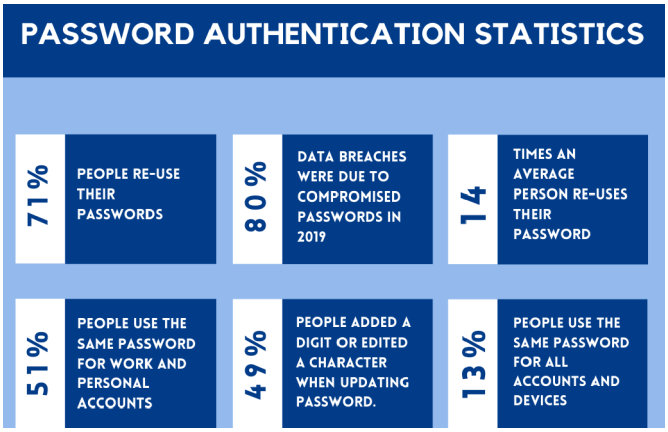
Reinforcing cybersecurity with Multi-Factor Authentication (MFA)

hexnode



What is the one thing you know which keeps others from accessing any of your accounts? Well, there are many ways to keep your account secure, but password authentication is what probably came to your mind. Using a password might seem reliable but after taking a look at the statistics, you might start having second thoughts on the matter.

Cybercrime on the rise

Since most enterprises are trying to digitalize everything, hackers can find almost anything when a data breach occurs. If you'd like to think, 'who would bother to hack into my device?' or 'Nobody would want to hack my system', then here's a fact. One in every three Americans gets hacked every year! A Clark study at the University of Maryland revealed that hackers are accessing devices with network access every 39 seconds on average. On top of that, Interpol had reported an increase in cybercrimes after the onset of the pandemic. Cybercrimes were rampant with phishing attacks contributing to 94% of Covid-related cyber-attacks across a two-week period. "Rather than fearing or ignoring cyber-attacks, do ensure your cyber resilience to them," said Stephane Nappo, Global CISO, Société Générale. Most organizations seem to be having the same idea and have started allocating resources for cybersecurity. By 2023, About $6 trillion is being anticipated to be globally invested in cybersecurity. This may seem like an exaggerated reaction, but then again nobody wants to take the risk of being breached. Still not convinced? Cybersecurity Ventures estimates a 15% increase in cybercrime costs for the next few years, projecting a whopping $10.5 trillion annually by 2025. Now it makes sense, right?

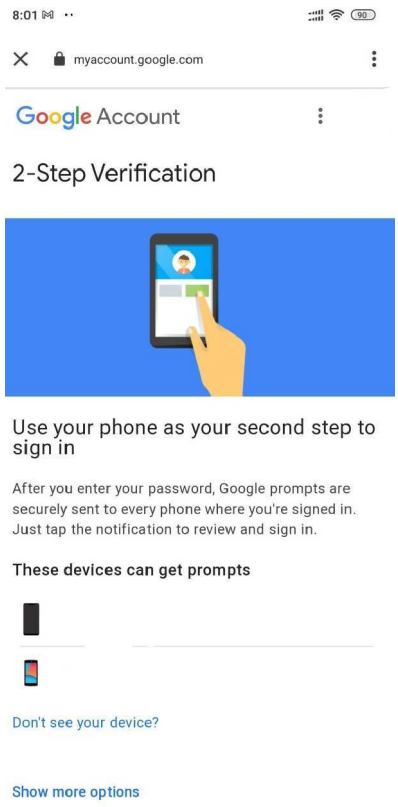
Password compromises lead to most data breaches; we know this from the numbers shown above. So, what exactly can we do? Firewalls and Anti-virus products are essential but redundant without proper user authentication. What is the point in all this security if we are going to leave the front door open? We could turn to Multi-Factor Authentication. Everyone has probably heard of a Two Factor Authentication (TFA), like entering an OTP

(One Time Password), answering security questions received on your mobile or desktop device after providing the login credentials. This means you need two factors to prove your identity and gain access to the account, making it harder to breach. MFA falls under Identity Access Management (IAM), which helps verify the identity of a person to see if they actually have the privilege to access the information he/she is requesting.

So, what exactly is Multi-Factor Authentication (MFA)?

MFA is pretty much used to log into most domains. It's weird how we probably didn't notice this even when we were authenticating using factors like entering OTPs and answering security questions. Multi-Factor Authentication sometimes referred to as two-factor authentication or 2FA, is an authentication technique where more than one factor (exactly two in the case of 2FA) is demanded to verify the identity of the user before he/she can access an online account, a VPN, an application, or the data on a mobile device. MFA is considered to be a crucial component of Identity Access Management (IAM). In any typical scenario, we only need the credentials such as username and password in order to get past security and gain access. But if MFA is implemented, we need two or more factors for user verification. It can belong to any of the three categories; something you know (which can be a pin or password), something you have (like an MS authenticator or smart card), or something you are (that is, biometrics).

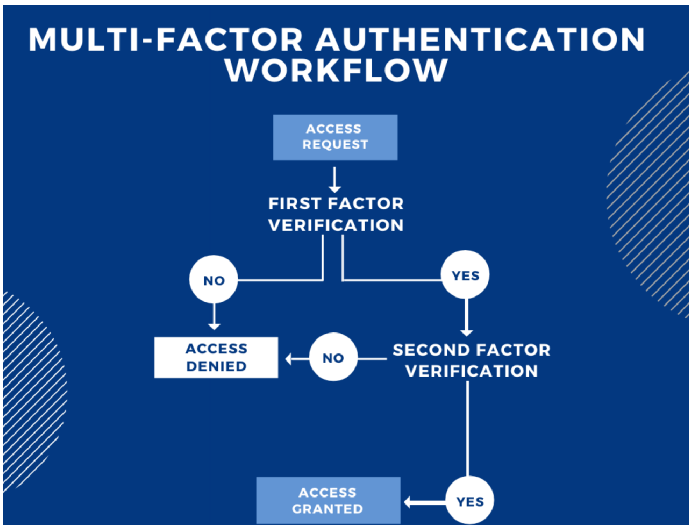
MFA in Google Accounts and Hexnode MDM



Let's say that you want to log in to your Google account from another device. Then Google initiates a two-factor authentication which mandates the user to have their linked mobile device log in to their account. Since everyone walks around with their mobile device, using your phone as the second factor is the most common form of MFA nowadays. Losing a google account could be a huge blow to an individual, but what about access to a device management portal with access to hundreds of employee devices? The repercussions of an unauthorized entry to a managed enterprise could prove to be disastrous. MDM solutions like Hexnode employ MFA in order to prevent this scenario. Hexnode MDM, within itself, utilizes MFA in order to authenticate IT technicians who request access to its portal. Hexnode adopts Two-Factor Authentication security using the login credentials along with the verification codes sent to the email or mobile number for its management portal.

Additionally, Hexnode also allows third-party authenticator apps such as Google Authenticator and Microsoft Authenticator to secure access to the management portal by enabling 2FA.
Using MFA gives an extended proof of the user, with the factors acting like evidence that helps in verifying whether it really is the user and not some random guy. In order to enhance security, it's usually recommended to use factors from different categories.

How does MFA work?



Suppose something urgent comes up and you have to access your work account from home.
When you click on 'login,' an access request gets sent, and another page pops up asking for your login credentials.
These credentials would be the first factor for authentication, that is, the first evidence you present which can vouch for your identity.

Suppose you messed up your password the first time and were denied access. So, you tried again and got it right this time. Let's say the next factor is an OTP, which, if entered right, would grant you access to the account; else, you'd be denied access again. By implementing more factors for verification, the security would be greatly enhanced.

MFA offers user convenience while also taking cybersecurity up a notch

While password authentication is one layer of protection, Multi-Factor Authentication provides more than one layer of protection. The more, the better right? Obtaining the credentials of a person is possible, but credentials and their device? More unlikely. What about their credentials, device, and fingerprint? Highly unlikely. Using Multi-Factor authentication reduces the chances of data breaches significantly when compared to password authentication. If somebody is very determined to hack into your device, you might have to get more layers of security, but in most cases, MFA would suffice.
While employing MFA all the time seems like a great idea, it could be cumbersome to keep trying to prove who you are. What if you only need to verify your identity only once if the context is always the same? Well, it isn't exactly an 'if' since the concept of adaptive MFA already exists. Adaptive/ Contextual or Risk-based MFA is used to

optimize the customer's or the employee's convenience while maintaining security. During low-risk situations, the organization might choose to decrease security or even bypass MFA. In high-risk scenarios, the level of security would increase, especially in high-value transactions. Any MFA utilizing a context verification step can also be referred to as Contextual MFA.

Multi-Factor Authentication also offers simple deployment and management while showing high scalability since it can be easily integrated into applications. Identity and Access Management (IAM) solution providers like Okta possess SDK integrations that can pretty much embed MFA into any custom-built enterprise app. MDMs like Hexnode integrates with Okta in order to provide reliable access and security to device and data via MFA.

The users get to decide what factors to opt for while verification, which makes things simple and less bothersome. It's used for things that we may not consider significant, like a Nintendo account, which even kids can create and use. We don't recall using MFA much, owing to the simplicity and triviality of the various authentication factors.

So, is MFA worth it?

So, does MFA really contribute much to cybersecurity? So here are some more statistics. About 99.9% of the Microsoft accounts that got hacked weren't secured with MFA, which means almost no Multi-Factor Authenticated accounts were hacked. Accounts with MFA have more security so, in case your credentials get stolen during a mass hack or data breach, your account will remain secure. MFA is also very popular with almost all personal and professional platforms. Social media, enterprise, and gaming platforms have all decided to switch to MFA to the point where it has already become an integrated part of our lives. With its simple deployment, enhanced security, and popularity, the real question is, why haven't you set up MFA already?