NCSC
National Cyber
Security Centre

Multi Factor Authentication

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Multi Factor Authentication

A Quick Guide

Move Beyond Passwords

Passwords are the most common form of authentication, but they are the least secure. Research by Google found that 52% of users reuse the same password for multiple accounts. Users often choose passwords that are easy to remember but are also easy to guess, such as using their children's names or their favourite football team. Threat actors can access passwords via phishing or avail of billions of stolen usernames and passwords available on the dark web to use in attacks on online digital service accounts.

What is Multi-Factor Authentication?

Multi-factor authentication (MFA) is a security measure that requires two or more proofs of identity to grant a user access to a network, system, or application.

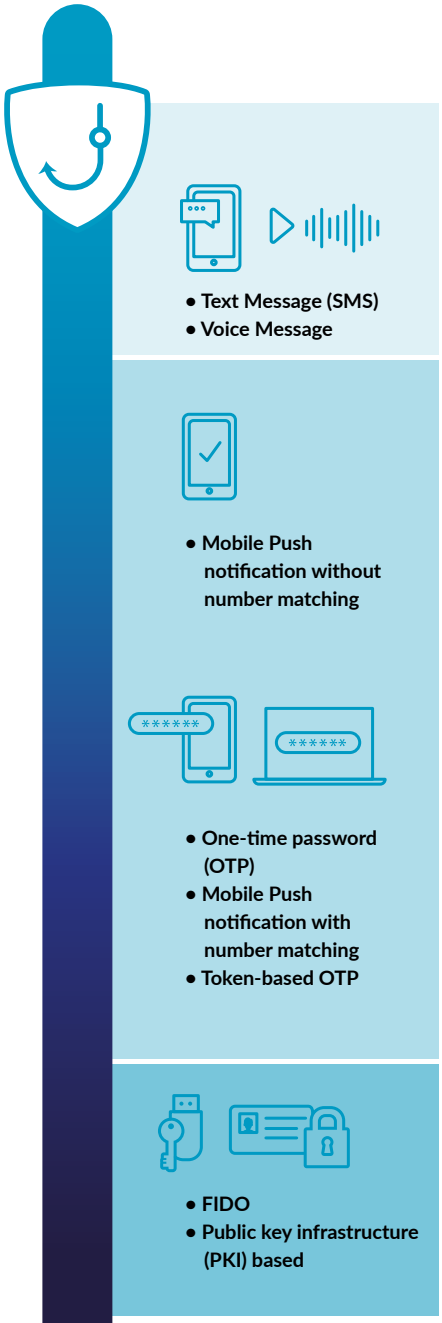
How does MFA work?

MFA typically works by requiring one or more verification factors such as scanning a fingerprint or entering a code received by phone in addition to a traditional user ID and password. MFA makes user accounts and computer systems much more secure. If a user's primary credentials are compromised, a threat actor still needs the secondary authentication factor to gain access.

Most authentication factors can be categorized into one of the following groups:

- **Something You Know:** This includes PINs and passwords created by the user, as well as answers to security questions.
- **Something You Have:** This credential requires users to generate or receive security tokens or certificates. This can be done using an authenticator application, or a time sensitive One-Time-Password **(OTP)** delivered by SMS, email, or secure link.
- **Something You Are:** This includes biometric identifiers based on physiological characteristics such as fingerprints, facial or voice recognition.

Weakest



Strongest

MFA For Your Organisation

There are many types of authentication/ authorisation methods that organisations can implement to authenticate their customers when accessing online services.

SMS or Voice: This is a weak type of MFA which works by sending a code to the user's phone or email. The user then retrieves this second factor code from their text or email inbox to use for login authentication. This is the weakest form of MFA. It is vulnerable to phishing, and SIM swap attacks.

App-based authentication: This is stronger than SMS or Voice MFA. Examples of app-based authentication include one-time password (OTP), mobile push notification and token-Based OTP. They verify a user's identity either by generating OTP codes or by sending "push" pop-up notifications to a user's mobile application for their approval.

Mobile Push Notifications are vulnerable to MFA fatigue, where scammers use a strategy in which they bombard victims with MFA push notifications until they slip up and mistakenly authenticate the wrong login attempts. This method can be further strengthened by using number matching. This is an additional step between receiving and accepting the prompt. The user is required to enter numbers from the identity platform into the application to approve the authentication request.

Phishing-resistant MFA: This is currently the gold standard in MFA. This involves the same authentication process, but people are removed from the process as much as possible. The most common way to implement this is through the FIDO2 standard which uses "WebAuthn" technology. This can significantly reduce the risk of phishing as well as the usefulness of a stolen session token.

Multi Factor Authentication

A Quick Guide

How Do I Enable MFA?

Users can often enable MFA in their account's security settings, or when they create an account. A user may see options to enable MFA listed as "Two Factor Authentication". Popular forms of MFA include authenticator applications such as Google Authenticator, and One-Time-Passwords (OTP) received via email or SMS. A guide on how to set up MFA on different accounts is found below under Further Information.

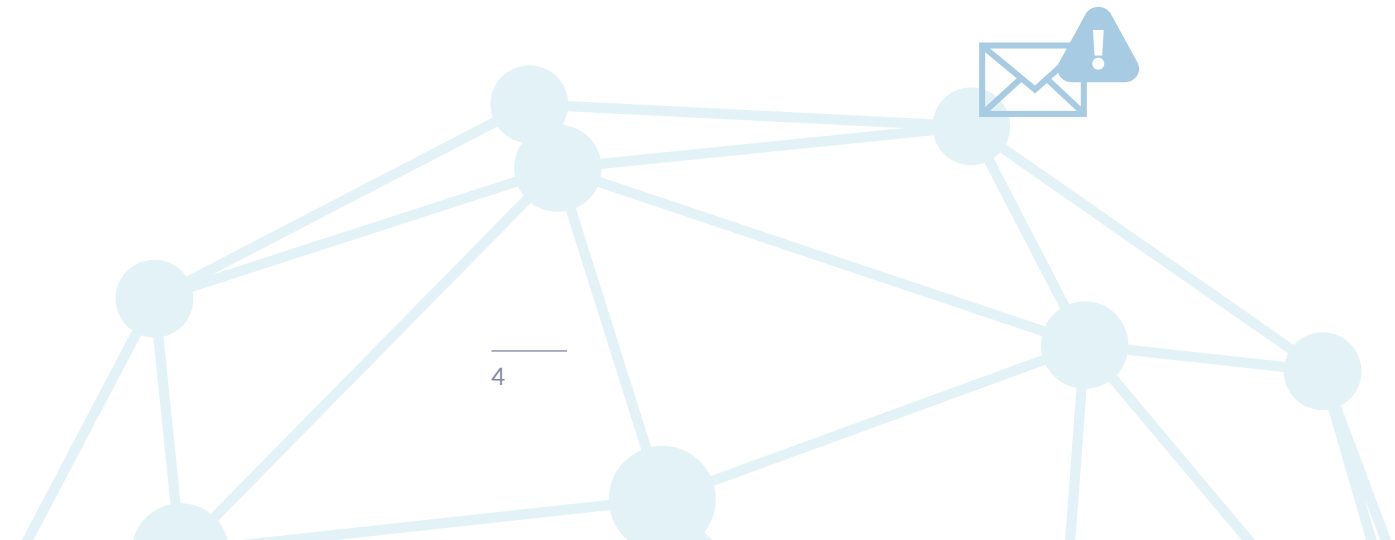
When should I use MFA?

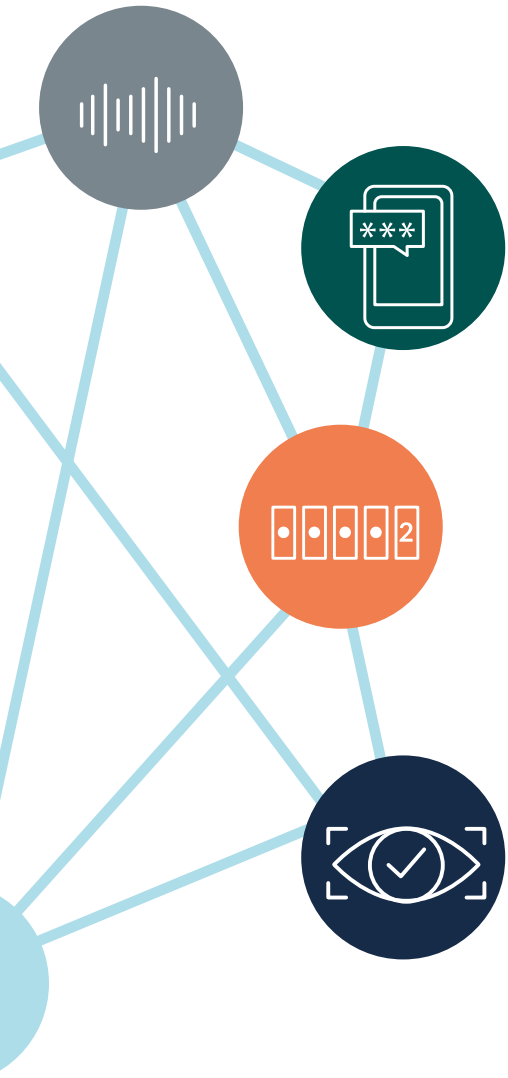
You should use MFA wherever possible, especially when it comes to your most sensitive data like your primary email, your financial accounts, and your health records.

MFA is not a silver bullet cybersecurity solution, but it is vastly superior to just passwords alone. It is important to note that MFA, when combined with other basic security hygiene - utilizing antimalware, applying least privilege principles, keeping software up to date and protecting data - still protects against 98% of all attacks.

Reporting

If you are the victim of a crime, it should be reported to your local Garda station. If you are a constituent of the NCSC, or you feel the incident is of national importance, you may also report cybersecurity incidents to the NCSC at certreport@decc.gov.ie or info@ncsc.gov.ie.





Multi Factor Authentication

A Quick Guide

Further Information

Additional guidance resources can be found on the NCSC website using the following links:

NCSC Guidance

https://twitter.com/ncsc_gov_ie

https://www.ncsc.gov.ie/

A guide on how to activate MFA on popular platforms can be found on the Australian Cyber Security Centre website;

Easy steps to secure your devices and accounts | Cyber.gov.au

Google Security Research

Google

Authentication methods: choosing the right type

Ncsc UK

Implementing Number Matching in MFA Applications

CISA

FIDO Alliance - Open Authentication Standards More Secure than Passwords

FIDO Alliance

Token tactics: How to prevent, detect, and respond to cloud token theft

Microsoft

Microsoft Digital Defense Report 2022

Microsoft

Contact Us

National Cyber Security Centre,
Department of the Environment, Climate and Communications,
29-31 Adelaide Road, Dublin, D02 X285, Ireland.

If you believe that you are experiencing a cyber security incident that is of national concern and wish to notify us directly you may email us at: incident@ncsc.gov.ie **or** certreport@decc.gov.ie

For any other matter please email: info@ncsc.gov.ie

+353 1 6782333

@ncsc_gov_ie

www.ncsc.gov.ie

An Roinn Comhshaoil, Aeráide agus Cumarsáide
Department of the Environment, Climate and Communications

NCSC
National Cyber Security Centre