Multi-Factor Authentication | CISA

Have you ever worried about hackers getting into your accounts? Us too.

The most common password in the country is still 123456. But maybe you've taken the time to come up with a password only you'll know.... Are you sure, though? If someone can guess your password from looking at your Facebook page, you're probably not as secure as you think.

And even if you have a complex password, and – extra points for a password keeper! -- unfortunately, bad cyber actors still have ways of getting past your password.

Wouldn't it be nice to make it MUCH MORE DIFFICULT for them? Actually, YOU CAN!!! You just need to add a second way of identifying yourself in your accounts.

What you need is …More Than A Password!!

You might be happy using only a password to access your online accounts, but we can tell you that hackers are even more excited.

Once they have your password, they're in. And you know what happens once bad actors access your accounts… You'll see your money …walking away.

Let's talk a minute about using a second method to verify your identity. First, it's freely available and called Multi-Factor Authentication (MFA). It is also known as "Two Factor Authentication" or "Two Step Authentication." Look for it under the security settings of your online account. Second, it only takes a minute or two to enable and a few seconds to use.

WHAT IS MULTI-FACTOR AUTHENTICATION?

Multi-factor authentication (MFA) is a layered approach to securing your online accounts and the data they contain. When you enable MFA in your online services (like email), you must provide a combination of two or more authenticators to verify your identity before the service grants you access. Using MFA protects your account more than just using a username and password. Users who enable MFA are significantly less likely to get hacked, according to Microsoft. Why? Because even if one factor (like your password) becomes compromised, unauthorized users will be unable to meet the second authentication requirement ultimately stopping them from gaining access to your accounts.

It goes by many names: Two Factor Authentication, Multi-Factor Authentication, Two Step Authentication, MFA, 2FA. They all refer to using a combination of something we have, something we know, or something we are when confirming we are who we say we are online.

Your bank, your social media network, your school, your workplace… they want to make sure you're the one accessing your information, and more importantly, they want to prevent unauthorized individuals from accessing your account and data.

So, online services are taking a step to double check. Instead of asking you just for something you know (e.g., a password) – which can be reused, more easily cracked, or stolen – they can verify it's you by asking for two forms of information:

They'll ask for something you know …. like a PIN number or a password, along with

- Something you have …. like an authentication application or a confirmation text on your phone, or
- Something you are …. like a fingerprint or face scan.
- Two steps are harder for a hacker to compromise. So, prove it's you with two … two steps, that is.

Now that you know what it is, you'll see prompts for multi-factor authentication all over. So whenever available - opt-in. Start with your email account, then financial services, then social media accounts, then online stores, and don't forget your gaming and streaming entertainment services!

And if you don’t see a prompt for multi-factor authentication on one of these accounts, send a note to each company asking them to enable the feature. After all, it’s your security at stake!

Reprinted from: https://www.cisa.gov/mfa