Click “Download PDF” above to activate the article’s links.

Password Managers, a 2024 update

LastPass & bitwarden

When I speak on “Safe Computing”, I typically ask the audience whether they use a password manager. About two-thirds respond that they do. So, about one in three still rely on memory or a printed list. If you can remember a password, a hacker can figure it out, and lists can fall into the wrong hands.

Hackers may discover your password by compromising a system in which that password is used. They may discover your password by trial-and-error, using information they uncover about you, like your child’s name, your birthday month, or favorite color. If you reuse the same password, or variations of it, once a hacker discovers it on one site, all other sites where you use it are not at risk.

Steps that you can take to reduce the risk include (1) using a different password for each site that you visit, (2) strong passwords, and (3) multifactor authentication. In the age of artificial intelligence and superfast computing, you are more at risk than ever. So, wherever you can do so, use all three of these techniques to best protect yourself.

As there is no way any of us can remember dozens of strong passwords, we need a password manager to remember them. Password managers can typically enter your ID and password when you are logging in, create strong passwords on request, warn you of weak or potentially compromised passwords, and automatically record passwords that you create or update.

Browsers, like Chrome and Firefox, offer password management. You see this when you are asked by your browser whether you would like it to remember your password. I do not recommend browser-based password management as passwords stored directly in your browser are more easily hacked than those stored in the cloud. See Dangers of saving passwords in your browser.

Many password managers offer a free version along with fee-based versions including additional features. About ten years ago, after evaluating various password managers, I selected LastPass. I found that the free version was easy to use, rich in functionality, and did not constantly dun me to upgrade to a paid version. Recently, LastPass has experienced several breaches, the most serious one in August 2022.

Articles, like this one in Forbes, and LastPass’s own blog, sufficiently concerned me so that I decided that I would no longer use it. After evaluating several free alternatives, I recently switched to Bitwarden, which PC Magazine rates as the “Best Overall” free password manager. Here are links to PC Magazine’s current “best-rated” free and fee-based password managers.

Bitwarden has some catching up to fully compare with LastPass. For example, LastPass recognizes when a new password has been created or an existing one updated. Bitwarden does not and so such updates must be manually entered. I expect that Bitwarden will add this important feature as it matures. Review the best-rated password managers and select one that works for you. Don’t delay until you are hacked.

Bro. Hal Bookbinder

Bro. Bookbinder is a retired Information technology director and university instructor. This is the 98th article in this series. All articles can be accessed at https://tinyurl.com/SafeComputingArticles.