ARTISANS' BANK
SAFETY + SECURITY
SHARED MONTHLY NEWSLETTER

THE POWER OF MULTI-FACTOR AUTHENTICATION

JUNE 2024

Today, passwords and password security are an important part of life. Whenever a password is stolen and used by an unauthorized person, the information it protects is compromised.

To guard data and protect against password exploitation, many organizations and commonly used applications are implementing MFA, or multi-factor authentication.

In computer security, an authentication factor is anything that you use to authenticate yourself with a system. A password, for example. With MFA, you use two or more different factors to log in: for example, a password and a verification code sent to your smartphone.

By now, you have probably used or been prompted to set up MFA on one or more of your accounts. It may ask you to add an email account or phone number. It might even ask you to download a special app to use as an authentication factor.

One more step?!

Here's the deal. If one of your factors is stolen, the thief still doesn't have the other factor and cannot access your account. The more factors you use or the stronger the factor, the better your security. So yes, there are additional steps, and a few different ways to go about it.
Three different authentication factor types can be used in the MFA process. For optimal security, it is best to use two different factor types.

Authentication Factors

1. **Something you know**

This is the most common authentication factor. Passwords and security questions are the most common examples of something you know. Unfortunately, using two factors of the same type together can reduce their effectiveness.

2. **Something you have**

We are seeing a rise in this factor and for good reason. Examples include a key card, a verification code sent to your smartphone or a random number produced on an authentication app. These are becoming very common and easy to add to your login process.

3. **Something you are**

This is the rarest factor but the most difficult to counterfeit. This security method authenticates you by measuring or recording something unique about you using biometrics. It could be fingerprints, palm prints, iris patterns, face or voice.
Multi-factor authentication is a major part of security in today's fast-paced digital world. Hackers are getting more sophisticated with their attacks. When it comes to cyberattacks, MFA is one of the best tools you have.

MFA, OR LACK THEREOF, IN ACTION

In November 2023, Midnight Blizzard hackers breached Microsoft through a single account. This account was created in-house by Microsoft and used for testing purposes. However, someone had mistakenly given this account admin privileges. And it didn't have multi-factor authentication. If you had the password, you were in.
The hackers probed for weaknesses by trying the same password on many different accounts at once. This test account turned out to be a match. Once inside, the hackers used its admin privileges to create malicious applications and elevate their access.
In October 2023, hackers started selling personal genetic information on the dark web. This information appeared to come from 23andMe, a DNA testing service. How?
Attackers used a technique called "credential stuffing." They took login information and passwords stolen from other services — such as email programs and online shopping platforms. Then they tested these logins and passwords on 23andMe. Unfortunately, many people reuse login and password information across different sites, and some of these stolen credentials allowed hackers to log into real 23andMe accounts.
This attack could have been avoided if the affected users had enabled 23andMe's MFA options with their accounts. They would have received a message saying there was a login, and they could have denied entry to the attackers.