Phishing, Smishing and Vishing
(How these cyber attacks work and how to prevent them?)

Okan YILDIZ
Murat Can ASLAN

Smishing and vishing: How do these cyber-attacks work, and how to prevent them?

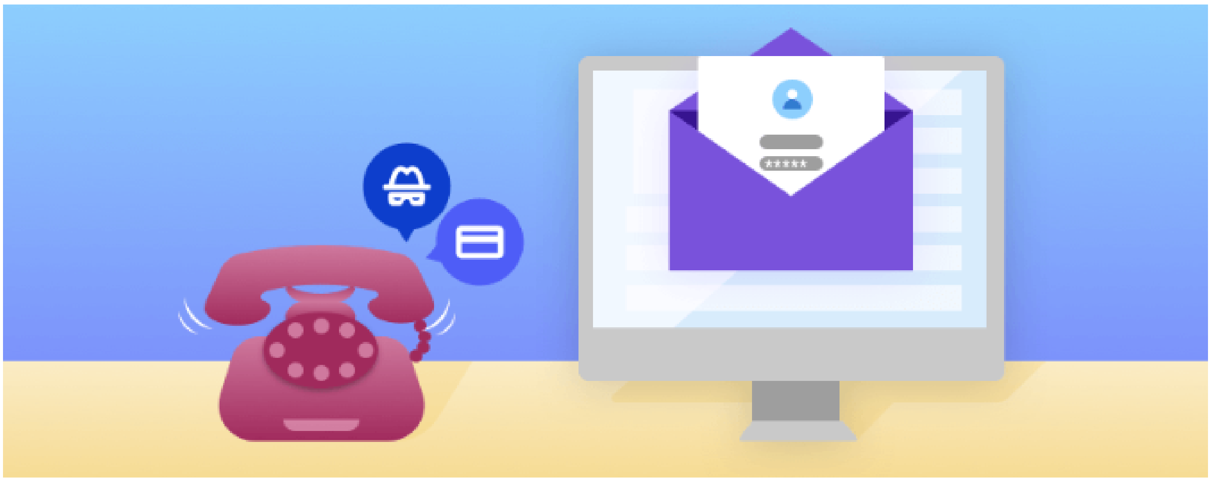
As scammers aim to manipulate people into handing over sensitive data, phishing attacks are expanding into new channels and growing even more sophisticated.

Smishing and vishing are phishing attacks that lure victims via SMS messages and voice calls. Both rely on the same emotional appeals employed in traditional phishing scams and are designed to drive you into urgent action. The difference is the delivery method.

“Cyberthieves can apply manipulation techniques to many forms of communication because the underlying principles remain constant,” explains security awareness leader Stu Sjouwerman, CEO of KnowBe4. “Lure victims with bait and then catch them with hooks.”

What is phishing?

As with real fishing, there's more than one way to reel a victim: Email phishing, smishing, and vishing are three common types. Phishing is an attack in which the threat actor poses as a trusted person or organization to trick potential victims into sharing sensitive information or sending them money. Some attackers take a targeted approach, as is the case with spear phishing or whale phishing (more on the types of phishing below).



How does a phishing attack work?

- Phishing attacks begin with the threat actor sending a communication, acting as someone trusted or familiar. The sender asks the recipient to take action, often implying an urgent need. Victims who fall for the scam may give away sensitive information that could cost them. Here are more details on how phishing attacks work:
- The sender: In a phishing attack, the sender imitates (or "spoofs") someone trustworthy that the recipient would likely know. Depending on the type of phishing attack, it could be an individual, like a recipient's family member, the CEO of the company they work for, or even someone famous who is supposedly giving something away. Often phishing messages mimic emails from large companies like PayPal, Amazon, or Microsoft, and also banks or government offices.

- **The message**: Under the guise of someone trusted, the attacker will ask the recipient to click a link, download an attachment, or to send money. When the victim opens the message, they find a scary message meant to overcome their better judgment by filling them with fear. The message may demand that the victim go to a website and take immediate action or risk some sort of consequence.
- **The destination**: If users take the bait and click the link, they're sent to an imitation of a legitimate website. From here, they're asked to log in with their username and password credentials. If they are gullible enough to comply, the sign-on information goes to the attacker, who uses it to steal identities, pilfer bank accounts, and sell personal information on the black market.

Who is targeted by phishing?

A phishing attack can target anyone, but some types are done to particular people. Some threat actors will send out a general email to many people, hoping a few will take the bait based on a common trait. An example would be saying something is wrong with your Facebook or Amazon account, and you need to click this link right away to log in and fix it. The association could lead to a spoofed web page where you might give away your login credentials.

Threat actors use more targeted phishing attacks if they are after something specific, like access to a particular company's network or data or information from a politician or political candidate. In this case, they may research information to make their attack sound familiar and credible, so the target is likely to click a link or provide information. An example would be studying the name and communication style of a target company's CEO, then emailing or texting specific employees at that company pretending to be the CEO asking for something. This is called spear phishing.

While threat actors often pretend to be CEOs in their phishing attacks, sometimes the target is the CEO themself. "Whale phishing" describes phishing attacks toward high-profile people like company executives, celebrities, or well-known wealthy individuals. Whether an attack is general or highly targeted, sent to one person or many people, anyone can become a phishing target, so it's essential to.

Types of phishing attacks

Despite their wide varieties, the common denominator of all phishing attacks is their use of a fraudulent pretence to acquire valuables. Some major categories include:

Email phishing

Email phishing is one of the most common types of phishing. It has been widespread since the early days of e-mail. The attacker sends an e-mail purporting to be trustworthy and familiar (online retailer, bank, social media company, etc.) and asks you to click a link to take significant action or download an attachment.
Some specific examples of e-mail phishing include:

- Business e-mail compromise (BEC): A business e-mail compromise (BEC) attack targets someone in the finance department of an organization, often the CFO, and attempts to deceive them into sending large sums of money. Attackers often use social engineering tactics to convince recipients that sending the money is urgent and necessary.
- Clone phishing: In this attack, criminals make a copy—or clone—of previously delivered but legitimate e-mails that contain either a link or an attachment. Unsuspecting users either click the link or open the attachment, often commanding their systems. Then, the phisher replaces the links or attached files with malicious substitutions disguised as the real thing. Then the phisher can counterfeit the victim's identity to masquerade as a trusted sender to other victims in the same organization.
- 419/Nigerian scams: A verbose phishing e-mail from someone claiming to be a Nigerian prince is one of the Internet's earliest and longest-running scams. This "prince" either offers you money but says you need to send him a small amount first to claim it, or he says he is in trouble and needs funds to resolve it. The number "419" is associated with this scam. It refers to the section of the Nigerian Criminal Code dealing with fraud, charges, and penalties for offenders.

Vishing (voice call phishing)

With phone-based phishing attempts, sometimes called voice phishing or “vishing,” the phisher calls claiming to represent your local bank, the police, or even the IRS. Next, they scare you with some problem and insist you clear it up immediately by sharing your account information or paying a fine. They usually ask that you pay with a wire transfer or prepaid cards, so they are impossible to track.

Smishing (SMS or text message phishing)

SMS phishing, or “smishing,” is vishing's evil twin, carrying out the same kind of scam (sometimes with an embedded malicious link to click) by means of SMS texting.

Catphishing

Catfishing (spelled with an “f”) is a kind of online deception wherein a person creates a presence in social networks as a sock puppet or a fictional online persona for the purpose of luring someone into a relationship—usually a romantic one—in order to get money, gifts, or attention. *Catphishing* (spelled with a “ph”) is similar, but with the intent of gaining rapport and (consequently) access to information and/or resources that the unknowing target has rights to.

Spear phishing

Spear phishing attacks a specific person or organization, often with tailor-made content for the victim or victims. It requires pre-attack reconnaissance to uncover names, job titles, email addresses, and the like. The hackers scour the Internet to match this information with other researched knowledge about the target's colleagues and the names and professional relationships of key employees in their organizations. With this, the phisher crafts a believable email.
For instance, a fraudster might spear phish an employee whose responsibilities include the ability to authorize payments. The email purports to be from an executive in the organization, commanding the employee to send a substantial amount either to the exec or to a company vendor (when the malicious payment link sends it to the attacker).
"A verbose phishing email from someone claiming to be a Nigerian prince is one of the Internet's earliest and longest-running scams."

Whale phishing

Whale phishing is what it probably sounds like: Phishing that targets high-profile victims. This can include celebrities, politicians, and C-level businesspeople. Typically, the attacker is trying to trick these well-known targets into giving them their personal information and/or business credentials. Whaling attacks usually involve social engineering efforts to trick the victim into believing the deception.

How to identify a phishing attack?

Recognizing a phishing attempt isn't always easy, but a few tips, a little discipline, and some common sense will go a long way. Look for something that's off or unusual. Ask yourself if the message passes the “smell test.” Trust your intuition, but don't let yourself get swept up by fear. Phishing attacks often use fear to cloud your judgment.

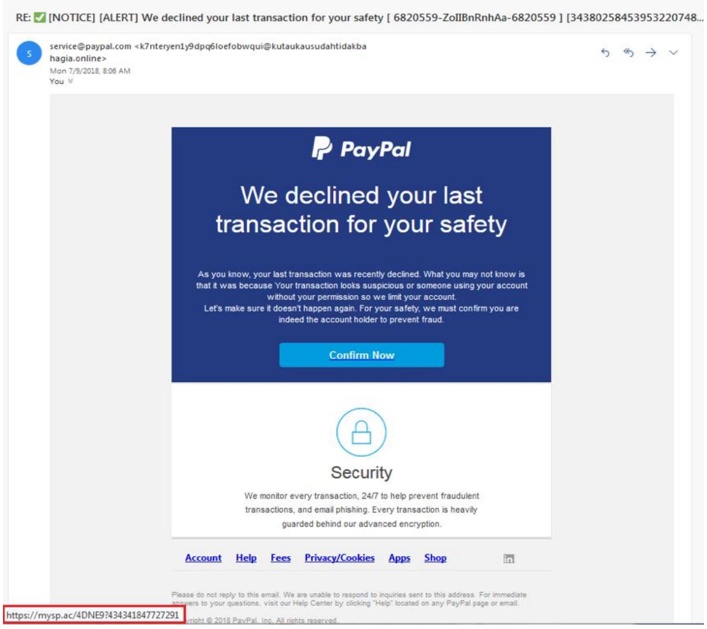
Here are a few more signs of a phishing attempt:

- The email makes an offer that sounds too good to be true. It might say you've won the lottery, an expensive prize, or some other over-the-top item.

- You recognize the sender, but it's someone you don't talk to. Even if the sender's name is known to you, be suspicious if it's someone you don't normally communicate with, especially if the email's content has nothing to do with your normal job responsibilities. Same goes if you're cc'd in an email to folks you don't even know, or perhaps a group of colleagues from unrelated business units.
- The message sounds scary. Beware if the email has charged or alarmist language to create a sense of urgency, exhorting you to click and “act now” before your account is terminated. Remember, responsible organizations do not ask for personal details over the Internet.
- The message contains unexpected or unusual attachments. These attachments may contain malware, ransomware, or another online threat.
- The message contains links that look a little off. Even if your spider sense is not tingling about any of the above, don't take any embedded hyperlinks at face value. Instead, hover your cursor over the link to see the actual URL. Be especially on the lookout for subtle misspellings in an otherwise familiar-looking website, because it indicates fakery. It's always better to directly type in the URL yourself rather than clicking on the embedded link.

Examples of phishing attempts

Here's an example of a phishing attempt that spoofs a notice from PayPal, asking the recipient to click on the “Confirm Now” button. Mousing over the button reveals the true URL destination in the red rectangle.



RE: ✅ [NOTICE] [ALERT] We declined your last transaction for your safety [6820559-ZoIIBnRnhAa-6820559] [34380258453953220748...

service@paypal.com <k7nteryen1y9dpq6loefobwqui@kutaukausudahtidakba
hagia.online>
Mon 7/9/2018, 8:06 AM
You

PayPal

We declined your last transaction for your safety

As you know, your last transaction was recently declined. What you may not know is that it was because Your transaction looks suspicious or someone using your account without your permission so we limit your account.
Let's make sure it doesn't happen again. For your safety, we must confirm you are indeed the account holder to prevent fraud.

Confirm Now

Security

We monitor every transaction, 24/7 to help prevent fraudulent transactions, and email phishing. Every transaction is heavily guarded behind our advanced encryption.

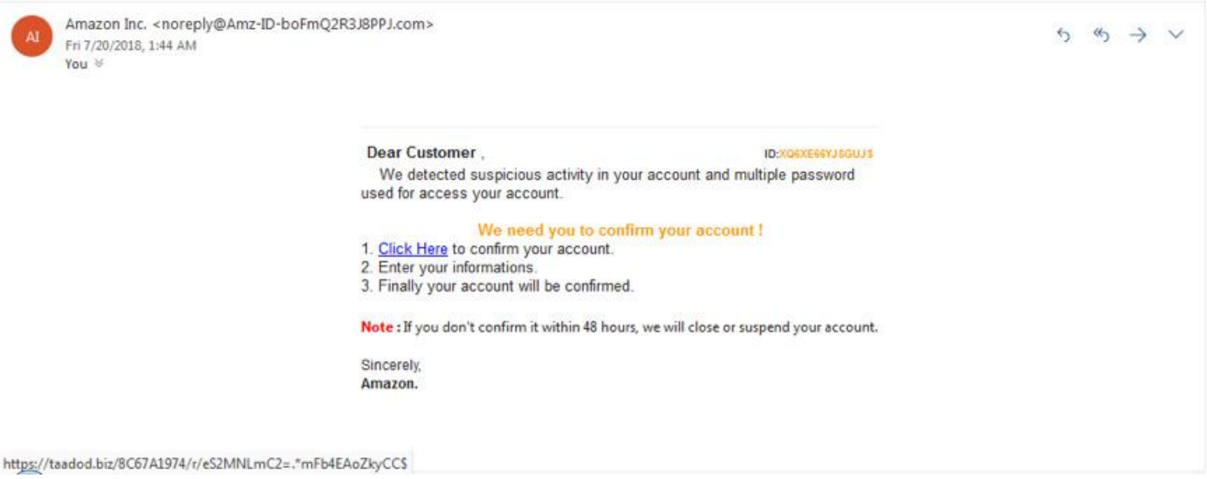
Account Help Fees Privacy/Cookies Apps Shop

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help Center by clicking "Help" located on any PayPal page or email.

https://mysp.ac/4DNE9?434341847727291

yright © 2018 PayPal, Inc. All rights reserved.

Here's another phishing attack image, this time claiming to be from Amazon. Note the threat to close the account if there's no response within 48 hours.



Amazon Inc. <noreply@Amz-ID-boFmQ2R3J8PPJ.com>
Fri 7/20/2018, 1:44 AM
You

Dear Customer , ID:XQ6XE66YJ5GUJ$

We detected suspicious activity in your account and multiple password used for access your account.

We need you to confirm your account !

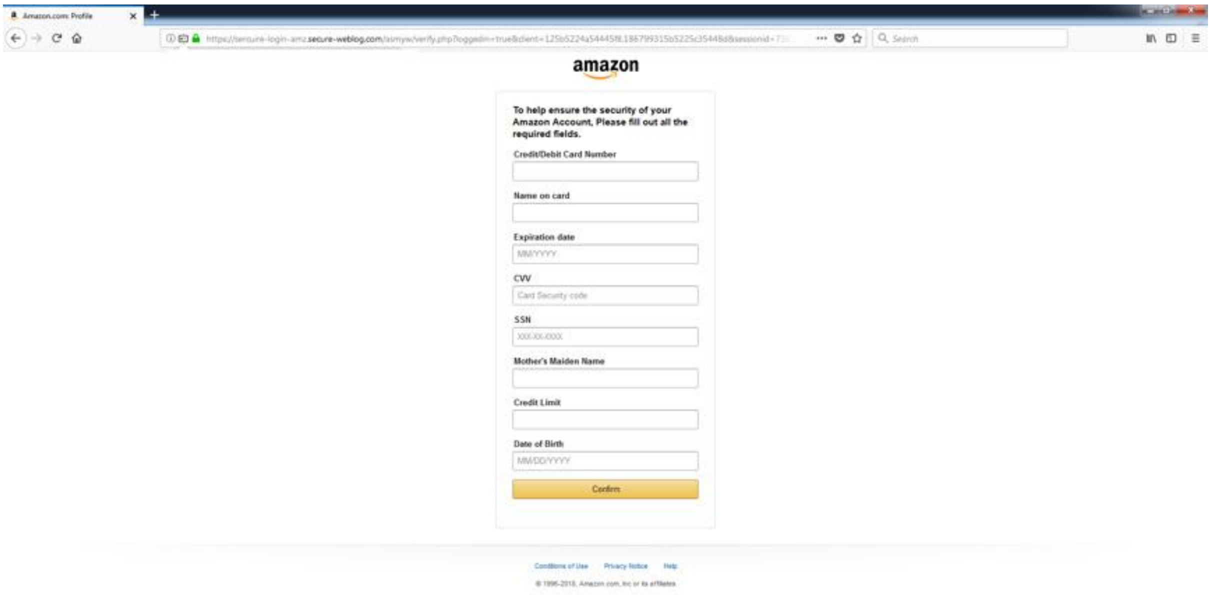
1. Click Here to confirm your account.
2. Enter your informations.
3. Finally your account will be confirmed.

Note : If you don't confirm it within 48 hours, we will close or suspend your account.

Sincerely,
Amazon.

https://taadod.biz/8C67A1974/r/eS2MNLmC2=.*mFb4EAoZkyCC$

Clicking on the link leads you to this form, inviting you to give away what the phisher needs to plunder your valuables:



To help ensure the security of your Amazon Account, Please fill out all the required fields.

Credit/Debit Card Number

Name on card

Expiration date

CVV

SSN

Mother's Maiden Name

Credit Limit

Date of Birth

Confirm

Amazon.com: Profile
https://secure-login-amz.secure-weblog.com/asmyw/verify.php?loggedin=true&client=125b5224a544458.186799315b5225c35448d&sessionid=73
Search
amazon
MM/YYYY
Card Security code
XXX-XX-XXXX
MM/DD/YYYY
Conditions of Use
Privacy Notice
Help
© 1996-2018, Amazon.com, Inc or its affiliates

How do I protect myself against phishing?

As stated previously, phishing is an equal opportunity threat, capable of showing up on desktops, laptops, tablets, and smartphones.

Most Internet browsers have ways to check if a link is safe, but the first line of defense against phishing is your judgement.

Train yourself to recognize phishing signs and practice safe computing whenever you check your e-mail, read Facebook posts, or play your favourite online game.

Once again, from our own Adam Kujawa, here are a few of the essential practices to keep you safe:

- Only open e-mails from senders you are familiar with.
- Only click on a link inside of an e-mail if you know exactly where it is going.
- To layer that protection, if you get an e-mail from a source, you are unsure of, navigate to the provided link manually by entering the legitimate website address into your browser.
- Lookout for the digital certificate of a website.
- If you are asked to provide sensitive information, check that the URL of the page starts with "HTTPS" instead of just "HTTP." The "S" stands for "secure." It's not a guarantee that a site is legitimate, but most legitimate sites use HTTPS because it's more secure. HTTP sites, even legitimate ones, are vulnerable to hackers.
- If you suspect an e-mail isn't legitimate, take a name or text from the message and put it into a search engine to see if any known phishing attacks exist using the same methods.
- Mouse over the link to see if it's a legitimate link.

What is Smishing?

Smishing definition: Smishing (SMS phishing) is an attack conducted using SMS (Short Message Services) on cell phones.
Like email phishing scams, smishing messages typically include a threat or enticement to click a link or call a number and hand over sensitive information. Sometimes they suggest you install some security software, which turns out to be malware.
Smishing example: A typical smishing text message might say something along the lines of, “Your ABC Bank account has been suspended. To unlock your account, tap here: https://bit.ly/2LPLdaU”, and the link provided will download malware onto your phone. Scammers are also adept at adjusting to the medium they’re using, so you might get a text message that says, “Is this a pic of you? https://bit.ly/2LPLdaU” and if you tap that link to find out, once again, you’re downloading malware.

What is Vishing?

Vishing definition: *Vishing (voice phishing) is a type of phishing attack that is conducted by phone and often targets users of Voice over IP (VoIP) services like Skype.*

It’s easy to for scammers to fake caller ID, so they can appear to be calling from a local area code or even from an organization you know. If you don’t pick up, then they’ll leave a voicemail message asking you to call back. Sometimes these kinds of scams will employ an answering service or even a call center that’s unaware of the crime being perpetrated.

Once again, the aim is to get credit card details, birthdates, account sign-ins, or sometimes just to harvest phone numbers from your contacts. If you respond and call back, there may be an automated message prompting you to hand over data and many people won’t question this, because they accept automated phone systems as part of daily life now.

MFA Bypass Techniques: How Does it Work?

Identification and authentication are the first phase of verification in the login processes of Information Systems. Malicious threat actors use various methods, such as **brute force** to pass this phase unauthorized. Authentication solutions are named by the number of factors used in the process. Single-Factor Authentication (SFA) requires only one element (e.g., password) to authenticate the login. The name of the authentication process will turn into **Two-Factor Authentication (2FA)** if two factors (randomly generated code etc.) are required, then named **Multi-Factor Authentication** if more than two elements are needed to verify. Security experts recommend using two or rather Multifactor Authentication (MFA) solutions in login processes.

Additionally, there are two authentication types which are **in-band and out-of-band authentication**. It is called in-band authentication if the identity check is made in the same system or communication channel. A login page requests a security code on the same page is an example of in-band authentication. When the authentication factor is sent over a different system or channel, such as approving the login from another application or entering a pin from a separate location is out-of-band authentication.

What is Multifactor Authentication?

Multifactor Authentication (MFA) is a **security approach** that uses multiple verification methods to authenticate the user to access their profile, system, etc. MFA adds a new layer to the authentication process, strengthening security. Infrastructures and endpoint devices can be safer and more secure using protection methods such as MFA.

Why Do We Need MFA?

Verifying user identity using MFA became essential because threat actors have been using stolen or exploited user credentials, and another layer must deny connection by unauthenticated ones.

We understand that there is a need for another factor, but why do we need "Multi-factor" Authentication? Single-factor Authentication (SFA) requires only one piece of evidence to authorize the user, primarily passwords. Brute force attacks or stealing credentials bypasses the SFA technology; we need another factor to add a layer to this security process.

Multifactor Authentication (MFA) is a technique that requires more than one piece of evidence to authorize the user. If two pieces of evidence are needed to verify, this approach is called **Two-factor Authentication (2FA) or 2-step verification**. It depends if asked how many factors we need to be more secure, but it is known that 2FA or MFA is more secure than SFA. The difference between 2FA and MFA is that 2FA requires only two factors; on the other hand, MFA can add more layers until the login attempts do not seem **suspicious** anymore.

What are the Types of MFA?

There are three main types of Authentication factors that work with MFA:

1. The first is Knowledge Factor (something you know), which is anything the user knows to verify its identity. This could be a password, credit card PIN, or One-time Password (OTPs).
2. Another one is the Possession factor (something you have) which means any tool the user uses to verify itself. It could be a security token such as a smart card, a USB flash drive, a wireless tag, or one of the **mobile authentication methods** such as a mobile app, text message, or an automatic phone call directly to the user.
3. The last MFA factor is called the **Inherence Factor** (something you are), which only the user has to verify biologically. This could be a retina or an iris scan, fingerprint, user's voice, or the user itself to recognize its face.

Top 10 Most Commonly Used MFA Bypass Techniques

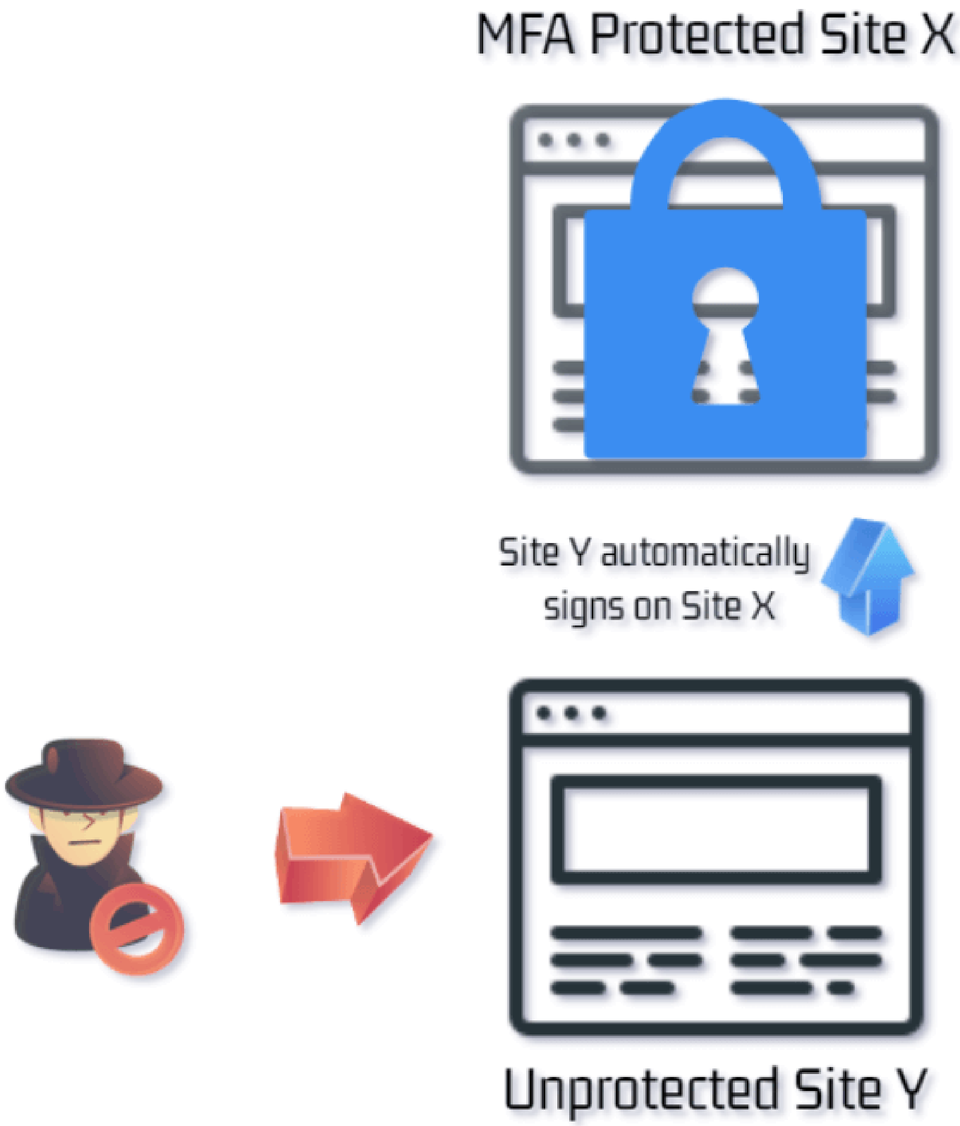
Although MFA is much more secure than other authentication solutions, it can be bypassed by **various techniques**. These techniques can be categorized into three main groups: Social engineering techniques, technical methods, and a mixture of both.

Social Engineering techniques are generally non-technical to MFA itself that exploit human error.

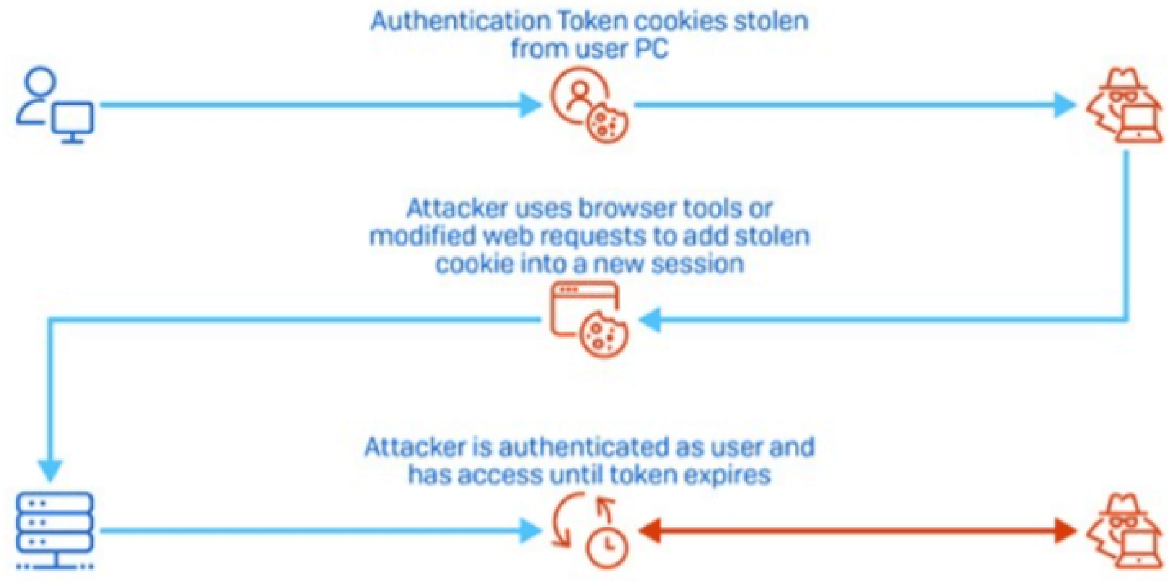
- Stealing the victim’s security/recovery questions’ answers with a fake website using phishing is a widespread technique to bypass the MFA.
- Attackers usually concoct a story (such as the victim losing their phone or being in a hurry to get access) by acting like the victim itself and trying to disable the MFA or gain access by contacting tech support of the firm.

Technical approaches to bypass MFA usually exploit MFA itself or steal credentials using various techniques to eliminate the victim’s MFA.

- Skimming is used in Automated Teller Machines (ATMs) when stealing people’s credit card credentials by directly bypassing Factored Authentication.
- The victim could be using an already hacked device, or the attacker could get admin access. The attacker could do anything that the device’s user can typically do. This technique is known as the **Man-in-the-Endpoint Attack**.
- Attackers also use the single sign-on technique, which uses the sharing authentication systems. If a website that **does not use MFA** is connected with another website that requires MFA to log in, the attacker prefers the one without authentication service to gain access to another.



- Using authorization code flaws (also known as **Response Manipulation or Status Code Manipulation**) to bypass is another common way to eliminate MFA; if the response is like “Success: false,” turning it to “Success: true” may work to bypass or change the status code to 200 (OK) from 401, 402, 403, etc.
- Stealing a victim’s session cookie and bypassing the MFA with the stolen cookie, also known as the **pass-the-cookie attack**, is increasingly used by attackers nowadays.


Authentication Token cookies stolen from user PC
Attacker uses browser tools or modified web requests to add stolen cookie into a new session
Attacker is authenticated as user and has access until token expires

- Some MFA applications use **One-Time Passwords (OTPs)**. OTP displays a randomly generated number from a predetermined “seed value,” and the authentication system waits for the user to enter the code to verify the identity. The attacker can generate its OTP code to bypass the MFA if the attacker accesses this seed value. This process is known as duplicate code generating.
- Another bypass technique is the **SMS Swap scam (Simjacking)**. Usually, people contact the provider to get their SIM information back when their phone is stolen or lost. Attackers currently use this idea as they know the victim’s personal information well. They contact the providers using the gathered credentials of the victim and port a phone number to another device the victim does not own. In this way, the attackers can steal codes generated by SMS-based MFA.
- **MFA Fatigue** is one of the most recent techniques to bypass MFA and is becoming a common technique among attackers. It seems like a **brute force attack**; the attacker sends many access notifications until the victim approves.

How Hackers Can Bypass Multi-Factor Authentication?

Multi-factor authentication (MFA) is an authentication protocol that asks users for additional factors in order to login to their accounts. Such additional factors include:

Something you know: This might include a password, PIN number, or an answer to a security question.

Something you have: This could be a mobile phone, hardware token, fob, security key, etc.

Something you are: This includes biometric information such as fingerprints, facial recognition, retina scan, or voice recognition.

Users are required to provide at least two of these additional factors to verify their identity.

How can Cybercriminals Bypass Multi-Factor Authentication?

Hackers can bypass MFA in much the same way as they would for two-factor authentication, where there is just a username and password. Below are some of the most common ways that MFA can be bypassed:

Social Engineering

Social engineering techniques, such as phishing, are standard for attackers to obtain credentials. For example, in some cases, they will try to log in to an organization's cloud service provider, which sends an SMS message with the verification code to the account owner. The hacker will email the account owner asking them for the verification code. Of course, for this to work, the hacker must convince the user that they are a trusted entity.

In some cases, the hacker will email an unsuspecting employee to obtain basic personal information. Using this information, they might try to call the service provider and explain that they have been locked out of their account and want help getting back in.

Consent Phishing

Another social engineering technique that is becoming popular is known as "consent phishing". This is where hackers present what looks like a legitimate OAuth login page to the user. The hacker will request the level of access they need, and if access is granted, they can bypass MFA verification.

Brute Force

One of the main benefits of multi-factor authentication is that it makes it a lot harder for hackers to brute-force-guess account passwords. Although it makes it more challenging, it doesn't make it impossible. For example, hackers may look for the user's photos on social media, which they can use to bypass MFA, which uses facial recognition as an additional factor. In some extreme cases, they may try to find the user's fingerprints by dusting a smooth or non-porous surface with fingerprint powder and then photographing the prints using a high-resolution camera.

Exploiting Generated Tokens

Many online services use authentication apps, such as Microsoft Authenticator and Google Authenticator, to generate temporary tokens which can be used as an authentication factor.

In some cases, these services will keep a list of authentication codes, which the service provider uses in case of an account lock-out. Hackers will try to obtain this list by exploiting poor data security practices to bypass MFA.

Session Hijacking

Session hijacking is where an attacker steals session cookies, which contain a user’s authentication credentials. Session cookies are used by many web applications to provide a customized browsing experience and track the user’s activity. These session cookies remain active until the user logs out and are sometimes sent to the server over an insecure connection.

Hackers can easily find out if the session cookies are not secure, and are able to steal these cookies via a man-in-the-middle attack. Once they have access to a session cookie, they can bypass MFA.

SIM Hacking

Cybercriminals are able to gain access to your mobile device using one of three methods: SIM-jacking, SIM swapping, and SIM cloning, which are explained in more detail below:

SIM-jacking: Hackers will send a piece of spyware-like code to a target device using an SMS message. If the user opens the message the hacker will be able to spy on the victim, thus potentially gaining access to their credentials.

SIM swapping: The hacker will contact your mobile service provider and ask for a replacement SIM card.

Since it is not uncommon for users to request new SIM cards, perhaps because they are upgrading to a new device, the service provider may oblige and send them a new card. Once the hacker has the new SIM card, they can use it to gain access to your account, assuming the account uses SMS verification as one of the MFA factors.

SIM cloning: This is where the hacker gains access to your physical device, removes the SIM card, and using smart card copying software, copies the SIM data onto a blank card. The hacker will then insert the newly created SIM card into their phone, and receive phone calls and text messages to that SIM, including MFA authentication codes.

How to Strengthen Multifactor Authentication?

Given that the easiest way to bypass MFA is to convince users to hand over credentials and/or personal data, it is crucially important that your employees are trained to identify social engineering attacks, such as phishing emails, suspicious phone calls, and SMS messages. Below are some more tips to strengthen MFA:

How to Strengthen Multifactor Authentication

Choose your authentication methods wisely

Use adaptive multi-factor authentication

Use complex passwords, restrict access, and monitor logon attempts

Choose your authentication methods wisely

If you want to be extra secure, it’s probably a good idea to avoid SMS-based authentication altogether, as SMS OTPs are easier to compromise than other methods. If you do want to use SMS verification, consider setting up a SIM card lock, which means that a PIN number is required to modify your SIM card. Try to use biometric authentication whenever possible. After all, few hackers will bother to dust your door knobs with powder in order to get a copy of your fingerprint.

Use adaptive multi-factor authentication

Consider using adaptive multi-factor authentication (AMFA), which is a more contextual approach to MFA. With AMFA, each request is validated by examining the user’s geolocation, IP reputation, device, and login behaviors.

Use complex passwords, restrict access and monitor logon attempts

Make sure that your users are using strong and unique passwords. Passwords should either be long alphanumeric strings with upper and lower case characters or a passphrase that is difficult to guess. It’s always a good idea to ensure that users are granted the least privileges they need to perform their roles. That way, if an adversary does manage to bypass MFA, there’s less damage they can cause. Ensure that you can detect and respond to abnormal login attempts. Some sophisticated real-time change auditing solutions can detect and respond to events that match a pre-defined threshold condition.

For example, Suppose x number of logon attempts occur within a given time frame. In that case, a custom script can disable a user account, shut down the affected server, and do anything else to help contain the threat. These solutions can also work in cloud-based environments.