How to protect your privacy
Simple steps for a more secure online presence

How to secure your passwords

A simple
three step guide
and a free tool
to secure passwords
on all your devices

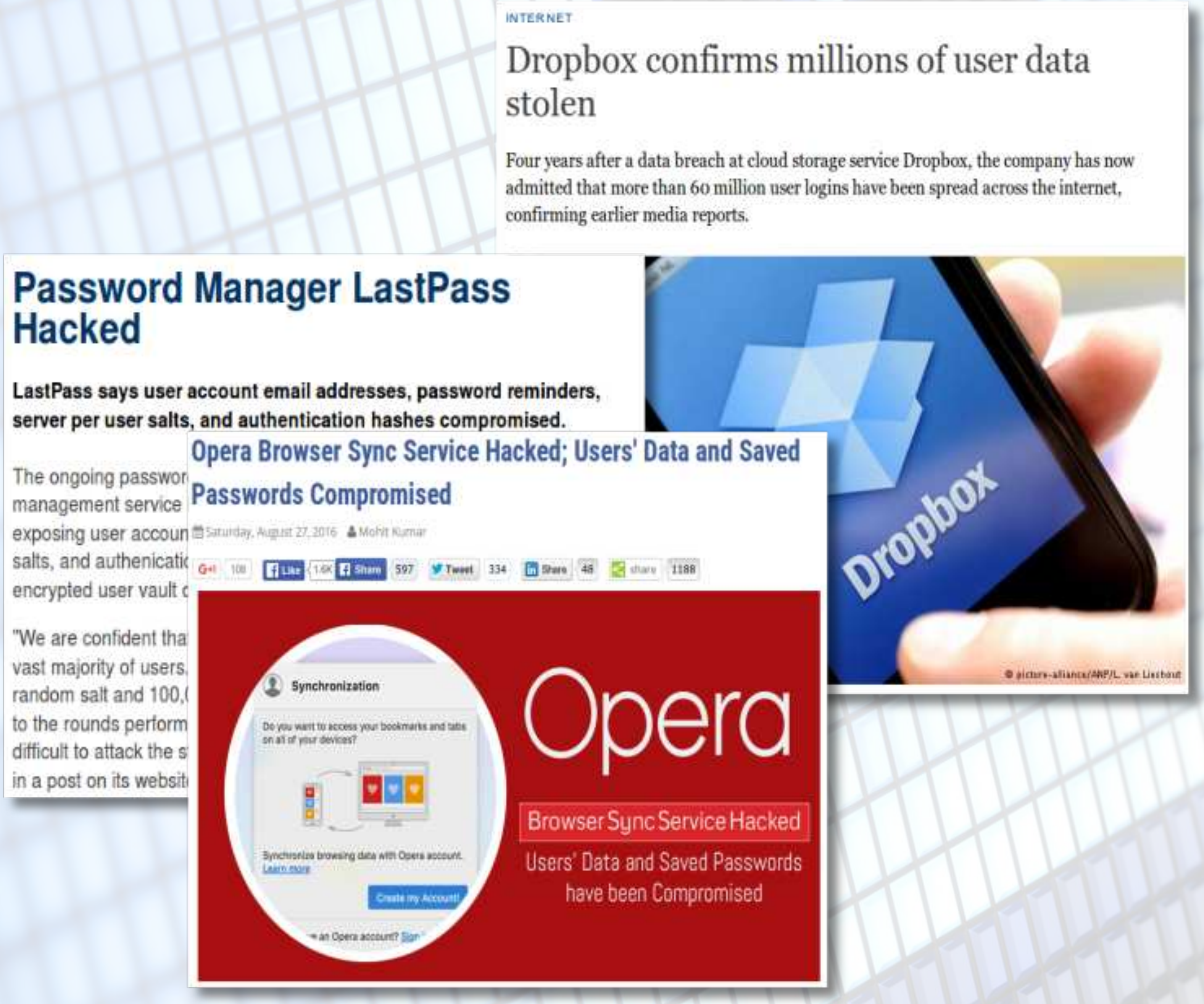
n° 092016-B

Secure your Passwords

You might be surprised to hear that you have valuable secrets. In fact, your secrets are so valuable that there are entire industries (legal and illegal) devoted to stealing them. Your secrets are your online passwords.

You use them all over the place--to prove your identity, to access information, to pay for products and services... and they are often easily hacked!

It's time now for you to proactively secure your passwords, and in this document we will give you all the tools you need.



INTERNET

Dropbox confirms millions of user data stolen

Four years after a data breach at cloud storage service Dropbox, the company has now admitted that more than 60 million user logins have been spread across the internet, confirming earlier media reports.

© picture-alliance/ANP/L. van Lieshout

Password Manager LastPass Hacked

LastPass says user account email addresses, password reminders, server per user salts, and authentication hashes compromised.

The ongoing passwor
management service
exposing user accoun
salts, and authenicatio
encrypted user vault c

"We are confident tha
vast majority of users,
random salt and 100,0
to the rounds perform
difficult to attack the s
in a post on its websit

Opera Browser Sync Service Hacked; Users' Data and Saved Passwords Compromised

Saturday, August 27, 2016 Mohit Kumar

G+1 108
Like 1.6K
Share 597
Tweet 334
Share 48
share 1188
Dropbox
Synchronization
Do you want to access your bookmarks and tabs on all of your devices?
Synchronize browsing data with Opera account.
Learn more
Create my Account!
an Opera account? Sign
Opera
Browser Sync Service Hacked
Users' Data and Saved Passwords have been Compromised

The three most effective tips to secure your passwords and make them

1. Unique

Each of your passwords should be unique to each individual service provider (email, banking, social networks, cloud services, etc.).

Why? Because online services get hacked*!

If you use the same password for every service, your identity will be compromised on all of those services once the first one is hacked.

Online services are often hacked by professional hackers, and there are no enforceable laws obliging those services to inform users. The moment an online service is hacked, your password is exposed. A professional hacker will use it on all other online services in the hope that you repeated yourself. Don't make it so easy!

2. Hard to find

Ideally you should not write them anywhere, neither on a post-it nor on a piece of paper hidden in your wallet.

If you really want to keep them somewhere, then you'll need to secure this place as well. Please consider that online services providing secure password storage are a prime target for all worldwide hackers!

3. Hard to guess

Not only should you avoid writing your password anywhere, but those passwords should also be difficult to hack.

Hackers today apply a science called social engineering. They mine your public social profiles (Facebook, Twitter, etc.) for names and dates, then all available details are put into a profiled vocabulary used to generate random passwords. Today, a simple PC can test thousands of combinations per second.

The ideal password should be a combination of letters, numbers, and symbols, and up to 43 characters in length.

Is this realistic? YES!

Here is the way to remember and keep track of tens or hundreds of extremely long and complex passwords!

Password Manager

An appropriate password manager will help you:

Generate and retrieve a unique password for each individual digital service you access;

Generate each password as a combination of letters (upper and lower case), numbers, and symbols;

Make each password at least 16 characters in length, ideally 43 characters (unfortunately, not all online services accept such long passwords).

Which One?

Choose only a ubiquitous password manager that allows you to access passwords on any digital device you use (whether it is a PC, Mac, or Linux machine, a phone, tablet, whatever), so that you can always access your locked services, no matter where you are.

Do NOT use online password managing services: such services are hacked even more often than other online services! The moment your password manager provider is hacked, all of your passwords are exposed.

Not only this, but in the case that passwords are exchanged between your local device and the remote service provider, even a man-in-the-middle attack can hack your passwords indirectly without accessing your device or your service provider.

Choose a password manager that do NOT store all passwords on your device. Instead, use solutions that generate a password any time you request it. In case your device is stolen or hacked, your passwords are not compromised. An open source password manager is preferable, so that its source code can be checked against any potential back-door.

Your Free Tool

We recommend Password Maker Pro as a password manager because:

- ✓ It is open-source;
- ✓ It runs on any platform and/or device (Mac OS X, Linux, Windows, iOS, Android, etc.);
- ✓ It does not access any online service to store your passwords;
- ✓ Your passwords are actually never stored--they are generated by the most advanced algorithm whenever you need them;
- ✓ It is free and you can find it here:

https://passwordmaker.org/

*And if you want to know if your credentials have been hacked in the past, check out this other free on-line database:

https://haveibeenpwned.com/

Please note we are not affiliated in any way with any of the contributing developers of the several PasswordMaker versions available for each platform. It is an open project and we recommend it because it satisfies all our requirements.

Instructions and tutorials for the PasswordMaker application should be easily available online. However, for any questions regarding settings or anything discussed in this document, please feel free to contact us personally at info@isher.club

Is that all?

Protecting your secrects, your passwords, is one thing. Protecting your identity and, ultimately, your privacy, is another. When online services such as Adobe, LinkedIn, Dropbox, and countless others get hacked, your profiles are exposed. That includes your user-id, your mail, your personal questions, if any, your relationships, your passwords, and so far and so forth. Using a different password for each service is a good start. In a subsequent guide we will illustrate how to use different e-mail addresses and how to keep your identity distinct from services you use online. Stay tuned, or write us at info@isher.club if you need more urgent advice.