Why Saving Passwords in Browsers is a BAD Idea

SECURITY IS A TOP PRIORITY THESE DAYS

As you know, security is a top priority these days — especially as data breaches become more common, complex and costly. And if you're a sysadmin or you work anywhere in or around SecOps or InfoSec, you also know that end users are usually the weakest link in the network security chain.

Unfortunately, browser-based password saver features are usually part of the problem and rarely the solution.

The Background

Organizations that develop browsers — such as Google (Chrome), Mozilla (Firefox), Microsoft (Edge), Apple (Safari), and Opera Software (Opera) — focus on enhancing UX with various add-ons. One feature they know users love is the "password saver," which **makes it faster and easier to log into various websites.**

However, sometimes "faster and easier" go against basic security practices, and this is one of those cases. Stored passwords are about as secure as a spreadsheet or yellow sticky note, as **it would take a hacker about 10 seconds to copy a stored password** — without even leaving a trace.

What About Smart Lock?

Things are a little better thanks to [Google Smart Lock](#), which lets users save passwords through their Google accounts. It's also useful for sharing passwords between an Android phone and a desktop/laptop. But it's (obviously) only available to Chrome and/or Android users. While Smart Lock is better than browser password savers, **it's not the most robust solution out there.**

Closing the Password Security Gap

The best — and really, the only — way to close the password security gap is by using a legitimate password manager. These are available for every platform at various price points. They are also **much easier to use than in years past**. Plus, they make it possible to save other sensitive and confidential data, such as credit cards numbers, social security numbers, and so on.

Choosing the right password management solution is critical, and you may not have the time right now to explore your various options. But don't worry — we have your back! My colleague Jenny reviewed some of the most popular password managers [here](#). It's a great (and fast) way to learn about each solution does strengths, and how they differ from one another.

How We Can Help

I don't pretend that we offer the best solution to your problem, but we definitely offer a good one. First, if you want to keep your personal data safe, I recommend looking into a password manager like [LastPass](#) or [Dashlane](#), as cited in [Jenny's article.](#) Of course, at Devolutions, we offer a solution called [Remote Desktop Manager](#), which **lets you centralize your passwords, your remote connections and your sensitive information.** If you'd

rather not pay for a solution because you'll only be using it for personal use, you can download the free version here.

To make things even easier, we've recently launched a product called [Devolutions Web Login](#) that lets you **create, store and auto-fill your login credentials and passwords to any websites** directly from your browser. It works a little bit like Google password saver, but **way safer**. We offer multiple ways to store your passwords, but for free users, I would recommend creating a [cloud account](#) and using [Devolutions Online Drive](#), which is totally free for storing your passwords.

Once you've found your ideal password manager, you'll have to go back to your Chrome browser advanced settings and find your passwords under "manage passwords". You can then add your passwords manually in the password manager of your choice; sadly, there is no way to export these from the Google password saver.

On the other hand, if you're looking for a solution that works in a company environment, we also offer [Devolutions Server](#) (DVLS) that features more functionalities and integration, **including AD integration**. DVLS lets you share passwords and information between end users using the database of your choice. You can always request a free 30-day trial [here](#).

Need More Help?

If you're interested in learning more about how we can help you close the password management gap on your team or in your organization, you can email our inside sales group at [sales@devolutions.net](#). They'll help you understand your options and they can also put together a custom proposal based on your objectives and budget.