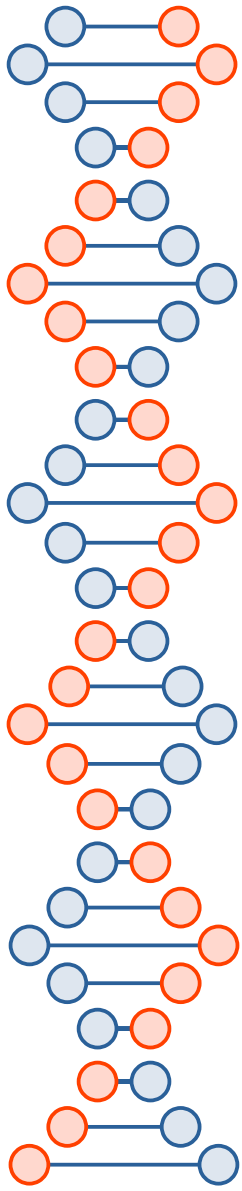


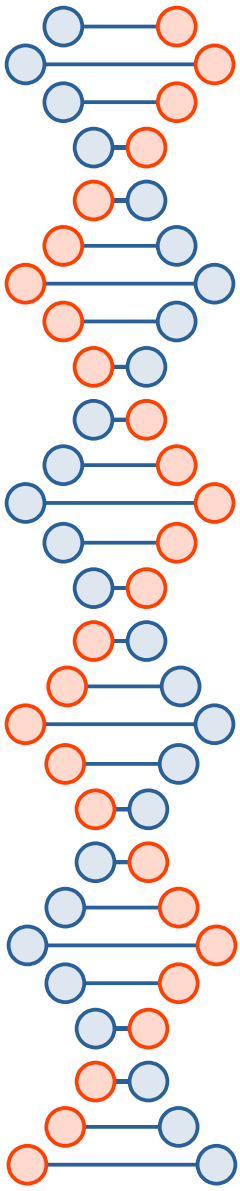
# MFA

## Multi-Factor Authentication



# MFA

## Definition of MFA



# MFA

Multi-factor authentication, MFA, two-factor authentication, or 2FA, along with similar terms, is an electronic authentication method in which a user is granted access to a device, website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism:

**knowledge** (something only the user knows)

**possession** (something only the user has), and

**inherence** (something only the user is).

**MFA** protects user data—which may include personal identification or financial assets from being accessed by an unauthorized third party that may have been able to discover, for example, a single password.

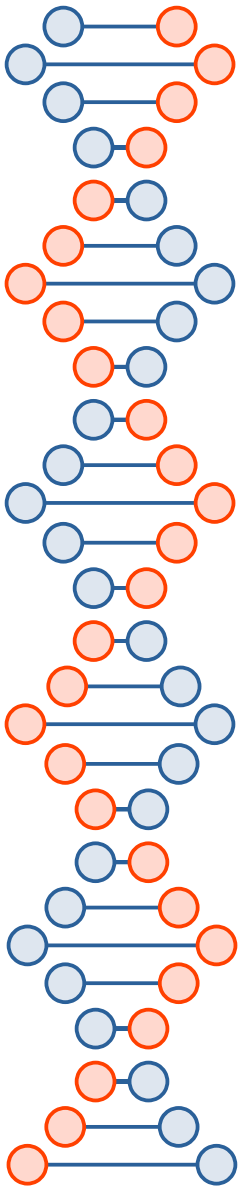
We will explain the most common uses of **MFA** today, and how **MFA** is being implemented in our environment (research computing).

# MFA

## Knowledge

**Knowledge** factors are a form of authentication. In this form, the user is required to prove knowledge of a secret in order to authenticate.

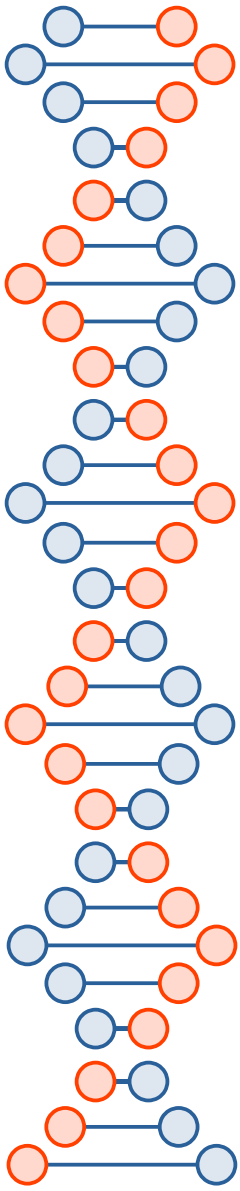
A password is a secret word or string of characters that is used for user authentication. This is the most commonly used mechanism of authentication. Many multi-factor authentication techniques rely on passwords as one factor of authentication. Variations include both longer ones formed from multiple words (a passphrase) and the shorter, purely numeric, PIN commonly used for ATM access. Traditionally, passwords are expected to be memorized.



# MFA

## Possession

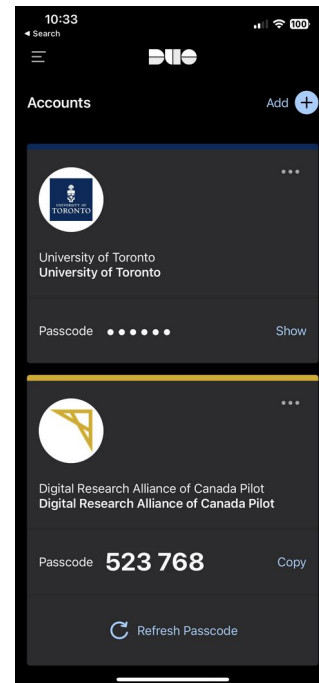
**Possession** factors ("something only the user has") have been used for authentication for centuries, in the form of a key to a lock. The basic principle is that the key embodies a secret that is shared between the lock and the key, and the same principle underlies possession factor authentication in computer systems. A security token is an example of a possession factor.



# MFA

## Possession (continued)

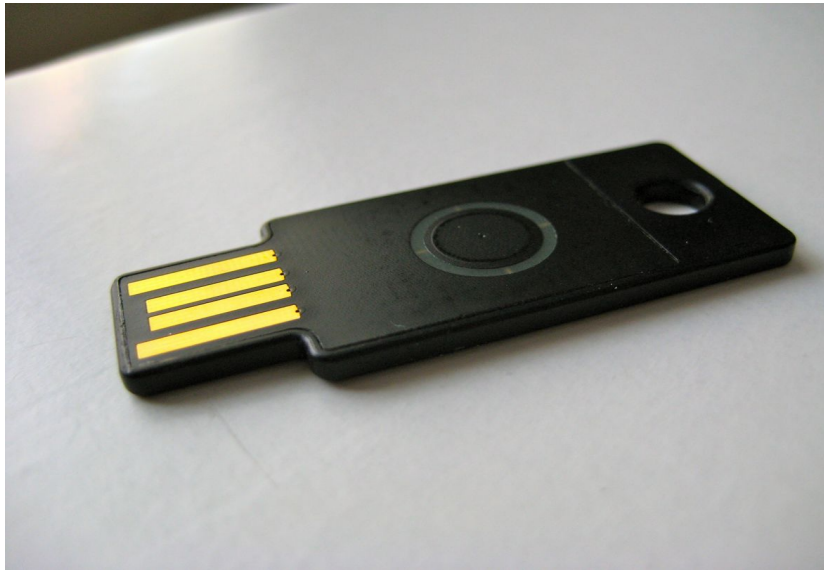
Disconnected tokens have no connections to the client computer. They typically use a built-in screen to display the generated authentication data, which is manually typed in by the user. This type of token mostly uses a OTP (One Time Password) that can only be used for that specific session.



# MFA

## Possession (continued)

Connected tokens are devices that are physically connected to the computer to be used. Those devices transmit data automatically. There are a number of different types, including USB tokens, smart cards and wireless tags.

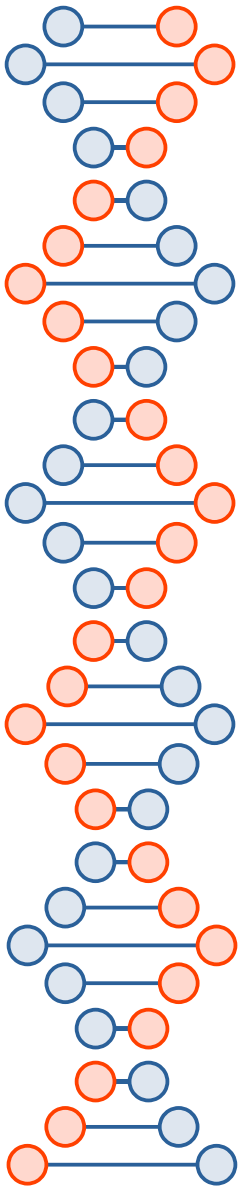


# MFA

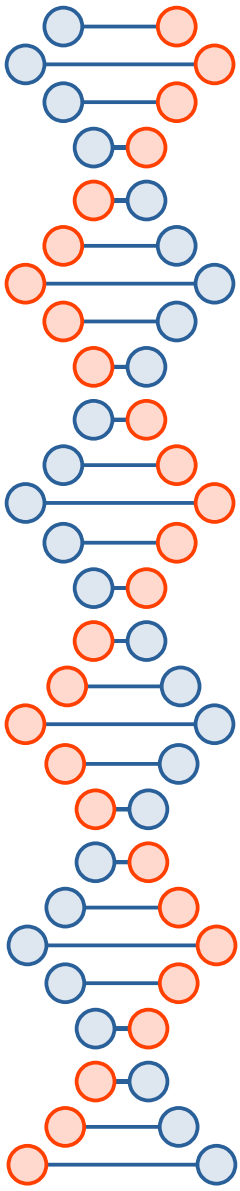
## Inherent

These are factors associated with the user, and are usually biometric methods, including fingerprint, face, voice, or iris recognition. Behavioural biometrics such as keystroke dynamics can also be used.

Multi-factor authentication also has application in physical security systems. These physical security systems are known and commonly referred to as access control. Multi-factor authentication is typically deployed in access control systems through the use, firstly, of a physical possession (such as a fob, keycard, or QR-code displayed on a device) which acts as the identification credential, and secondly, a validation of one's identity such as facial biometrics or retinal scan. This form of multi-factor authentication is commonly referred to as facial verification or facial authentication







# MFA

Why is MFA important in IT security?

# MFA

## Some Password Hacks:

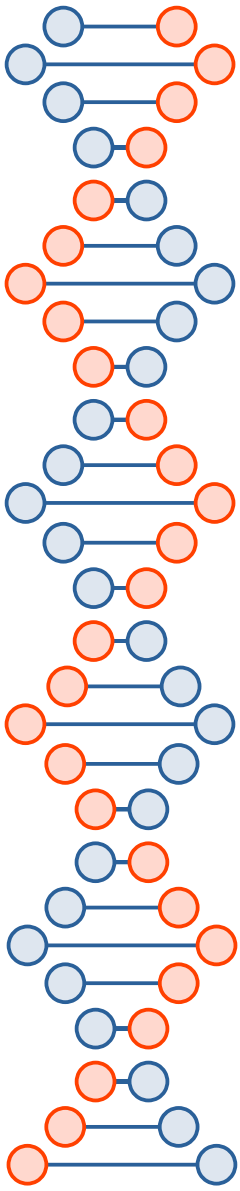
- PlayStation Network (2011)  
77 Million accounts hacked
- Adobe (2013)  
38 Million accounts hacked
- Yahoo (2014)  
3 Billion accounts hacked (that B is not a typo)
- Under Armour (2018)  
150 Million accounts hacked

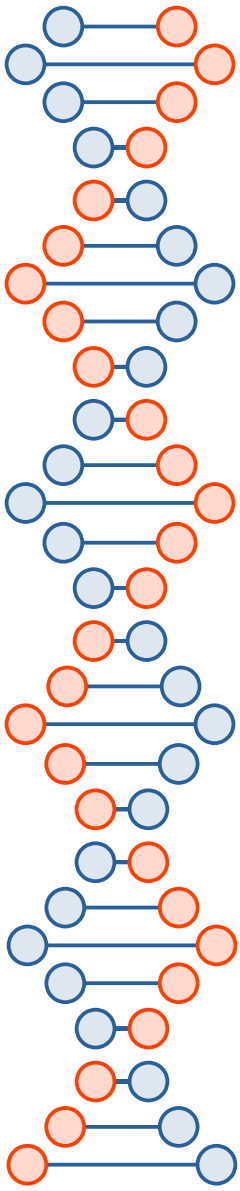
# MFA

Why passwords are easily hacked.

Hackers have several methods to get your password such as social engineering, brute force, malware, phishing, among others.

Basically, if a hacker wants your password they will get it; one way or another.





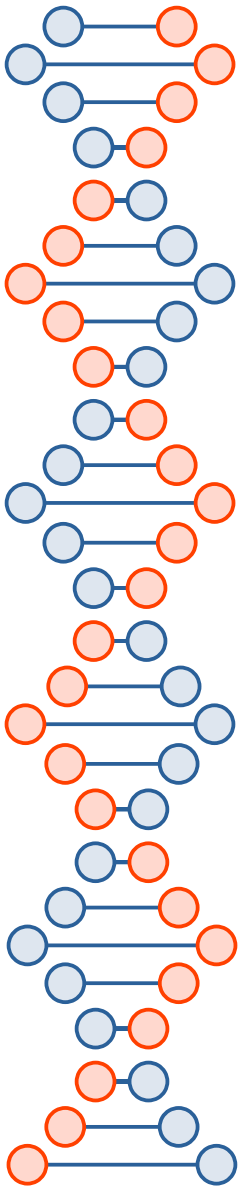
# MFA

You can't stop a data breach, but you can make your password less useful to hackers.

How?

Use MFA if possible.

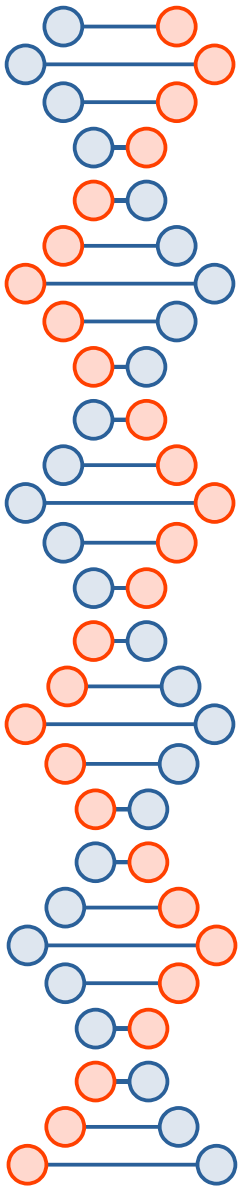
Even if someone gains access to your password, you still might be protected.



# MFA

The main benefit of MFA is it will enhance your organization's security by requiring users to identify themselves by more than a username and password.

While important, usernames and passwords are vulnerable to brute force attacks and can be stolen by third parties. Enforcing the use of an MFA factor like a thumbprint or physical hardware key means increased confidence that your organization will stay safe from cyber criminals.

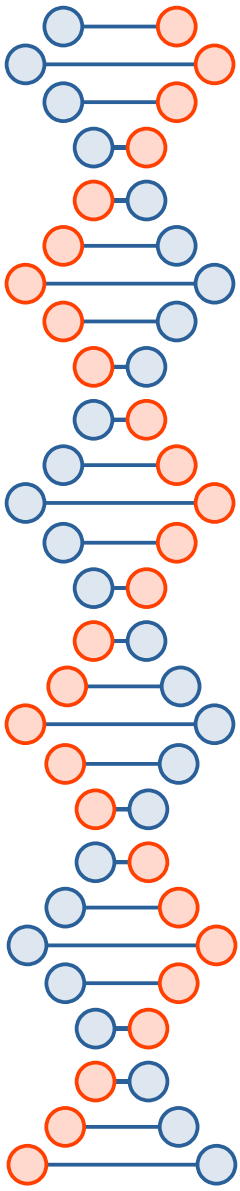


# MFA

MFA at The University of Toronto

## UTORMFA

**UTORMFA**  
Login with Confidence



# MFA

The University of Toronto chose DUO as the Multi-Factor Authentication provider:

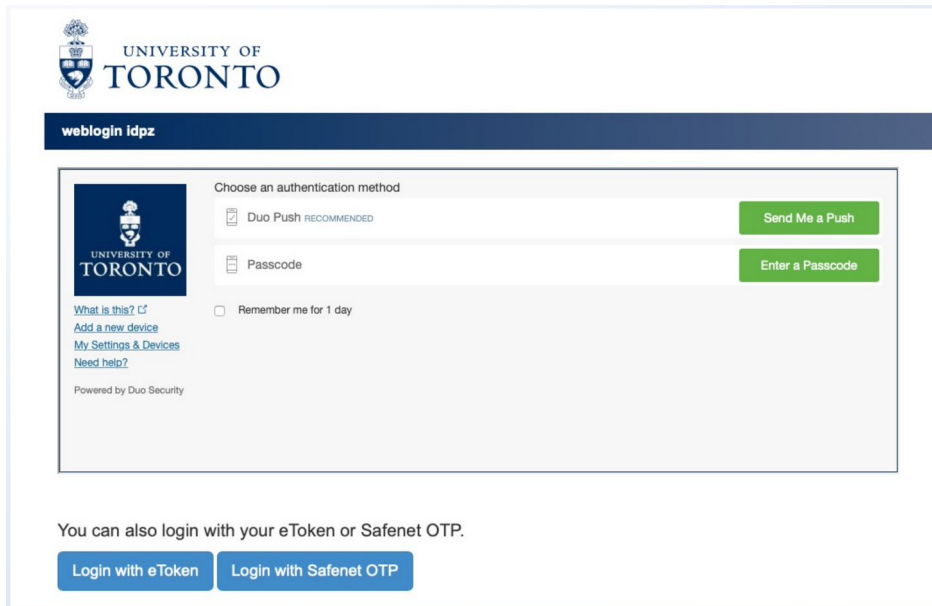


DUO is a Cisco company:



# MFA

When connecting to a UofT web site or system, first the user will provide a username and a password as usual, then the user will be prompted to provide a second factor:

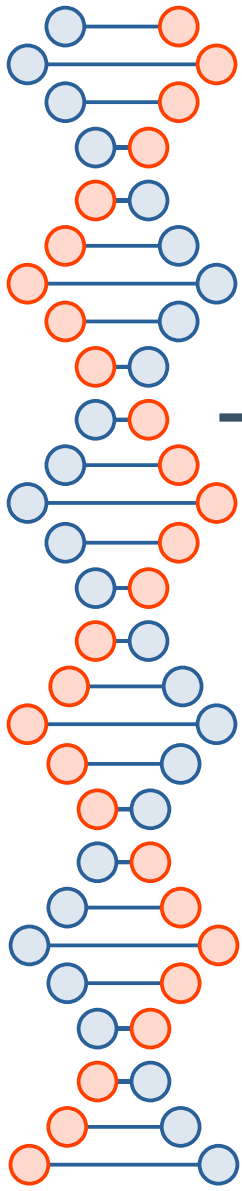


The screenshot shows the University of Toronto weblogin idpz interface. At the top left is the University of Toronto logo. Below it is a dark blue header with the text "weblogin idpz". The main content area is titled "Choose an authentication method" and contains two options: "Duo Push RECOMMENDED" with a "Send Me a Push" button, and "Passcode" with an "Enter a Passcode" button. There is also a checkbox for "Remember me for 1 day". On the left side of the main content area, there is a small University of Toronto logo and links for "What is this?", "Add a new device", "My Settings & Devices", and "Need help?". Below the main content area, there is a note: "You can also login with your eToken or Safenet OTP." and two buttons: "Login with eToken" and "Login with Safenet OTP".

The user then may choose to provide an OTP (One Time Password) provided by the DUO app, or to receive a “PUSH”.

When using “PUSH” the user will receive a notification in their phone asking for their approval.





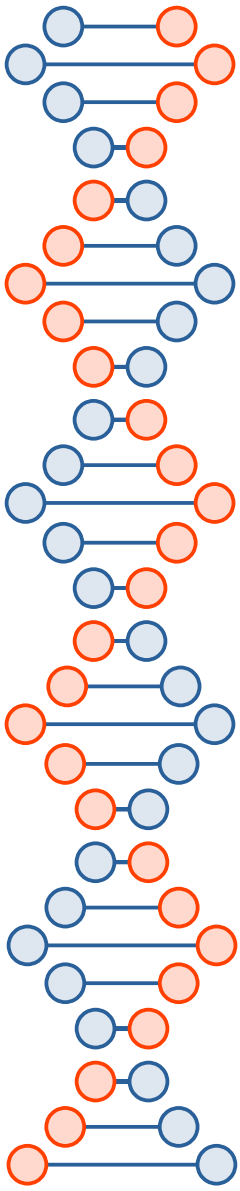
# MFA

## MFA at The Digital Research Alliance of Canada



**Digital Research  
Alliance** of Canada

**Alliance de recherche  
numérique** du Canada



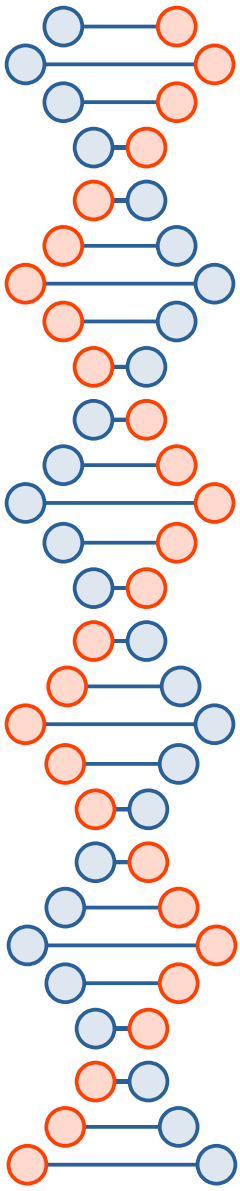
# MFA

The Digital Research Alliance of Canada also chose DUO as the Multi-Factor Authentication provider:



DUO is a Cisco company:





# MFA

The Digital Research Alliance of Canada was deciding between two viable solutions:



# MFA

## Google Authenticator

If you were to implement your own MFA solution for your own use or your department use, Google Authenticator is a good, open source and free option.

Google Authenticator can be deployed in Linux servers.

On the client side, users just have to download the Google Authenticator app, which runs on virtually any cellular phone platform.

Google Authenticator uses TOTP (Time-based One Time Password)

