

# Your Password

your online safety



Photo by [Muhammad-taha Ibrahim](#) on [Unsplash](#)

*Have you experienced that dreadful feeling after receiving an email that reads: “Someone logged into your account” and you know it wasn’t you?*

*A weak password, and generally poor password security, can put all your accounts in danger from online threats. Significant financial and reputational losses have been experienced by many arising from this and getting back on your feet after such may take ages. Protecting your confidential information from cyber threats starts with having a good password etiquette.*

## What are passwords

A password is an arbitrary string of characters used to authenticate that the provider is who he claims he is and determine the level of access to resources that the user is entitled to. The use of passwords in human civilization goes back to ancient times, especially in security where guards challenge those wishing to access secured areas to provide a password or watchword.



**Moringa Cyber** CYBER EDUCATION & TRAINING  
Proactive Actionable Intelligence

Tel: +234 (0) 906 575 8292  
Email: [cyber@moringacare.ng](mailto:cyber@moringacare.ng)  
Web: [www.moringacare.ng](http://www.moringacare.ng)

## Why are passwords important?

In Cyber Security, the aim is to assure the Confidentiality, Integrity, and Availability of the information asset. The

use of passwords helps in ensuring these.

With respect to confidentiality, passwords help to ensure that only those that should have access to certain resources are granted access. When files are encrypted or digitally signed, some form of password usage is also involved in ensuring that the data being exchanged has not been modified in any form or shape while in transit. Lastly, bypass wording access to resources such as devices and network, it helps to deter threat actors from making changes that can cause disruptions and downtimes in the resource availability. Imagine what happens if a life-saving equipment cannot function when it is needed because of it having been sabotaged by a threat actor.

## How do passwords work?

The application, website, or account (the "verifier") asks the user (the "claimant") to type a string of characters that matches the characters stored with

the verifier. Before permitting access, the verifier checks the entered phrase against its list of approved credentials to ensure the phrase and user ID match. If it matches, access is granted, otherwise access is denied.

## Risks with passwords

When used properly, passwords can be very effective and play key roles in multi-factor authentication (MFA). However, inattentive user behavior and insufficient

protection of credentials can be a cause of damaging security breaches.

The first password systems assumed that users would memorize their passwords, which would create a secure form of password management. However, passwords have proliferated in home and work life and have also become more complex. Users have too many passwords to remember and often reuse passwords making a breach in one place of significant danger in other places where same passwords have been utilized.

Here are some common practices that make passwords vulnerable to different attacks:

### 1. Having non unique passwords

Non unique passwords may pose the biggest threat to security. When a password is reused across multiple logins, the hacker who gains access to a single user account will have access to all of that user's accounts.



**Moringa Cyber** CYBER EDUCATION & TRAINING  
Proactive Actionable Intelligence

Tel: +234 (0) 906 575 8292

Email: [cyber@moringacare.ng](mailto:cyber@moringacare.ng)

Web: [www.moringacare.ng](http://www.moringacare.ng)

## 2. Creating obvious passwords

Passwords that consist of characters such as "1234", "password" or "admin" are surprisingly common. Cyber attackers know that users may choose these easy-to-guess passwords and can use this knowledge to easily breach networks and applications.

## 3. Using personal information in passwords

Users may believe that using information such as names (e.g Mr. Olabode using "olabode" as his password), birth dates (e.g 15031974), and birthplaces (e.g Ikeja or Modakeke etc.) will help them remember passwords. But Cyber criminals view this practice as a valuable tool for their exploits. Attackers can often find this personal information on social media or in public records and then use it in guessing the passwords.

## 4. Replacing letters with numbers

The practice of replacing letters with numbers in passwords—such as replacing "E" with "3," for example—is well known. Hackers can use this knowledge to guess passwords.

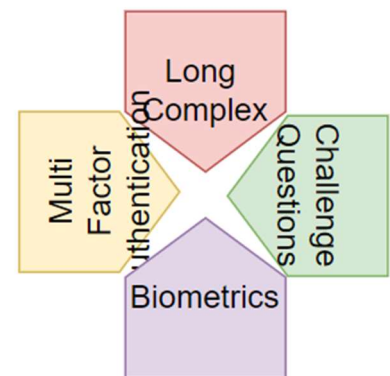
## 1. Create long, complex passwords.

Passwords should be at least 8 characters in length but the longer they are, the better. They should also contain a combination of upper and lowercase letters, numbers, and special characters. Users are encouraged to desist from using sequential characters e.g. "1234" or repeated characters e.g "bbbb".

**Password – best practices**

## 2. Deploy multi-factor authentication.

Multi-factor authentication (MFA) is a security process that requires users to respond to requests to verify their identities before they can access networks or other online applications. MFA may use knowledge, possession of physical objects, or geographic or network locations to confirm identity. When MFA is enabled, never give your password or MFA pass code to anyone over the phone or accept an MFA push notification that you did not request.



## 3. Require challenge questions.

When users want to change passwords or recover forgotten passwords, challenge questions (which ask for correct responses to questions known to the user) can provide further confirmation of a user's identity. For example, a challenge question might ask for a mother's maiden name or the name of a user's first car.

## 4. Use biometric passwords.

Instead of having users store or remember complex passwords, biometric passwords provide physical proof of identities using devices that scan attributes such as fingerprints, faces, and



voices. Requiring fingerprint or face scans has become a common security practice on smartphones.

## 5. Other considerations when using passwords.

- a. When using public Wi-Fi, do not enter your password on any site that is not https. Better still, use a Virtual Private Network (VPN) to ensure secure communication over an unsecure medium.
- b. Unless you trust the source of the email, never log onto secure sites by clicking a link in an email: this is a common phishing scam.
- c. Only use *remember password* facilities on secured personal or corporate computers and never on a public computer.
- d. Don't enter passwords where someone may see what you are typing.
- e. Never send passwords by email.
- f. Never share passwords or leave them written down next to your computer or in an easily found place.
- g. Don't re-use passwords after giving them a break.

*The publication is presented free of charge by the Cyber Capability Education and Training team of Moringa Cyber. At Moringa Cyber, we are passionate about safeguarding people, businesses, and the environment from threat actors. We believe that if enough entities are protected, everyone benefits through herd immunity, the reason we are continuously promoting a culture of cybersecurity.*

*Visit our webpage or contact us using the details below for all your cyber security concerns. We've got you covered, why don't you call us today?*



**Moringa Cyber** CYBER EDUCATION & TRAINING  
Proactive Actionable Intelligence

Tel: +234 (0) 906 575 8292

Email: [cyber@moringacare.ng](mailto:cyber@moringacare.ng)

Web: [www.moringacare.ng](http://www.moringacare.ng)