# Multifactor Authentication

**What is Multifactor Authentication?**

Multifactor Authentication (MFA) is a security control that requires two or more factors to prove identity to gain access to a system. MFA requires something user know (password or PIN) and something you have (token or key card) or something you are (biometric such as fingerprint).

Key benefits of MFA are:

* Security against identity theft via stolen passwords
* Protect against weak employee passwords
* Mitigate the use of unmanaged devices
* Stay Compliant

**Where things can go wrong without Multifactor Authentication.**

In 2020 Nintendo suffered a data breach affecting 160,000 people resulting account takeovers and financial loses for set of users. The cause of the attack was a combination of malware and previously stolen passwords to take over vulnerable accounts. Hackers used account checker tools to scan lists of stolen credentials to find credentials matched to user’s credentials to exploit the accounts.

https://www.techrepublic.com/article/nintendo-data-breach-reportedly-caused-by-credential-stuffing/

**Where your organization may require Fortify’s advisory service.**

You believe your staff is following password complexity requirements and they know how to defend against a Phishing Attack. But in reality, credential theft can still occur as hackers use sophisticated techniques, social engineering and phishing email attacks.

Multifactor Authentication adds a strong element of protection against credential theft and you are keen to implement such solution so as to protect your organisation.

An MFA solution can be challenging and expensive to implement and you know that need to get professional assistance to establish and enable a solution. Being a small not-for-profit organization, you have a very limited budget to get this done. You are also not aware of whom to approach and how to go on about engaging a consultant to help you achieve what is required.

**Where Fortify can help**

Fortify is a not-for-profit organization with cybersecurity expertise, resourced by volunteer professionals. We provided Cybersecurity advisory services at minimal, or at no cost, to assist organizations such as yours that have limited resources.

* Fortify will provide a self-assessment guideline and questionnaire so you can assess your requirements in this area.
* Depending on your needs we will then assign a professional consultant to review your environment and propose a solution with estimated cost.
* The Fortify consultants can assist configure and enable MFA for the organisation.
* Where licencing, devices and other software are required, the consultant will scope of what is required for a procurement activity.
* Fortify consultants will test the solution for successful deployment and will train and provide information to your staff on how to use MFA in accessing their accounts and systems.

**How to engage Fortify**

There are a few simple steps to follow in engaging our services

1. Go to the website: fortify.com.au
2. Register your organization
3. Read the guidelines and start to complete the self-assessment questionnaire. Please allow 50 minutes to complete the questionnaire as some areas may be complicated and require some careful thought
4. If you required assistance to complete the questionnaire, please submit a request via the “require assistance” button or go to fortify.com.au/assistance.