5 Multi-Factor Authentication Vulnerabilities and how to fix them

Multi-Factor Authentication (MFA) elevates cybersecurity standards by requiring users to prove their identity in multiple ways before accessing the network.

Hackers can bypass the unique authentication process of providing a username and password, such as through phishing or identity theft. The second verification method is a useful way to confirm that the user is genuine.

While multi-factor authentication tightens security and access, it also has a number of vulnerabilities that cybercriminals can exploit. So what are these vulnerabilities and how can you prevent them?

1. SIM Swap Attack

In a SIM Swap attack, an intruder impersonates you and asks network providers to transfer your phone number to another SIM he owns.

Once the network provider initializes the port, the attacker will start receiving all your messages and notifications. They will try to log into your account and enter the verification code that the system sends to their number.

You can prevent a SIM Swap attack by asking your network provider to create a port block on your account so that no one can do this to your number, especially over the phone. You can also add a means of authentication other than SMS. Device-based authentication where the system sends a code to a specific mobile device that you connect to your account is sufficient.

2. Channel Hijacking

Channel Hijacking is a process in which a hacker hijacks a channel, such as your mobile phone, app, or browser by infecting it with malware. An attacker can use the Man-in-the-Middle (MitM) hacking technique to eavesdrop on your communications and get all the information you transmit on that channel.

If you set up your MFA authentication on a single channel, after a threat agent intercepts that authentication, they can access and use the MFA code received by the channel.

You can limit the ability of cybercriminals to exploit your MFA by channel hijacking by using a virtual private network (VPN) to hide your IP address and restrict the browser to only go to HTTPS sites. safer.

3. OTP-based attack

A one-time password (OTP) is a code that the system automatically generates and sends to users trying to log in to the application to verify their identity. A network attacker who cannot provide an OTP will not be able to log into said network.

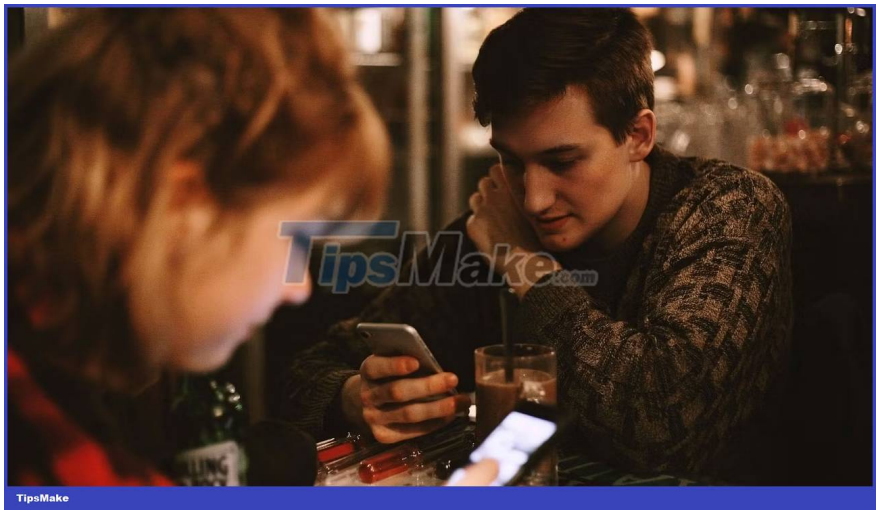
A cyber-threat actor uses a way of hijacking OTP-containing media so that they can gain access. The mobile device is usually the device that receives the OTP. To prevent OTP-based vulnerabilities in MFA, implement a Mobile Threat Defense (MTD) system to identify and stop threat vectors that could expose authentication codes.

4. Real-time phishing attack

Phishing is the process of enticing gullible victims to provide their login information. Cybercriminals deploy phishing attacks to bypass MFA through proxy servers. They are clones of the original servers.

These proxy servers require users to verify their identity through an MFA method that can be obtained on legitimate servers. Once the user provides the information, the attacker will use it on the legitimate website immediately, i.e. while the information is still valid.

5. Recovery Attack



Recovery attack refers to a situation where a hacker takes advantage of you forgetting your credentials and tries to recover them to gain access. When you initiate action to go through the recovery process through alternative means, they interfere with those means to access the information.

An effective way to prevent Recovery attacks is to use a password manager to store passwords, so you don't forget them, and use recovery options.

Multi-factor authentication can be vulnerable, but still strengthens the security of your account access points. Intruders cannot gain access just by bypassing basic username and password authentication on the app if you have MFA enabled.

To make the system more secure, implement multiple authentication layers on different devices and systems. If an attacker hijacks a specific device, they also need to take control of other devices to bypass complete MFA authentication.

You finished reading the article "**5 Multi-Factor Authentication Vulnerabilities and how to fix them**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
