How to Manage Your Online Passwords on Multiple Devices

A TrendLabs Digital Life E-guide
Managing passwords has never been more important and complicated than it is today.

Nowadays, you have to create and keep track of numerous passwords to various accounts. It’s also tedious to manage every single one of them stored on each of your devices.

If you don’t do it properly, you may find yourself at the mercy of password-hacking cybercriminals. They can steal your information, identity, and money.

Every three seconds, there is another victim of identity fraud. One in five users in the US also experience having their credit card details stolen and used for unauthorized purchases.

Don’t let cybercriminals ruin your digital life. Start properly managing your passwords for all your online accounts on all of your devices.
Don’t Reuse, Reduce, and Recycle

The three Rs may be great for the environment, but not when it comes to your passwords.

Your passwords need to be unique. They can’t be as common as ‘password’ or ‘123456’, which, coincidentally, are two of the most popular passwords ever. Even cybercriminals know these. You can bet they’ll use them while attempting to hack into your accounts.

Make your passwords long and uncrackable. Use nonsensical words or phrases strung together, or even a mishmash of numbers and letters. A secure password management tool can help here. It can generate random passwords for your various accounts and store these passwords under a master password so that you never have to remember all of them.

Never recycle your passwords. Once you’ve used one, don’t use it again for anything else. If cybercriminals get a hold of your password, they will have access to everything it unlocks.
Double Your Security

Enable **two-step verification** whenever available. Two-step verification is a feature now becoming more common with websites that require login information. It gives you a verification code to use along with your password. This verification code can’t be stolen, because it’s randomly generated for that login session alone, and it’s given to you through another way besides your computer, like your mobile phone or email account.

You may have experienced two-step verification as a Facebook user trying to log in to your account from a different device. Once Facebook detects that the device you’re logging in with is unfamiliar, it sends you an SMS message with a code that you have to use in conjunction with your original password. This will confirm that you are indeed the person logging in.

This process lets you have sole access to your account. Since your account can only be accessed with a password and a verification code stored on the device in your possession, cybercriminals will find it harder to hack into your account.
Clean Out Your Cookies

We’ve all relied on the “Remember Password” option offered by our Internet browsers at least once. It allows you to log in automatically whenever you load up your page instead of requiring you to manually type in your details every time.

Cybercriminals know that users love this option, and they’ve developed ways to steal your passwords through it. Cookiejacking, for instance, lets cybercriminals take control of your browser cookies and use them to access your accounts. Cookies are data that websites use to record your website visits. If you have any saved data on a website, like login information, the site will automatically reload it for you. If cybercriminals get hold of your cookies, they can trick a website into thinking they’re you.

Don’t rely on cookies. Instead, save your passwords in a secure password management tool. Good tools will also enable you to use secure browsers to access your accounts, especially when they require very sensitive information like online banking details. Unlike your normal browsers, secure browsers disable unnecessary browser add-ons or plug-ins that could compromise your privacy.
Enable Your Device’s Security Features

Mobile device manufacturers are now savvier about security. Google, for example, acknowledged how their current issue with Android updates puts their users at risk. At the same time, there’s the ongoing Android malware problem, which is ever increasing. To help their users, Google developed free additional security features for Android devices.

Enabling these features, preferably before you use your device to connect to the Internet, can prevent malware from stealing your passwords. You can find out how to do this through our e-guide, 5 Simple Steps to Secure Your Android Phones.

Installing a comprehensive mobile security app is also highly recommended, since it can protect not just your passwords, but also your data.
Look Into Password Management Tools

Managing your passwords across your PC, Mac, and mobile devices can be difficult. Not everyone can instantly create and memorize 16-character passwords with random alphanumeric combinations. Not everyone can keep track of which password goes where, either.

There are password management tools and apps that automate these tasks for you. They do all the hard work without cutting corners and risking security.

Look for software that automatically generates strong and secure passwords for all of your accounts, using one master password for secure access to all user names and passwords, across all devices. A good solution will also include a secure browser to help protect financial transactions.
TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.