OUCH! March 2026

Stop Password Pain: Use a Reliable Password Manager

A Cautionary Tale

Emily prided herself on simplifying her online, digital life with the belief, “one password to rule them all.” She kept things simple by using one password for all her shopping sites, a different password for her social media accounts, and one “special” password for anything related to financial accounts.

One morning, she woke up to a string of emails: a huge number of purchases were made in her name using her credit card, across numerous shopping sites. It turned out that the amazing deal she purchased online yesterday wasn’t a deal at all, but a fake shopping website designed to steal her information, including the login and password she created. Unfortunately, it was the very same login credentials she used for all of her other shopping sites, which the cyber attacker was taking advantage of. The attacker logged in as Emily and made numerous purchases across multiple websites she had used, all billed to her. It took days to recover, and even then, not everything was restored.

Emily’s story is common, but avoidable. We all know passwords are important, but trying to create, manage, and remember all the different passwords for all of our different online accounts is almost impossible. In addition, it seems every website has different password rules. Wouldn’t it be great if there was a single solution that took care of all your password problems? There is: password managers.

Password Managers Simplify and Secure Your Digital Life

Password managers are software that stores all your passwords in a protected database, sometimes called a vault. The password manager encrypts the vault's contents and protects it with a primary password that only you know. When you need your passwords, such as when logging in to your online bank or email account, you simply type your primary password into your password manager to unlock the vault. The password manager, which integrates with your web browser, automatically retrieves the correct password and securely logs you into the website. This enables you to easily maintain a unique password for each of your accounts, keeping your digital life secure.

In addition, most password managers support synchronization across multiple devices. This means you can use the same password manager software on all your devices, and always have access to all your passwords. As a result, the only password you have to remember is the primary password to your password manager. It's vitally important that you remember your primary password to avoid getting locked out of your password manager, and it’s critical that you make this password long and unique. If your password manager supports multi-factor authentication, use that as well.

Choosing a Password Manager

When trying to find the one that's best for you, keep the following in mind:

- Use only well-known and trusted password managers. Be wary of products that have not been around for a long time or have little or no community feedback.
- Your password manager should be simple to use. If you find the password manager solution too complex, research a different one that better fits your needs.
- Your password manager should be compatible with and synchronize across all your devices.
- Make sure the vendor actively updates the password manager, and be sure you are always using the most recent version.
- Be very wary of password managers that let you recover your primary password or that allow their tech support organizations to change it for you.
- You may want to write down your primary password, store it in a sealed envelope, and secure the envelope in a protected location in case you forget the password or a loved one needs access. Many password managers also provide the ability to share passwords or even entire vaults with trusted family members.

Password Managers Not for You?

We understand that some people may find password managers overwhelming and too complicated to use. Yet how can you safely remember all of your unique passwords? One option is to write those passwords in a notebook. This is not an option for work, but can be an alternative to use at home for personal accounts. The key step is *securing* that notebook. If you or a loved one does use a notebook to write passwords down, be sure that the notebook is stored in a safe place that only you or trusted family members have access to.

Guest Editor

Dr. Yansi Keim is an Assistant Professor of Information Security and Digital Forensics at SUNY Albany. Her research is at the intersection of gamification, higher education, and workforce development. Her work bridges academia and industry through hands-on training, gamification, and real-world pen-testing and defense exercises. LinkedIn: http://linkedin.com/in/yansi-keim

Resources

How Cybercriminals Exploit Your Emotions: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/
How Cybercriminals Steal Your Passwords: https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords/
The Power of Passphrases: https://www.sans.org/newsletters/ouch/power-passphrase/

You can find more Ouch! On the following link: https://www.sans.org/newsletters/ouch