The Freelancer's Guide to Cybersecurity Podcast Episode 9: Manage Those Passwords!

Episode released 12/02/2020

Transcript

Today on the podcast, I'm going to discuss passwords, a really essential part of cybersecurity for any professional or individual account, and how to manage them effectively.

Passwords form the first line of cybersecurity in most situations, and by now most users know to make their passwords unique, long, and a mixture of lowercase and uppercase letters, numbers, and special characters when possible—although there is a growing school of thought that passphrases are just as good. I'm not sure I agree with that theory if the passphrase uses a string of words found in the dictionary, since those are the easiest passwords to hack. Most users also know to keep their passwords secret. Given all of these best practices, using a password manager—essentially keeping all of your secret keys stored in one place, maybe even online—seems counterintuitive. So today I am going to make the case for why you should use a password manager.

The world of password managers comprises myriad options: free versus paid, locally stored—meaning store on your computer—versus stored online, freestanding versus integrated into another program (like your browser). The whole concept of putting your passwords into a password manager runs counter to the "don't put all of your eggs in one basket" adage that serves so well in most situations.

No doubt, you should fully research password managers before selecting one, as they are not uniformly secure. The non-profit internet privacy group The Mozilla Foundation suggests that users should only consider a password manager that:

- Doesn't know your master password (so hackers can never steal it)
- Only stores encrypted versions of your credentials—meaning your username and password combinations—and data on their servers
- Can generate strong, secure passwords

As a quick aside, when researching password managers, you will find that some have an additional selling point: they will store your credit card information to facilitate online purchases, which I think is a bad idea. The fewer places your credit card information is stored, the better. I would suggest using PayPal if you would like an easy and secure way to pay for your online retail therapy.

So do your research to find which password manager fits your budget and your needs. But don’t forget the main point here. In many ways, the strongest argument for using a password manager is that not doing so usually leads users to violate the basic concepts behind strong passwords, because strong passwords are hard to remember. Eight-character combinations of letters (upper- and lower-case), numbers, and special characters don't stick unless they are either really easy to guess, which is not secure, or they’re posted with a sticky note to your monitor—which is also obviously not a secure or convenient option if you travel.

For those still concerned about using a password manager (and I admit I was slow to adopt its use and still keep mine on a very tight leash), for those people I offer an additional thought. With the wide adoption of multi-factor authentication, the password maintains its stature as the first line of security for accounts, but now it has solid backup. Whether by SMS text, a physical key, or an authentication app, multi-factor authentication adds a formidable second line of security. Of course, 2FA security can have its limits for high-profile targets—so choose your second form of authentication based on your specific situation and needs.