Microsys
Smart IT Solutions

(416) 425 0444

The Beginner's Guide to Multifactor Authentication

A quick look at **haveibeenpwned.com** shows startling statistics: passwords aren't all that effective.

Even the best combination of numbers, letters, and special characters can be stolen in several ways. Perhaps the hacker lured you into typing your password into a fraudulent account login page or using a keylogger program to track each keystroke. Even if you successfully evaded these tactics, your password may have been leaked in a massive data breach - as is known to **occur commonly**.

One **survey** found that over 2 billion data records have been compromised - including passwords and usernames. To put things into perspective, nearly one million passwords are stolen every week.

This is why cybersecurity experts at **Microsys** recommend changing your password at least once every three months. However, in light of the sobering statistics above, you can't take any chances. If only there were an additional method of authenticating your identity...

Enter multifactor authentication. As the term suggests, multifactor authentication requires users to submit a second, third, or even more verification factor to access an account. For obvious reasons, this can be very inconvenient to users since logging into an account is no longer as seamless as entering a password.

How Effective Is Multifactor Authentication?

Microsoft **says** that multifactor attacks are very effective - in fact, rolling out MFA can block nearly 100% of account hacks. Once your accounts have been protected with MFA, stealing a password or brute force attempts will no longer provide access to hackers.

With that said, multifactor authentication isn't bulletproof and, in certain scenarios, could be used to land you in the middle of a breach. As multifactor authentication pops up everywhere, attackers are becoming more creative at circumventing the security method. One of the biggest culprits is one-time passwords (OTPs).

It can be relatively easy to find an OTP using phishing scams. For example, this **Reddit** breach was caused by a phishing scam when an employee was tricked into clicking a fraudulent link.

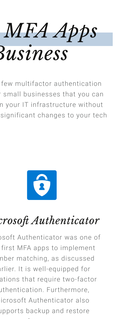
Hackers often do a lot of groundwork for a phishing attempt to work. They will build a fraudulent website that mimics the source website to trick users into entering their OTPs.

Just like OTPs, SMS-based codes can also become susceptible to hacking attempts. Attackers are known for using SIM swap attacks to mimic an authorized device and stealing a user's OTP or SMS codes. There have also been reports of hackers using brute force tactics to crack PINs (relatively easy since they are usually composed of 4-digit numbers). It is also possible to compromise recovery emails.

Another common method of circumventing MFA is to trick users into accepting a security challenge by repeatedly sending push notifications to the user. The victim eventually gives in to the endless barrage of notifications and approves it to put an end to them. MFA fatigue was used to break into **Uber's internal systems** in September 2022.

Making MFAs More Effective

We've rounded up three quick and easy tips to make MFA more effective and address the vulnerabilities discussed above. Check them out below!



Avoid Vulnerable MFA Factors

For starters, try to avoid MFA factors that require push notifications, voice calls, SMS OTPs, and others. In its place, you can implement a phishing-resistant MFA that uses a strong possession factor. Examples include a private cryptographic key (embedded at the hardware level) and strong inherence factors such as facial or touch recognition.

For more information on phishing-resistant MFAs and how you can implement them in your business, contact the **cyber security services experts** at **Microsys**

Spread Awareness

The strongest cybersecurity tool is only as good as the person behind it. Humans are often the weakest link in a cybersecurity system, and MFA is no exception. The best way to make your MFA rollout successful is to provide your users with information about why you are implementing them. User awareness is key to the effectiveness of MFA, so make sure to spread awareness through education sessions.

Use Number Matching

Number matching is a feature that requires users to enter the number displayed on the sign-in screen for approving requests. This is a great way of countering MFA fatigue attacks that spam push notification spams. Most authenticators, including those from Microsoft, Duo, and Okta TOTP, are implementing number matching to keep their users safe.

Best MFA Apps for Business

Below are a few multifactor authentication software for small businesses that you can implement in your IT infrastructure without making any significant changes to your tech stack.

Google Authenticator

Google authenticator is as basic as it gets with no tacky user interfaces. It is very minimalistic and straightforward to use, which is both a strength and a weakness. Minimalism is good because you can start using the app the right way without having to worry about a learning curve. On the flip side, there are no other special features, such as encrypted cloud backups.

Microsoft Authenticator

Microsoft Authenticator was one of the first MFA apps to implement number matching, as discussed earlier. It is well-equipped for situations that require two-factor authentication. Furthermore, Microsoft Authenticator also supports backup and restore features.

Duo Security

Duo is mostly geared toward business users and offers enterprise features such as user provisioning, one-tap push authentication, and multi-user deployment. Duo is compatible with any site that supports Google Authenticator. It is available on iOS, Android, Windows Phone, and BlackBerry. Installing Duo is easy, and you can start using it within minutes.

Auth0

Auth0 is a huge step up from Google Authenticator because it provides organizations with an entire suite of identity management features. The only catch is that learning all the features will require a learning curve, but you will find the app to be more than capable of meeting your needs. Auth0 is free, with up to 7,000 active users and unlimited logins.

Wrapping Up

MFAs aren't here to make passwords obsolete. Rather, MFAs provide an additional layer of security to prevent cybersecurity incidents.

Start implementing MFA today to protect your data, network, and IT infrastructure. Roll out MFA without disrupting your existing workflows and tech stack. Contact **Microsys** for all your cybersecurity needs.

Contact Us