January 2022

BWN COMPUTER
Repair/Service/Upgrade
940-282-0290

NEWSLETTER

The Unexpected Benefits of Password Managers

The main advantage of a password manager is obvious to anyone with more than one account online (i.e. everyone). Instead of remembering all 100 usernames and passwords, the password manager autofills them. It's a boon. But it's not the only reason to use a password manager. This article shares several more unexpected benefits.

Password manager programs generate, manage, and store many different passwords. You may be concerned about whether a password manager is safe to use. But the cybersecurity industry consensus is "yes, it is."

A password manager uses top-notch encryption to protect passwords. Plus, they take a zero-knowledge approach. They can't see the passwords they store and prefill on sites. The password is encrypted before it reaches the manager's server and can't be deciphered. Therefore, you need to be careful not to forget your master password!

That said, the password manager offers more than a vault for encrypted credentials.

More Benefits of Password Managers

For one thing, many password managers have apps for download onto mobile devices. Then, you can use the password manager to prefill forms on those, too. This gives you the advantage of convenience not only on your desktop computer but also on the go.

Some password managers offer added security benefits, as well. They might:

- warn you of weak password and login credentials;
- remind you to change your passwords;
- notify you if your passwords may have been compromised in a breach;
- advise you against repeating access credentials if you're about to do so.

Another advantage is that you can conveniently share passwords with others. Maybe you want to give family members shared access to streaming accounts or allow a work colleague access to applications you're using remotely. A managed password sharing feature can allow them to see selected passwords. You aren't showing everything: you can pick what you make available. Plus, when you change your credentials, the password will change on their end, too. This doesn't need to be permanent either. You can easily revoke password sharing.

You can also use a password manager to secure other important information. You might store things such as credit card numbers or other personal identifying information. Keeping that kind of data in an unencrypted note on your desktop or mobile device is unsafe, but you can take advantage of password manager encryption to safely store those precious details.

Secure your passwords with a manager

You can't expect to remember all your unique passwords. Yet the days of writing down passwords on Post-it notes are over. Use cloud-based password management to secure your passwords and do more.

Contact our IT experts today to find out more about password management. We are happy to suggest the best solution for your needs and set it up, too.

Call us now at 940-282-0290.

3 Reasons to Avoid Signing in with Facebook or Google Accounts

Nine out of ten times today when you visit a website, you're asked to sign in. To add convenience, many sites offer the ability to sign in using a Facebook or Google account. Sure, it's simpler, but this article will share three key reasons why you might want to avoid this easy route.

It's estimated that we each have an average of 100 passwords. That's a lot to remember, especially as we need unique logins for every site to lower our risk of cyberattack.

At the same time, every website wants us to set up an account. It helps them get to know their users. This can help them to target marketing and product development efforts. They might also share the information with third parties as another source of income.

Still, the website wants to keep its users coming back, so they allow you to sign in with Google or Facebook accounts to streamline the process. Weigh the value of that added convenience against these three considerations.

#1 You're giving away more data

By using Google or Facebook to sign in on other websites, you are giving the sites greater access to information about you. Now, they not only know what you do on their sites, but you're also allowing them to build out their picture of you with data insights from the shared sites.

Google and Facebook have powerful tools to dig deeper into your online activity, and other websites can also extract data from your Facebook and Google accounts. If you don't read the privacy policies, you may not know what sensitive data the platforms share.

#2 You could lose access

You may join those who are deciding to quit Facebook or leave Google in favor of another platform. If you do so, and you have used that account to access other sites, you'll have to create new logins.

Even if you're not ever going to do away with your Facebook or Google account, you could still lose access. If there's a major outage at one of those two sites, you won't be able to log in at any of your connected sites either. The other websites won't be able to authenticate you until Facebook or Google is back up and running.

#3 Your attack surface gets bigger

If you have one, unique login credential for a website, you risk your data there only if that site gets hacked. However, if you use Facebook or Google login, and bad actors compromise that account, they can access any shared sites.

Think of it like dominos. The Facebook or Google account is the first to fall, but all those other accounts you "conveniently" login to using those credentials will come tumbling down soon after. Don't think the attacker won't bother looking for other connected accounts. All they must do, once they breach one account, is go into your settings to see what you have connected.

Social media accounts are also a prime target. Don't believe us? Bet you've seen a post from a Facebook friend (or ten) telling you to ignore strange activity due to a hacked account.

Protect your online identity

Account compromise is a top cause of data breaches worldwide. Protect your online identity by following best practices for cyber hygiene.

Need help with password security? Our IT experts can set you up with a password manager or provide other online security help. Contact us today at 940-282-0290.