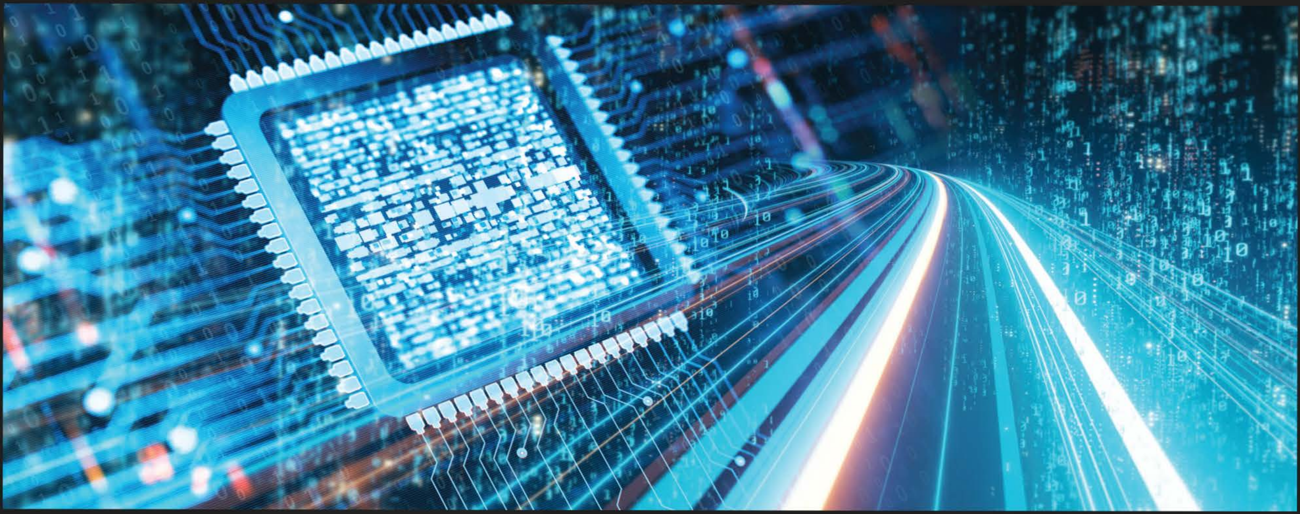


1ST EDITION

# Implementing **Multifactor Authentication**

Protect your applications from cyberattacks with the help of MFA

MARCO FANTI

# Implementing Multifactor Authentication

Protect your applications from cyberattacks with the help of MFA

**Marco Fanti**

packt

BIRMINGHAM—MUMBAI

# Implementing Multifactor Authentication

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

**Group Product Manager**: Mohd Riyan Khan
**Publishing Product Manager**: Prachi Sawant
**Senior Editor**: Runcil Rebello
**Technical Editor**: Arjun Varma
**Copy Editor**: Safis Editing
**Project Coordinator**: Ashwin Kharwa
**Proofreader**: Safis Editing
**Indexer**: Rekha Nair
**Production Designer**: Shankar Kalbhor
**Marketing Coordinator**: Agnes D’souza

First published: June 2023

Production reference: 1300523

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham
B3 2PB, UK.

ISBN 978-1-80324-696-3

`www.packtpub.com`

# Contributors

## About the author

**Marco Fanti**'s career skyrocketed from software engineering to cybersecurity as he discovered his passion for inventing innovative security tools. A prominent figure in the security community, he has collaborated with start-ups such as enCommerce and BehavioSec and giants such as Oracle and Accenture to create products that protect millions worldwide. A lifelong learner, Marco holds two MSc degrees (NYIT and NYU) and an MBA (UF), which enable him to craft bespoke solutions for clients by fusing the best features of various products. Originally from Brazil, Marco lives in Florida with his wife, perpetually exploring the cybersecurity frontier.

# 2
# When to Use Different Types of MFA

There is no magic bullet to solve all security needs. Hackers will actively look at ways to break it even if one existed, just as security companies create more and more solutions to improve the chances of better defending against threats. This chapter discusses when and when not to use different forms of **multifactor authentication** (**MFA**). We will also look at some websites for up-to-date information about MFA and new threats.

We are going to cover the following topics:

- Not all MFA is created equal – when to use different types of MFA
- Keeping up with bad actors – good sources for up-to-date information on MFA and related topics

## Not all MFA is created equal – when to use different types of MFA

In May 2021, the President of the United States issued **Executive Order** (**EO**) 14028 to initiate a government-wide effort to improve cybersecurity. As part of this effort, the **Office of the Management and Budget** (**OMB**), part of the Executive Office of the President, issued a memorandum entitled *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*. The memo was sent on January 26, 2022, to all heads of executive departments and agencies of the government with specific cybersecurity standards and objectives that need to be in place by the end of the fiscal year 2024 (`https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf`).

The initiative's goals are to "*ensure that baseline security practices are in place, migrate the Federal Government to a zero-trust architecture, and realize the security benefits of cloud-based infrastructure while mitigating associated risks*."

The **Zero Trust model** is based on the principle that no actor, system, network, or service can be trusted. Therefore, we must verify anything and everything attempting to establish access. This initiative is a dramatic shift in how the government previously secured infrastructure, networks, and data and followed the principles recommended by all security experts.

In addition to relying on centralized, secure, enterprise-managed identity systems, the strategy emphasizes stronger enterprise identity and access controls, including MFA.

While the memorandum issued by the OMB was explicitly for government agencies, vendors, and contractors they work with, the guidance provided regarding MFA is one that I recommend all companies follow.

In addition to considering MFA "*a critical part of the Federal Government's security baseline*," the memo also includes additional suggestions and requirements that we will discuss in the rest of this chapter:

"*Many approaches to multi-factor authentication will not protect against sophisticated phishing attacks. For agency staff, contractors, and partners, phishing-resistant MFA is required.*"

As discussed earlier, MFA will generally protect against some common methods of unauthorized account access that affect password-only systems. For example, one-time passwords, SMS, and magic links can be phished by bad actors and should be discontinued:

"*Agencies are encouraged to pursue greater use of passwordless multi-factor authentication as they modernize their authentication systems.*"

In authentication systems that include passwords as one of the factors in MFA, passwords can make it much easier to obtain access than when passwords are not one of the factors. We will discuss different systems that support passwordless MFA throughout this book and recommend using passwordless MFA whenever possible.

## Why use MFA then?

Writing a book about MFA might be counterintuitive if bad actors can circumvent it. However, like most decisions in security, the answer is not always black and white. Instead, it depends on the risks that the user, the company, or the service provider are willing to accept and the inherent value of the protected information. By delving deeper into these aspects, we can understand the nuances of this issue and better appreciate the importance of MFA.

First and foremost, MFA provides an additional layer of security, making it more difficult for unauthorized users to access sensitive information. In addition, by requiring at least two independent authentication factors, MFA creates a more robust authentication process. Consequently, even if one factor is compromised, the likelihood of a successful breach is still reduced.

Now, it is true that MFA is not infallible and can be bypassed in some instances. However, the complexity of bypassing MFA often acts as a deterrent for potential attackers. The effort and resources required to circumvent MFA are significantly higher than traditional single-factor authentication methods. This is particularly important when considering the value of protected information; the more valuable the data, the more attractive it becomes as a target. Thus, MFA adds cost for potential attackers, who must weigh the investment against the potential payoff.

Furthermore, the risk tolerance of the parties involved also plays a role in the decision to use MFA. For users, companies, and service providers, the consequences of a security breach can be devastating – ranging from financial losses to reputational damage. The implementation of MFA serves as a demonstration of commitment to security, which may help mitigate these risks. Also, as we saw in the memo from the president, "*For agency staff, contractors, and partners, phishing-resistant MFA is required.*"

Finally, it is essential to remember that security is constantly evolving. Security measures such as MFA must adapt and improve as new threats emerge to remain effective. In this ever-changing landscape, using MFA is not a guarantee of absolute security but rather a tool that helps minimize the likelihood of a breach.

## Different types of MFA

Different types of authenticator factors can be used in **two-factor authentication** (**2FA**) and MFA. The cybersecurity and infrastructure agency classifies the MFA types into three tiers (`https://www.cisa.gov/mfa`):

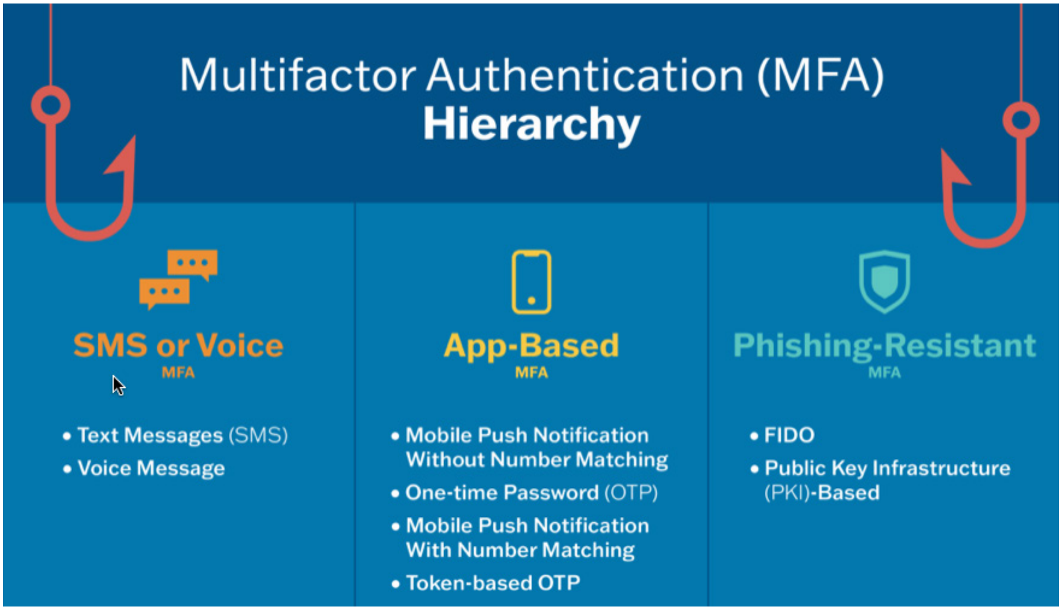

Multifactor Authentication (MFA)
Hierarchy
SMS or Voice
MFA
• Text Messages (SMS)
• Voice Message
App-Based
MFA
• Mobile Push Notification Without Number Matching
• One-time Password (OTP)
• Mobile Push Notification With Number Matching
• Token-based OTP
Phishing-Resistant
MFA
• FIDO
• Public Key Infrastructure (PKI)-Based

Figure 2.1 – The strengths of different types of authentication factors

The weakest types are text messages (SMSs) or voice messages. In addition to phishing, they are also susceptible to **SIM swap** attacks.

At the next level, app-based MFA is also divided into two types. Push notifications without number matching are weaker than the other types in this category – that is, **one-time password** (**OTP**), **token-based OTP** (**TOTP**), and push notifications with number matching.

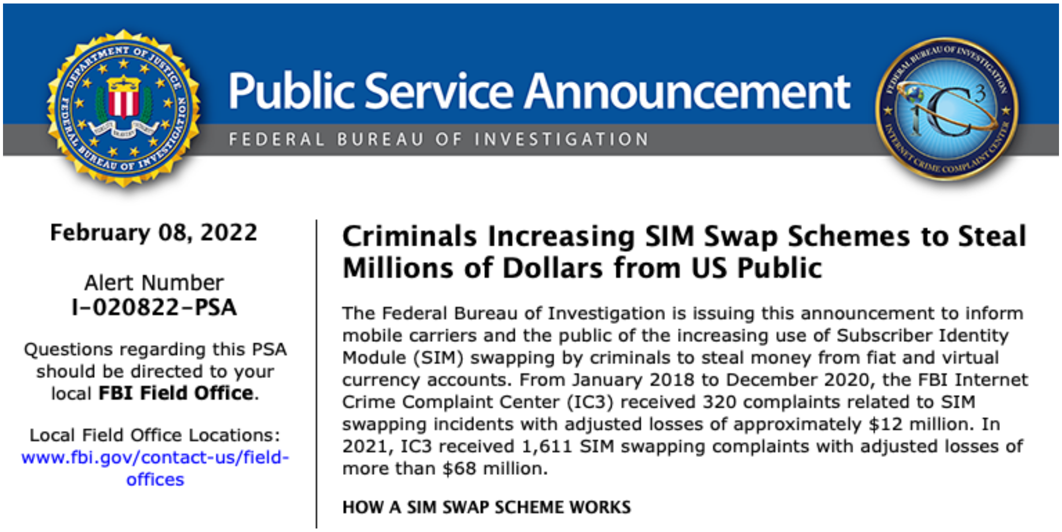
Finally, the strongest level includes phishing-resistant MFA types such as FIDO and public-key infrastructure-based MFA. Recall that FIDO was discussed in *Chapter 2*. For more information, please go to `https://fidoalliance.org/what-is-fido/`.

## SIM swap and why SMSs and voice messages are the weakest authenticator factor types to use

In February 2022, the FBI issued a public service announcement (`https://www.ic3.gov/Media/Y2022/PSA220208`) that included the following text:

"*From January 2018 to December 2020, the FBI Internet Crime Complaint Center (IC3) received 320 complaints related to SIM swapping incidents with adjusted losses of approximately $12 million. In 2021, IC3 received 1,611 SIM swapping complaints with adjusted losses of more than $68 million.*"

Here is a screenshot from the FBI website:



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

**February 08, 2022**

Alert Number
**I-020822-PSA**

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

**Criminals Increasing SIM Swap Schemes to Steal Millions of Dollars from US Public**

The Federal Bureau of Investigation is issuing this announcement to inform mobile carriers and the public of the increasing use of Subscriber Identity Module (SIM) swapping by criminals to steal money from fiat and virtual currency accounts. From January 2018 to December 2020, the FBI Internet Crime Complaint Center (IC3) received 320 complaints related to SIM swapping incidents with adjusted losses of approximately $12 million. In 2021, IC3 received 1,611 SIM swapping complaints with adjusted losses of more than $68 million.

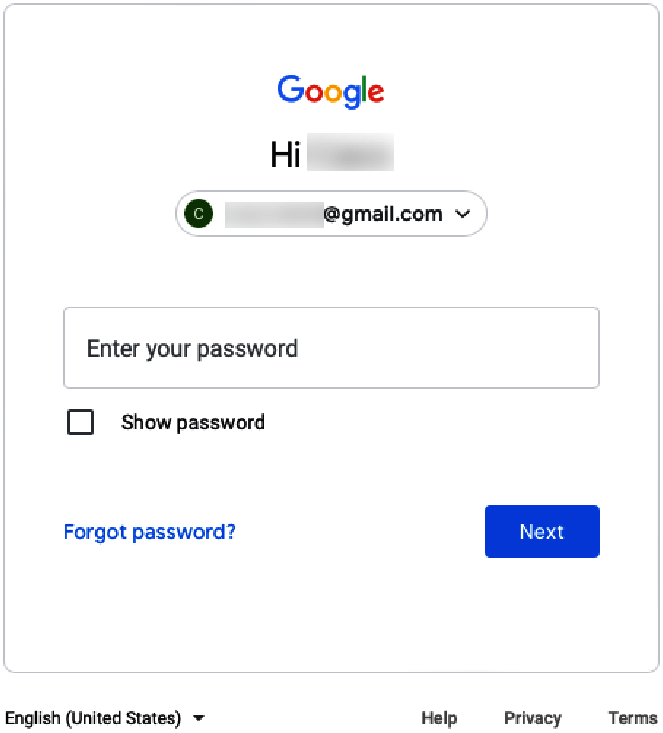
**HOW A SIM SWAP SCHEME WORKS**

Figure 2.2 – FBI's PSA on SIM swap schemes

A **SIM swap** is a type of social engineering attack in which a malicious actor uses social engineering or another method to convince a phone company to transfer the victim's phone number to a new SIM card that they control. This allows the attacker to intercept calls and text messages meant for the victim, potentially giving them access to sensitive information such as one-time codes used for recovering their accounts or MFA.

Let's see what happens if your phone number is transferred to a cybercriminal:

1. The hacker goes to the account login page and clicks on **Forgot password?**:



Google

Hi [redacted]

C [redacted]@gmail.com

Enter your password

□ Show password

Forgot password?

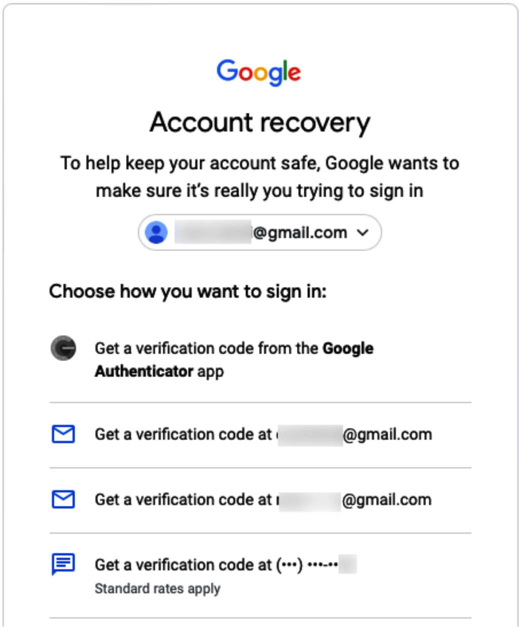
Next

English (United States)

Help Privacy Terms

Figure 2.3 – Login page with Forgot password?

2. The hacker selects the phone number they now control as a recovery mechanism:



Google

Account recovery

To help keep your account safe, Google wants to make sure it's really you trying to sign in

[redacted]@gmail.com

Choose how you want to sign in:

Get a verification code from the **Google Authenticator** app

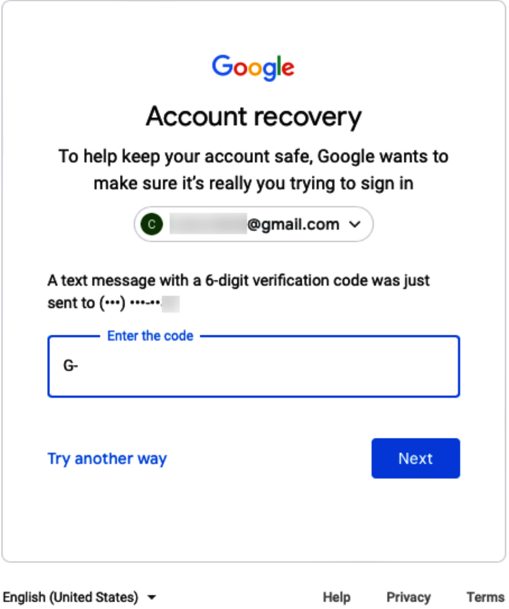
Get a verification code at [redacted]@gmail.com

Get a verification code at [redacted]@gmail.com

Get a verification code at (•••) •••-••[redacted]
Standard rates apply

Figure 2.4 – Account recovery selection page

3. The hacker enters the code:



Google

Account recovery

To help keep your account safe, Google wants to make sure it's really you trying to sign in

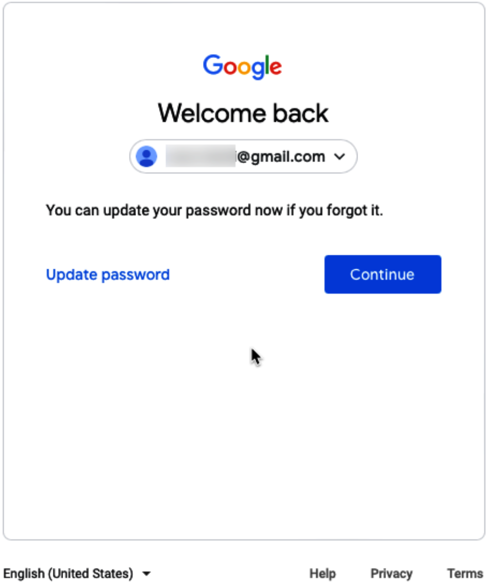
[redacted]@gmail.com

A text message with a 6-digit verification code was just sent to (•••) •••-••[redacted]

Enter the code: G-

Figure 2.5 – Account recovery page

4. That's it – the account takeover is complete. The hacker can continue without changing the password or change the password and possibly complicate the process of the original owner recovering their account:



Welcome back

[redacted]@gmail.com

You can update your password now if you forgot it.

Figure 2.6 – The Welcome back page

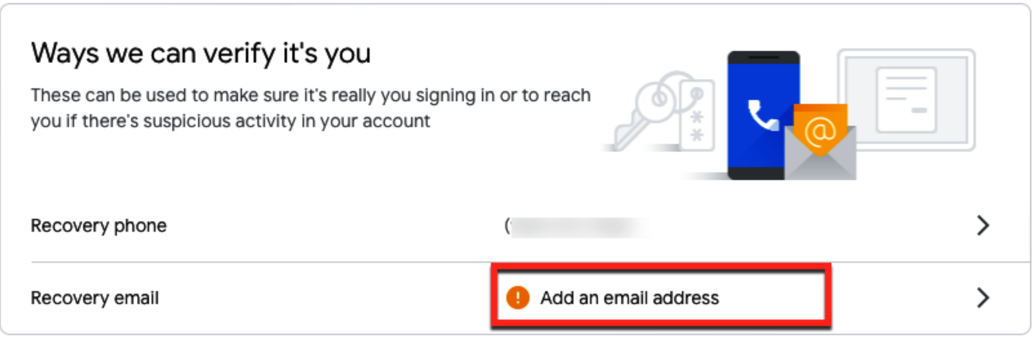
SIM swap is one of the worst attacks because it is tough for the service provider to prevent. As seen in the preceding example, even though the account was protected by MFA, the cybercriminal was able to bypass the password and use only one factor to take over the account.

In a typical scenario, the security of services depends on the company providing them and the user using them. If the service provider allows the use of SMSs or voice messages as a recovery mechanism, the security of the service will also rely on the phone company, which neither the service provider nor the user can control. If SMSs or voice messages are only allowed as a second factor during a password-based login, and not for account recovery, the cybercriminal needs to obtain the user's ID and password, and also obtain control of the victim's phone using SIM swap.

## What can the service provider do?

The service provider can mandate app-based or phishing-resistant authentication factors for account recovery and as a second factor of authentication. If that is not an option, it can at least recommend and educate users on the benefits of a stronger factor of authentication.

A service provider can also enhance the chances of a successful session or account takeover being detected by suggesting or mandating a second recovery mechanism:



Ways we can verify it's you

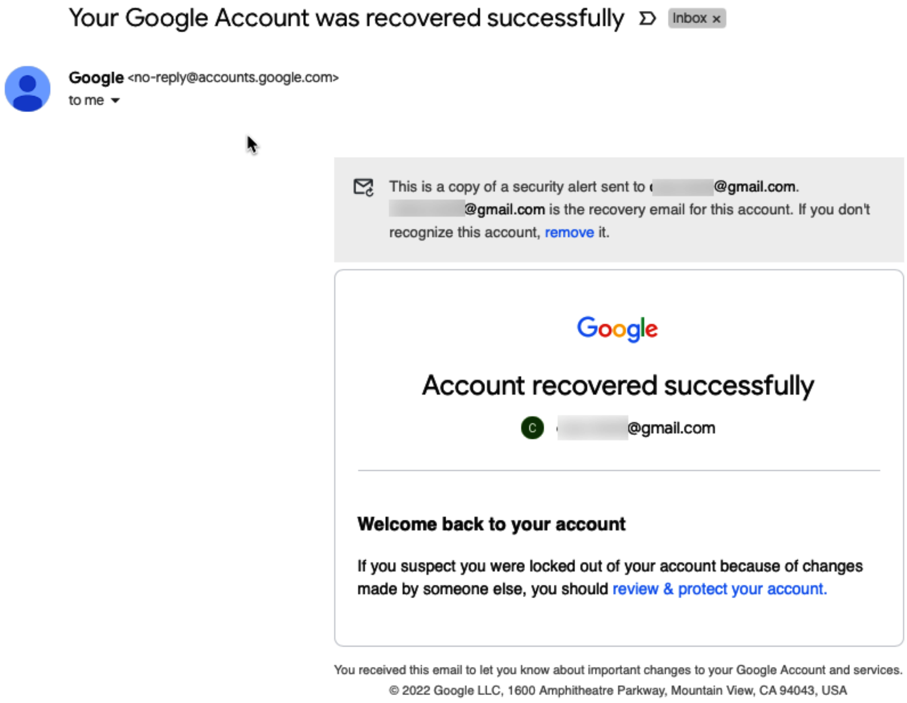
These can be used to make sure it's really you signing in or to reach you if there's suspicious activity in your account

Recovery phone [redacted] >

Recovery email ! Add an email address >

Figure 2.7 – Account recovery mechanism selection page

Users with an email address and a phone number as security mechanisms will be notified when one of the security mechanisms is used for account recovery:



Your Google Account was recovered successfully

**Google** <no-reply@accounts.google.com>
to me

This is a copy of a security alert sent to [redacted]@gmail.com. [redacted]@gmail.com is the recovery email for this account. If you don't recognize this account, remove it.

Google

Account recovered successfully

C [redacted]@gmail.com

**Welcome back to your account**

If you suspect you were locked out of your account because of changes made by someone else, you should review & protect your account.

You received this email to let you know about important changes to your Google Account and services.
© 2022 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

Figure 2.8 – Account recovered notification email

This is what the service provider can do to recover an account. Let's see in the next subsection what the user can do.

### What can the user do?

To avoid being the victim of **SIM swap** fraud schemes, users should avoid using SMS messages and voice messages for 2FA as well as for recovering their accounts.

If quickly recovering the account is more important than avoiding the possibility of being the victim of a SIM swap, users should make sure that more than one method of recovery is enabled. This way, as we saw in the previous example, the user will be notified if someone recovers the account inappropriately, or if a user logs in to the account from an unknown computer.

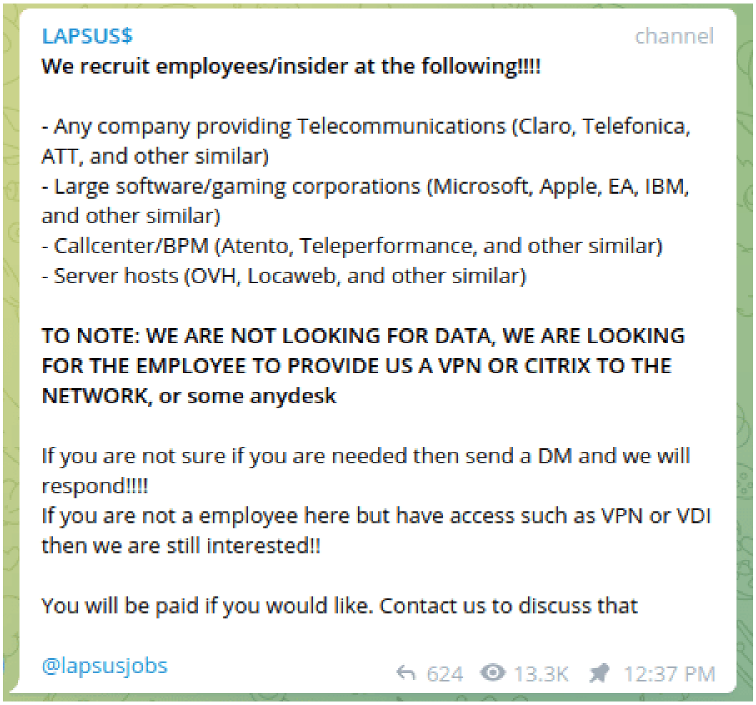
## MFA fatigue – also known as MFA push spam

As service providers and users become more security conscious and avoid SMS-based MFA, hackers increasingly use a technique that does not require SIM swap and can bypass authentication factors classified as more secure. This method is called **MFA fatigue**. MFA fatigue was used in confirmed cyberattacks on Cisco (`https://blog.talosintelligence.com/recent-cyber-attack/`), Microsoft (`https://www.microsoft.com/en-us/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/`), and other companies. Several security companies, including Mandiant, have published reports about Russian actors using the technique (`https://www.mandiant.com/resources/blog/russian-targeting-gov-business`) to target the US government and private companies.

MFA fatigue is commonly initiated by compromising the user's identity to obtain initial access to the organization or the victim's account. This is typically done via the following methods:

- Deploying malware such as Redline Stealer or Loki Password Stealer
- Obtaining credentials and session tokens in criminal underground forums

- Recruiting current and former employees who have access to specific company networks, as depicted in *Figure 2.9*:



LAPSUS$ channel

**We recruit employees/insider at the following!!!!**

- Any company providing Telecommunications (Claro, Telefonica, ATT, and other similar)
- Large software/gaming corporations (Microsoft, Apple, EA, IBM, and other similar)
- Callcenter/BPM (Atento, Teleperformance, and other similar)
- Server hosts (OVH, Locaweb, and other similar)

**TO NOTE: WE ARE NOT LOOKING FOR DATA, WE ARE LOOKING FOR THE EMPLOYEE TO PROVIDE US A VPN OR CITRIX TO THE NETWORK, or some anydesk**

If you are not sure if you are needed then send a DM and we will respond!!!!
If you are not a employee here but have access such as VPN or VDI then we are still interested!!

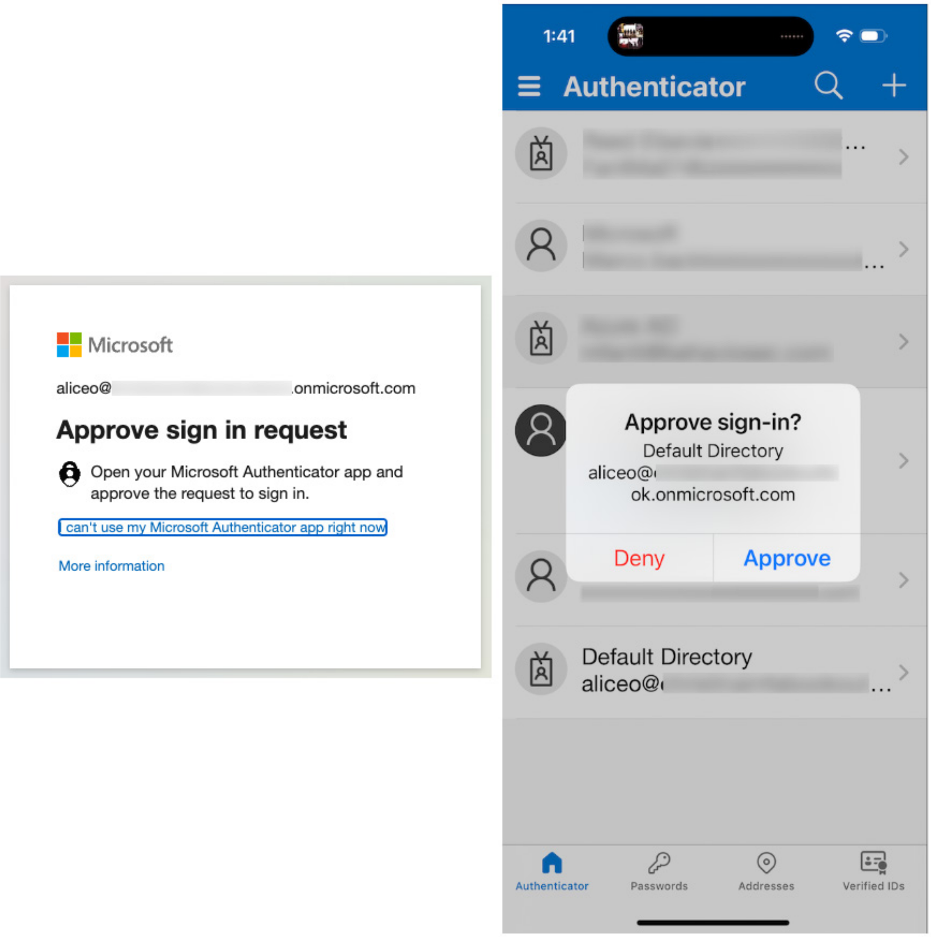
You will be paid if you would like. Contact us to discuss that

@lapsusjobs

624 13.3K 12:37 PM

Figure 2.9 – Recruitment message from the group LAPSUS$

When companies use mobile apps as a second factor of authentication, where a user sees a notification on their phone that they must approve, cybercriminals will attempt to cause the legitimate user to accept one of the repeated MFA prompts and let the cybercriminal in. In some cases, the attacker will also send a message to the victim pretending to be from the company and urging the user to accept the MFA push:


Microsoft

aliceo@[redacted].onmicrosoft.com

Approve sign in request

Open your Microsoft Authenticator app and approve the request to sign in.

Approve sign-in?
Default Directory
aliceo@[redacted]ok.onmicrosoft.com

Default Directory
aliceo@[redacted]...

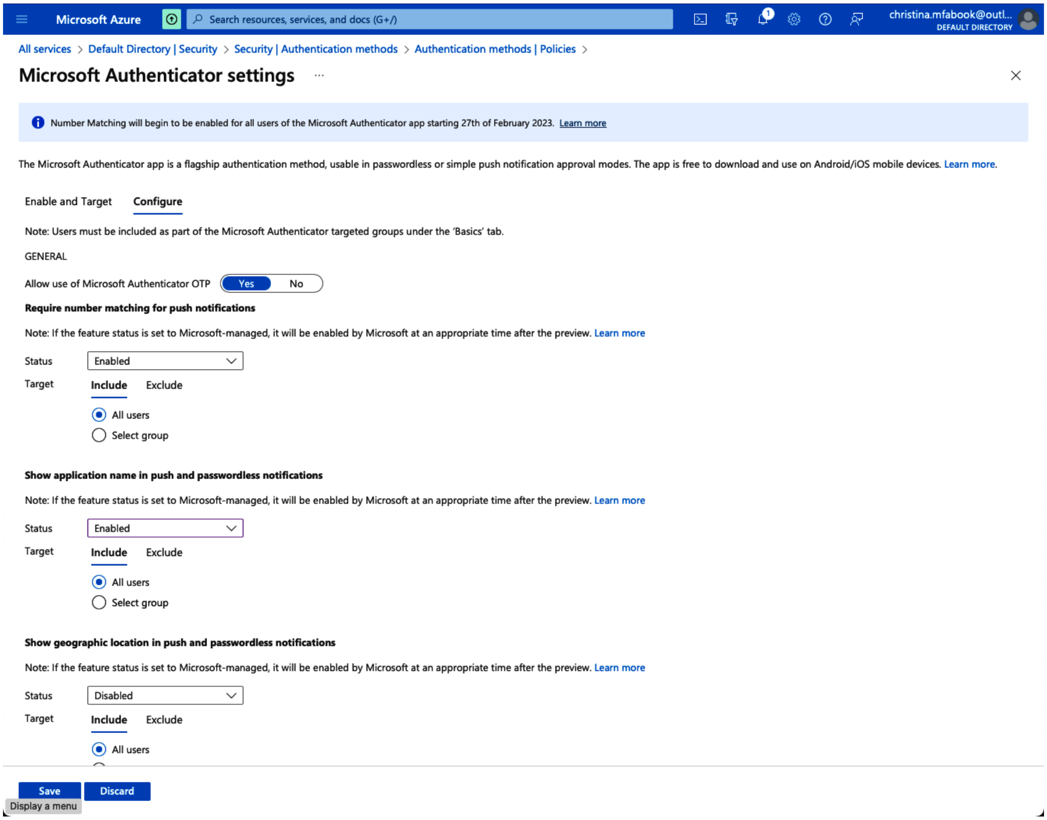
Figure 2.10 – Push-based notification without number matching

## What can the service provider do?

Service providers can provide additional security against MFA fatigue by enabling **number matching**. If enabled, the user must enter a number in the authenticator that matches the number shown in the authentication sign-in. Microsoft considers number matching a critical security upgrade and will enforce number matching starting in 2023 (`https://learn.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match`). Duo, another product we will use as an authentication factor, starting from *Chapter 3*, also supports using a verification code to avoid MFA fatigue. This is called **Verified Duo Push**.

Another way that service providers can avoid scams based on MFA fatigue is by providing additional context for the push authentication, if enabled by the MFA application.

The following figures show number matching and other settings for Microsoft Authenticator. Starting February 27, 2023, Microsoft Authenticator will enforce number matching for all users tenant-wide, eliminating the need for this configuration. This is a crucial security enhancement over traditional second-factor push notifications:


Microsoft Azure
Search resources, services, and docs (G+/)
christina.mfabook@outl...
DEFAULT DIRECTORY
All services > Default Directory | Security > Security | Authentication methods > Authentication methods | Policies >

Microsoft Authenticator settings

Number Matching will begin to be enabled for all users of the Microsoft Authenticator app starting 27th of February 2023. Learn more

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or simple push notification approval modes. The app is free to download and use on Android/iOS mobile devices. Learn more.

Enable and Target | Configure

Note: Users must be included as part of the Microsoft Authenticator targeted groups under the 'Basics' tab.

GENERAL

Allow use of Microsoft Authenticator OTP: Yes [✓] No

**Require number matching for push notifications**

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview. Learn more

Status: Enabled

Target: Include | Exclude

● All users
○ Select group

**Show application name in push and passwordless notifications**

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview. Learn more

Status: Enabled

Target: Include | Exclude

● All users
○ Select group

**Show geographic location in push and passwordless notifications**

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview. Learn more

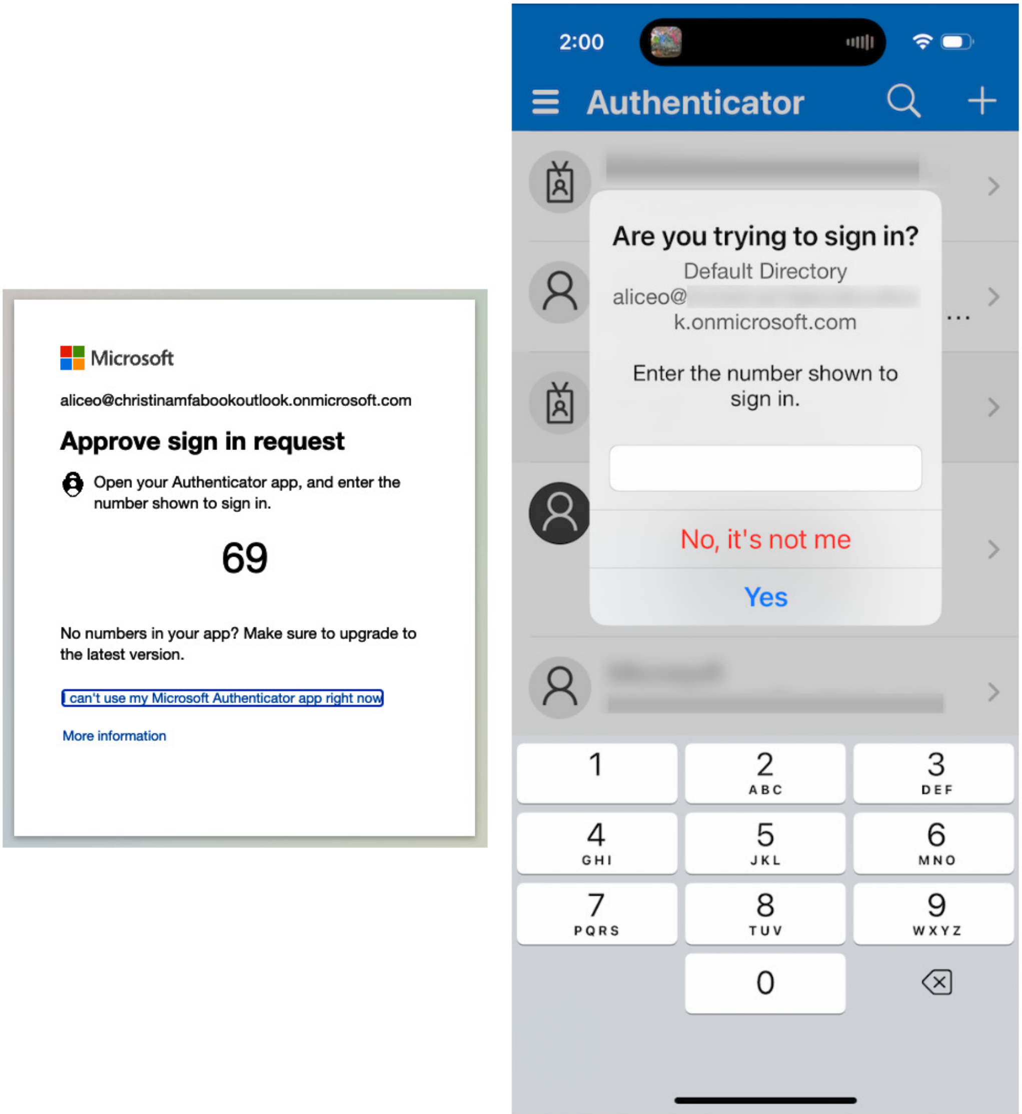
Status: Disabled

Target: Include | Exclude

● All users

Figure 2.11 – Enabling number matching in Microsoft Authenticator

**Number matching** is a feature that requires the user to input numbers from the identity platform into their app to confirm the authentication request:



Microsoft

aliceo@christinamfabookoutlook.onmicrosoft.com

Approve sign in request

Open your Authenticator app, and enter the number shown to sign in.

69

No numbers in your app? Make sure to upgrade to the latest version.

I can't use my Microsoft Authenticator app right now

More information

Are you trying to sign in?

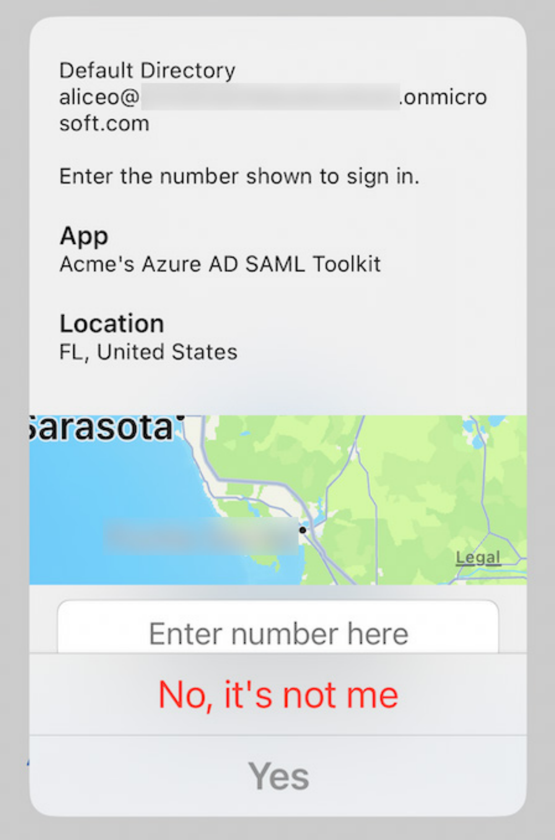
Default Directory

aliceo@[redacted]k.onmicrosoft.com

Enter the number shown to sign in.

Figure 2.12 – MFA push with number matching in Microsoft Authenticator

As seen in the following figure, Microsoft allows the application name and the geographic location to also be shown during the authentication process:



Default Directory
aliceo@[redacted].onmicrosoft.com

Enter the number shown to sign in.

App
Acme's Azure AD SAML Toolkit

Location
FL, United States

Figure 2.13 – MFA push with the application name and location in Microsoft Authenticator

Finally, we are going to look at the most secure authentication factor type: **phishing-resistant MFA**.

## Phishing-resistant MFA

While writing this chapter, I received an email from my financial institution. Curiously, the picture in the email showed users protecting their passwords. However, passwords were not the focus of the document – phishing was.

The email described a typical financial institution phishing attack, where bad actors utilize mass email campaigns to a broad group of people designed to collect account credentials. In addition to mass email attacks, modern, targeted attacks are a more sophisticated way of infiltrating corporate security. They use social engineering to research information about users in select organizations and use real names to create an urgency for the target user to respond.

In either case, a hacker creates a fake email account or website with variations of legitimate email and website addresses, trying to make fake accounts appear authentic. They then send spear-phishing emails pretending to be a trusted sender (either the financial institution or, in the case of companies, somebody from the IT department – the boss or CEO of the target user).

When you download a file attached to an email or click on an email link, you can unsuspectingly install malware that can capture your credentials and access your accounts. In addition, you can be redirected to a fake website created to look exactly like your original website.

In *Figure 2.15*, you can see one example where cybercriminals created a copy of the popular encrypted email service Tutanota (`https://tutanota.com`) using a URL similar to the original, `https://tutanota.org`:

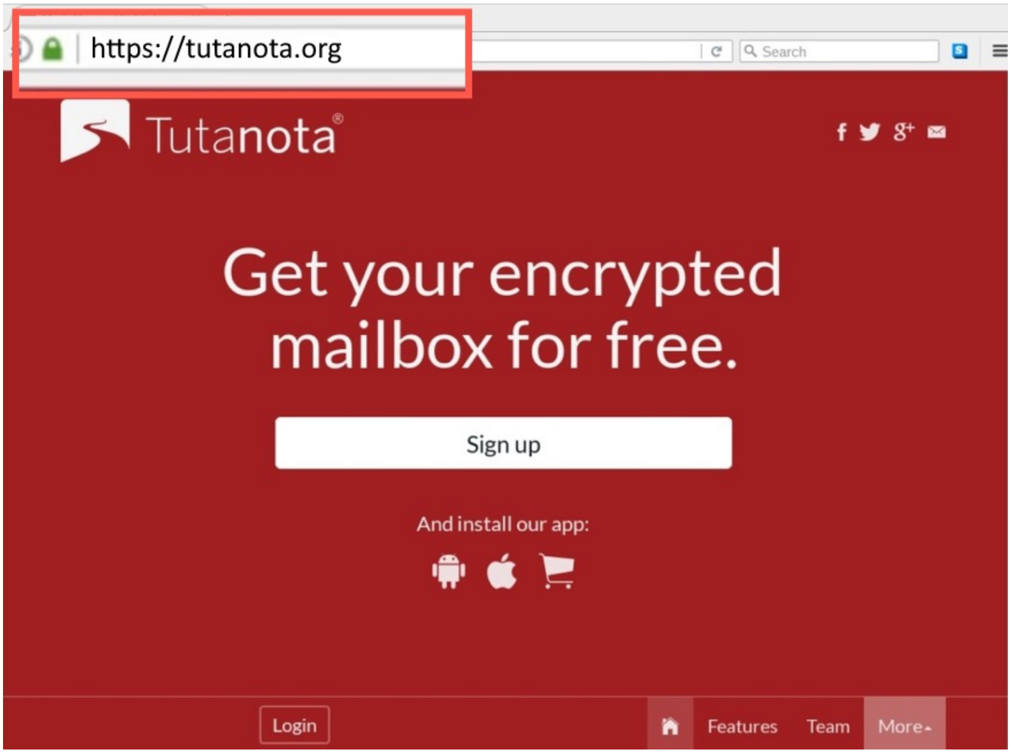
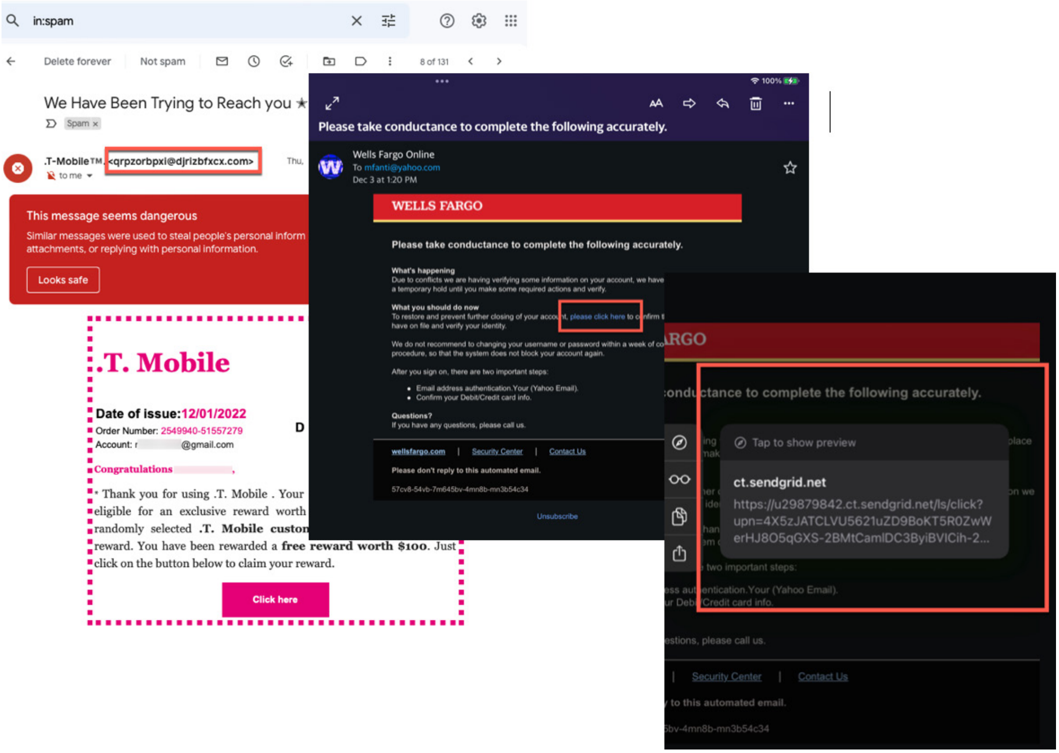


Figure 2.14 – Fake tutanota.org web page imitating tutanota.com

A typical phishing attack works like this:

1. The user receives a phishing email or a WhatsApp or SMS message. Note the unknown from addresses and fake URL links in *Figure 2.16*:



We Have Been Trying to Reach you

.T-Mobile TM <qrpzorbpxi@djrizbfxcx.com>
to me
Thu,

This message seems dangerous
Similar messages were used to steal people's personal inform
attachments, or replying with personal information.

.T. Mobile

Date of issue:12/01/2022
Order Number: 2549940-51557279
Account: r[redacted]@gmail.com

Congratulations [redacted],

* Thank you for using .T. Mobile . Your eligible for an exclusive reward worth randomly selected .T. Mobile custon reward. You have been rewarded a **free reward worth $100**. Just click on the button below to claim your reward.

Please take conductance to complete the following accurately.

Wells Fargo Online
To mfanti@yahoo.com
Dec 3 at 1:20 PM

WELLS FARGO

Please take conductance to complete the following accurately.

What's happening
Due to conflicts we are having verifying some information on your account, we have a temporary hold until you make some required actions and verify.

What you should do now
To restore and prevent further closing of your account, please click here to confirm t have on file and verify your identity.

We do not recommend to changing your username or password within a week of co procedure, so that the system does not block your account again.

After you sign on, there are two important steps:

- Email address authentication.Your (Yahoo Email).
- Confirm your Debit/Credit card info.

Questions?
If you have any questions, please call us.

wellsfargo.com | Security Center | Contact Us

Please don't reply to this automated email.

57cv8-54vb-7m645bv-4mn8b-mn3b54c34

ct.sendgrid.net
https://u29879842.ct.sendgrid.net/ls/click?upn=4X5zJATCLVU5621uZD9BoKT5R0ZwWerHJ8O5qGXS-2BMtCamIDC3ByiBVICih-2...

Figure 2.15 – Identifying a fake Wells Fargo email message with different email readers

2. The user clicks on the link that points to a website unrelated to the original URL.
3. The user doesn't notice that the URL is not what they were expecting it to be. In this case, it is `https://fakegoogle.com`:

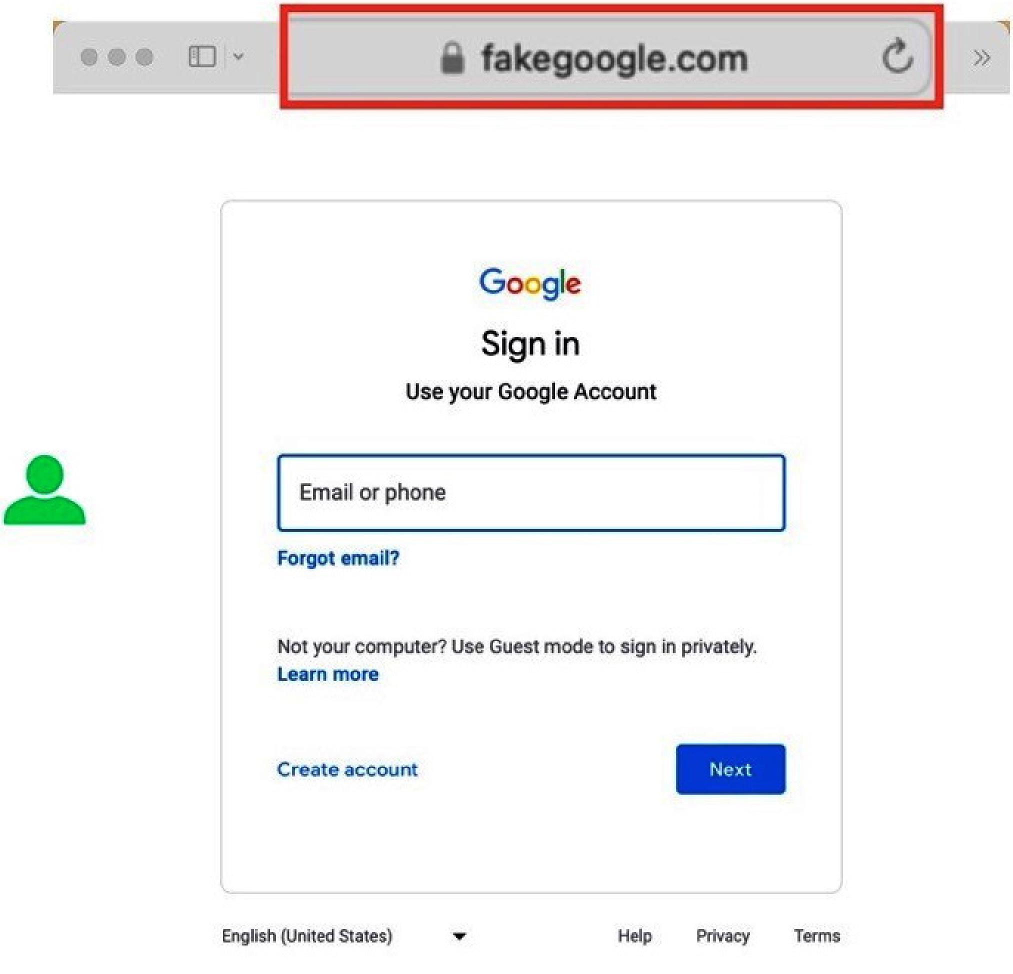


Figure 2.16 – Fake login page

4. The user enters their username. A **Man-in-the-Middle** (**MitM**) proxy forwards this username to the real website (`https://accounts.google.com`):

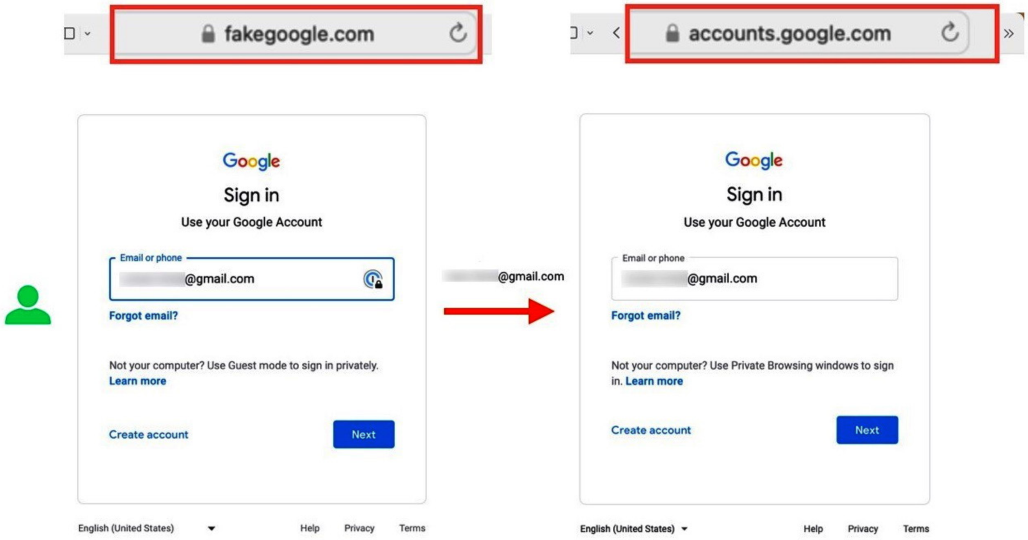


Figure 2.17 – Username used on the real login page

5. The user enters their password. Again, the MitM proxy forwards the password to the real website:

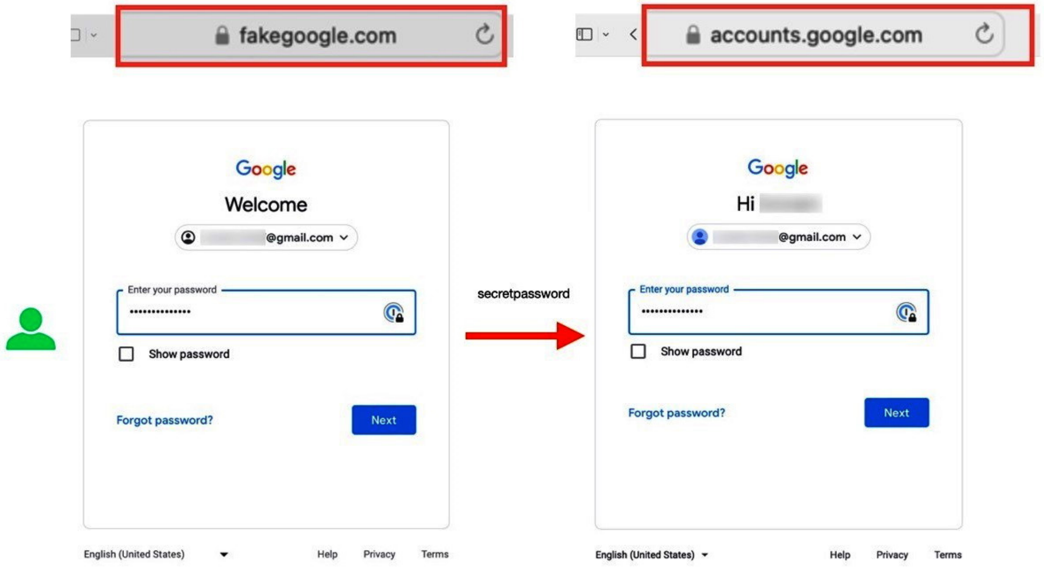
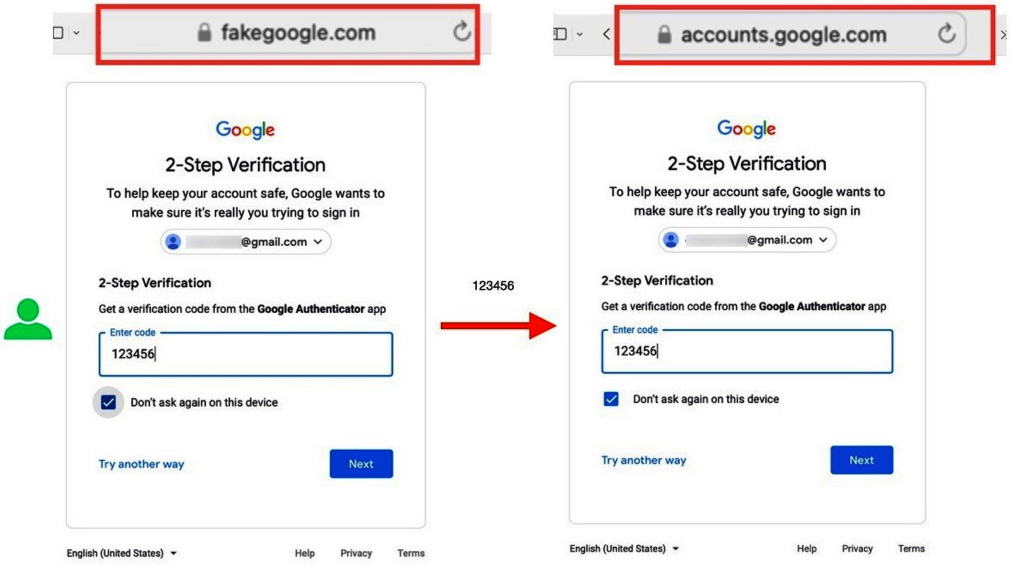


Figure 2.18 – Password used on the real login page

6. Finally, the user enters the OTP from the authenticator app. And again, the MitM proxy forwards the OTP to the real website:



2-Step Verification

To help keep your account safe, Google wants to make sure it's really you trying to sign in

[redacted]@gmail.com

2-Step Verification

Get a verification code from the **Google Authenticator** app

Enter code: 123456

☑ Don't ask again on this device

2-Step Verification

To help keep your account safe, Google wants to make sure it's really you trying to sign in

[redacted]@gmail.com

2-Step Verification

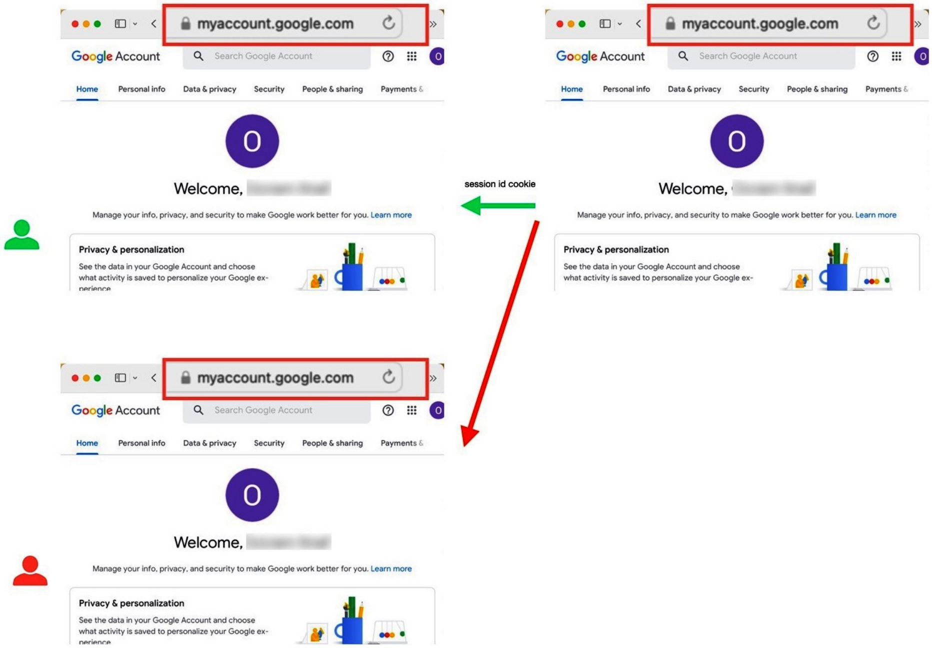
Get a verification code from the **Google Authenticator** app

Enter code: 123456

☑ Don't ask again on this device

Figure 2.19 – OTP copied to the real login page

7. To avoid suspicion, the user is now redirected to the real website. The session ID cookies are then copied to the cybercriminal's browser, who can then impersonate the user on the real website:



Welcome, [redacted]

Manage your info, privacy, and security to make Google work better for you. Learn more

Privacy & personalization

See the data in your Google Account and choose what activity is saved to personalize your Google experience

Welcome, [redacted]

Manage your info, privacy, and security to make Google work better for you. Learn more

Privacy & personalization

See the data in your Google Account and choose what activity is saved to personalize your Google ex-

Welcome, [redacted]

Manage your info, privacy, and security to make Google work better for you. Learn more

Privacy & personalization

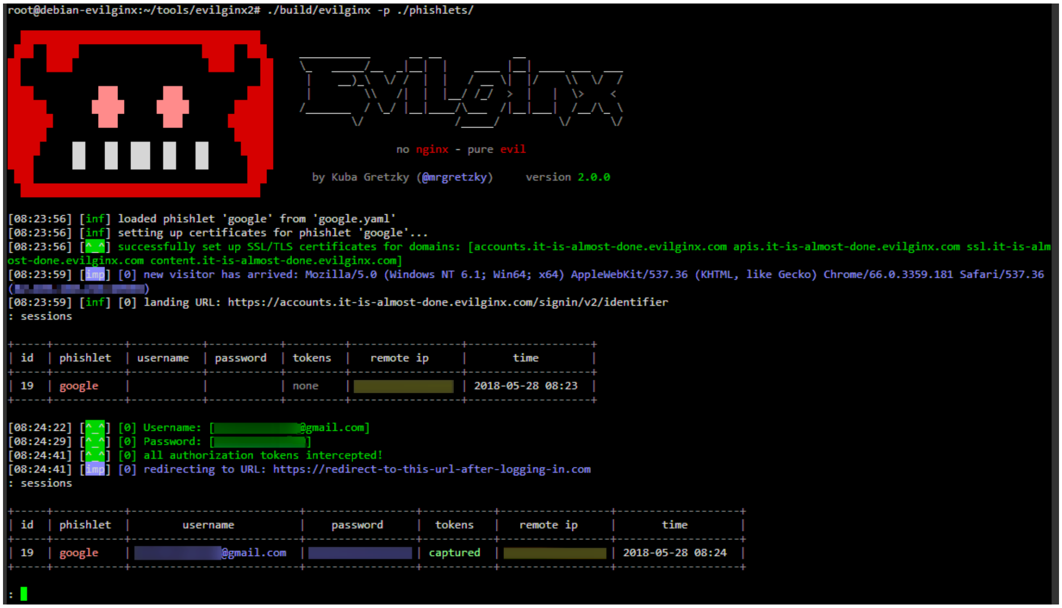
See the data in your Google Account and choose what activity is saved to personalize your Google experience

Figure 2.20 – Session ID copied to the hacker's page

Most phishing attacks can be prevented with user education. Unfortunately, cybercriminals only need to be successful once to be able to take over an account. At the same time, education may work for workforce users but not for external customers.

Another factor that makes phishing and MitM attacks easier for cybercriminals is the number of MitM toolkits, such as **evilginx2** and **Modlishka**, which come with videos and other guides that make it very easy for anyone to attempt phishing attacks.

As seen in *Figure 2.22*, the process described earlier (except for the phishing email or other social engineering scheme used to have the victim access the attacker's URL) is done by the tool. The session tokens that are captured can then be used by the criminals with very little effort:



```
root@debian-evilginx:~/tools/evilginx2# ./build/evilginx -p ./phishlets/

                         no nginx - pure evil

                    by Kuba Gretzky (@mrgretzky)     version 2.0.0

[08:23:56] [inf] loaded phishlet 'google' from 'google.yaml'
[08:23:56] [inf] setting up certificates for phishlet 'google'...
[08:23:56] [^_^] successfully set up SSL/TLS certificates for domains: [accounts.it-is-almost-done.evilginx.com apis.it-is-almost-done.evilginx.com ssl.it-is-alm
ost-done.evilginx.com content.it-is-almost-done.evilginx.com]
[08:23:59] [imp] [0] new visitor has arrived: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.181 Safari/537.36
([redacted])
[08:23:59] [inf] [0] landing URL: https://accounts.it-is-almost-done.evilginx.com/signin/v2/identifier
: sessions

+-----+------------+----------+----------+--------+----------------+------------------+
| id  | phishlet   | username | password | tokens |   remote ip    |       time       |
+-----+------------+----------+----------+--------+----------------+------------------+
| 19  | google     |          |          | none   | [redacted]     | 2018-05-28 08:23 |
+-----+------------+----------+----------+--------+----------------+------------------+

[08:24:22] [^_^] [0] Username: [[redacted]@gmail.com]
[08:24:29] [^_^] [0] Password: [[redacted]]
[08:24:41] [^_^] [0] all authorization tokens intercepted!
[08:24:41] [imp] [0] redirecting to URL: https://redirect-to-this-url-after-logging-in.com
: sessions

+-----+------------+-------------------------+-------------------+----------+------------------+------------------+
| id  | phishlet   |        username         |     password      |  tokens  |    remote ip     |       time       |
+-----+------------+-------------------------+-------------------+----------+------------------+------------------+
| 19  | google     | [redacted]@gmail.com    | [redacted]        | captured | [redacted]       | 2018-05-28 08:24 |
+-----+------------+-------------------------+-------------------+----------+------------------+------------------+

: 
```

Figure 2.21 – evilginx2 MitM toolkit

Being an online bad actor used to require specific skills and access to hard-to-find groups and resources. Finding valuable information on a compromised system was also time-sensitive and challenging, making it easier for defenders to detect malicious activity.

However, the rise of specialization in the online crime sector brought about **initial access brokers** (**IABs**), which specialize in gaining and maintaining access to compromised systems for others. This has led to the industry's professionalization, resulting in the emergence of polished marketplaces.

The most famous IAB is the **Genesis Marketplace**. The Genesis Marketplace, also referred to as the **Genesis Store** or **Genesis Market**, is an exclusive platform specializing in the sale of stolen credentials, cookies, and digital fingerprints collected from compromised systems. The marketplace not only offers the stolen data itself but also provides well-maintained tools to facilitate its use.

Since its establishment in 2017, Genesis has listed over 400,000 compromised systems, or **bots**, from over 200 countries. The attractiveness of Genesis lies not in the quantity of its data aggregation but in the quality of the stolen information that it offers and its commitment to maintaining the accuracy of this information.

A **bot**, in this context, refers to a compromised system that harvests credentials and includes automated malware that collects information. By utilizing persistent bots on victims' systems, Genesis can keep the stolen information up-to-date for its customers, making the data more valuable to attackers. Additionally, Genesis claims to have access to the compromised system, ensuring its fingerprints will be updated as they change.

In addition to its extensive collection of stolen data, Genesis offers a polished interface with effective data-correlation capabilities and well-maintained tools for its customers, including a robust search function. The marketplace also provides mainstream amenities such as an FAQ, user support, pricing in dollars (payable in Bitcoin), and professional copy editing, making it a convenient and user-friendly platform for malicious actors.

The increased sophistication of tools used by bad actors makes the use of phishing-resistant MFA even more critical.

# Keeping up with bad actors – good sources for up-to-date information on MFA and related topics

The US government is an excellent source of information for security. There are multiple government websites we can go to for up-to-date security and (multifactor) authentication information. Similarly, the European Union, Australia, the UK, and Israel provide important and simplified guidance to their citizens that can be beneficial to anyone looking for more information on new security threats and how they affect MFA specifically.

## Cybersecurity and Infrastructure Security Agency

**Cybersecurity and Infrastructure Security Agency** (**CISA**) (`https://www.cisa.gov/about-cisa`) is "*part of the Department of Homeland Security that leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. CISA connect their stakeholders in industry and government to each other and to resources, analyses, and tools to help them build their own cyber, communications, physical security, and resilience. This helps ensure a secure, resilient infrastructure for the American people.*" In addition to CISA's **Zero Trust model** referenced in the memorandum mentioned earlier, CISA has many resources related to MFA and its benefits. For example, the MFA page (`https://www.cisa.gov/mfa`) includes links describing how to enable MFA for use with the government and consumers. Resources for consumers, for example, explain how to set up MFA for Microsoft accounts, Facebook, Gmail, and Apple ID.

Other valuable documents from CISA include the following:

- *Implementing Strong Authentication* (`https://www.cisa.gov/sites/default/files/publications/CISA_CEG_Implementing_Strong_Authentication_508_1.pdf`)
- *Implementing number matching in MFA applications* (`https://www.cisa.gov/sites/default/files/publications/fact-sheet-implement-number-matching-in-mfa-applications-508c`)

## National Institute of Standards and Technology

**National Institute of Standards and Technology** (**NIST**) is a non-regulatory agency of the United States Department of Commerce responsible for promoting innovation and industrial competitiveness. NIST's activities are organized into laboratory programs focusing on physical science, engineering, applied technology, information security, and communication standards.

NIST publishes digital identity guidelines that the government and private companies widely use. For example, its famous *NIST Special Publication 800-63-3 Digital Identity Guidelines* (`https://pages.nist.gov/800-63-3/sp800-63-3.html`) describe identity guidelines in three significant areas:

- Enrollment and identity proofing (SP 800-63A)
- Authentication and life cycle management (SP 800-63B)
- Federation and assertions (SP 800-63C)

As part of authentication and life cycle management, it defines the **authentication assurance level** (**AAL**) that helps companies decide which types of MFA they require, depending on the level of assurance that the user being authenticated is who they claim to be. NIST also publishes a blog with cybersecurity insights (`https://www.nist.gov/blogs/cybersecurity-insights`) and several security-related special projects, such as *Multifactor Authentication for E-Commerce* (`https://www.nccoe.nist.gov/multifactor-authentication-e-commerce`).

## National Security Agency

The **National Security Agency** (**NSA**) leads the US government in signals intelligence insights and cybersecurity services and products. The NSA's Cybersecurity Collaboration Center harnesses the power of industry partnerships to prevent and eradicate foreign cyber threats.

One of NSA's publications is the *Assessment of common multi-factor authentication solutions* (`https://media.defense.gov/2020/Sep/22/2002502665/-1/-1/0/CSI_MULTIFACTOR_AUTHENTICATION_SOLUTIONS_UOO17091520.PDF`). The document reviews commonly used MFA mechanisms against NIST standards.

Other US government websites include the **Government Services Administration** (creators of `Login.gov`, the public's one account and password for business with the government) and websites that focus on specific industries, such as the **National Credit Union Administration** (**NCUA**). One example of a publication from NCUA is *Guidance on Authentication in Internet Banking Environment* (`https://ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/guidance-authentication-internet-banking-environment`).

The European Union is also a giant in cybersecurity and privacy topics. The website `https://digital-strategy.ec.europa.eu/en/policies/cybersecurity` in particular is a good example. It "*aims to build resilience to cyber threats and ensure citizens and businesses benefit from trustworthy digital technologies*."

Other countries also provide resources related to MFA. The UK's **National Cyber Security Centre** (**NCSC**) is a good example. Its goal is "*Helping to make the UK the safest place to live and work online. Understands cyber security, and distills this knowledge into practical guidance*." NCSC publishes guidance documents on passwords, authentication, phishing, and more. In addition, guidance documents are available for organizations (such as *Advice for organisations on implementing multi-factor authentication*: `https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services` and customers to recognize common scams.

Similarly, in Australia, the Australian Cyber Security Council provides essential and simplified guidance to its citizens that can benefit anyone. An excellent place to start is `https://www.cyber.gov.au/`.

As listed in this section, the US government and other countries offer useful information on security and MFA through their websites. These resources provide up-to-date information on new security threats and how they impact the use of MFA by organizations and individual users.

## Summary

In this chapter, you were introduced to how fraud schemes can impact different authentication factors and how to reduce the associated risks. You were also provided with a comprehensive overview of the various sources to follow to stay informed about the latest security threats and the measures that can be taken to counteract them.

With the information you have acquired in this chapter, you are now equipped to understand the importance of MFA in ensuring the security of an organization's workforce. In the next chapter, we will delve into a specific case study of how ACME Corporation has utilized Microsoft's **Azure Active Directory** (**AAD**) to implement MFA and improve the security of its workforce. This chapter will give you a hands-on understanding of how MFA can be integrated into an organization's existing infrastructure and how it can provide a more robust layer of security to protect against potential threats.