SPECIAL REPORT: Protecting information online from hackers

Author: Lindsey Berning, Reporter
Published On: Jul 06 2015 09:45:31 PM CDT
Updated On: Jul 06 2015 10:34:04 PM CDT
IT experts share the best practices to increase the security of your passwords.

COLUMBIA, Mo. - In an age where passwords are needed for nearly everything, it can be tricky keeping track of them all.

Experts recommend using password managers, but are they really safe?

Last month, LastPass, one of the the most common online password managers, announced it was hacked. The hackers took account email addresses, master passwords, password reminders and more.

But IT experts Abc 17 News talked to said password managers are still one of the best ways to go and said users should not worry.

"According to all the reports, everyone who has an account with them should still be safe," Marcus Files with Nate's Computer repair said. "The form of encryption they use on the passwords that these hackers essentially stole, said they would take a great deal of time to break through. So nobody needs to be too concerned about losing their information. But they should change their master password because that's what's actually at risk now."

With LastPass, users have one master password to get into their account which stores passwords for every other login the user has. Users can enter their own passwords, or the site can generate a random complex one for you. All passwords are stored in an encrypted, or coded, form.

Prasad Calyam, an assistant professor for the University of Missouri Computer Science Department, said between work accounts and his personal life, he has hundreds of passwords.

"The scale of the work is in hundreds," Calyam said. "But definitely in terms of my personal life it's a few tens I would say."

Calyam said although they are necessary, passwords make you vulnerable.

"Unfortunately, if you ask any cyber security researcher, passwords are the worst thing that ever happened in how we access systems and applications and how we communicate with people with data and things like that," Calyam said. "But that's what we have today."

IT experts said the three top things you can do to protect your information online are: create a strong complex password, use two-factor authentication and change your master password often.

To create a strong password:

"It's all in the length of your password," Calyam said. "The longer it is and the more complex it is, in terms of lowercase, uppercase, special characters and you see this all the time when you're setting passwords, the more secure it is."

Use a combination of lowercase letters, uppercase letters, numbers and symbols. Calyam said your passwords should be eight to 12 characters, the longer the better. Do not use key combinations on the keyboard, for example "QWERTY" or "12345".
Two-factor authentication:

Those security questions you’re asked is among the strongest measures out there.

"That ensures that they’re sending the code to the right person, and it's actually you logging in," Files said. "And that’s probably the safest way that's out there right now to ensure that your accounts aren’t being hacked into."

Two factor methods can also be text messages or biometrics like a thumbprint scan.

Change master password often:

"Essentially there's not much you can do to prevent, to make a site 100 percent non-hackable," Files said. "Companies always create new kind of encryption methods, new kinds of security precautions, but there always seems to be someone out there that’s just a bit smarter or a bit more capable of getting into them. So the best practice is that they ensure their users are updating their passwords."

Files recommended changing your password every three to six months. He said you should definitely change it more than once a year.

After the hack, LastPass prompted all users to update their master passwords and required all users logging in from a new device to verify their account through email. LastPass said it is also working with the authorities and security forensic experts to investigate the hack.

Both Files and Calyam said even though password managers are hackable, they are still safer than storing your passwords on your personal computer, writing them down or just storing a few in your head.

Copyright © 2015 KMIZ - The Networks of Mid-Missouri. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Comments

The views expressed are not those of this company or its affiliated companies. Please note by clicking on "Post" you acknowledge that you have read the Terms Of Service and the comment you are posting is in compliance with such terms.