Issued on 06/25
Updated on 05/26

Joint Advisory against using NRIC Numbers for Authentication by the Personal Data Protection Commission (PDPC) and Cyber Security Agency of Singapore (CSA)

The PDPC and CSA advise organisations against using NRIC numbers to authenticate persons.

What does it mean to authenticate a person?

Authentication refers to the process of proving that a person is who he claims to be, before granting him access to services or information intended only for him. This differs from identification, where identifiers such as names are used to tell people apart.

Organisations are responsible for deciding whether and how to authenticate

Organisations are responsible for deciding whether and how to authenticate their users, based on considerations such as the value and amount of services or information being protected from access, and the possible impact on people if an impersonator or other bad actor gains access to the services or information.

Passwords are a method of authenticating a person. When a person possesses a properly issued and secured password, he is deemed to have proven that he is the intended recipient of services or information. Therefore, we should not share our passwords with others. Also, when passwords are the chosen method of authenticating persons, strong passwords that are not easily guessed should be used. Otherwise, another person who correctly guesses the password may gain access to services or information intended for the genuine user. Passwords containing information that can be obtained easily, including personal data such as names, NRIC numbers or birthdates, are not strong passwords.

Stop the use of NRIC numbers to authenticate persons

NRIC numbers should not be used as passwords to authenticate a person. This is because they are issued to uniquely identify a person and must be assumed to have been disclosed to at least a few other persons.

Organisations that are using full or partial NRIC numbers to authenticate persons should stop this practice as soon as possible. They should not set NRIC numbers as default passwords[1], nor should they use full or partial NRIC numbers together with other easily obtainable personal data for authentication (e.g., passwords combining an individual's partial NRIC number and date of birth, such as "567A01Jan80"). Organisations should also be aware that a person may not be who he claims to be just because he is able to state that person's NRIC number.

[1] *For example, in password-protected files sent via e-mail.*

Considerations and options to authenticate persons

If it is necessary to authenticate persons, organisations should consider using other method(s). Organisations should take a risk-based approach when choosing the authentication method(s), considering factors such as:

- Value and sensitivity of what is being protected
- Potential threats and vulnerabilities of the authentication method
- User experience and accessibility when using the authentication method

Options to authenticate a person[2] include:

- Something only the person knows (e.g., strong passwords)
- Something only the person owns (e.g., security token, smart card)
- Something only the person has (e.g., fingerprint, face, iris, palm vein)

[NEW] Alternatives to using NRIC numbers as passwords to protect documents

Where authentication is assessed to be necessary, organisations may consider the following examples of authentication methods that do not use NRIC numbers or easily obtained personal data. Organisations should assess what works best for their circumstances and be aware of the limitations of these methods. For instance, the methods listed do not protect individuals from social engineering attacks, which primarily exploit human psychology and behaviour rather than technical vulnerabilities. Individuals must remain vigilant and learn to recognise social engineering attempts[3].

[2] *"Something only the person owns" and "something only the person has" are preferred as these offer stronger phishing resistance. For "something only the person knows", opt for a strong password such as a passphrase made up of a series of random words that is harder to crack but easier to remember (e.g., LearnttoRIDEabikeat5). Do set up two-factor authentication for an additional layer of security.*

[3] For more information, refer to the *Joint Advisory on Safeguarding Online Accounts by the Singapore Police Force and Cyber Security Agency of Singapore.*

[NEW] Table: Alternative Authentication Methods when Sending or Accessing Electronic Documents

S/N	Method	Description	Additional guidance	Possible use cases
1	Website/ app with user account	Document is accessed via a website or mobile application. Recipient uses existing account credentials to view or download the document.	Use secure authentication controls and enhance with multi-factor authentication (MFA).	Documents that the recipient may need to access for future reference
2	Expiring or single-use link with unique password	Document is accessed via a link that is valid for a limited period or number of uses. Recipient uses a unique password sent via a separate communication channel (e.g., SMS to registered mobile number).	Limit link validity (e.g., links that expire after a set time or can only be used once) and send unique password via a separate channel. Avoid sending both the link and unique password through the same communication channel.	Documents sent on a once-off basis, without need for future access by recipient
3	Emailed document with unique password set by organisation	Password-protected document is sent to the recipient's email address. Recipient uses a unique password sent via a separate communication channel (e.g., SMS to registered mobile number; or email to a different registered address).	Generate unique password and send it via a separate communication channel. Avoid sending both the document and password through the same channel.	Documents that the recipient may need to access for future reference, and where web or mobile app access is not feasible

Resources and guidance

1. CSA
    - Enable 2FA and use strong passphrase
    - SingCERT Password Checker
    - SG Cyber Safe cybersecurity toolkits for organisations
    - [New] Joint Advisory on Safeguarding Online Accounts

2. PDPC

    - Advisory Guidelines on Key Concepts in the PDPA (see especially chapter 17 on the Protection Obligation)
    - Data Protection Practices for ICT Systems