# How Your MFA Can Be Hacked

Usually when writing about how something can be hacked, you run the risk of accidentally creating a tutorial for aspiring hackers. When it comes to password-based multi-factor authentication (MFA), which relies on easily hackable credentials as the first factor, this is not the case since these methods of hacking are so far from being zero-day exploits that some have been around for decades. This paper serves as a warning to those relying on password-based MFA—since bad actors are already well aware of everything we will discuss.

The commonality between these hackable MFA solutions is that they still rely on a password as a first factor. Since passwords are insecure, the entire authentication process that relies on them will be insecure. For a hacker, these MFA solutions, which include one-time codes, SMS-confirmation, mobile push notifications, and "security" based questions, are equivalent to protecting a screen door with another screen door. It adds inconvenience to the hacker (and also the user) but not much security.

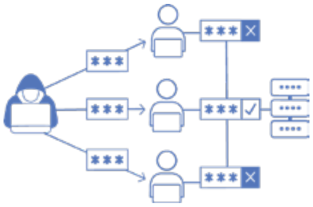
## Hacking MFA via Phishing Email

Multi-factor authentication is often adopted as a response to phishing attacks targeting users to give up their username/password. However, phishing attacks can be just as effective against organizations using multi-factor authentication as those without. The hacker just needs to phish one additional password or pin out of the user, which can be done with a spoofed landing page that requests the confirmation code and then enters it on the back end to the real landing page. This is equally as effective against both in-band or out-of-band authentication methods.

You can read an example of a widespread phishing campaign that utilized this method on Google, Yahoo, and ProtonMail accounts here.

## Hacking MFA via SIM Swap

What if the hacker didn't need to get the second-factor of authentication from you? What if they could have the 2FA code sent directly to them when they try to login? When a mobile phone is used to receive the code, SIM swapping techniques in which they essentially turn their phone into yours they can do just that. All it requires is a call to the phone company and a bit of social engineering and your number can be given to them. They never have to even be in the same continent as you to essentially steal your phone.
You can read the FBI warnings surrounding this method of MFA bypass here.



## Hacking MFA via Man-in-the-Middle Attack

A man-in-the-middle attack is exactly what it sounds like. The hacker places a proxy between the client and the server, intercepting everything the user types until the access token is granted. Once access is granted, the hacker enters undetected. This is also referred to as session hijacking and if you want to see a live example of how it works, KnowBe4's Chief Hacking Officer made an eye-opening video demonstrating the technique here.

## Hacking MFA via Man-in-the-Endpoint Attack

This type of attack relies on installing malware on the endpoint device that is capable of starting rogue sessions in the background once you have authenticated. Imagine logging into your corporate HR platform to request time-off and a hidden session is started that is only visible to the hacker who then proceeds to change the bank account to which your paychecks are routed.

## Hacking MFA by Rebuilding the Passcode Generator

The one-time use passcodes generated by MFA solutions are often generated by an algorithm based on a seed number. Although one of the more difficult methods, hackers have been able to reverse engineer the algorithm and seed number to accurately generate the one-time codes themselves. This is the equivalent of measuring a keyhole in order to build a key that will unlock it. This may sound far-fetched but hackers once got their hands on RSA's seed values and were able to reverse engineer the algorithm to breach Lockheed Martin.

## A Continuous Work in Progress

This list will never be completely inclusive. While these are the major categories of hacks that are able to bypass MFA, this list is growing on a near daily basis. Each individual MFA provider has their own unique vulnerabilities and zero-days that are being discovered. Hackers are constantly finding new ways to bypass MFAs of all types since they are merely a band-aid to an underlying weak authentication, the password. The takeaway from this is that adding new factors can't solve the security issue if the base factor, the password, remains.

## Beyond Identity

Beyond Identity is fundamentally changing the way the world logs in–eliminating passwords and all phishable factors to provide users with the most secure and frictionless authentication on the planet. Our invisible, passwordless MFA platform enables companies to secure access to applications and critical data, stop ransomware and account takeover attacks, meet compliance requirements, and dramatically improve the user experience and conversion rates. Our revolutionary zero-trust approach to authentication cryptographically binds the user's identity to their device, and continuously analyzes hundreds of risk signals for risk-based authentication. For more information on why Snowflake, Unqork, Roblox, and IAG use Beyond Identity, check out www.beyondidentity.com.