Why Multi-Factor Authentication Is Right For You

hastingsmutual.com/blog/blog-post/mutual-understanding/2021/12/09/why-multi-factor-authentication-is-right-for-you

Dec 9, 2021, 1:24 PM
Leave a comment

An extra layer of security protects every person and every business.

If you're in the computer business, you're immediately familiar with the acronym "MFA." If not, you've probably heard the term "multi-factor authentication" at some point. You might have had to take part in multi-factor authentication the last time you logged in at work, for example.

It's a simple method for confirming that you are who you say you are online. A single authentication, like typing in your username and password, is a good place to start when you're trying to get to your bank or your school. But passwords can be guessed. A second line of defense is essential.

Simple techniques

There are all kinds of authentication techniques available: I use one that texts a short string of numbers to my phone, which I then have to type to log in. Another gives me a code from an app, and if I don't type quickly enough the code is replaced by another one (it happens instantaneously, so I can just wait a few seconds to get the next code).

I haven't used these ones yet, but they're authentication types too: selecting "Approve" or "Decline" when a pop-up appears on your device before you can go forward, and a phone call instead of a text message that asks you to press the # key or just hang up.

The idea is to combine two different things: something you know (your password) and something you have (like your phone). It's possible a hacker could steal your password or your phone; it's less likely they'll have both to use to break into your bank account.

Be cautious

MFA is an extra layer of security for the things you do online and your electronic devices. And just like everything you do online, you need to be careful. If you receive an MFA code you're not expecting (as in, you didn't request it just moments before), delete it! Confirming just one code can expose your device or system to someone who shouldn't have access to it.

Once you've typed in a code from a text message, delete the text message. There's no need for anyone else to see the code, and it will expire after you use it, so you don't have a reason to hang on to it, either.

Secure systems like those for your bank often have MFA in place. So do other sources of personal information, like an email account. It's a good idea to opt into MFA whenever possible. Sure, it's an extra step to log in, but the security in place for you is definitely worth it.

The Mutual Understanding blog and Hastings Mutual videos are made available for educational purposes only. The information referred to is not an official company statement, corporate policy, or offer of coverage. Refer to your insurance policy for specific coverage. There is no representation as to the accuracy or completeness of any information found by following any link on this site. Please contact your local independent insurance agent with further questions and for more details on any insurance policy-related information you read here.

Leave a comment

New code

Return to Blog List

Related Blog Posts