Password Managers

Jere Minich

APCUG Advisor Region 5 – FL, GA, AL, SC.

jminich@apcug.org

Program Director - Lake Sumter Computer Society

April 2018

Password Managers

- People use very weak passwords.
  - And reuse them on different websites.
- **How are you supposed to use strong, unique passwords on all the websites you use?**
- The solution is a **password manager.**

Password managers
What do they Do?

- Store your login information for all the websites you use.
  - User ID and Password.
- Help you log into the Web Site automatically.
- Encrypt your password database:
  - with a master password
- The master password is the only one you have to remember.

Don’t Reuse Passwords!

- Password **reuse** is a serious problem.
- When your password leaks, malicious individuals have:
    - an email address, username, and password combination they can try on other websites.
- Using the same login information everywhere:
    - a leak at one website could give hackers the ability to use password-reset links to access other websites.
        - Online banking or PayPal account.
- To prevent: **use unique** passwords on every website.
    - These should also be strong passwords – long, unpredictable passwords that contain numbers and symbols.

Why Browser-Based Password Managers Aren’t Ideal

- Web browsers - all have integrated password managers.
- They can’t compete with dedicated password managers.
- Example: Chrome and Internet Explorer store your passwords on your computer in an unencrypted form.
    - People could access the password files on your computer and view them, unless you encrypt your computer’s hard drive.
- Mozilla Firefox has a “master password” feature:
    - encrypts your saved passwords with a single “master” password,
    - storing them on your computer in an encrypted format.
    - The interface doesn’t generate random passwords
    - No cross-platform syncing (Firefox can’t sync to iOS devices).

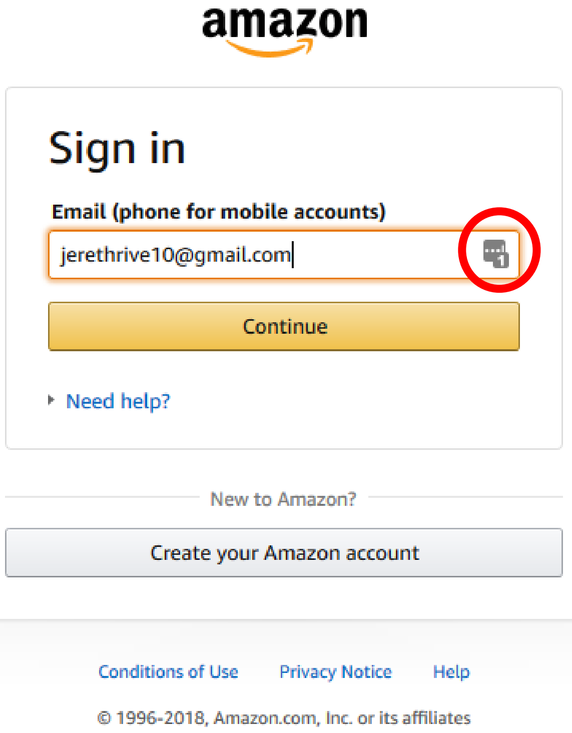
Types of password managers include:

- locally installed software applications   (Last Pass)
  - reside on the user's personal computer or mobile device.
  - in the form of a locally installed software application.
- online services accessed through website portals
  - a website that securely stores login details.
  - used on any computer with a web browser.
  - user trusts the hosting site.
- locally accessed hardware devices that serve as keys
  - a form of token-based password manager.
  - such as smart cards or secure USB flash devices.
  - still require software loaded on the PC.

advantages of password-based access controls.

- Prevents or Thwarts;
- Hackers, crackers, malware and cyber thieves to break into individual accounts.
- A defense against <u>phishing </u>and <u>pharming.</u>
  - sending emails purporting to be from reputable companies.
  - directing Internet users to a bogus website that mimics the appearance of a legitimate one.
- Protect against keyloggers or keystroke logging malware.
  - a software program or hardware device (keylogger) to record all keystrokes on a computer keyboard.

What Pass Word Managers Do



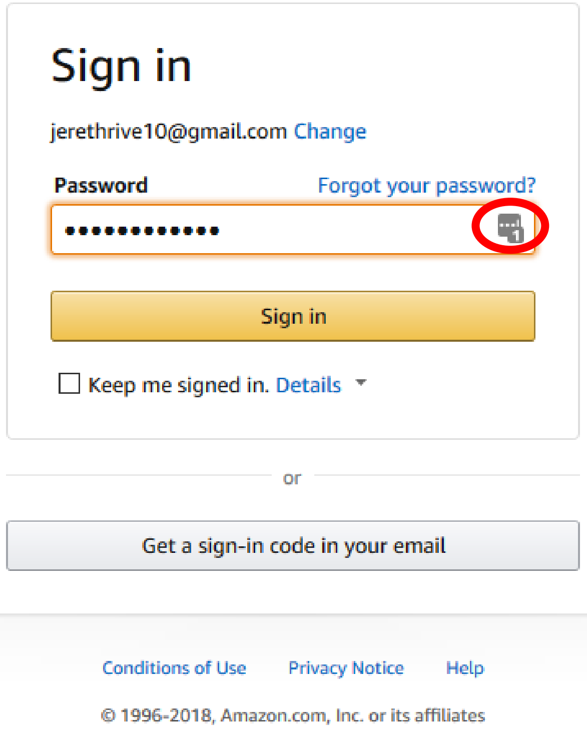
Sign in

Email (phone for mobile accounts)

jerethrive10@gmail.com

© 1996-2018, Amazon.com, Inc. or its affiliates

What Pass Word Managers Do



Sign in

jerethrive10@gmail.com Change

Password Forgot your password?

•••••••••••••

Sign in

☐ Keep me signed in. Details

or

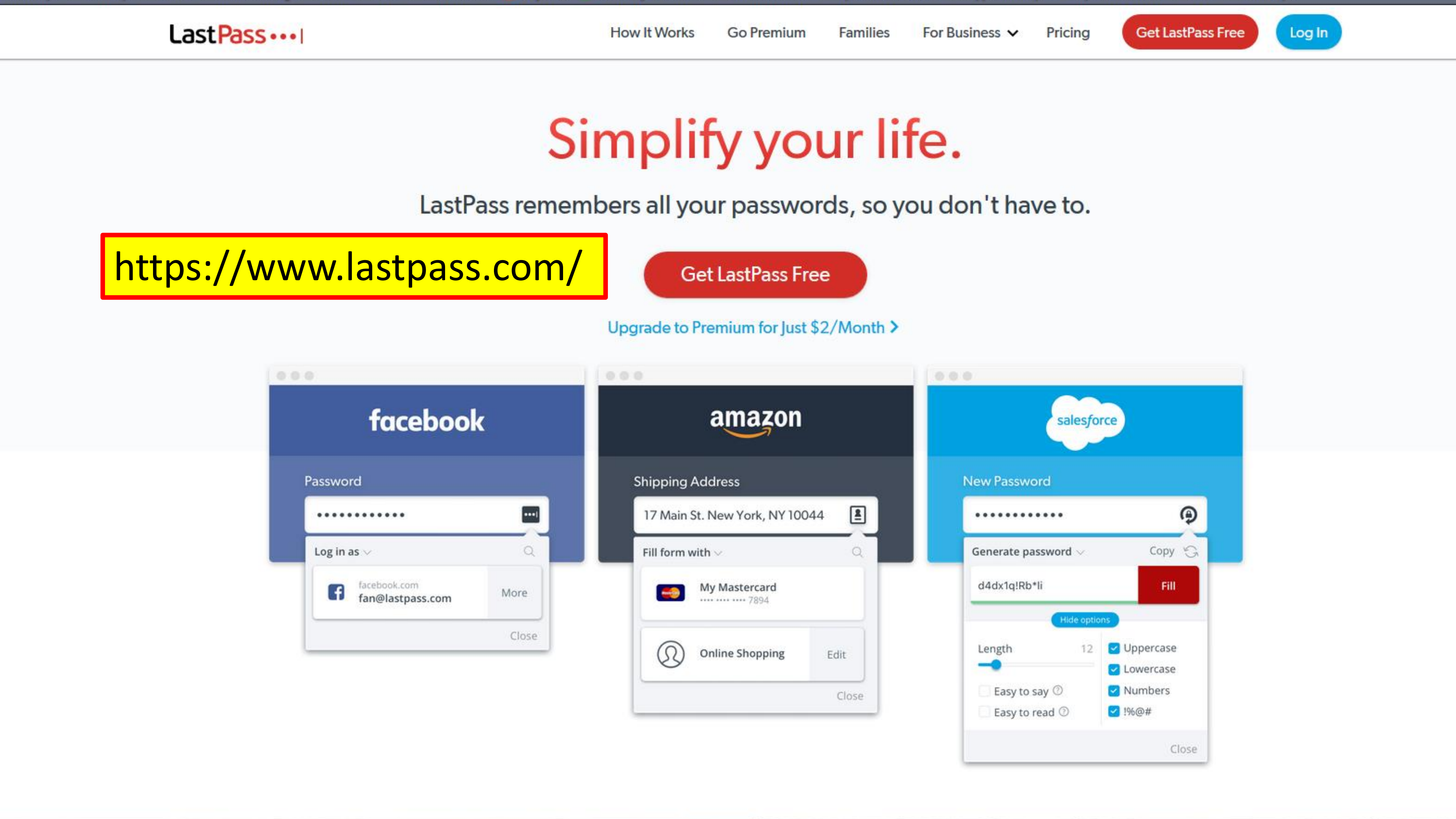
Get a sign-in code in your email

Conditions of Use Privacy Notice Help

© 1996-2018, Amazon.com, Inc. or its affiliates

LastPass:

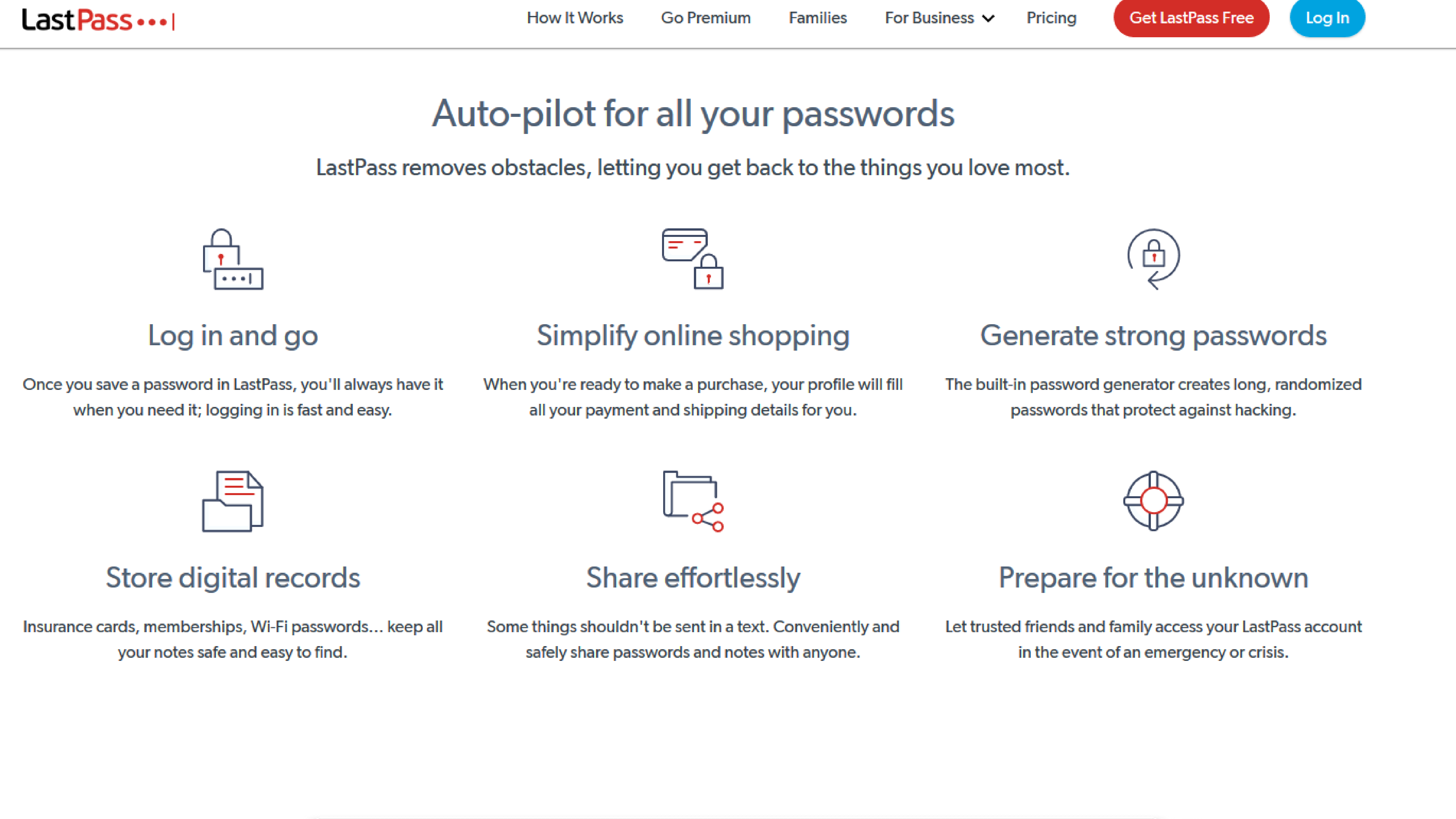
- A cloud-based password manager with:
  - extensions, (extend (add on to) what another computer program (called the base program) is able to do)
  - mobile apps,
  - desktop apps.
- For all the browsers and operating systems you could want.
  - Windows (browser Extension)
  - iOS, Android, Mac (App)
- It's extremely powerful:
  - two-factor authentication options
  - stores your passwords in the cloud, on LastPass's servers in an encrypted form,
  - the extension or app locally decrypts and encrypts them when you log in,
  - LastPass couldn't see your passwords if they wanted to.



Simplify your life.

LastPass remembers all your passwords, so you don't have to.

https://www.lastpass.com/



Auto-pilot for all your passwords

LastPass removes obstacles, letting you get back to the things you love most.

Log in and go

Once you save a password in LastPass, you'll always have it when you need it; logging in is fast and easy.

Simplify online shopping

When you're ready to make a purchase, your profile will fill all your payment and shipping details for you.

Generate strong passwords

The built-in password generator creates long, randomized passwords that protect against hacking.

Store digital records

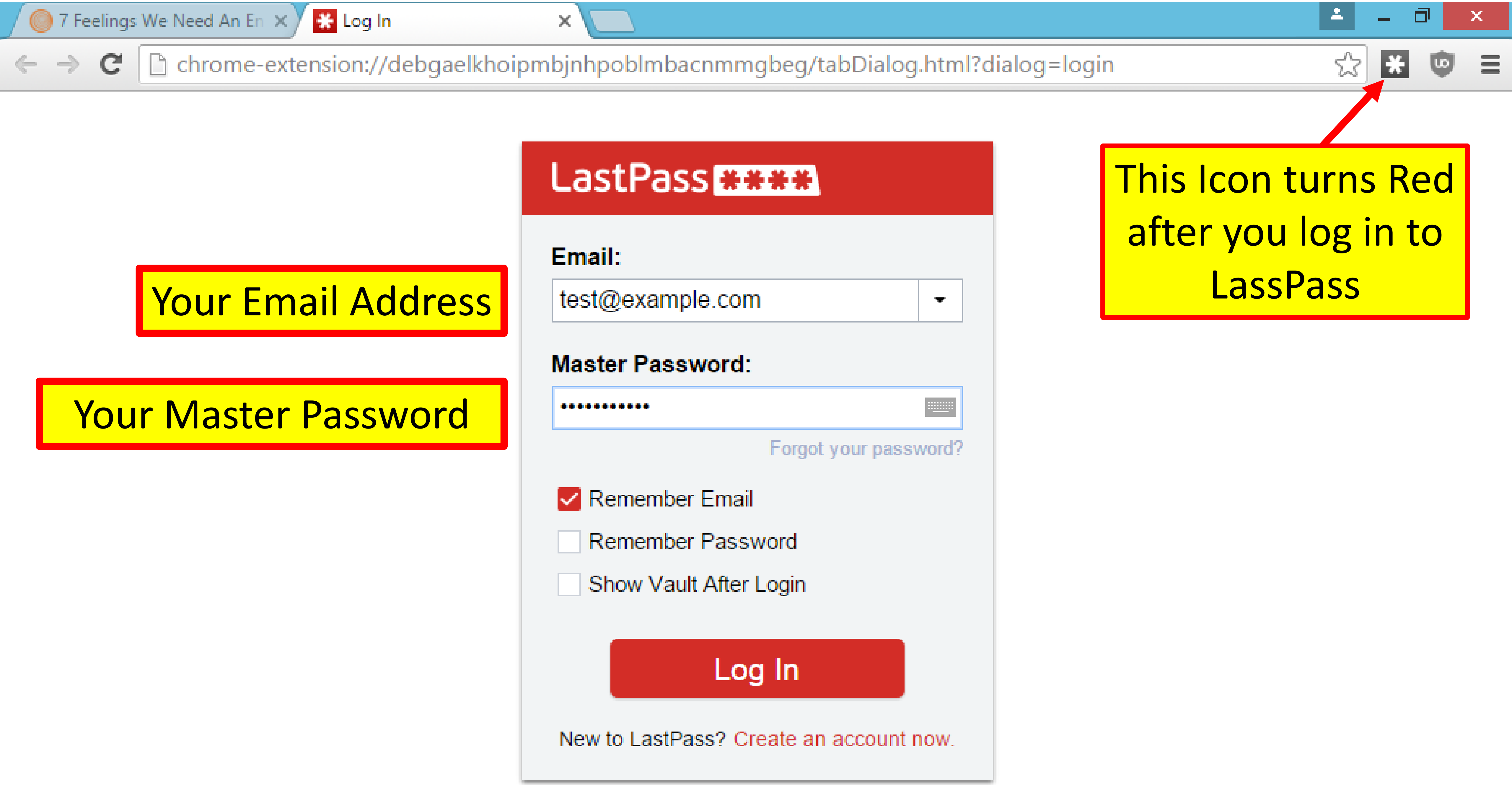
Insurance cards, memberships, Wi-Fi passwords… keep all your notes safe and easy to find.

Share effortlessly

Some things shouldn't be sent in a text. Conveniently and safely share passwords and notes with anyone.

Prepare for the unknown

Let trusted friends and family access your LastPass account in the event of an emergency or crisis.



chrome-extension://debgaelkhoipmbjnhpoblmbacnmmgbeg/tabDialog.html?dialog=login

Email: test@example.com

Master Password: ••••••••••••

Forgot your password?

☑ Remember Email

□ Remember Password

□ Show Vault After Login

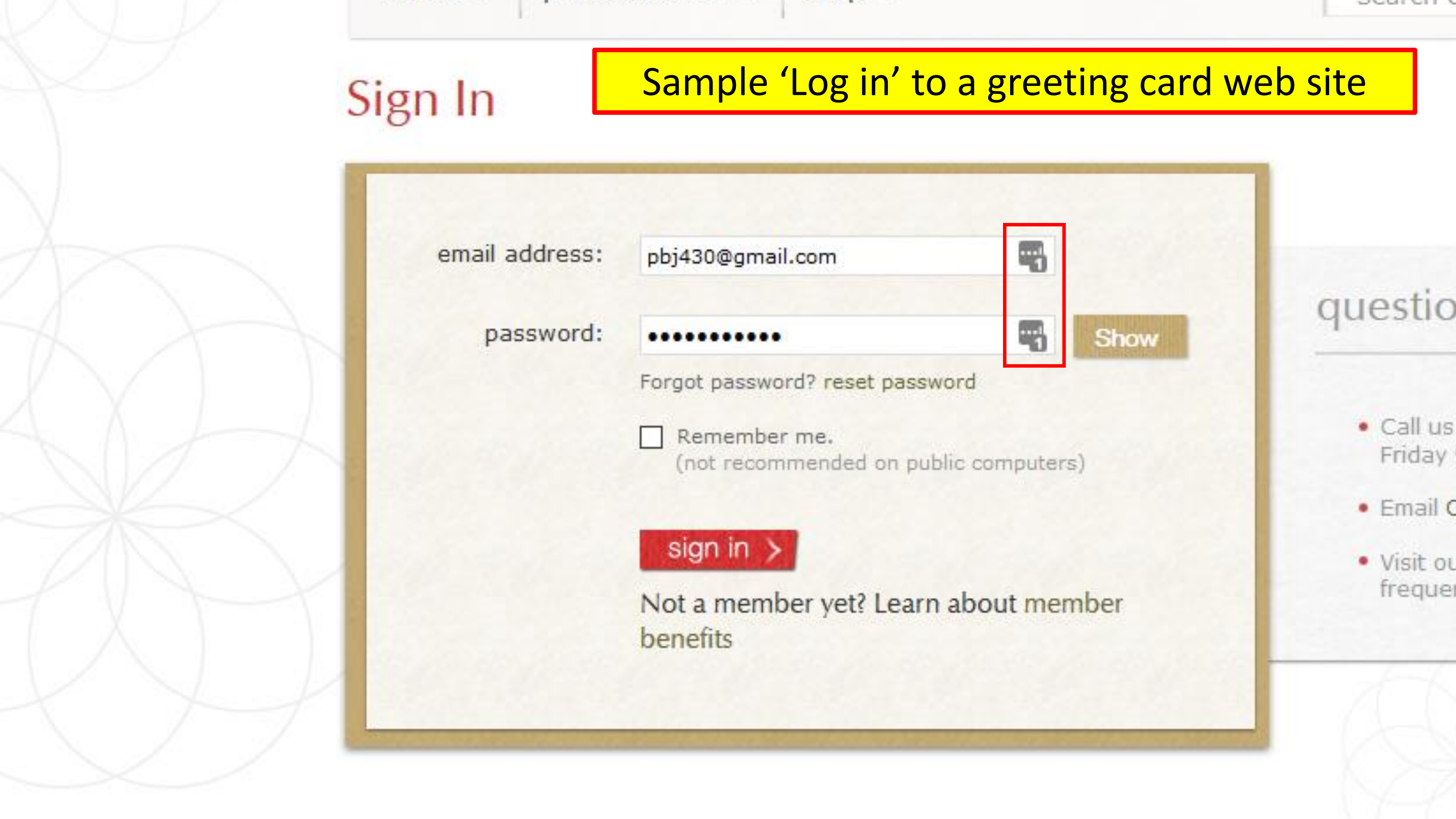
New to LastPass? Create an account now.

Your Email Address

Your Master Password

This Icon turns Red after you log in to LassPass

Sample ‘Log in’ to a greeting card web site



Sign In

email address: pbj430@gmail.com

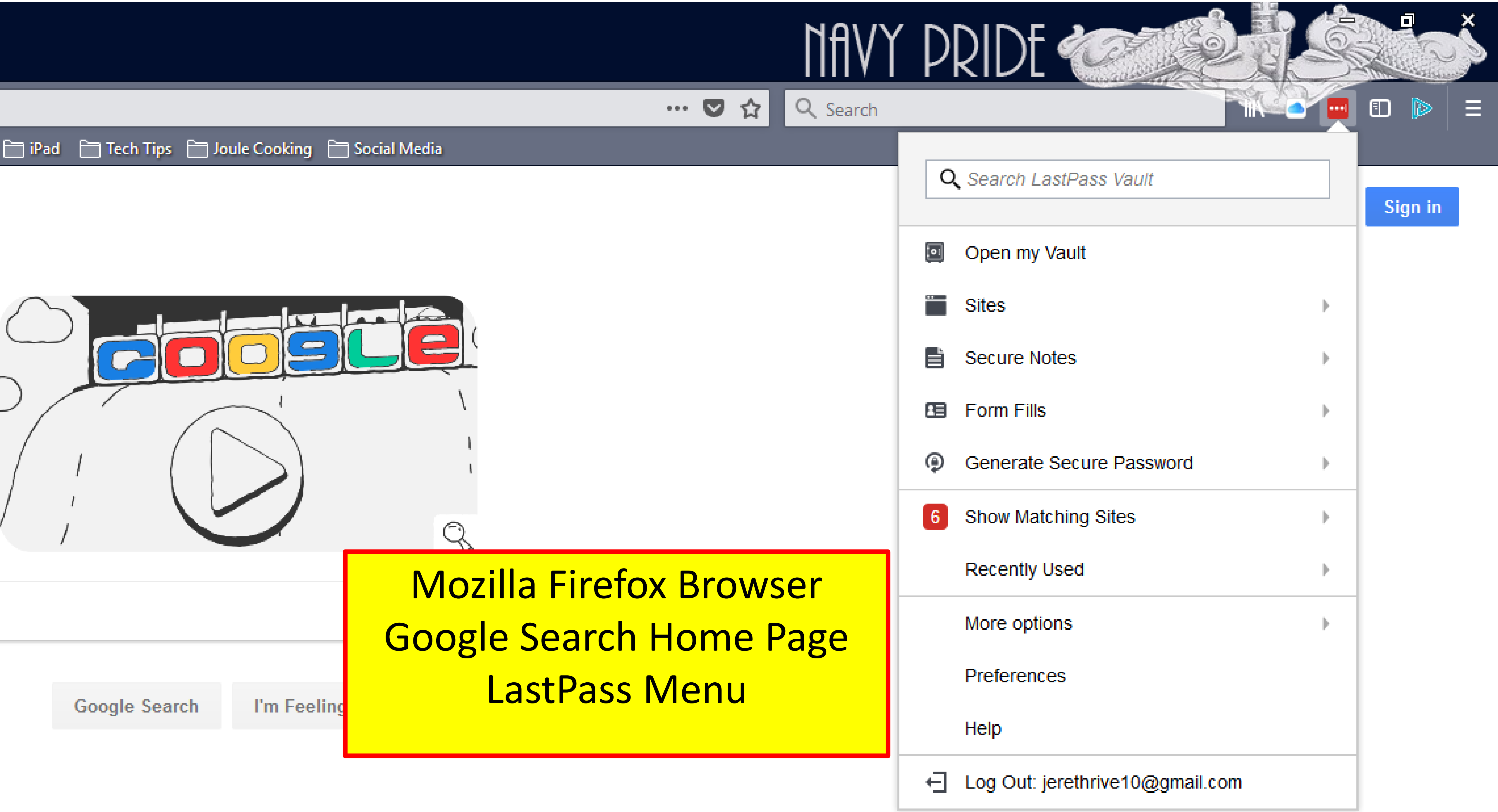
password: ●●●●●●●●●●● Show

Forgot password? reset password

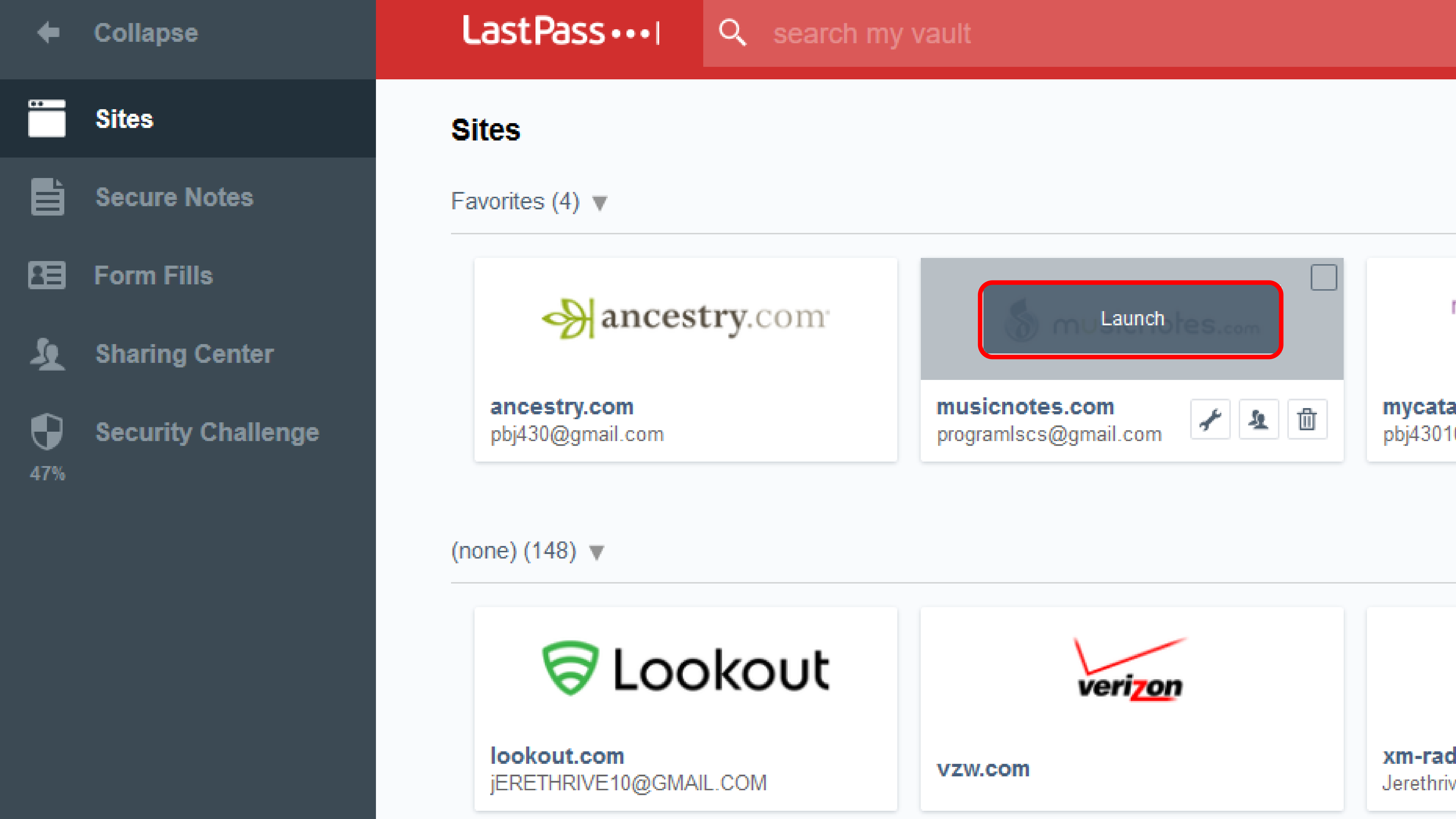
□ Remember me.
(not recommended on public computers)

sign in >

Not a member yet? Learn about member benefits



Mozilla Firefox Browser
Google Search Home Page
LastPass Menu



Sites

Favorites (4) ▼

ancestry.com
pbj430@gmail.com

musicnotes.com
programlscs@gmail.com

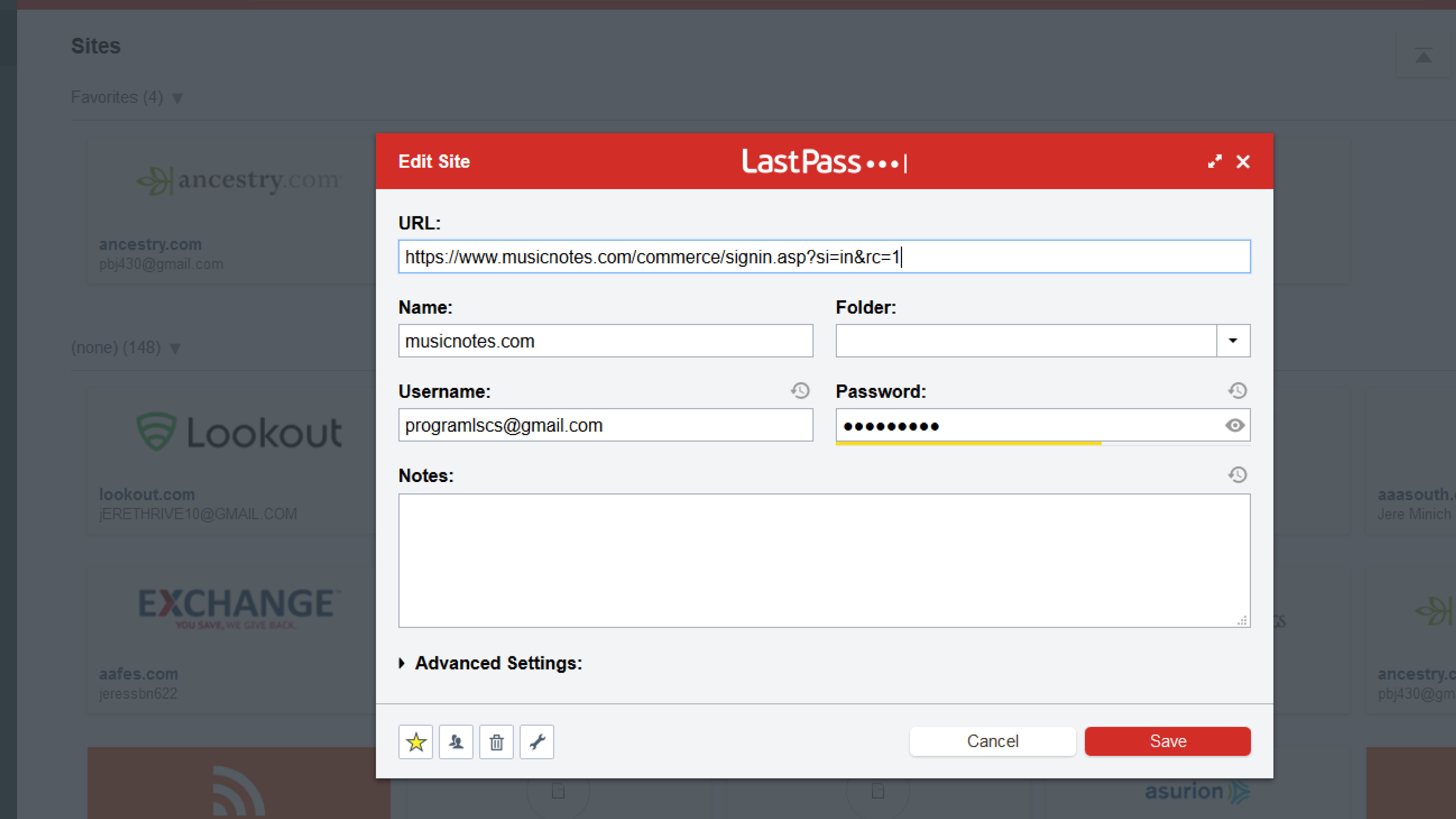
mycata
pbj4301

(none) (148) ▼

lookout.com
jERETHRIVE10@GMAIL.COM

vzw.com

xm-rad
Jerethriv



Edit Site

URL: https://www.musicnotes.com/commerce/signin.asp?si=in&rc=1

Name: musicnotes.com

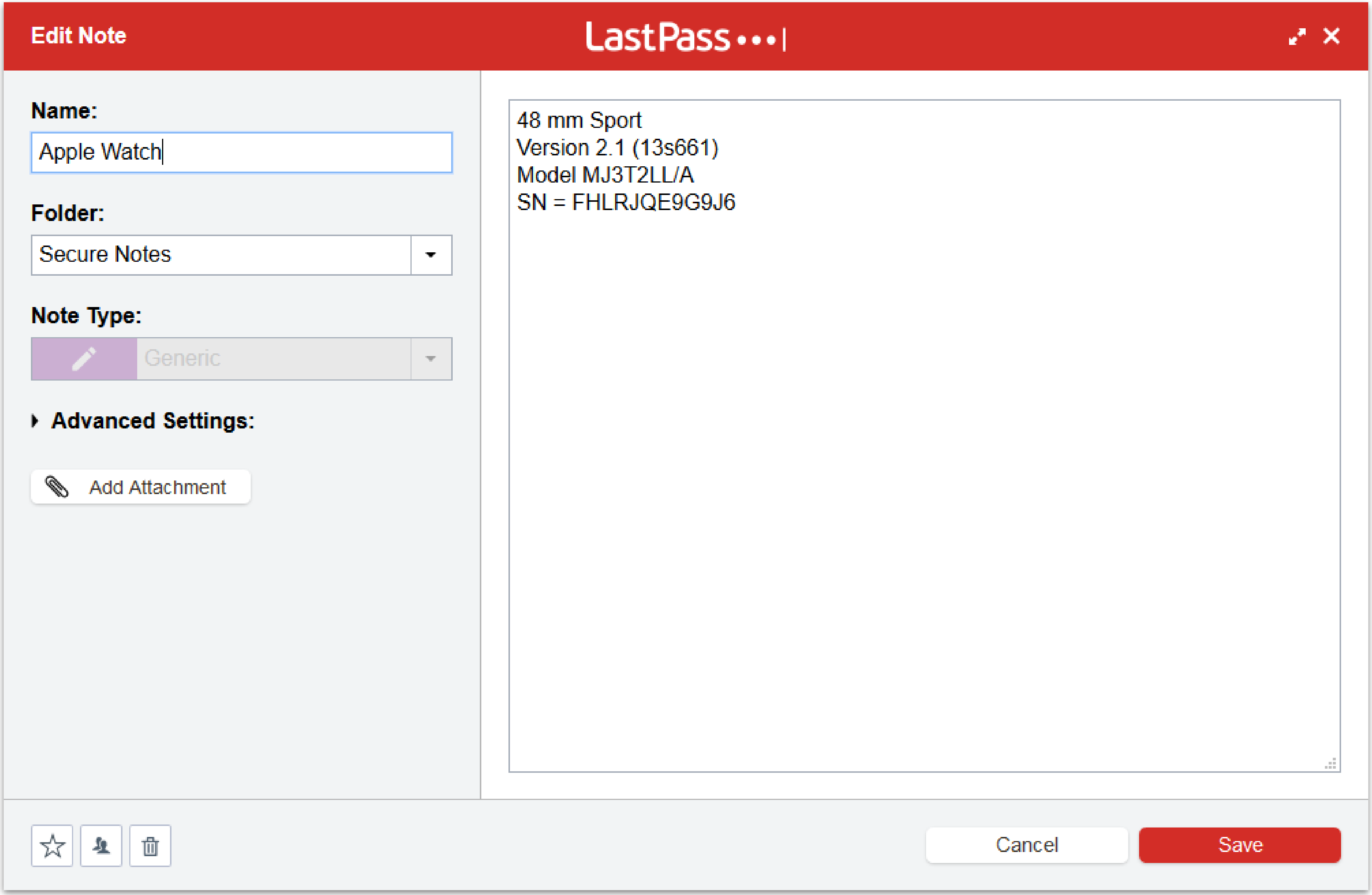
Folder:

Username: programlscs@gmail.com

Password: ●●●●●●●●●●

Notes:

Advanced Settings:

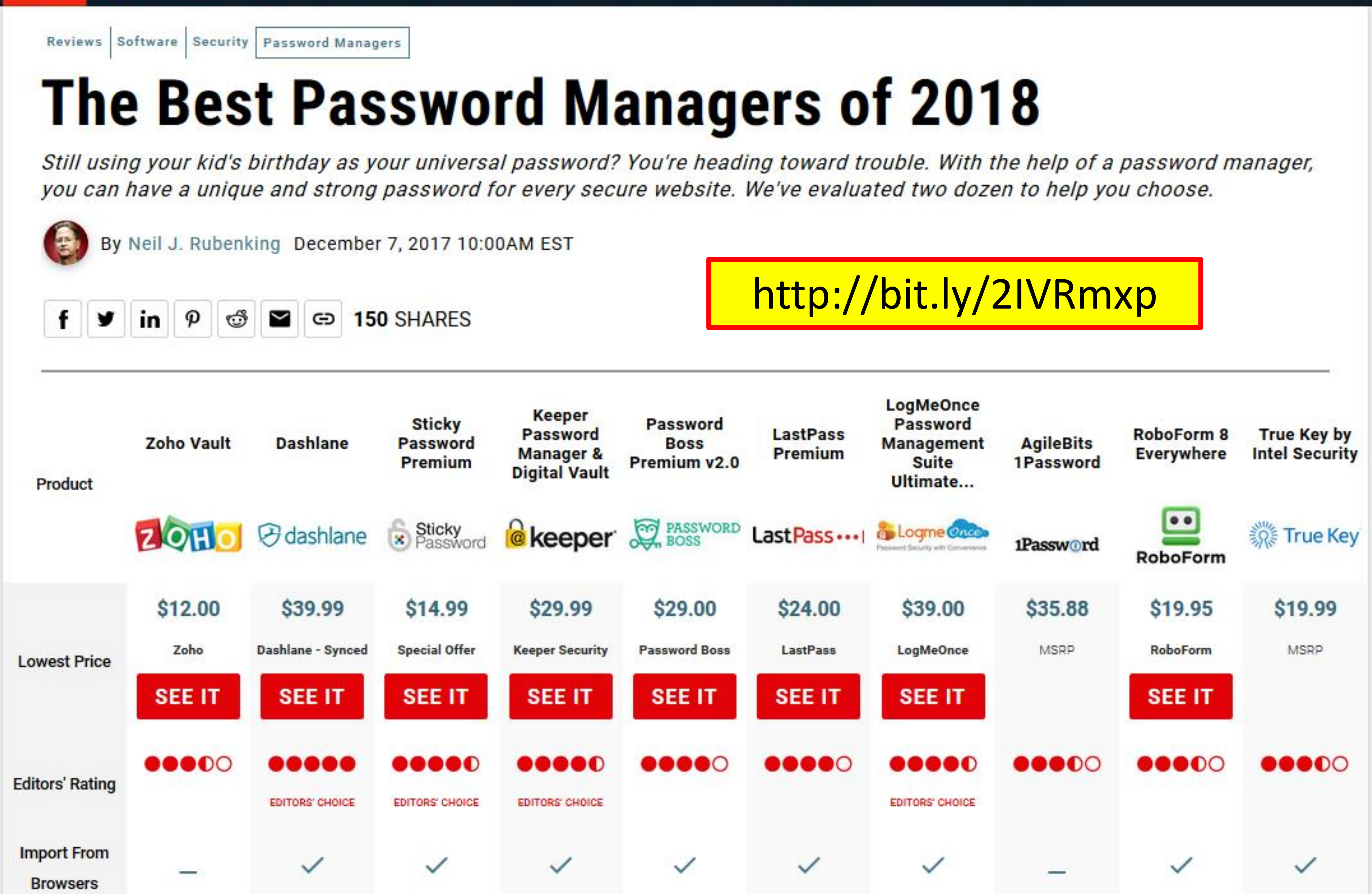


Name: Apple Watch

Folder: Secure Notes

Note Type: Generic

48 mm Sport
Version 2.1 (13s661)
Model MJ3T2LL/A
SN = FHLRJQE9G9J6



Reviews | Software | Security | Password Managers

The Best Password Managers of 2018

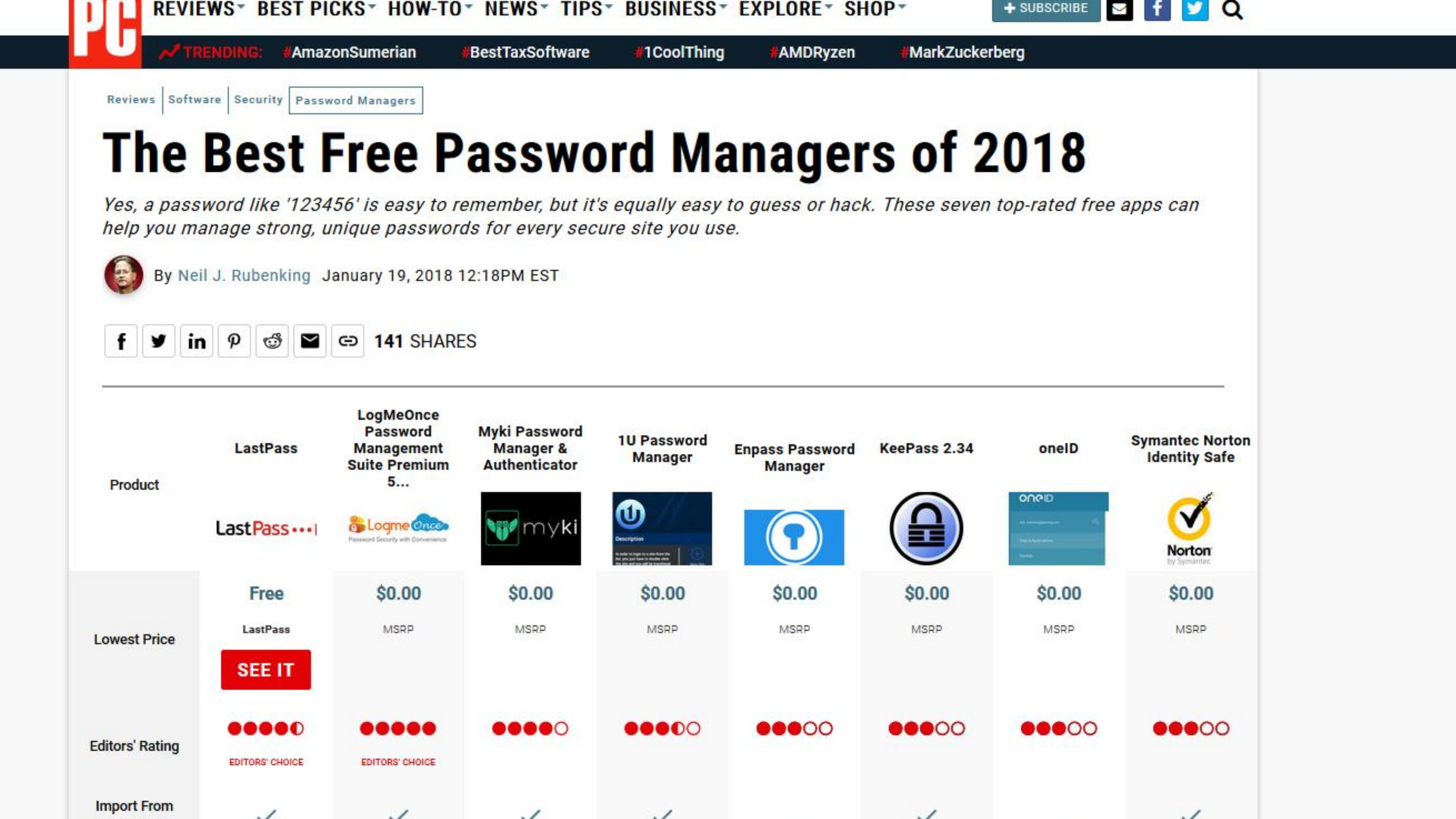
Still using your kid's birthday as your universal password? You're heading toward trouble. With the help of a password manager, you can have a unique and strong password for every secure website. We've evaluated two dozen to help you choose.

By Neil J. Rubenking December 7, 2017 10:00AM EST

150 SHARES

http://bit.ly/2lVRmxp

Product	Zoho Vault	Dashlane	Sticky Password Premium	Keeper Password Manager & Digital Vault	Password Boss Premium v2.0	LastPass Premium	LogMeOnce Password Management Suite Ultimate...	AgileBits 1Password	RoboForm 8 Everywhere	True Key by Intel Security
Lowest Price	$12.00 Zoho SEE IT	$39.99 Dashlane - Synced SEE IT	$14.99 Special Offer SEE IT	$29.99 Keeper Security SEE IT	$29.00 Password Boss SEE IT	$24.00 LastPass SEE IT	$39.00 LogMeOnce SEE IT	$35.88 MSRP	$19.95 RoboForm SEE IT	$19.99 MSRP
Editors' Rating	●●●◐○	●●●●● EDITORS' CHOICE	●●●●◐ EDITORS' CHOICE	●●●●◐ EDITORS' CHOICE	●●●●○	●●●●○	●●●●◐ EDITORS' CHOICE	●●●◐○	●●●◐○	●●●◐○
Import From Browsers	—	✓	✓	✓	✓	✓	✓	—	✓	✓



The Best Free Password Managers of 2018

Yes, a password like '123456' is easy to remember, but it's equally easy to guess or hack. These seven top-rated free apps can help you manage strong, unique passwords for every secure site you use.

By Neil J. Rubenking January 19, 2018 12:18PM EST

141 SHARES

Product	LastPass	LogMeOnce Password Management Suite Premium 5...	Myki Password Manager & Authenticator	1U Password Manager	Enpass Password Manager	KeePass 2.34	oneID	Symantec Norton Identity Safe
Lowest Price	Free LastPass SEE IT	$0.00 MSRP	$0.00 MSRP	$0.00 MSRP	$0.00 MSRP	$0.00 MSRP	$0.00 MSRP	$0.00 MSRP
Editors' Rating	●●●●◐ EDITORS' CHOICE	●●●●● EDITORS' CHOICE	●●●●○	●●●◐○	●●●○○	●●●○○	●●●○○	●●●○○
Import From	✓	✓	✓	✓		✓		✓

Bottom Line

- **Liability** — You can’t protect everyone from stupid. Password1234 will pass most checks.
  - Not encrypting your password database will buy you big-time problems, just ask your favorite home improvement store.
- **Technology** —There are some good canned password management products on the market.
  - I highly recommend looking at a couple of the big players and pick one.
  - Internally developed products are fraught with difficulty and impossible to maintain, simply not worth it.
- **Peripherals** —HIPAA requires that proper standards for password safety — good old length & strength — be employed.
  - Password database encryption is not currently required, but after recent breaches where passwords were stored unencrypted, it’s sure to be coming.
  - With all these regulations and it looking more and more like the federal government is going to get involved, why not look like a champ?
- Password management and storage should be a part of every well managed user.
- It is unfathomable that proper password management is not employed everywhere.
  - If not, this should be priority one.
- And that is the bottom line.

If you do not want a password manager, then:

- Go to this Website and read what Rick has to say.
- https://www.ricksdailytips.com/create-secure-password/
    - His method is the wave of the future.
    - long and obscure.
    - easy to remember phrase and mix it up a bit.
- Bonus tip: You can easily lock your online accounts down tight by enabling **two-factor authentication** on them!
- IMHO – If you do not use some method to keep your passwords secure;
    - Keep your gun handy so you can shoot yourself in the foot.