October 30, 2019

Should You Use Facebook to Log In to Other Sites When Offered?

Using large services like Facebook to provide authentication is definitely a trend. It's not just Facebook: you can use your account with Google, Twitter, or some other accounts to log in at all sorts of random and unrelated services.

The reasons vary, but the most important is simply basic security.

- The third-party service does not get your Facebook login ID or password.
- Facebook does get information about each third-party service where you use your Facebook login.
- Using the same account everywhere is less secure than using same password everywhere (which you *also* should not do).
- Using a unique login ID and password for each service is *much* more secure.
- However, if you must use it, make sure your Facebook account is secured.

You can log in traditionally by creating your own account, or you can choose from one of the other authentication providers, like Facebook.

In some rare cases, it's not an option. The third-party service has elected not to provide its own sign in and relies entirely on using Facebook or other platforms to authenticate its users.

These third-party services want to make it as easy as possible for you to sign up with them. Not making you create yet another account and password to manage is one way they do so.

Be mindful that these other services may get your ID (your email address, in the case of a Facebook login), but they do *not* get your password.

This practice uses an industry standard protocol called OAuth, short for Open Authorization. You authenticate directly with Facebook, who then tells the third-party service that yes, you are who say you are, by virtue of having successfully logged in to your Facebook account.

They may ask for additional information from your Facebook profile, such as contacts, or permission to post to Facebook on your behalf, or more.

When this happens, you'll be notified exactly what additional permissions and information you're allowing to be shared when you set up that login with the third-party service, and you'll be given the opportunity to either alter the permissions given or abort the login completely. Be sure to read these carefully so as not to give more access than you're comfortable with.

Unfortunately, you can't pick-and-choose which permissions to give — it's all-or-nothing — and one big reason to avoid Facebook based logins.

When you do log in to these third-party services, you're telling Facebook which third-party services you use. Giving Facebook even more seems a little counter-intuitive.

Facebook Hacked? What You Need to Do NOW.

Same password everywhere is bad enough

Security experts and tech writers frequently advise against using the same password everywhere. If one account gets hacked and your password is exposed, then all your other accounts that use the same password are at much greater risk of getting hacked as well.

By using Facebook for authentication, you're using the same *account* to sign in everywhere.

If your Facebook account is ever compromised, then every other account where you use Facebook for login is immediately compromised as well. Someone with access to your Facebook account can quickly and easily determine exactly which other accounts you have[1] and access them.

Separate accounts, each with a unique login ID and password for each online service, are more secure and strongly recommend.

This limits the exposure of any one of them getting hacked to only that single service. It also removes the possibility of accidentally allowing them access to your Facebook account information for other purposes.

Yes, that means unique passwords for every site. The best way to manage that is to use a password manager which allows you not only to manage them all without needing to remember them, but enables you to use long, complex, safe passwords for each account.

If the appeal of using your Facebook login everywhere possible is just too compelling, then secure your Facebook account as much as you can. At a minimum, that means long and strong passwords, as well as adding two-factor authentication.

Social Security Account Holders….. BEWARE!

I received an odd, unfamiliar number phone call with a voice message stating "Your Social Security Number has been compromised. You need to call this number and press '1' to talk to an operator for your account to be 'unfrozen".

This is an obvious scam but to be sure I accessed my account to check notifications and to verify what, if any misdeeds had been a victim.

Like the IRS, the Social Security Administration will NEVER call you first. You will be sent a letter with all the official seals and signatures, case number and explanation for the inquiry. There will likely be a number for you to call and possibly the extension for a case agent if there are questions needed to resolve the issue.