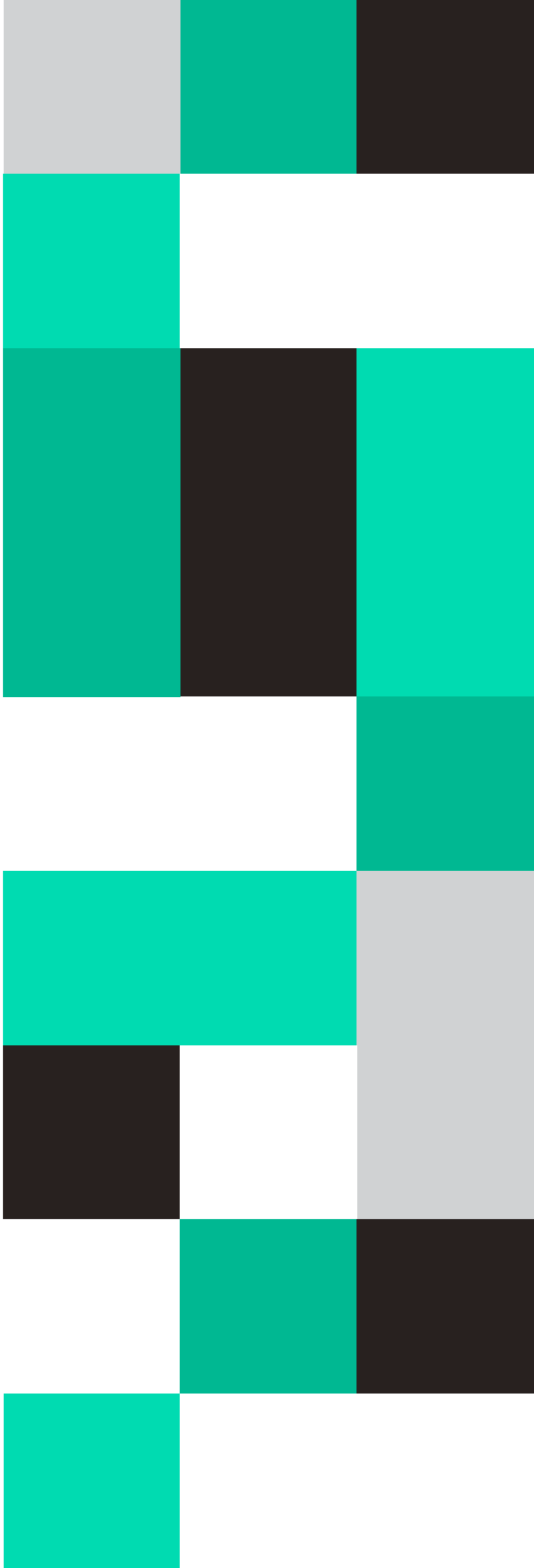
GUIDE

MFA BYPASS 101

How Cybercriminals **Combine Attack Methods and Stolen Identity Data** to Sidestep Multi-Factor Authentication



SpyCloud

Table of Contents

A decade ago, MFA was heralded as a "magic bullet" that would make it much harder for criminals to break into an account. Today, it's just another hurdle for determined bad actors, who have developed an ever-growing list of ways to bypass it.

WHAT IS MFA?

Any discussion of MFA must begin with passwords, which, despite their flaws, haven't diminished in popularity. Collectively, people have a habit of creating easy-to-guess passwords and reusing them across multiple accounts. To criminals, this is like leaving house keys in the lock on the front door – gaining access couldn't be easier.

Around a decade ago, security experts responded by encouraging organizations to embrace MFA. Designed as a security enhancement to the standard username/password combo, MFA required users to present two pieces of evidence before logging into an account.

Today, acceptable evidence, or "factors," generally amount to two of the following three categories:

SOMETHING YOU KNOW
a password, PIN, or passphrase

SOMETHING YOU HAVE
a smartphone or physical token

SOMETHING YOU ARE
your fingerprint or face

The obvious benefit of MFA is additional layers of protection. The idea is that more factors should make it harder for a potential intruder to gain access to accounts, systems, or data. MFA can also help organizations achieve and maintain compliance, which can reduce liability concerns. But like all cybersecurity measures, it has its shortcomings.

- **Adoption isn't universal:** According to **Okta's Secure Sign-in Trends Report**, only 66% of workforce users are using MFA and it varies greatly by country. That's because in many MFA implementations, passwords are still necessary. So now in addition to having to manage the password, users have to manage the additional layer of security.
- **Some users will accept any MFA request:** Sometimes criminals don't even need to socially engineer someone into helping them. Members of SpyCloud's Customer Advisory Board have shared that some of their users will accept any MFA request, even if they're not currently trying to log into anything. A big part of this could be attributed to MFA fatigue, by which users just go through the motions and let their guard down, allowing attackers to capitalize.

STOLEN CREDENTIALS AND COOKIES ARE FUEL FOR BYPASSING MFA

According to **Microsoft's research**, accounts are "more than 99.2% less likely to be compromised if you use MFA."

But this doesn't take into consideration the impact of already-stolen credentials, which are widely available on underground marketplaces and forums, and serve as the initial access vector in **22%** of breaches.

To give you an idea of what's available to criminals, in our recent **Identity Exposure Report**, security researchers at SpyCloud analyzed more than 2.2 billion credential pairs recaptured from data breaches, phishing attacks, and malware-infected device logs. When looking to bypass MFA on their way to account takeover (ATO), these credentials are of high value to criminals for a few reasons:

- Rampant password reuse means if a criminal has login info for one of your accounts, they can assume you use the same password (or a close variation) for other accounts. SpyCloud's research shows an alarming **70%** of users exposed in breaches reused previously exposed passwords.
- So much of our PII is shared willingly on social media that criminals can use it to guess answers to common MFA security questions (place of birth, high school mascot, etc.).
- Access to stolen phone numbers makes it easy for SIM-swapping to occur, where criminals intercept MFA codes sent via text message.

Criminals are also stealing billions of active session cookies

to use in session hijacking attacks, ***with more than***

17 BILLION COOKIES

recaptured from malware logs on the dark web last year alone...

Our research shows the criminal use of infostealer (information-stealing) malware is rampant, with nearly 50% of corporate users having been victimized by infostealer malware at some point in their digital history. Once user devices are infected, system information is exfiltrated, exposing details ranging from login credentials and browser history to geolocation data, autofill info, and – notably – session cookies.

Exposed session cookies can be used to completely bypass authentication and fraud controls, including MFA. With the recent effectiveness of large-scale infostealer attacks, and the corresponding capabilities to bypass MFA completely, stolen cookies are now as valuable, if not more so, than stolen login credentials.

MFA BYPASS METHODS

Cybercriminals can now easily, frequently, and cleverly get around MFA – and you can imagine how damaging a single successful bypass can be. While these attacks can take on many technical methods or combinations of methods, it's safe to assume that attackers already have user authentication data.

SESSION HIJACKING OR COOKIE HIJACKING

Session hijacking is a method criminals use to take over a user's web session without the need to authenticate via login credentials, MFA, or passkeys. When a user successfully logs into a web application (with one factor, two factors, or ten factors), the server sets a temporary session cookie in the browser. This allows the remote server to remember that you're logged in and authenticated. Cybercriminals steal session cookies in a variety of ways, including:

- Infostealer malware
- Man-in-the-middle (MiTM) attacks or adversary-in-the-middle (AiTM) attacks, using phishing kits like **Tycoon 2FA**
- Tricking the user into clicking a malicious link that contains a prepared session ID

With the **stolen cookie** and an anti-detect browser, the attacker can take control of the already-authenticated session in their own browser – the system is fooled into thinking that the attacker's connection is the same as the real user's original session.

Once the attacker has hijacked the session, they can do anything that the original user is authorized to do. Depending on the targeted website, this can mean fraudulently purchasing items, accessing detailed personal information that can be used for identity theft, stealing confidential company data, or draining a bank account. Session hijacking can also be an easy way to launch a ransomware attack, as a criminal can hijack the session of a company VIP, and then access and encrypt valuable company data.

BRUTE FORCE ATTACKS

Brute force attacks are less about trickery and more about trial-and-error. With the aid of automation tools, attackers will rapidly generate and plug in combinations until they find the right one – which can entail thousands or even millions of attempts per second. These attack methods are most commonly used against SMS and text-based MFA, where attempt limits are often not set by default.

FORGING RECOGNIZED DEVICES

Many times, an application will not require MFA from a device where users have logged in before. This is sometimes called adaptive multi-factor authentication (aMFA). In this case, attackers can try to figure out how the application recognizes a device and forge the signature of a recognized or "trusted device." For example, if a site marks recognized devices by using a predictable cookie, attackers can add that cookie value to their requests.

PHISHING EMAILS AND TEXTS

One of the oldest types of cyber tactics, phishing has evolved over the years but the goal remains the same – to trick an email or text recipient into believing that the message is something they want or need and to click a link or download an attachment. In MFA bypass attacks, these can involve technical support scams in which criminals convince users to install software that allows a "tech support expert" to log in remotely to solve their issue. In other phishing attacks, unsuspecting users are presented with a login experience that looks normal, but is actually a fake site that captures their authentication codes and user credentials. Misleading SMS messages, or "smishing," are also increasingly common in recent years, with cleverly worded texts designed as urgent support messages or prizes to claim with a link that directs to a malicious website or forces a malware download.

According to recent SpyCloud research

94% OF FORTUNE 50 COMPANIES

have had employee data exposed in a phishing attack.

STEALING ONE-TIME PASSWORDS

When MFA requires "something you own," it usually means your mobile device, hardware security key, or email account. These devices and accounts enable the use of one-time passwords (OTPs) as the secondary authentication factor, which are generated for a limited period and serve as an additional factor in the authentication process.

One method that gets around the use of OTP as a factor for authentication goes back to phishing. One such phishing scam begins when the victim lands on a spoofed website. The first step will be to steal their credentials ("what they know"), and then the scam will be initiated behind the scenes without the victim's knowledge. A direct authentication process against the targeted website or login portal using the stolen credentials will initiate a request for the OTP that will lead to a token being sent to the victim's device.

The victim is now connected to the phishing website and unaware that it is a scam. They will willingly provide their OTP token to the phishing website, which gives the scammers the ability to take over their account.

SIM SWAPPING

Despite education advising otherwise, many services still offer SMS text messaging for MFA. At this point, criminals have figured out ways to infiltrate cellular carrier networks, where with knowledge of the victim's cell phone company, they can easily perpetrate SIM swapping attacks.

In a SIM swapping attack, typically the attacker calls the phone companies' customer service department and finds someone who is willing to provide information to complete the SIM swap. Once the attacker has control over the customer's phone number, they call the bank to request a wire transfer from the victim's accounts to another account they own. The bank, recognizing the phone number as belonging to the customer, does not ask for full security questions but instead requests a one-time code sent to the phone number from which the attacker is calling.

ANSWERING SECURITY QUESTIONS

If you've ever had to have your MFA reset or turned off temporarily because you've gotten a new phone, for example, personally identifiable information (PII) is often used to prove that you are who you say you are. But PII is constantly exposed in data breaches, and we also give it away on social media – your pet's name, the last time you bought a car, how many kids you have, etc. All manner of data is out there and has been exposed either willingly or via breaches and it doesn't take much for a criminal to connect the dots and use our PII to circumvent MFA.

PREVENTATIVE MEASURES

Think about account security like a home alarm. With a home alarm system, we place sensors on the doors and windows in an effort to slow intruders – but what happens when they don't trip those sensors? The motion detectors are the failsafe.

MFA is an important first step, but if a user logs in with valid credentials, the organization has no way to determine if the user is a criminal because they trip no sensor. Additional layers of security are required to safeguard the identities of the employees, consumers, and suppliers logging into your systems.
Although it's clear that attackers can circumvent MFA through social engineering and technical attacks, that doesn't mean you shouldn't use it. Any implementation of MFA should be predicated on the fact that it can be penetrated and does require additional considerations. Among them:

CONTINUOUSLY MONITOR FOR COMPROMISED CREDENTIALS & COOKIES

It only takes one errant click, stolen credential, or stolen session cookie for the bad guys to break in and take over an account. The ability to know which of your users' credentials or cookies have been exposed and quickly remediate those exposures is critical to mitigating the risk of breaches and fraud.

IMPLEMENT CONTINUOUS ZERO TRUST VERIFICATION

With the spread of today's workforce and complexity of IT environments, between remote worker security and the number of devices and accounts being used, security teams need to enforce **Zero Trust policies** that require continuous identity verification, so nothing or no one slips through the cracks. Pre-auth and mid-session "policy decision points" and "access decisions" that not only reverify that users are who they say they are, but reevaluate sessions for any potential exposures along the way to malware, phishing, or third-party breaches. These real-time insights can be synced with automated exposure remediation to streamline security resources, reduce analyst fatigue, and optimize response times.

INSTALL ANTIVIRUS AND ANTI-MALWARE SOFTWARE

With the barrier to entry lower than ever for cybercriminals through commoditized tools like malware-as-a-service (MaaS) and AI, there is no better time to step up your malware protection and overall cybersecurity than now. Trusted antivirus software could help protect your devices against malware attacks threatening your organization and valuable information. With that said, SpyCloud research shows **66% of malware infections** occur on devices with endpoint detection solutions or antivirus software, so additional efforts are necessary.

EDUCATE USERS

It is critical to be aware that some MFA technologies are not fully protecting users from scams that compromise their accounts. This is bad news for individuals, but it can have severe consequences for organizations. All it takes is one employee to accept an illegitimate MFA push and the attacker has full account access. And with more individuals working remotely and potentially accessing professional tools and sites from personal devices, it's imperative that employees understand the risk of these infiltrations and that organizations have mitigation efforts in place to combat them.

SHIFT TO A HOLISTIC IDENTITY THREAT PREVENTION APPROACH

Across an organization's employees, contractors, customers, suppliers, and even non-human accounts, there are inevitable exposures on the dark web that your security tools won't catch – that can create a back alley for criminals to target a business. For complete coverage of the "entire digital identity," your company should adopt **a holistic identity lens** that captures and ties together data from each individual's many online personas – across time and systems, including both managed and unmanaged devices – and automates remediation that stops attacks by making stolen data useless.

We recommend bolstering your cybersecurity program with SpyCloud's

ENTERPRISE PROTECTION
and **CONSUMER RISK PROTECTION** solutions

so you are alerted when accounts are compromised very early in the breach lifecycle (before criminals can exploit them for the forms of MFA bypass mentioned above), and so you can remediate exposures proactively.

Ultimately, there is no one "magic bullet" for cybersecurity. Implementing **NIST guidelines**, which include MFA operating in parallel with continuous monitoring for exposed credentials, allows organizations to easily pivot if fraud trends change or a new threat emerges.

"Our customers are everything to us. We have a core value around protecting them at all costs. So by adding Session Identity Protection to the rest of our SpyCloud instance, we basically get rid of the threat of account takeover, whatever the source – which means our customers and their data are safe."

SEE HOW ATLASSIAN USES SPYCLOUD TO PREVENT MFA BYPASS >

FIND OUT WHY CUSTOMERS CHOOSE SPYCLOUD >

The SpyCloud Difference

SpyCloud transforms recaptured darknet data to disrupt cybercrime. Its automated identity threat protection solutions leverage advanced analytics and AI to proactively prevent ransomware and account takeover, detect insider threats, safeguard employee and consumer identities, and accelerate cybercrime investigations. SpyCloud's data from breaches, malware-infected devices, and successful phishes also powers many popular dark web monitoring and identity theft protection offerings. Customers include eight of the Fortune 10, along with hundreds of global enterprises, mid-sized companies, and government agencies worldwide. Headquartered in Austin, TX, SpyCloud is home to more than 200 cybersecurity experts whose mission is to protect businesses and consumers from the stolen identity data criminals are using to target them now.

Discover how much data SpyCloud has recaptured for your domain.
Once you know, you can take action.

SEE YOUR COMPANY'S RISK >