CYBER WORKS

# Authentication

## Are you really who you say you are?

Audience: General

Reading Time: 20 Mins

*Multi-factor authentication is one of the easiest methods to ensure that your accounts stay secure, and no one apart from you can access your personal data. A wide range of methods are available on almost all websites, and there is little reason not to enable it!*

## Key Points

- Authentication and Authorisation are foundation principles to internet and information security.
- Multi-factor authentication enables the security of an account to be increased dramatically, with little time or effort.
- Password managers can be used to store and automatically fill our passwords on login pages – making it easy to use long, complex passwords.
- Using existing accounts to sign into 3rd party apps or websites can greatly reduce the number of account details we have to remember.
- Password-less authentication makes it much easier to login to our accounts, meaning we no longer have to remember our passwords.

# Authentication

**Authentication** and **Authorisation** are both integral to almost every single task we do online. We *authenticate* and *authorise* multiple times a day, often without even realising it. So, what are authentication and authorisation and how do we authenticate and authorise on the web?

Put simply, authentication is determining if someone is who they say they are; and authorisation is the process of determining if that someone is permitted to do what they are trying to do. When you want to enter a country you use your passport to authenticate yourself. The passport officer is able to verify that you are indeed who you claim to be, and your passport is also authenticated to ensure that it is real. Your passport and/or visa is used to authorise that you are permitted to enter the country.

## What is Authentication?

Authentication is the process or action of verifying the identity of a user; ensuring that the user is who they claim to be. When you authenticate you do so with an identity, and you aim to prove that the identity belongs to you. This identity, or digital identity, can be one of many things, such as a username, email address or account number. Once we know which identity we want to authenticate, we need to prove that we are the owner of that identity. Once we have proven that we are the owner of the identity, we are authenticated. Simple enough, but how does authentication work?

### Definitions

**Authentication** - The process of determining if someone is who they say they are.

**Authorisation** - The process of determining what someone is allowed to do with certain data or resources.

**One-time password** - A password that is very short lived and can only be used once, often used as a two-factor authentication method.

**Two-Factor Authentication (2FA)** - A system in which two different methods are required to authenticate.

**"Need to Know" & "Least Privilege"** - Principle methods to restrict who can view information, what they can do with it and how long they have access to the information for.

**Data Breach** - An event where someone who does not have permission to access certain data does so. Usually associated with hackers stealing data from websites. These can contain a huge amount of sensitive data about people.

The ways in which we can authenticate fall into three categories:

- **Knowlege -** something you know
- **Ownership -** something you have
- **Characteristic -** something you are

Multi-factor authentication is authentication that requires methods from multiple of the above categories. This gives a higher level of security as it makes it much more difficult for someone who is not you to authenticate as you. **Two-factor authentication (2FA)** is a type of multi-factor authentication that

uses methods from exactly two of the above categories.

To withdraw money at a cash machine, you need both your card (something you have) and your PIN (something you know) to withdraw money. Therefore, requiring two-factors for your authentication.

Increasingly common is password-less authentication, this is currently offered by both Google and Microsoft, which enables you to login with just ownership and characteristic methods - not requiring any knowledge factors. This aims to both increase security as knowledge-based factors have traditionally offered poor security, and to make authentication an easier process.

## What is Authorisation?

Authorisation is the process which determines what an authenticated identity can do. For example, once you have authenticated to login to your bank account, authorisation ensures that you can only see your own account balance, and only send money from your account.

Authorisation can take many forms and can be applied to many scenarios:

- Authorise someone else to view or edit a file on OneDrive
- Authorise someone to see a private GitHub repo
- Authorise a 3rd party-app or website to access your data
- Authorise people to view your profile, photos, and friends on Facebook

Generally, and except in special circumstances, access is not granted by default. You would only authorise a party access to your data or a resource if absolutely necessary, and this should be done for the minimum time and with the least privilege necessary. These are known as the **"need to know"** and **"least privilege"** principles. These ensure that a party (a person, website, or app) is only given the minimum amount of information, duration and abilities required to complete their given task.

For example, if you would like a colleague to review a piece of work you have stored on say, OneDrive, you can share this document with them and only giving them the "View only" permission. This ensures that they can only see the document, but not edit it and may simply send you their feedback in an email. Once they have reviewed the document, you can revoke their permission as they no longer require it, and will no longer be able to see it. With online storage providers such as OneDrive, Google Drive or Dropbox, this can easily be achieved with the click of a button or two.

## Knowledge - Something You Know

- Passwords
- PINs
- Passphrases
- Security Questions

The *something you know* authentication methods are ones you are probably already familiar with – they are the ones we all struggle to remember. However, these can often be the weak points of account security. Due to the fact we need to remember these, we tend to choose easy to remember passwords and reuse these everywhere. Humans are predictable creatures, and someone trying to gain access to your account may be able to quickly guess your details. The problem is amplified if you use

the same password everywhere, because if the manage to access one then they can access all your accounts!

An attacker trying to guess your password will leverage these two factors to increase their likelihood of gaining access to your account. Data breaches happen all the time, where hackers gain unauthorised access to data held by websites, they then sell this data. This data often contains email addresses and passwords of users from the affected website. Attackers can use these breaches to identify the most common passwords and identify accounts whose passwords have been leaked and try to login to other websites with the same email and passwords.

However, you can also take advantage of these data breaches too to make your accounts more secure. Troy Hunt (@troyhunt on Twitter) is an Australian Cyber Security researcher, he runs the website https://haveibeenpwned.com. He tracks data breaches and uses his website to enable people to identity if their accounts have been included in a breach and see how often their password has been breached. You can see if your email address has been included in a breach at the website above. You can also see how often a password has been seen in a data breach.

If you own a domain name, for example for your business, you can also register to be informed if any emails for your domain have been breached. Furthermore, security questions are traditionally a very poor method of knowledge-based authentication. This is often due to a poor choice or selection of security questions. These often have answers that are in the public domain: your birthday, place of birth, mother's maiden name or pet name, for example.
Beware of what information you give away on social media. A common example, though varied on the theme, are "challenges" to get you to post your "Superhero Name" by simply combining the name of your favourite pet, your street name, and mother's maiden name. Unfortunately, each constituent part is actually a potentially sensitive piece of your personal data. Data that is often used to secure online account information.

> "Beware of what information you give away on social media"

A password manager is a tool that can be used to create and store passwords on your behalf. These come packaged with most browsers, they can suggest strong passwords and then automatically fill these in on login pages. This may result in increased account security as we now do not have to remember our passwords. We can safely create more complex passwords and simply get the password manager to fill these out for us. However, the password manager itself can be a weak point, if it stores all your passwords then if someone were to gain access to this, they will gain access to all your accounts!

A solution to this is to choose a very strong password for your password manager – but you will have to remember this one! Multi-factor authentication should be enabled on

your password manager, and all the accounts it protects. Furthermore, you may wish to pick-and-choose which accounts you store in your password manager.

**Ownership - Something you Have**

- One-time Password (SMS OTP, Email OTP, TOTP or HOTP)
- Certificate
- Hardware Security Key
- Smartcard

*Something you have* methods mostly involve you having a physical device in your possession. To authenticate, you simply hand over the device and the website will check that it belongs to the user you are attempting to authenticate as. Other methods, such as One-time passwords (OTPs) and certificates, are software methods but are used in the same way. These methods are much easier to use than *something you know* methods as there is nothing to remember. However, you need to ensure that you do not lose access to the item – otherwise you may lose access to your account.

There are two major types of One-time passwords: those that you generate yourself, usually on an app, and those that are sent to you, usually via text message or email.

User generated one-time passwords are passwords that are automatically generated based upon either the current time or a counter, and something known only to the party you are trying to authenticate with and yourself. These are often manifested on mobile apps, such as Google Authenticator, Microsoft Authenticator or Authy. To set these up, the website usually presents you with a QR code which you scan with your chosen authenticator app. When you need to authenticate, the app will then present a 6 or 8 digit code which you can then use to login.

On the other hand, OTPs can be sent to either your phone number or email address when you try to login which can then be entered on the website. This method ensures that you have access to either the phone number or email address associated with your account.

However, text message based OTPs have faced criticism. Through a technique called "sim jacking", sometimes called "sim swapping" an attacker somehow hijacks your phone number and will thus receive the OTP instead of you,

meaning that they may be able to login to your account. As such, SMS OTPs should not be used when other methods are available. However, despite the criticisms, utilising SMS based OTPs are still better than using no OTPs.

A certificate is simply a file that is issued to you from the website. When authenticating you send the certificate to the website so the website. This verifies that the certificate belongs to you and was issued by the website in question – like a passport.

Hardware security keys and smart cards are both similar, but their representations are different. Hardware security keys are usually USB sticks that may also be contactless, meanwhile smartcards are similar in look to credit cards. These work in the same way to certificates, but the certificate is stored on the hardware device instead. To authenticate, you simply insert the device into your computer which will recognise it as a device used for authentication and will send the certificate to the website.

# Authentication

Research conducted by Google has shown that hardware security keys, which it offers as a method on all Google accounts, prevents 100% of account takeover attempts.

## Characteristic - Something You Are

- Fingerprint
- Eye
- Voice
- Face (Face ID)

*Something you are* methods rely on physical attributes of your body, such as your fingerprint, eyes, voice or face, all forms of biometrics. Again, these are much better than "something you know" methods as there is nothing to forget and are also better than the "something you have" methods as there is nothing you can lose. These methods are becoming more popular and are nearly ubiquitous on the latest mobile phone models.

## Password-less Authentication

Password-less authentication is the latest method of authentication being used by both Google and Microsoft. It aims to eliminate the need for passwords completely; relying only on "something you have" and "something you are" methods of authentication instead. Passwords are hard to use, we must choose a unique, complex password for every single website or service, and are a common weak point in system security.

Authentication methods where the website will send you a notification on a device such as a mobile phone, that require you to confirm it is you attempting to authenticate to your account also form part of this.

## Sign in with...

An alternative to creating a new account for each website, and thus new authentication credentials (passwords, OTPs, certificates, and keys), is to login to that new website with one of your existing accounts. This means that you can use an account you already have to login to a 3rd party website, this means you do not need to create a new account and remember a new password. Not all websites offer this 3rd party sign in, but Google, Apple and Facebook all do. This is often shown as a button on the same page as where you would register an account, usually of the form "Sign in with..." or "Continue with...".

## In Summary

Authentication and Authorisation are the foundations of maintaining secure access to data; they allow you do ensure someone is who they say they are and create fine-grained access controls. Multi-factor authentication can be achieved using a huge variety of methods, from simple passwords we all struggle to remember to certificates and biometrics.

Multi-factor authentication should be added to all accounts where available to add an additional degree of security to your accounts – to prevent others from accessing your accounts.

More streamlined, password-less methods are becoming available which aim to increase security and make authentication a more straightforward process.

Password managers can help us create more complex passwords and store these, so we do not have to remember them; but should be used with caution.

## READ MORE


1. NCSC. Passwords, passwords everywhere. [ONLINE] Available at: https://www.ncsc.gov.uk/blog-post/passwords-passwords-everywhere [Accessed 13th September 2020]

2. Google. 2019. New research: How effective is basic account hygiene at preventing hijacking. [ONLINE] Available at: https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html. [Accessed 13th September 2020]

3. Microsoft. The end of passwords, go passwordless. [ONLINE] Available at: https://www.microsoft.com/en-gb/security/business/identity/passwordless. [Accessed 13th September 2020]

4. VICE. 2019. SIM-Jackers Can Empty Your Bank Account with a Single Phone Call. [ONLINE] Available at: https://www.vice.com/en_uk/article/3kx4ej/sim-jacking-mobile-phone-fraud. [Accessed 13th September 2020]

5. Microsoft. Share OneDrive files and folders. [ONLINE] Available at: https://support.microsoft.com/en-us/office/share-onedrive-files-and-folders-9fcc2f7d-de0c-4cec-93b0-a82024800c07. [Accessed 13th September 2020]

6. Troy Hunt. Haveibeenpwned.com [ONLINE] Available at: https://haveibeenpwned.com/. [Accessed 13th September 2020]




# About the Author

**Henry Clarke** is currently studying at Lancaster University. Henry has completed his BSc in Computer Science at Lancaster and is now studying his MSc in Cyber Security. Henry is part of Lancaster's Cyber Security society **LUHack**, his interests are cyber security and programming.