THE COMPUTER CORNER

No. 175: IF YOU THINK PASSWORDS ARE PROTECTING YOU, THINK AGAIN

Stan Kaplan, WB9RQR
715 N. Dries Street, Saukville, WI 53080-1664 (262) 268-1949 skaplan@mcw.edu

This is a guest article, written by the guys at majorgeeks.com, the best site in the world for safe software. Printed with permission of the authors. Happy computing!

Passwords as a defensive measure are complete rubbish. There's no two ways about that. The fact that high-value services such as online banking, corporate email and data storage use simple passwords as the only real security mechanism is a sad commentary on the state of defensive technologies. But, as the continued parade of password leaks of late proves on a daily basis, users who believe these companies are protecting their passwords are sadly mistaken.

The companies that provide these online services, such as email, cloud storage, online banking and others, would really rather not store your passwords, truth be told. As we've seen, it's just one more piece of data that they need to protect and can potentially lose. The business models at banks, retailers and social networks do not include acting as secure storage facilities user passwords. If there was some way for these services to exist without having to deal with user passwords, they would have found it.

But no one has yet, and there doesn't seem to be a good solution to the problem on the horizon. Passwords were a terrible idea at the beginning, they're still terrible now and they'll continue to be terrible in the future.

That's not going to change. What could change is the way that users think about their passwords and handle them. At this point, users need to consider that any password they create for a given site is going to be compromised. It may not happen, but if you go into the transaction thinking that somewhere down the line this combination of letters and numbers will be in the hands of someone other than you, then you can start to think about passwords in a different way.

Think of them as disposable tokens that you need to present to the site in question. With that in mind, you should change your passwords as often as you can. Many Web sites will never require you to change a password once it's set, so this is something that you'll need to do on your own.

Of course, the passwords you choose should be complex and not easily guessable. There are a number of random password generators you can use for this, including Random.org. You pick the parameters and it generates the password for you. Also, password managers and secure password generation apps such as LastPass and 1Password can be nice additions and remove some of the burden of remembering passwords.

But, if you need to make sure that you can remember the password, you have a new problem. If you're dealing with passwords for personal use at home, it's not a bad idea to write them down. The odds of someone breaking into your house and stealing your passwords and then using them online is negligible. If you're worried that someone else in your house will misuse them, you probably have bigger problems.

So, once you've done all that, followed all of the guidelines and logged into your favorite sites and gone about your online business, you have ceded all control of the security of your account to the site and its security policies. And you're right back where you started. You can do everything right, take all of the precautions possible and be diligent about your own personal security and still end up with your password sitting on Pastebin.