The Last Password You'll Ever Need

YOU'LL NEED THIS

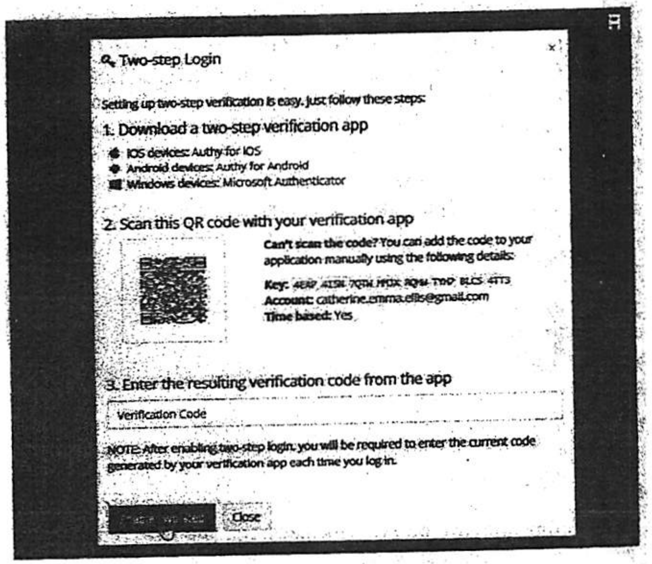
BITWARDEN
Head to https://bitwarden.com.

SOMETHING TO PROTECT
An Internet-connected PC and smartphone.

WE ALL KNOW WE SHOULDN'T RE-USE PASSWORDS, but with so many websites requiring user accounts, creating a different, secure, memorable login for each is all but impossible. That's before you consider how you're going to change them regularly (a policy enforced by some companies).

This leads to an problem: If someone can crack the password for one of your accounts, it can open the door to many others. That's where password managers come in, storing all your account details in a central location, and automatically completing login screens so you don't have to remember them yourself (or jot them down on sticky notes). The password vault is secured by a single master password, which is the only one you need to commit to memory.

Bitwarden is a free, open-source password manager that stores your account details in the cloud, enabling you to access them from any Internet-enabled device. Bitwarden encrypts everything using AES 256-bit encryption and salted hashing, so the data on its servers is no use without your master password—and your smartphone, if you enable two-factor authentication. Because Bitwarden is cloud-based, it can't be used to secure passwords for Wi-Fi access points, Windows user accounts, or other offline services, but for web accounts, it's excellent. –CAT ELLIS



Two-step Login

Setting up two-step verification is easy. Just follow these steps:

1. Download a two-step verification app
- iOS devices: Authy for iOS
- Android devices: Authy for Android
- Windows devices: Microsoft Authenticator

2. Scan this QR code with your verification app

Can't scan the code? You can add the code to your application manually using the following details:

Key: 4EAP 4I5K 7QTM HYDX 3Q4M T9DP BLCS 4TT3
Account: catherine.emma.ellis@gmail.com
Time based: Yes

3. Enter the resulting verification code from the app

Verification Code

NOTE: After enabling two-step login, you will be required to enter the current code generated by your verification app each time you log in.

1 CREATE ACCOUNT AND ENABLE TWO-STEP VERIFICATION

Visit https://bitwarden.com and select "Create an account." The master password that you enter here will be the only way to access your encrypted logins in the future, so make sure it's memorable, and add a hint that only makes sense to you. Once you've finished, log in.

» It's a good idea to initiate two-factor authentication so that even if your master password is compromised, your logins can't be decrypted without verification from your smartphone. Click "Settings → Two-step login." Enter your master password again, then download the appropriate mobile app (Authy for iOS or Android, or Microsoft Authenticator for Windows devices), and follow the on-screen instructions to create an authentication account. Use the smartphone app to scan the QR code on your Bitwarden account page **[Image A]** to connect the two accounts. Now, to log into Bitwarden, you'll need not only your master password, but also a seven-digit security token generated by the mobile app every 20 seconds. Bitwarden provides you with a backup code in case you lose your phone; keep this in a safe place.

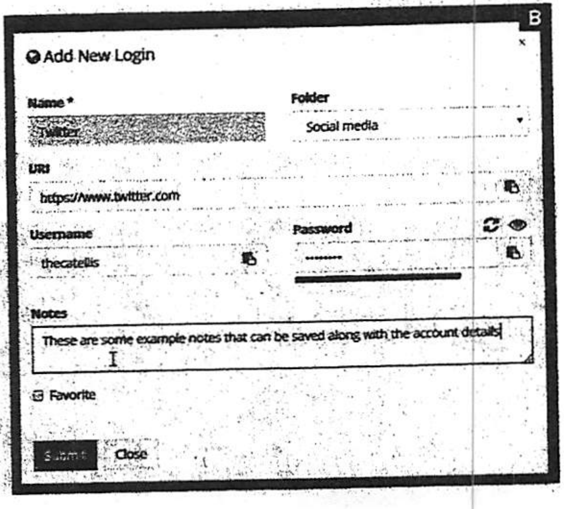
2 STORE YOUR LOGINS

Now you're ready to start saving your usernames and passwords. You probably have dozens of logins, so it's useful to keep them organized by type; click "My vault → New folder," and make some directories for different account types (social media, email, shopping, forums, and so on). Now click "Add a login," and fill in the form provided **[Image B]**. Bitwarden shows you the strength of your password as you type it. Click the eye icon to make sure you've typed the password correctly, or click the refresh icon to generate a new, stronger one. There's also an area to store notes, which are encrypted along with the username and password.

» Add the rest of your logins in the same way. Now, whenever you visit one of those sites while logged into Bitwarden, the username and password fields are completed for you automatically.

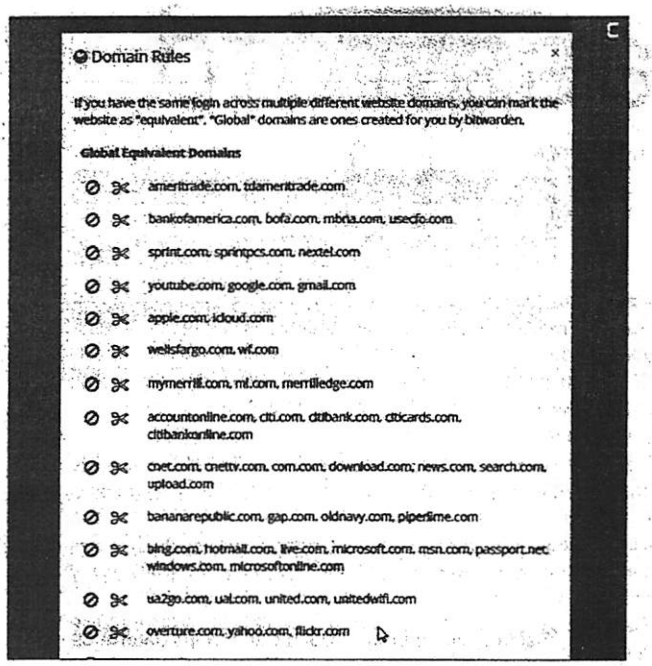
3 SET DOMAIN EQUIVALENTS

If you want to keep using the same logins for multiple accounts, you can connect them to avoid



Add New Login

Name *: Twitter
Folder: Social media
URI: https://www.twitter.com
Username: thecatellis
Password: ••••••••
Notes: These are some example notes that can be saved along with the account details

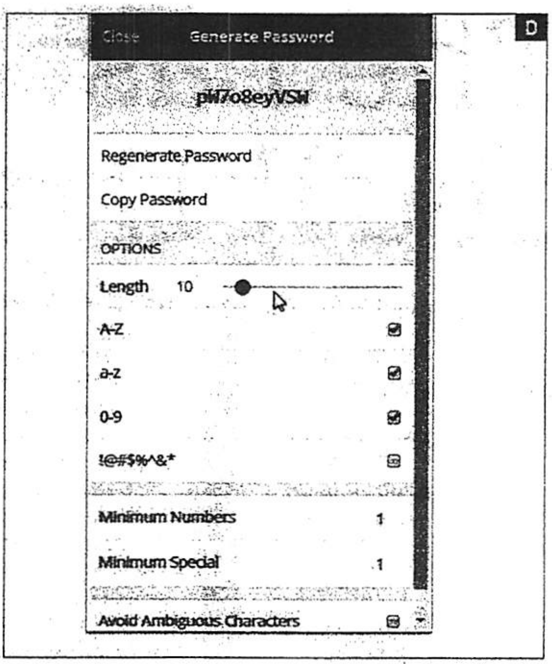


Domain Rules ×

If you have the same login across multiple different website domains, you can mark the website as "equivalent". "Global" domains are ones created for you by bitwarden.

Global Equivalent Domains

- ameritrade.com, tdameritrade.com
- bankofamerica.com, bofa.com, mbna.com, usecfo.com
- sprint.com, sprintpcs.com, nextel.com
- youtube.com, google.com, gmail.com
- apple.com, icloud.com
- wellsfargo.com, wf.com
- mymerrill.com, ml.com, merrilledge.com
- accountonline.com, citi.com, citibank.com, citicards.com, citibankonline.com
- cnet.com, cnettv.com, com.com, download.com, news.com, search.com, upload.com
- bananarepublic.com, gap.com, oldnavy.com, piperlime.com
- bing.com, hotmail.com, live.com, microsoft.com, msn.com, passport.net, windows.com, microsoftonline.com
- ua2go.com, ual.com, united.com, unitedwifi.com
- overture.com, yahoo.com, flickr.com



Close | Generate Password

pli7o8eyVSH

Regenerate Password

Copy Password

OPTIONS

Length 10

A-Z ☑

a-z ☑

0-9 ☑

!@#$%^&* ☐

Minimum Numbers 1

Minimum Special 1

Avoid Ambiguous Characters ☐

duplicating the effort of entering them. Set one up in your vault, then click "Settings → Domain rules." Bitwarden comes with a list of related sites that are likely to use the same login details—such as Google and YouTube—which can be toggled on and off **[Image C]**. To add your own equivalents, scroll right down to the bottom of the list, and click "Add new." Enter the domains you want to connect, separated by commas, then click "Submit." Note that you can only use "base" domains—not subdomains.

4 IMPORT AND EXPORT LOGINS

If you're moving to Bitwarden from a different password manager, you don't have to re-enter all your logins manually. Most password managers offer the ability to export your archived logins in CSV (comma-separated value) format. To add them to Bitwarden, select "Tools → Import" from your dashboard, then locate the file, and click "Import." If, for whatever reason, you decide Bitwarden isn't the tool for you, you can also export logins in the same way.

5 GET THE BROWSER EXTENSION

The Bitwarden browser extensions are a convenient way to manage passwords on the sites you visit, without visiting https://bitwarden.com to start a new browsing session. There are currently plugins available for Firefox, Chrome, and Opera—just search for "bitwarden" in the appropriate store, install it, and log in with your username and master password (plus a verification code from your phone if you've enabled two-factor authentication). Most of the features will be familiar from https://bitwarden.com, but the password generator **[Image D]** is a very handy extra tool that helps you make secure logins for sites that demand specific character counts or types. Click "Tools → Password generator," and use the checkboxes to choose whether the password should be upper case, lower case, or a mixture of both, and whether it should contain numbers or special characters (and how many).

6 TRY BITWARDEN'S MOBILE APP

Bitwarden also has a mobile app for iOS and Android. Once it's installed on your smartphone, log in using your username, password, and verification code. Again, most of the features will be familiar, but there are some interesting extras. Tap "Settings" and you'll find additional security options, including the ability to log in with a fingerprint or PIN, and how long your session should remain active before it's locked and you have to re-enter your master password.

» To visit a site and log in, tap "Vault," then tap the site's URL, and it opens in your default browser. Bitwarden's developer is currently working on an improved auto-fill feature, but for the time being, you have to copy and paste passwords from Bitwarden into other apps. ⏻

REMOTE OR LOCAL VAULTS

There are lots of other password managers. Some, including KeePass, store your encrypted logins locally. This means you retain complete control of your logins, and you can access them offline, but setting up synching is complicated (the options are explained at), and they're less convenient if you use multiple devices. Others, such as LastPass and Bitwarden, store your logins on remote servers after encrypting them. This is more convenient for multiple devices, but means you have to trust that the servers will remain up, and won't have their security compromised. In 2015, LastPass reported that user data had been stolen from its servers, including email addresses, password reminders, and authentication hashes. The hashes were sufficiently encrypted to prevent anyone accessing user accounts, but all users had to reset their master passwords to be safe. It's up to you to decide what your biggest priority is—however, since Bitwarden has far fewer users than LastPass, it's less likely to be a target.