The Power and Pitfalls of Multifactor Authentication: How to Safeguard your Business

By David Plutner, Manager and Thomas J. DeMayo, Partner

The authentication systems we use every day for services, such as Netflix, Apple TV, Microsoft Office365 and IT devices, historically utilized only a username and password as a method of validating who you are. Over time, the use of a password alone proved ineffective, predominantly because of poor practices by the creator and owner of the password. To date, many of the breaches we read about on a daily basis are the result of passwords being weak and/or the use of a single password across multiple services. The greatest weakness of a password by itself is that once obtained, no other mechanism exists to stop its usage.

Authentication Methods

In order to mitigate this weakness, it became clear that a password alone is not sufficient; thus, multifactor authentication (MFA) was born. Some users are familiar with this terminology while others may not be aware of what it means. Multifactor authentication employs the concept of having any two of the three methods below work in combination with one another in order to authenticate an individual and grant access.

These methods for authentication are:

1. **Something you are** – Biometric feature, e.g., iris scanner, thumb print, facial recognition.
2. **Something you have** – Component only a specific individual should have in their possession, e.g., Google Authenticator App code, DUO code, YubiKey, etc.
3. **Something you know** – Specific knowledge that only the individual knows, e.g., a password, passphrase, security question, etc.

Unbeknown to many, when you withdraw cash from an ATM, you are in effect using MFA. The PIN is something you know, and the card is something you have. The only way to access your account is with the combination of the two. Having one without the other is useless.

Many companies utilize MFA. The adoption has accelerated over the years as a result of the pandemic-induced remote work shift, and cyber insurance now mandating it as a condition of coverage. Surely this means that the company is safe when MFA is deployed? Unfortunately, that is not the case. While MFA is important, it alone is no longer sufficient. Cybercriminals have been able to find multiple ways to bypass MFA. As more companies have adopted MFA, so have the tactics to bypass it.

Bypassing MFA

The current known methods that attackers are using to bypass multifactor authentication are:

- ***Social Engineering*** is the act of tricking an unsuspecting user, through emotional hooks, into taking an action, e.g., supplying privileged information (password), utilizing a fictitious login site,

or downloading a malicious file. Social engineering is one of the primary ways that cyber criminals will bypass MFA in combination with some of the other methods described below. Cybersecurity awareness training and phishing testing remains the primary defense mechanism.

- ***Consent Phishing*** is a form of social engineering and is designed to trick users into granting permissions to malicious cloud applications. These malicious applications can then gain access to legitimate cloud services and data of users. Unlike credential compromise, threat actors who perform consent phishing target users who can grant access to their personal or organizational data directly. The consent screen displays all permissions the application receives. Most users do not read and interpret the access level being requested and just click accept, allowing MFA to be bypassed. Organizations can prevent this attack by removing the employee's ability to download and/or consent to applications that are not approved and managed by the organization.

- ***Brute Force*** is the method of repeatedly trying different permutations of one-time codes, in combination with the identified password, until a successful combination is received. This has become more of a difficult method in multifactor bypass due to the one-time passcode length. However, should a service or system require a passcode short in length (a PIN of four characters) which allows for an finite number of entry attempts, then that system may be vulnerable to a brute force attack with regard to multifactor authentication. In this scenario, the organization relies on its head of IT, or security team, to perform their due diligence by ensuring that any PIN that is required for MFA is longer than four characters and that the application being utilized restricts the organization's employees from having the capability of changing that requirement.

- ***Generated Token Recovery Keys*** are produced when multifactor authentication is implemented on an account. These keys are preauthorized one-time-use PINS utilized in case there are any issues where the device used to generate the one-time code is no longer available. When this option is available, employees tend to take screenshots or keep these keys available in plain text on their desktop and/or in their documents folder. An attacker who compromises a machine could potentially find this key and bypass multifactor authentication when discovering said file. Organizations either need to block this method and require IT to be contacted, or, if necessary, provide employees with a password manager such as 1Password, NordPass or Bitwarden to contain these types of recovery keys.

- ***Session Hijacking*** works by stealing a user's established session. This is primarily performed by implementing what is known as a "man in the middle" attack. The cybercriminal will trick (socially engineer) the user to logging into a legitimate-looking site under the control of the cybercriminal. As the user logs into the malicious site, behind the scenes the credentials are being sent to the legitimate site. This allows the authentication to function as normal. After the user has entered their credentials and provided their second factor, a legitimate session is established with the real website. The session is then hijacked by the cybercriminal. Since the session is already authorized, no additional authentication is required.

  Organizations can defend against this by training against social engineering attacks as described above or adopting YubiKeys. Yubikeys are effectively another factor that will only work when it verifies it's communicating with the legitimate site. This removes the ability for a man in the middle type of attack.

- ***SIM Swapping*** is the process in which a cybercriminal contacts the target's cell phone provider and persuades them to move the target's cell phone number to their own device. This means that they will receive all calls, texts and/or push MFA type of notifications. This allows the attacker to obtain any MFA tokens, texts and/or calls required to verify the second factor of authentication for the targeted user. Furthermore, any business accounts tied to that phone are now compromised by the attacker. To prevent this, organizations and individuals should contact their mobile provider and establish a secret PIN or code which they must provide before porting or transferring over their number to a new device will be authorized.

- ***MFA Fatigue*** is initiated when authenticator apps are utilized, such as Google Authenticator. An option for the second factor is known as a "push" notification. This is when a person logs in and the second factor is sent to a device in the form of a question to allow the connection and verify it is you who authorized it. Attackers had adopted tactic-run automated programs or scripts that attempt to log in with stolen credentials on a consistent basis, thus causing endless "push" notifications to pop-up on the employee's device asking to grant access. To stop the barrage of notifications, people will simply accept the push, granting the person access. To prevent this, train your employees to be aware of the tactic, but also, configure your MFA application to block multiple phish attempts in a defined period from a single site.

Be Aware and Be Ready

Attacks will continue to evolve, and we will continue to be in a cat and mouse game. As artificial intelligence and quantum computing move into the landscape, new threats will surely enter the playing field. What is critical is that you continue to be aware of the threats and adopt the necessary policies, practices, procedures and tools needed.

Contact Us

As your trusted advisor, PKF O'Connor Davies will be here to keep you informed and, if needed, lend a helping hand. Contact your engagement team or either of the following specialists:

David Plutner
Manager
Cybersecurity and Privacy Advisory
dplutner@pkfod.com | 646.449.6365

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Partner
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com | 646.449.6353