What's the Difference Between 2FA and MFA (and Why Does it Matter?)

THE CYBERTHREAT LANDSCAPE IS DEFINITELY GETTING WORSE

While some things around the world are (finally!) getting better, the cyberthreat landscape is definitely getting worse. The third annual Devolutions State of IT Security in SMBs in 2022/23 Survey found that:

- 67% of SMBs are more worried about IT security now vs. a year ago.
- 60% of SMBs experienced at least one cyberattack in the last year.
- The rise of remote/hybrid workers is triggering a wide range of security concerns for SMBs.

The good news, however, is that SMBs (along with all other types of organizations including larger enterprises) do not need to merely hope for the best while they brace for the worst. They can – and considering the severe costs of a data breach, frankly, they must — be proactive and reduce risks and vulnerabilities; especially where end users are concerned. And that is where a couple of critically important identity and access management security methods enter the story: two-factor authentication (2FA) and multi-factor authentication.

What is 2FA?

2FA enables unambiguous identification of end users through a combination of assigned credentials (username/password combination) and another component. This additional factor could be:

- Additional login credentials only known to an end user, such as the answer to a security question or a PIN.
- A code that is delivered on a device that an end user physically has in their possession, such as their smartphone.
- Biometric login credentials that are unique to an end user, such as retina scans and fingerprints.

What is MFA?

MFA takes 2FA further by requiring end users to authenticate their identity through three or more factors. For example, in order to access an account, device, or network, an end user may be prompted to:

- Input a PIN
- Input a code sent to their smartphone
- Input a fingerprint scan

Unlike 2FA, the end user is only granted access if all factors are verified. If one factor fails validation — for example, if an end user inputs the correct PIN and fingerprint scan, but the incorrect code — then they will not be granted access.

Also, some organizations deploy passwordless MFA, which excludes the "something an end user knows" factor, and relies instead on something an end user has in their possession and/or biometric login credentials.

The Overlap Between 2FA and MFA

On various websites and articles, it is common to see 2FA and MFA used interchangeably. Is this an error? Not necessarily. Technically, all 2FA methods are also MFA methods — because as noted earlier, the "M" in MFA stands for "multi" (and two = multi). However, not all MFA methods are 2FA methods.

Why is the Difference Between 2FA and MFA Important?

MFA is generally more robust than 2FA, since it adds at least one more layer of verification. However, the added security can degrade UX, which end users can find frustrating; especially if they need to log in and out of accounts and devices throughout the day. It can also lead to some confusion for end users who are not technically savvy, or who have spent years working in an environment that did not have MFA (and possibly did not have 2FA either). This is not to suggest that the learning curve for MFA is steep, because it really isn't. But as the saying goes: "old habits die hard"!

When 2FA is Stronger than MFA

Why do we say that MFA is "generally" more robust than 2FA, instead of "always" more robust than 2FA? This is because the strength and functionality of identity and access management security is not automatically determined by the method. Rather, it is rooted in the factors.

Consider this: two especially strong identity authentication factors are location (enforced by geofencing) and biometric (retina scan or fingerprint). Conversely, SMS messages, "secret" answers, and PINs are relatively weak factors (this does not mean that they are worthless, but just that they are on the weaker end of the spectrum).

An organization that deploys 2FA based on location + biometric arguably has a more robust identity authentication system than an organization that deploys MFA based on SMS messages, "secret" answers, and PINs. The takeaway here is that more factors are usually — but not automatically — better.

The Bottom Line

Both 2FA and MFA are categorically superior to using a single factor, which is typically a password. A whopping 81% of data breaches are due to weak passwords. And despite repeated warnings, many end users reuse passwords across multiple work and personal accounts, and share passwords through highly insecure methods (e.g., email, text message, etc.).

Of course, strong and unique passwords — or better yet, passphrases — are still important. But organizations should view 2FA/MFA as more than just a best practice: it should be seen as a mandatory requirement to reduce vulnerability on the cyberthreat landscape that is getting worse and worse.

We are pleased to note that Devolutions' suite of products including Remote Desktop Manager, Devolutions Server, and Password Hub Business all support 2FA (please note that 2FA for Password Hub Business is facilitated through Devolutions Account, which also governs other services such as Devolutions Force, Forum access, and more). Free trials of all products are available, please contact us for more information.