allows a secondary means of access to an account, which is really helpful in the event of a lost or damaged phone that served as the secondary device for authentication, and helps prevent unauthorized access because the back-up accounts also receive the password change options sent by Google. As always, take care to guard secondary email addresses and devices because they provide a potential avenue for intruders.

For an extra level of security, some applications such as Amazon and Google allow users to bypass a code sent by text or email in favor of MFA generated by an authenticator app like Google Authenticator, Authy, or Dashlane Password Manager's in-built authenticator feature. Users must set this feature up individually within their authenticator app, which can be tedious, but the payoff in security and ease of access far outweigh the inconvenience.

Uber and Lyft integrated privacy protection features into their apps, requiring users to confirm their identity through their mobile phone numbers before accessing an account. Additionally, users are occasionally prompted to confirm payment details to prevent unauthorized rides. These MFA features are particularly useful for apps, including payment apps such as Venmo or CashApp, which are linked directly to bank accounts or credit cards. Venmo allows users to add an authenticator app as a means of identity confirmation without a cell phone or email address.

By far the most ubiquitous accounts on the internet, social media platforms also allow MFA protection. While social media may appear innocuous, data collection operations they operate means your accounts provide far more valuable personal information than meets the eye. Take special care to enable one or even two-factor authentication, either through a confirmation code sent by text or email, authentication app, or by creating a series of security questions.

Users who operate online backups or use file transfer services should safeguard their accounts using MFA as well. Services such as Dropbox or Microsoft 365's Cloud Drive feature offer an enormous amount of safety in the event of file loss, but their online backups remain a target for savvy hackers. Particularly for users whose files contain highly sensitive or confidential information, safeguarding the files and backups, both in storage and in transfer, is paramount to practicing proper information security. Microsoft 365 offers users the ability to integrate an authenticator app, but users whose accounts are sponsored through a business or educational institution may find these features limited by the sponsoring organization.

Perhaps most importantly, users should absolutely employ multifactor authentication on any and all financial services or banking mobile apps. While applications such as Amazon or Uber may provide thieves access to the credit card information on file, no other application contains the wealth of vital information that banking and financial services apps do. When thieves access your mobile banking account, they can run amok with your money before you realize anything is wrong. While some banks offer asset and fraud protection to cover this type of theft, there's no guarantee of full coverage or asset recovery. Therefore, it is far better to erect a first line of defense by enabling MFA authentication for banking and financial applications. Frankly, if you haven't already done so, you are behind the curve and an easier target for a cyber-criminal. Finally, if you find that your bank *doesn't* offer MFA on their mobile app, your path forward is simple: change banks. Banks that don't offer MFA likely do not have an interest in protecting customers' money and financial security.

Can I Integrate MFA With My Password Manager?

To facilitate the implementation of MFA across all devices and accounts, users can take advantage of password manager apps such as Dashlane. Dashlane allows users to catalog and encrypt every password in its secure database. Additionally, the app's premium-level allows customers to use the app as an authenticator for most any MFA confirmation, bypassing the need to receive a code sent by email, text or phone call, and eliminating a potentially vulnerable link in the chain between account and user.

Diligent and liberal use of MFA provides enhanced security, protects users from potential theft or unauthorized account access, and offers a moderate increase in peace of mind. Though no security feature completely eliminates the risk of intrusion, MFA greatly decreases the likelihood with little to no downside.

About the Author

Trey Peacock, a partner at Susman Godfrey, has been winning cases based on science and data for over 25 years. He has also chaired the firm's IT committee for over two decades. Learn more about Trey here.