Password Security & Etiquette

A Netscylla whitepaper on the user management of passwords and guidelines on password policies.

Netscylla Cyber Security Ltd
GB 10571639

Address:
Telecom House,
125-135 Preston Road, Brighton,
East Sussex,
United Kingdom, BN1 6AF

Introduction

At Netscylla we often get asked questions about passwords.

- What is a secure password?
- How do I secure my passwords?
- How often should I change my password?

There are many conflicting sources and advice, depending on where you look and who you ask. This whitepaper outlines Netscylla's belief of good practise for the use and storage of passwords.

Password Re-use

It is important to first understand that passwords should never be repeated across important accounts. If one password is compromised, you risk losing everything associated to your digital identity.

However, on the contrary if you have several accounts for a number of small websites or services that store very little or next to no personal information (personal details, photos, etc) are not used for financial transactions and have no relevance to other personal accounts, or sensitive data. It is generally fine to **re-use passwords so long as they do not match the passwords of important accounts**.

Securing Passwords

Passwords are the keys to your digital identity, we recommend that you think about how you secure your passwords from rogue attackers.

Notebooks

A hand-written book is fine, but then your notebook needs to be secured; if the book is captured or destroyed you could have great difficulty recovering your accounts. Therefore, the book needs appropriate controls and protections, such as hiding the book in a locked safe when not in use.

Files

Plain-text files used to store passwords is a bad and insecure practise. This should always be avoided. As these could easily be recovered using forensic techniques. At the very least, encryption (protected by public-private key, or a suitably strong password) should be used to mask and hide your secure keys from any prying eyes.

Folders and Network Storage

It is common to backup or store your passwords on network devices. Users should be aware that their folder or network drive may not be securely locked down, and may be publicly accessible to everyone, or even a sub-set of other users of the system. Again, it is important to use encryption, but attackers can attempt to brute force the encryption key and recover the plaintext passwords. Therefore, **it is important that you manage your folder permissions correctly so that only you or your trusted peers can access your stored data**.

Password Managers

Password managers are useful for managing several accounts in your digital estate. They can help choose suitable passwords (as different vendors have different and varying complexity policies). They often utilise encryption to protect against digital attacks and forensic recovery techniques. They help store numerous passwords; Therefore, reducing the number of passwords you need to remember.

However, the downside is that password managers have become lucrative targets in their own right. If the password manager is compromised, you essentially lose the security and integrity of all your passwords, private keys, and accounts. Therefore, your master password needs to be appropriately backed-up, secured, complexed, of sufficient length, and most importantly easy for you to remember.

Two-Factor Authentication

In addition to using separate passwords for each account, you should consider enabling any two-factor authentication (2FA) capabilities to help further secure you online identities. 2FA can come in different implementations, and different 2FA schemes are supported by different vendors and service operators. A list of common 2FA implementations are below:

- RSA Token (Hardware keyring)
- RSA Token (Software)
- Pseudo Random Code & PIN (often used by Banks)
- FIDO (e.g. USB-OTP-key)
- Google Authenticator
- SMS text-message
- Linked to your phone's identity & PIN

The use of 2FA technology, should greatly increase the difficultly for an attacker to compromise your account; especially if they are a remote attacker on the other side of the world, as they would not have access to your secure tokens. A more local adversary could try to access your security token leveraging theft, or mislaid tokens; but without knowledge of your PIN they should not be able to compromise your 2FA protected accounts.

Password Policy

This section is not primarily aimed at users, but is a useful insight to help these users choose suitable passwords. Businesses should read and discuss what is outlined below with their developers, operations and security teams, to ensure that their policies fit the business model and its daily operations.

Password Length

A topic that varies between numerous businesses and vendors. Too long a length and passwords become difficult to manage and remember. Too short and brute-force attacks become a reality to compromising several accounts in a short amount of time. It is a trade-off that needs to be decided by the businesses and vendors; On how often they wish to support users that may have forgotten a password, and need their account reset. Against, how the business stores and manages and encrypted credentials.

For the **average user 8- 12 characters** should be sufficient for a potentially good password, depending on other criteria.

For enhanced and **important systems 14-18 characters** help protect against the majority of brute-force and dictionary based attacks.

For very **sensitive and upmost important accounts Netscylla recommend 28+ characters** passwords. Should the password hash ever be obtained this length of password should be difficult to crack against offline attacks, such as utilising specialist hardware, which is often used to quickly brute-force hashed and encrypted passwords.

Password Complexity

Password complexity is a difficult topic, but essentially when you create a password you should vary the use of characters to increase the entropy and reduce the chances of success from a brute-force attack. **Generally, we seek to see users use a mixture of case; upper and lower-case characters, digits, and special characters**. This can often cause issues in underlying authentication mechanisms, so the business needs to ensure the developers and operation teams understand the security policies and requirements. Sometimes special- or meta- characters can cause authentication mechanisms to malfunction, and may inadvertently allow an attacker to bypass the protection securing your accounts.

Account Lockout

Forcing a complicated policy also forces the users to remember difficult passwords. The account lockout policy may need to be adjusted to allow users to attempt a number of permutations of their password, before locking the account. Otherwise, an account Denial-of-Service may occur across numerous accounts, and the service desk may become overwhelmed with users requesting account resets. This need to clearly thought about and appropriate policies created to fit in with the current business needs and processes, the policy should be reviewed annually as businesses often evolve and the policies need to evolve with the business.

Consider the following examples as initial ideas, password attempts and lockout times should be adjusted to suite the business needs:

- Accounts pertaining to no PPI or financial data – 10x attempts, 1x day lockout
- Publicly accessible accounts – no 2FA – 5x attempts, support/service desk to unlock
- Publicly accessible accounts, protected by 2FA – 3x attempts, 30min lockout
- Corporate accounts – 5x attempts, 1-hour lockout
- Sensitive systems – 3x attempts, support/service desk to unlock

Password Age

Password age can be a complicated topic. Some policies advise users to change their password regularly (which is sound advice), but depending on how you define regularly, this could be too often or not enough. Frequent password changes can impose difficulties on choosing a new password. In practise password policies that enforce too frequent password changes (e.g. one or two weeks), eventually trains users into using simple passwords: dictionary words, dates, 6-8 digit numbers; all of which can be usually brute-forced (dependant on other possible mitigating defences such as 2FA).

We typically recommend a **minimum password age of one day**, this should help raise alerts to a password change not set be the account holder. Early detection of a compromised password means you can quickly and efficiently check and lockdown the security of your other accounts.

Netscylla has different recommendations on the maximum password age, dependant on the importance of the account and how frequently it is accessed. **A frequently used password for important accounts should have a maximum age between 60-90 days** (depending on the business processes and policies); However, when combined with 2FA technology these passwords could be used longer term. **For unimportant and non-sensitive accounts, we recommend a maximum password age of one year**, it is good practise to review and change your passwords annually.