6 TIPS TO CREATE PASSWORDS THAT ARE HARD TO CRACK

Getty Images

Matt Alderton, NowU
JANUARY 12, 2015

★★★★★ (5.00 / 5)
1 Votes

Like 0

🖨 👤 ↪ 💬 💬 ➕
4 MIN READ

Password Protected: How Safe Are You?

This is the first of two articles from NowU on creating and managing passwords.

Like a lot of people her age, 56-year-old Robin Caldwell can't always remember where she left her phone, or what she meant to get at the grocery store. People, places and things from 50 years ago, however, are crystal clear, as if they happened yesterday.

Those things, she ventures, she'll never forget, which is why she always uses them as Internet passwords.

"All of my passwords are some combination of the first things I had to remember as a child," said Caldwell, a St. Louis-based PR consultant, who typically combines a name — the name of her childhood playground, for instance — with a number, like the address of her childhood home. "Why? Because long-term memory improves with age while short-term memory diminishes."

The challenge of remembering passwords could explain the results of a 2012 study by social software services company Janrain: Thirty-eight percent of people, it found, would rather clean a toilet than come up with a new password.

> If you make your passwords a little harder to crack, you're going to be better protected.
>
> *Luke Klink, security strategy consultant*

No matter how much you hate changing your passwords, however, the specter of identity theft means it's critically important to do so, according to Luke Klink, security strategy consultant at Rook Security, an Indianapolis-based provider of IT security solutions.

"If you are connected to the Internet in any way, shape or form, you are a potential target for malicious actors," said Klink, who recommends changing your passwords once every six months in order to stay ahead of identity thieves.

Last year alone, those thieves victimized 13.1 million people, an increase of 500,000 from the year before, according to Javelin Strategy & Research.

"The good news is, if you make your passwords a little harder to crack, you're going to be better protected," Klink said.

To create a strong password — one that's easy to remember but hard to guess — follow these guidelines:

1. Avoid the Obvious

Nearly a third of online Americans (29 percent) use the names of pets, spouses and friends to formulate passwords, according to identity-theft protection company LifeLock. Although they're easy to remember, such passwords also are easier to hack.

Typically, information about your pets, spouse and friends — not to mention your alma mater, hobbies and interests — is readily available by searching public records or social media.

"A bad password is anything that somebody knows about you or can guess about you," Klink said. "I'm a Colts fan, for example; if my password were Colts123, that would be pretty easy to guess."

Even if they're seemingly random, simple passwords are just as weak as personal ones.

"Hackers can do what's called a 'dictionary attack,' which is an attack that uses software to enter all known words out of the dictionary into a password," explained Robert Siciliano, an online security expert for IT security company McAfee. "'Princess,' for example, is a weak password because it's a word out of the dictionary."

2. Go Long

When it comes to passwords, size matters, according to Klink. "The longer a password is, the longer it will take a password-cracking tool to crack it," he said.

Some websites may limit the length of your passwords. Generally, however, passwords should have at least eight characters, according to Siciliano, who said 10 characters are even better and 12 ideal.

3. Mix It Up

The strongest passwords aren't just long; they're also complex, including a mix of letters, numbers and symbols.

"Even if it's not in the dictionary — it's a gibberish word that you created — you still want to use a combination of upper- and lowercase letters, numbers and special characters like question marks and apostrophes," said Rob DiNuzzo, marketing manager for password management tool RoboForm.

4. Turn a Phrase

A word is weak. A sentence, however, is strong — especially if it follows the aforementioned recommendations about length and complexity.

For instance: Iam:)2b29! "This has 10 characters and says, 'I am happy to be 29!,'" Siciliano said.

Or: My_d0g'$_name_i$_Bernie! "If you use underscores and replace every 's' with a dollar sign and every 'o' with a zero — and you follow that same algorithm for every password you create — it will be easy to remember but very hard to crack," Klink said.

5. Picture It

A meaningful shape can be just as effective as a memorable phrase. For example: %tgbHU8. "Follow that on the keyboard. It's a 'v,'" Siciliano said. "Use 'w' if you are feeling all crazy."

6. Test Your Strength

Whether your password is a word, sentence or shape, the final step is using a free password analyzer to test its strength.

Try How Secure Is My Password? or The Password Meter. According to the former, it would take a desktop PC 2 nonillion years to crack Klink's "My dog's name is Bernie" password.

"Nobody likes passwords, but it's really important to think about creating stronger ones," Klink said. "If you don't, and malicious actors get ahold of your data, they could really do some damage."

Coming soon: How to organize and manage your passwords.

💬 ➕ **4** MIN READ

💬 ➕ **4** MIN READ

💬 ➕ **4** MIN READ

💬 ➕ **4** MIN READ

NEW DVD REVEALS PRINCE 'IN HIS OWN WORDS'

HOME COOKING 101: SECRETS OF INDIAN CUISINE

MORE TO LOVE FROM 'DOWNTON ABBEY'

NETWORKS COOK UP NEW SHOWS FILLED WITH FOOD AND FLAVOR

NEW CAMPAIGN URG DRONE SAFETY AHE OF HOLIDAYS