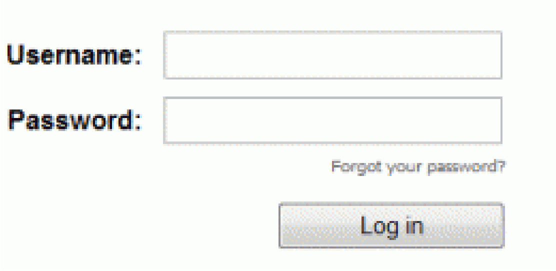
PHYS.ORG

Protecting our passwords, and our sanity

November 12 2013, by Katie Humphrey



Credit: Wikipedia.

Start counting. How many passwords do you have?

Rajean Moone of Minneapolis has so many - more than 75 - that he tracks most of them on a super-secret spreadsheet. Others he scribbles on hidden Post-It notes - coded in a foreign language.

"It's getting kind of ridiculous," he said.

As our lives have become digitized, the number of passwords we juggle has exploded.

There's e-mail, online banking, Facebook, Amazon, even the library.

At the same time, keeping passwords secret from increasingly sophisticated cybercriminals requires ever more complex requirements.

Yet a foolproof system to manage dozens of passwords (which should be a combination of letters, numbers and symbols) remains elusive, even as tech companies tease with gizmos like the fingerprint scanner on the new iPhone 5S.

In a fit of frustration, many of us default to easy passwords that we repeat across multiple websites - a practice that practically begs hackers to breach our penetrable defenses. While the average person isn't often the target of an all-out attack by cybercriminals, many of us become vulnerable when the sites holding our passwords are compromised. If that stolen password is the key to everything important in our lives - identity, finances, personal information - then we're in trouble.

"A little bit of prudence goes a long way," said Joseph Konstan, a computer science professor at the University of Minnesota.

Yet even Konstan admits the best practice - such as using a different complex password for every site - is tough to follow.

He heeds that suggestion for his most important info, say financial and e-mail accounts. But he uses repeated passwords for sites that seem to require passwords just so they know who you are, including basic apps or free news websites. If it's a site Konstan rarely uses, he simply forgets and resets the password the next time he visits.

"We have managed to engineer a password system that is extremely taxing on people," he said.

One of the biggest sticking points: Each site has its own rules for password length and complexity. Some let users opt for two-factor authentication - a combination of something you know and something you possess. For instance, Gmail's optional two-step security calls for a password and then a code sent to the user's smartphone. Twitter enabled a similar system this spring after prominent news organizations were hacked. A false tweet about bombs at the White House, sent through the Associated Press' compromised account, sent the stock market plummeting.

The dizzying list of security features can cause headaches for users. Password has almost become a curse word.

"It used to just be that you could use a word. Then you could have a combination of words and numbers. Now it's like you have to have words, numbers and some sort of symbol," said Angela Mattson of Mendota Heights, Minn., who keeps an assortment of passwords written down in different places. "It gets a little confusing."

Then there are security questions, odd personal trivia that can make you doubt your self-knowledge as you attempt to prove your identity. What was your first teacher's name? What street did you live on in fourth grade? What was your maternal grandmother's maiden name?

Experts say it's best to give a false answer when setting up security questions. Even if grandma's maiden name was Johnson, you should say it was Williams. That way intruders can't crack the questions through research, as a college student did when he hacked Sarah Palin's e-mail in 2008 by correctly answering questions about her birthdate and family. But good luck remembering those false answers.

Michelle Brooks of Fridley, Minn., was stumped recently when an attempt to reset a password led to this question: What was your childhood nickname?

"Not only did I not remember having a childhood nickname, if I had answered it (at some point), I couldn't remember what I answered," she said.

Frustration with a folder stuffed full of written passwords prompted David Bergum to look for a better system. It was a particularly thorny problem because he divides his time between the northern Minnesota town of Isabella, North Carolina and New Zealand.

"I got sick of all the pieces of paper," he said. "Especially traveling around, if I forget that folder down here and go Up North, I'm dead."

He settled on 1Password, software that generates and remembers complex passwords along with user names for different sites. Now he only has to remember the master password to access 1Password via his Web browser or iPhone.

There are a variety of such apps, including LastPass, Roboform and KeePass, that all work a little differently but promise security through encryption. Some are free; others offer more features, such as synchronization across different devices, for a price. Experts say they can be a nice alternative for people who want to keep track of multiple passwords without writing them down.

Katie Leyman, of Edina, Minn., uses LastPass to track passwords, but isn't sure she wants to surrender all her secrets to the technology. She stores most of her passwords in LastPass, but commits her passwords for e-mail and financial sites to memory.

"If your whole life is in there, you can't get it back if you don't remember what (the master password) is," she said. "There was one moment I thought I forgot it. I was sitting there going, 'Omigod, I can't get to anything that I need.'"

The line between security and usability is a fine one.

Derek Meister, a Geek Squad agent, said it's important not to make security so complex that people get overwhelmed and default to insecure habits, like repeating simple passwords. He suggests thinking about digital security much like home security. It's not perfect, but it can be a deterrent to those aiming to make trouble.

"You're not looking to make your house into Fort Knox. You're looking to make your house hard enough to get into that somebody will say, 'I'm going to go elsewhere,'" Meister said. "It's the same with passwords."

—-

TIPS FOR SECURING YOUR MANY ONLINE PASSWORDS

In the ongoing struggle with online security, experts offer these tips to generate and manage passwords that will keep your information safe.

Mix it up. Ideally, every password is different. Realistically, there are a lot of repeats out there. At minimum, make sure your passwords to critical sites - especially financial information and e-mail, which is a gateway to so much more - are unique and tough to crack.

Words to the wise. Some hackers will try every word in the dictionary, so make sure your password is complex. If whole words are all you can remember, try pairs or groups of completely unrelated words for better security.

Think in phrases. Remembering a random combination of letters, numbers and symbols gets easier if they're related. Pick a phrase that's special to you but not widely known and adapt it. For example, "Thanksgiving dinner includes turkey, sweet potatoes, green beans and three pies" might become "Tdit(ASTERISK)sp(ASTERISK)b&3P."

Consider an app. There are multiple smartphone apps that remember passwords for you, including LastPass, 1Password, Dashlane, oneSafe and KeePass, which is an open source tool. While some are free, many require annual subscriptions to use all their features. Read the details and make sure they encrypt information. Even then, experts say, you may want to remember a few critical passwords (e-mail, financial sites, etc.) so that you're not stashing all your secrets in one place.

Just forget. Sometimes, especially for sites you seldom use, it's easier to reset the password on each visit. It might take an extra step or two, but that might be more secure than re-using passwords or writing them down somewhere unsecure.

—-

See your password here? It's probably time to change it

KEYS TO A BETTER PASSWORD

A lot of smart people use very dumb passwords. Then they repeat them over and over. Among the worst offenders:

- Password. The word itself is still one of the most common examples.

- Sequential or repeated numbers. Using 111111 and 123456 is just lazy.

- Names of pets, kids and family members are no-nos.

- Birthdates and hometowns. Hardly a secret.

- Clever but unoriginal, a la "letmein" and "trustno1."

- Favorite animals, sports, cars and colors. Try again.

Citation: Protecting our passwords, and our sanity (2013, November 12) retrieved 19 April 2024 from https://phys.org/news/2013-11-passwords-sanity.html