Supplementary document for paper:
Generating and Attacking Passwords with Misspellings by Leveraging Homophones

Shiva Houshmand, Smita Ghosh, Jared Maeyama

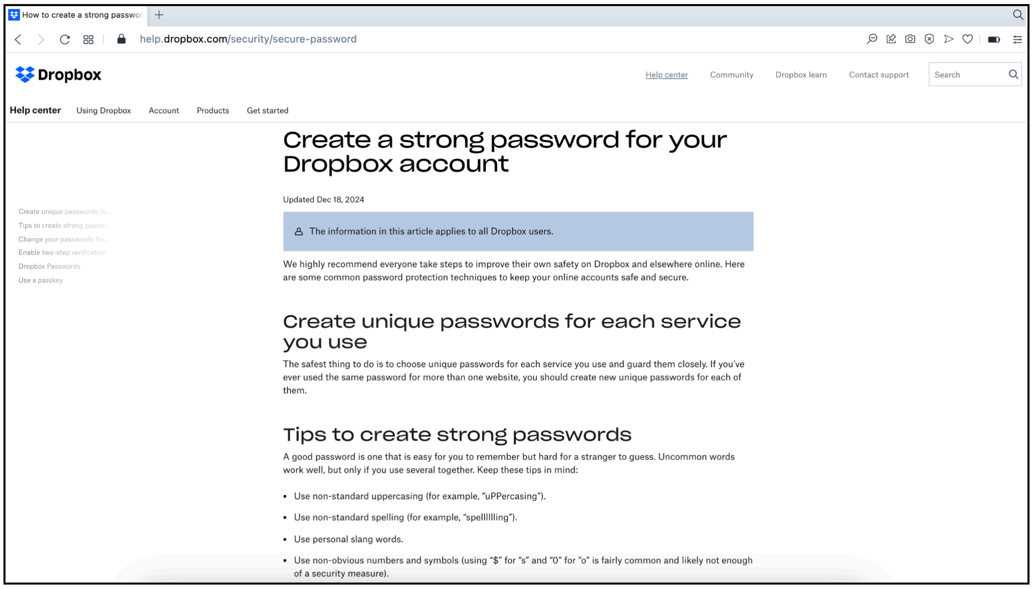
IFIP Sec 2025

An examination of today's password policies and advice from different websites reveals that many major companies suggest avoiding dictionary words altogether, even advocating for using misspelled or non-standard spellings. Below, we provide examples of these recommendations, along with links to the original statements. However, since websites frequently update their guidelines or change URLs, this page serves as an archive of screenshots documenting these policies. The links were last accessed on March 25, 2025.

1. **Dropbox**: Use non-standard spelling (for example, spellllllling).
2. **Paypal**: Misspelled words are stronger because they are not in the dictionary used by attackers.
3. **Fordham University**: Totally misspell an easily remembered word or phrase.
4. **Amazon**: Do not use a word that is in a dictionary.
5. **Twitch**: Be creative! Don't use single dictionary words.
6. **X (Twitter)**: Do not use common dictionary words.

Dropbox

Link: https://help.dropbox.com/security/secure-password


How to create a strong passwor
help.dropbox.com/security/secure-password
Dropbox
Help center
Community
Dropbox learn
Contact support
Search
Help center
Using Dropbox
Account
Products
Get started
Create unique passwords fo...
Tips to create strong passw...
Change your passwords fro...
Enable two-step verification
Dropbox Passwords
Use a passkey

Create a strong password for your Dropbox account

Updated Dec 18, 2024

The information in this article applies to all Dropbox users.

We highly recommend everyone take steps to improve their own safety on Dropbox and elsewhere online. Here are some common password protection techniques to keep your online accounts safe and secure.

Create unique passwords for each service you use

The safest thing to do is to choose unique passwords for each service you use and guard them closely. If you've ever used the same password for more than one website, you should create new unique passwords for each of them.

Tips to create strong passwords

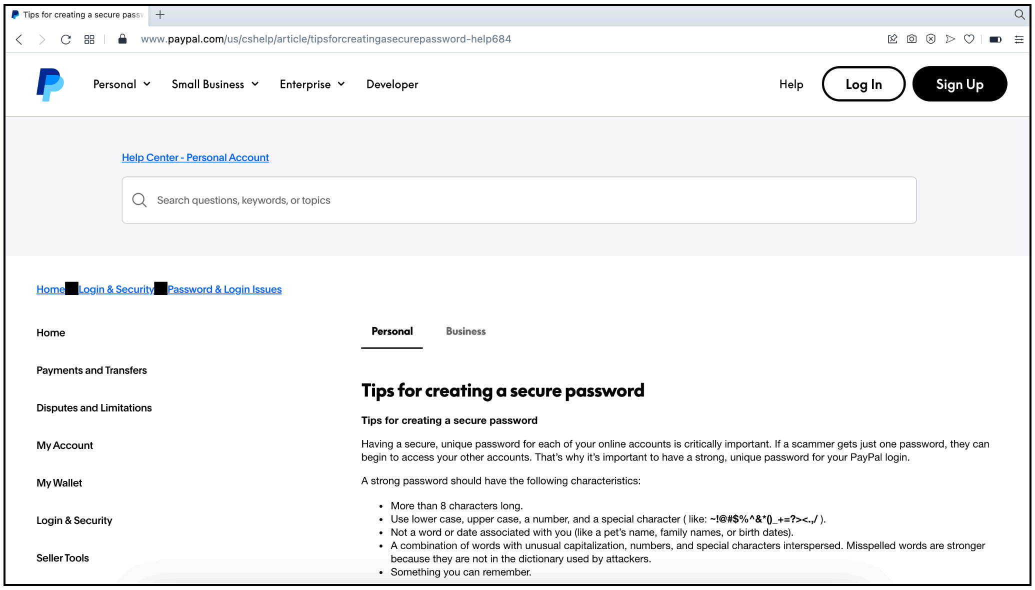
A good password is one that is easy for you to remember but hard for a stranger to guess. Uncommon words work well, but only if you use several together. Keep these tips in mind:

- Use non-standard uppercasing (for example, "uPPercasing").
- Use non-standard spelling (for example, "spellllllling").
- Use personal slang words.
- Use non-obvious numbers and symbols (using "$" for "s" and "0" for "o" is fairly common and likely not enough of a security measure).

Paypal

Link:

https://www.paypal.com/us/cshelp/article/tipsforcreatingasecurepassword-help684


Tips for creating a secure pass
www.paypal.com/us/cshelp/article/tipsforcreatingasecurepassword-help684
Personal
Small Business
Enterprise
Developer
Help
Log In
Sign Up
Help Center - Personal Account
Search questions, keywords, or topics
Home■Login & Security■Password & Login Issues
Home
Payments and Transfers
Disputes and Limitations
My Account
My Wallet
Login & Security
Seller Tools
Personal
Business

Tips for creating a secure password

Tips for creating a secure password

Having a secure, unique password for each of your online accounts is critically important. If a scammer gets just one password, they can begin to access your other accounts. That's why it's important to have a strong, unique password for your PayPal login.

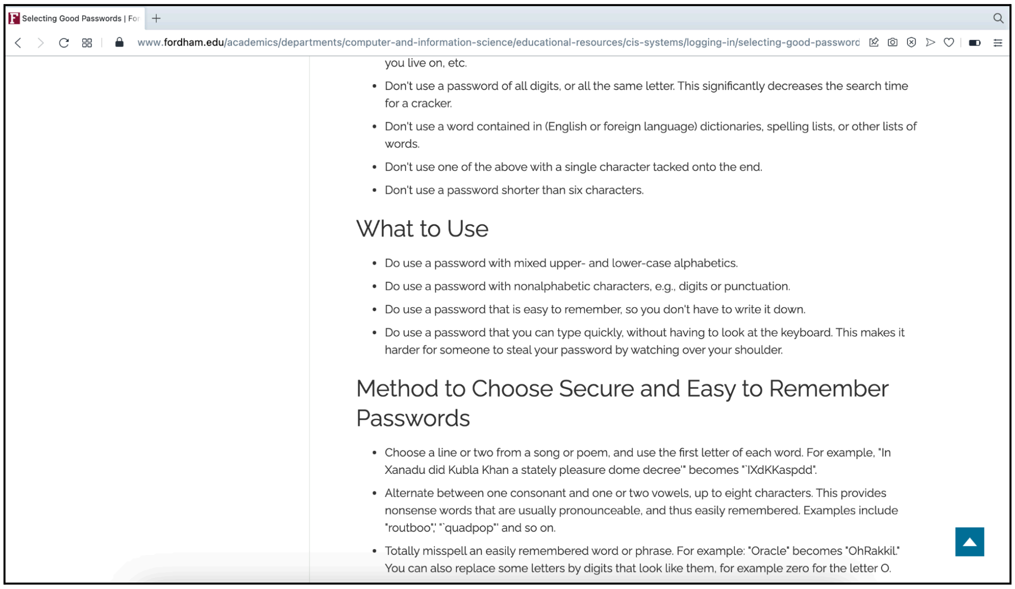
A strong password should have the following characteristics:

- More than 8 characters long.
- Use lower case, upper case, a number, and a special character (like: **~!@#$%^&*()_+=?><.,/**).
- Not a word or date associated with you (like a pet's name, family names, or birth dates).
- A combination of words with unusual capitalization, numbers, and special characters interspersed. Misspelled words are stronger because they are not in the dictionary used by attackers.
- Something you can remember.

Fordham University

Link:

https://www.fordham.edu/academics/departments/computer-and-information-science/educational-resources/cis-systems/logging-in/selecting-good-passwords/


Selecting Good Passwords | For
www.fordham.edu/academics/departments/computer-and-information-science/educational-resources/cis-systems/logging-in/selecting-good-passworc

you live on, etc.

- Don't use a password of all digits, or all the same letter. This significantly decreases the search time for a cracker.
- Don't use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words.
- Don't use one of the above with a single character tacked onto the end.
- Don't use a password shorter than six characters.

What to Use

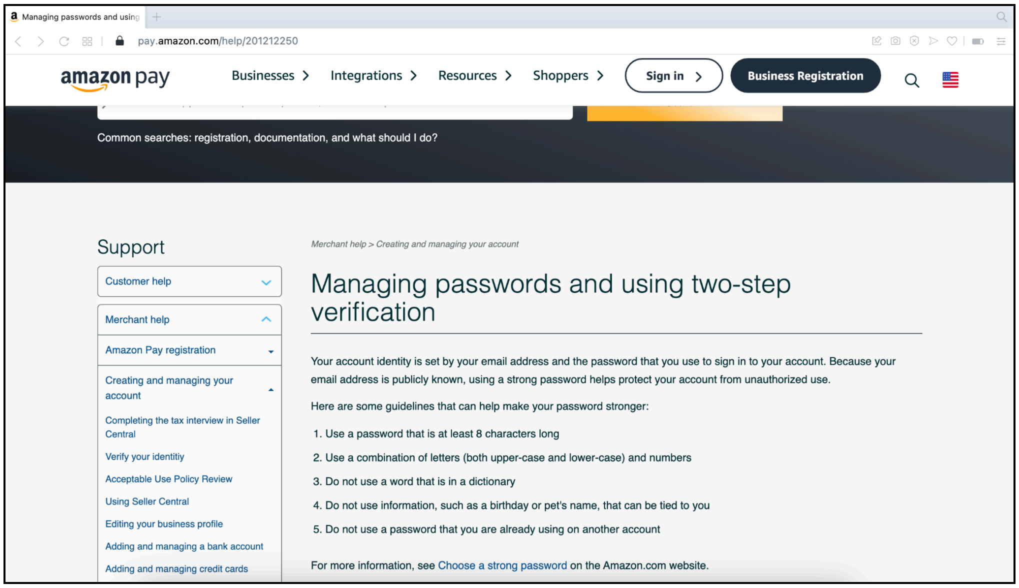
- Do use a password with mixed upper- and lower-case alphabetics.
- Do use a password with nonalphabetic characters, e.g., digits or punctuation.
- Do use a password that is easy to remember, so you don't have to write it down.
- Do use a password that you can type quickly, without having to look at the keyboard. This makes it harder for someone to steal your password by watching over your shoulder.

Method to Choose Secure and Easy to Remember Passwords

- Choose a line or two from a song or poem, and use the first letter of each word. For example, "In Xanadu did Kubla Khan a stately pleasure dome decree'" becomes "`IXdKKaspdd".
- Alternate between one consonant and one or two vowels, up to eight characters. This provides nonsense words that are usually pronounceable, and thus easily remembered. Examples include "routboo",' "`quadpop"' and so on.
- Totally misspell an easily remembered word or phrase. For example: "Oracle" becomes "OhRakkil." You can also replace some letters by digits that look like them, for example zero for the letter O.

Amazon

Link: https://pay.amazon.com/help/201212250



Common searches: registration, documentation, and what should I do?

Support

- Customer help
- Merchant help
- Amazon Pay registration
- Creating and managing your account
- Completing the tax interview in Seller Central
- Verify your identitiy
- Acceptable Use Policy Review
- Using Seller Central
- Editing your business profile
- Adding and managing a bank account
- Adding and managing credit cards

Merchant help > Creating and managing your account

Managing passwords and using two-step verification

Your account identity is set by your email address and the password that you use to sign in to your account. Because your email address is publicly known, using a strong password helps protect your account from unauthorized use.

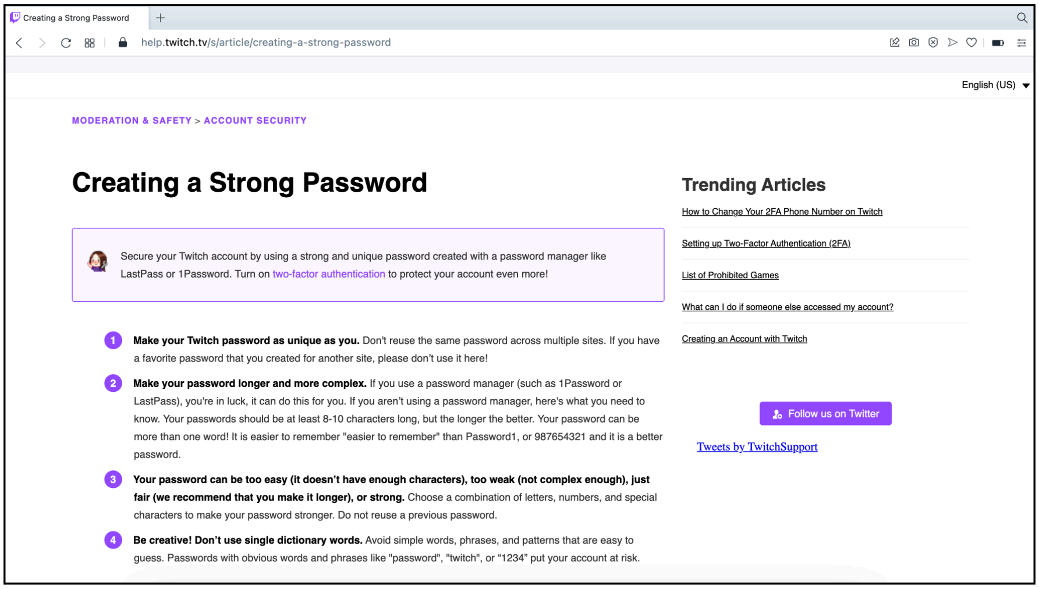
Here are some guidelines that can help make your password stronger:

1. Use a password that is at least 8 characters long
2. Use a combination of letters (both upper-case and lower-case) and numbers
3. Do not use a word that is in a dictionary
4. Do not use information, such as a birthday or pet's name, that can be tied to you
5. Do not use a password that you are already using on another account

For more information, see Choose a strong password on the Amazon.com website.

Twitch

Link: https://help.twitch.tv/s/article/creating-a-strong-password


Creating a Strong Password
help.twitch.tv/s/article/creating-a-strong-password
English (US)

MODERATION & SAFETY > ACCOUNT SECURITY

Creating a Strong Password

Secure your Twitch account by using a strong and unique password created with a password manager like LastPass or 1Password. Turn on two-factor authentication to protect your account even more!

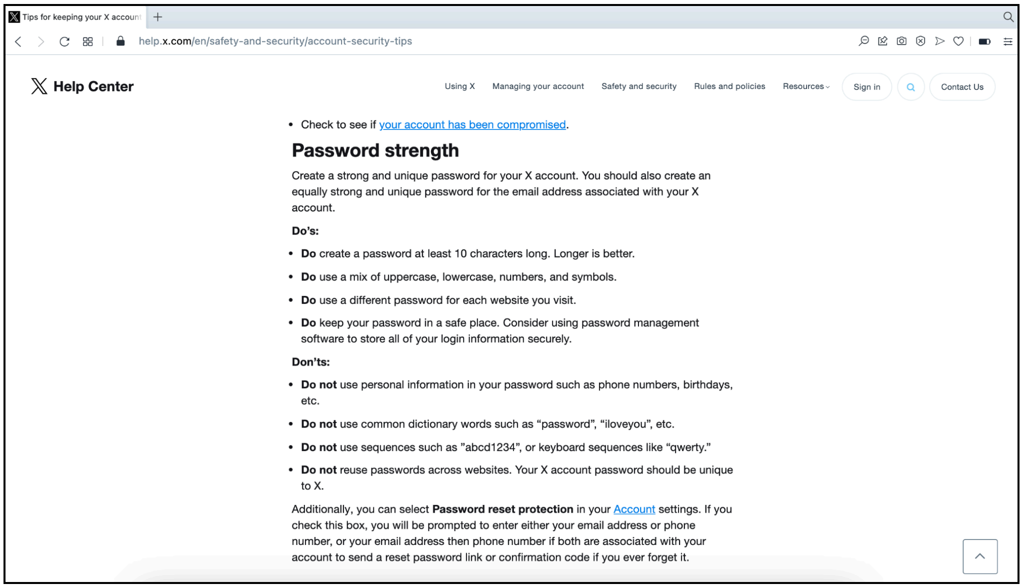
1. **Make your Twitch password as unique as you.** Don't reuse the same password across multiple sites. If you have a favorite password that you created for another site, please don't use it here!
2. **Make your password longer and more complex.** If you use a password manager (such as 1Password or LastPass), you're in luck, it can do this for you. If you aren't using a password manager, here's what you need to know. Your passwords should be at least 8-10 characters long, but the longer the better. Your password can be more than one word! It is easier to remember "easier to remember" than Password1, or 987654321 and it is a better password.
3. **Your password can be too easy (it doesn't have enough characters), too weak (not complex enough), just fair (we recommend that you make it longer), or strong.** Choose a combination of letters, numbers, and special characters to make your password stronger. Do not reuse a previous password.
4. **Be creative! Don't use single dictionary words.** Avoid simple words, phrases, and patterns that are easy to guess. Passwords with obvious words and phrases like "password", "twitch", or "1234" put your account at risk.

Trending Articles

- How to Change Your 2FA Phone Number on Twitch
- Setting up Two-Factor Authentication (2FA)
- List of Prohibited Games
- What can I do if someone else accessed my account?
- Creating an Account with Twitch

X (Twitter)

Link: https://help.x.com/en/safety-and-security/account-security-tips



- Check to see if your account has been compromised.

Password strength

Create a strong and unique password for your X account. You should also create an equally strong and unique password for the email address associated with your X account.

Do's:

- **Do** create a password at least 10 characters long. Longer is better.
- **Do** use a mix of uppercase, lowercase, numbers, and symbols.
- **Do** use a different password for each website you visit.
- **Do** keep your password in a safe place. Consider using password management software to store all of your login information securely.

Don'ts:

- **Do not** use personal information in your password such as phone numbers, birthdays, etc.
- **Do not** use common dictionary words such as “password”, “iloveyou”, etc.
- **Do not** use sequences such as "abcd1234", or keyboard sequences like “qwerty.”
- **Do not** reuse passwords across websites. Your X account password should be unique to X.

Additionally, you can select **Password reset protection** in your Account settings. If you check this box, you will be prompted to enter either your email address or phone number, or your email address then phone number if both are associated with your account to send a reset password link or confirmation code if you ever forget it.