Password Managers

Last Pass, 1Password, and Robo Form

Secure vs Open Network - What’s That??

Open Network: When connecting to a network, you are exposing your device and all your traffic to all other users of that network. In an **open WiFi** everyone and anyone can log in with you. So don’t log into anything sensitive that might give a hacker reason to check you out.

For example, if you're in a coffee shop or public library, make sure to verify the name of the network with staff or on signage before connecting.

https://www.cnet.com/how-to/tips-to-stay-safe-on-public-wi-fi/

Settings - privacy and security on phones, tablets, computers

Turn Off Sharing. When you're at home, you may share files, printers, or even allow remote login from other computers on your network. ...

Enable Your Firewall. ...

Use HTTPS and SSL Whenever Possible.

HTTPS// SSL What Does It Mean????

To put it simply, the extra "s" means your connection to that website is encrypted so hackers can't intercept any of your data. Have you ever noticed that some URLs start with "http://" while others start with "https://"? Perhaps you noticed that extra "s" when you were browsing websites that require giving over sensitive information, like when you were paying bills online.

The technology that powers that little "s" is called SSL, which stands for Secure Sockets Layer. But when you visit a website that's encrypted with SSL, your browser will form a connection with the webserver, look at the SSL certificate, This binding connection is secure so that no one besides you and the website you're submitting the information to can see or access what you type into your browser.

What Things NOT To Do on a Free WiFi

Don’t Check Email and Bank Accounts

Watch Out for Non-secure Sites

Avoid Using Apps - better on your home network, than on your phone

Avoid Accidental Sharing

At home, you may share files, printers, or even allow remote login from other computers on your network. Turn these features off

Keep your browser and internet-connected devices up to date with the latest versions, but make sure to do this on a trusted home or work network -- not on public Wi-Fi.

How LASTPASS CAN PROTECT YOUR DATA

Having a "strong password" lowers the overall risk of a security breach. It is not the 'end all' protection, but a strong step to deter "hackers" from getting your personal information.

But ...how do you remember all the site passwords, and user names?

For myself, on LASTPASS I store over 174 sites : Banking, Health, Credit Card,

Shopping, Email, Insurance, CPE Education, News, Reference, and Job -Intuit

Be safe: Improve computer security by choosing passphrases over passwords

Elijah Woodward
Special to The Explorer

I hate passwords.

They don't make sense, they're getting complicated and you have to remember so many of them these days. Why do they have to be so long? Why can't they be just a word, like "cat"? What's the purpose of them?

Passwords are generally a bad idea. We need to start thinking of pass phrases from now on. Eight characters is often the minimum required due to how quickly the passwords can be guessed when falling below that threshold. So using a string of words, or a phrase, is much easier to remember. Things like "Hangupanddrive" are easy to remember. According to the website www.passwordmeter.com, this password gets a score of 44 percent difficulty.

Mix and match numbers, capital letters and special characters to create even more diversity in your new pass phrase. H@ngup4ndDR1VE is a good example of taking our previous password and making it much stronger. Www.passwordmeter.com rates this password as 100 percent.

Pass phrases shouldn't be the only thing keeping people out of your email, banking or social media accounts. Use two-factor authentication, like requiring a text message with a code to login to your bank and email.

With websites being hacked all the time, this means passwords need to be discarded regularly. Since most people re-use passwords for different accounts and their email, if a criminal obtained your password from say, the LinkedIn breach in 2012, they could also get in to your email. From there all they have to do is reset the password for your bank account, which will be delivered to the email they already have gotten into.

We've taken many reports over the years from individuals whose banking and investment websites have been broken in to. While this may seem very technical and sophisticated, it's no more difficult than finding a car key in a parking lot and trying it in cars until you find one you can drive away. This, of course, is also highly illegal.

For 2017, start keeping yourself safer from cyber criminals by making yourself harder to hack. It doesn't take a lot of time, and is well worth it to save yourself the time and effort later of dealing with financial crimes.

BigStock

Changing how you think about cyber security can have huge benefits.

Editor's Note: Elijah Woodward has been an officer with the Oro Valley Police Department since 2007. He is also a local expert on cybercrime, internet-based scams and other crime trends, both in and out of Oro Valley, and works to inform citizens so they can better protect themselves.

Passphrases over Passwords
www.passwordmeter.com

CCubsrMyDad’$FAVTeam1904

M0eFAM+g^Gram1902

1. Use a unique password for each of your important accounts.
2. Use a mix of letters, numbers, and special characters in your password.
3. Don't use personal information or common words as a password.

How Does Last Pass Help You ?

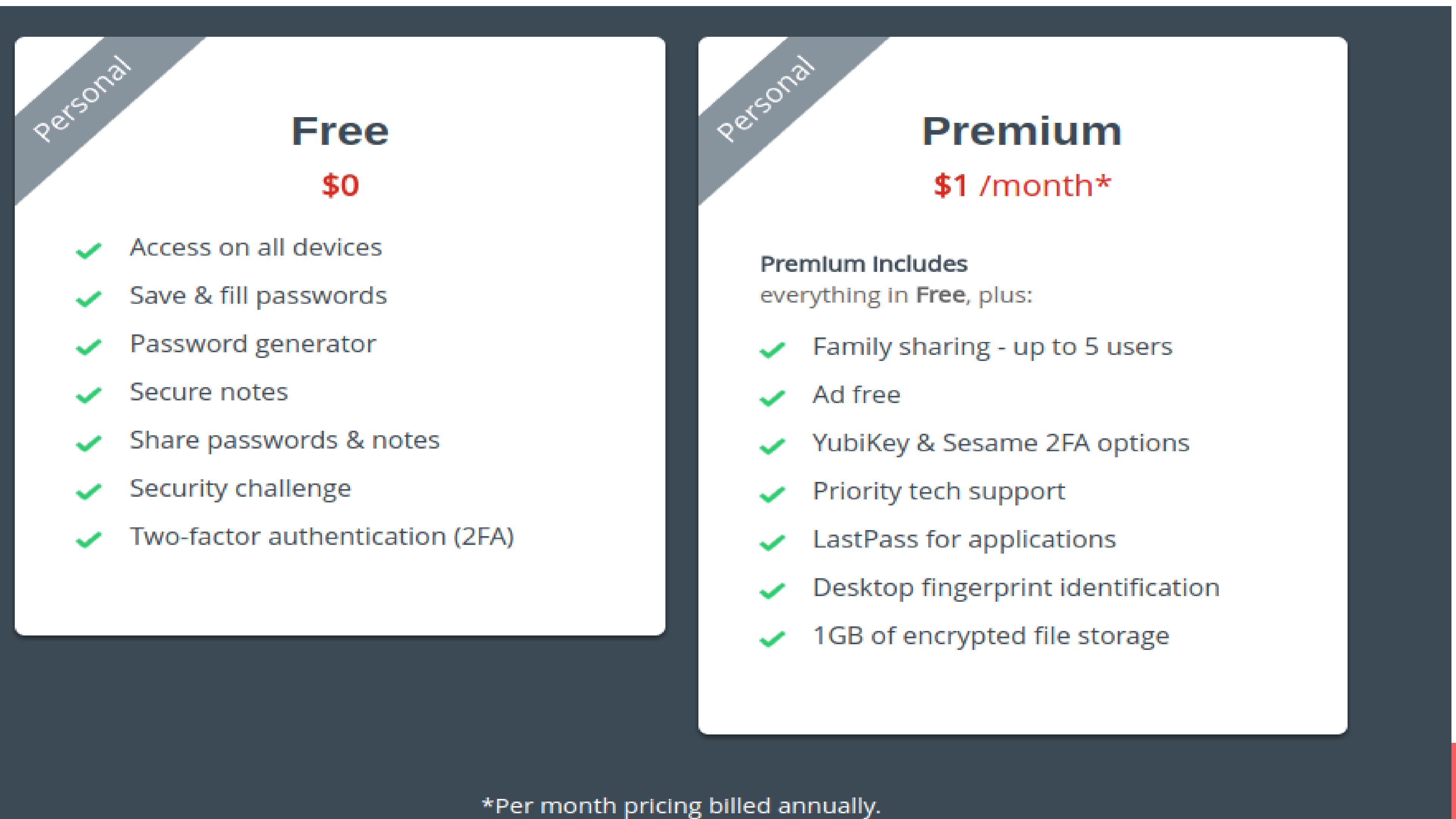
Generate a new password when visiting a site

Open in your browser to log into an existing site

Keep notes and additional information about the site

Autofill to automatically login

Yubikey with just plug it into a USB port, and touch the button for secure and strong authentication



Free

$0

- ✓ Access on all devices
- ✓ Save & fill passwords
- ✓ Password generator
- ✓ Secure notes
- ✓ Share passwords & notes
- ✓ Security challenge
- ✓ Two-factor authentication (2FA)

Premium

$1 /month*

Premium Includes
everything in **Free**, plus:

- ✓ Family sharing - up to 5 users
- ✓ Ad free
- ✓ YubiKey & Sesame 2FA options
- ✓ Priority tech support
- ✓ LastPass for applications
- ✓ Desktop fingerprint identification
- ✓ 1GB of encrypted file storage

*Per month pricing billed annually.

TESTIMONIALS

Just yesterday I had another great reminder why I love LastPass. A site I use was compromised and I was concerned about my credentials putting other services at risk. I checked my LastPass vault and the credentials were not used on any other site AND I had used a randomly generated 13 character password. I feel much safer knowing I have a much reduced risk profile in situations like this.

Jeff M., 4-year user, over 100 sites