Password Tips

Last Modified on 2022-Jul-05

In this article

- Use a password manager
- Use a passphrase instead of a password
  - How to create a passphrase
  - Using the Person-Object-Action Method
- Don't use things you post on social media
- Don't use a common phrase or quote as a passphrase
- Check to see if your logins have been leaked
- Don't use the same password across multiple accounts
- Changing passwords regularly
  - Password monitoring for Google, Apple and Windows

Your password is the first line of defense against theft and misuse of information in School Manager. To protect your own and your users' privacy, Linewize enforces a strong password policy. Strong passwords are long, hard to guess, and difficult to breach.

Here are tips to help you come up with a good, strong password!

Use a password manager

Using a password manager allows you to log in to websites without the need to remember your password or even type it. Password managers also let you generate complex passwords and store them securely, so that you don't need to remember or write them down.

If you use a password manager, you should turn on Multi Factor Authentication (MFA). Also called 2FA for 2 Factor Authentication, MFA verifies that you are who you say you are, usually by sending a text to your phone or asking you to get a code from an authenticator app.

View this explainer for more information about MFA.

Use a passphrase instead of a password

If you can't use a password manager, you should use a random phrase instead of a password. Passphrases allow you to remember longer passwords and make your account harder to crack. Passphrases are created by combining three or more random words to make a phrase that is both memorable for you and very hard to guess.

For example, this is a strong password:

y\9C8Tq&BPF:K`\n

But this passphrase is also a strong password:

sCruffy boogyMan? CalM vibes!

A story about a scruffy but strangely calming boogeyman is a lot easier to remember than a string of random letters, numbers, and characters. For example:

- scruffy Boogeyman, calM vibeS
- Scruffy bo0geymanman? Calm vibes!

How to create a passphrase

These are a few techniques you can use to generate a passphrase:

- Use your password manager
- Use a dice list like https://www.eff.org/dice
- Use the Person-Object-Action method

Using the Person-Object-Action Method

Think of three unrelated things: a famous person, a memorable place and an object, and then link them together, in any order, with an action. For example, Ringo Starr (person), Cable Beach (place), and maple syrup (object) becomes:

Ringo Starr drinking maple syrup at Cable Beach

Don’t use things you post on social media

Hackers can and will look through your social media accounts to get ideas about what your password might be. This means your passphrase shouldn’t include anything that someone could learn from your social media account, such as:

- the names or birth dates of family, friends and pets;
- your hobbies and interests;
- favorite sports teams, films, songs or books; or
- your profession, work history or employer.

Don’t use a common phrase or quote as a passphrase

Hackers make and share huge dictionaries of common passwords, names and phrases in many different

languages. These dictionaries often include the most common ‘misspellings’ of those words and phrases.

This means:

- Don’t use common sayings like, "absence makes the heart grow fonder" or quotes like, "To be, or not to be" as your passphrase.
- Don’t use famous lines from film, television, books, or scripture even if you misspell them or substitute numbers for letters.
- Don’t use lines from songs or poetry.

Remember: If you can quickly think of the line, so can somebody else.

Check to see if your logins have been leaked

Hackers don’t just share dictionaries, they share lists of email addresses matched to passwords taken from sites that they’ve broken into. Services like have I been pwned (https://haveibeenpwned.com) can be used to check and see if your email addresses or other personal data have been taken and shared by hackers.

Just be careful to only use breach notification sites that are reputable and familiar to you. Never put your password into an unfamiliar site, even to check. You should change your password as soon as possible if it may have been compromised in a data breach.

Don’t use the same password across multiple accounts

When you use the same password in multiple accounts, hackers can easily access all of those accounts if the password gets out. You mustn’t use the same password for your email account. Always use a different, completely unique passphrase from all of your other accounts when you create your email login.

Changing passwords regularly

While many experts recommend changing passwords every few months, others also advise against it. Instead of cycling passwords, a better solution is still using MFA and long passwords or passphrases.

Password monitoring for Google, Apple and Windows

Google, Apple and Windows now inform users of potential password leaks and recommend actions for unsafe or weak passwords, or passwords that are reused in multiple accounts.

To enable this feature on iOS: Go to **Settings** > **Passwords** > **Security Recommendations**, and toggle **Detect Compromised Passwords**.

Visit the following pages for more information about monitoring and changing passwords:

- macOS: Change password preferences on Mac
- Windows: Protect your online accounts using Password Monitor
- Google: Change unsafe passwords in your Google Account.