The Worst Passwords of 2020: **How to Avoid Becoming the Next Cyber Crime Victim**

EBOOK

CALIAN®

If there is one thing people around the world have been trained to do, it's to create highly secure passwords. In fact, the need for digital passwords of six characters including uppercase, lowercase, special characters, numbers and so on is commonplace on every platform today.

But just because society has been conditioned to create passwords in a specific manner, that doesn't mean we're doing it right. Just look at this year's most popular passwords:

1. 123456
2. 123456789
3. picture1
4. password
5. 12345678
6. 111111
7. 123123
8. 12345
9. 1234567890
10. senha
11. 1234567
12. qwerty
13. abc123
14. Million2
15. 000000
16. 1234
17. iloveyou
18. aaron431
19. password1
20. qqww1122

Of this list of dangerously predictable passwords, three of them (picture1, Million2, and aaron431) took three hours each to crack (Osborne, 2020).

One—qqww1122—took 52 minutes.

All others took less than a second.

EBOOK

CALIAN®

Easy to crack, easy to scam

When it's easy to guess or crack a password, it's easy to scam others. And you could be the next victim.

One of the more recent scams popping up is the "I have your password, now give me money" email.

Usually, it comes in the form of an old password prominently displayed on the subject line. When you open the email, you get the threat. Here's an excerpt from one of many emails currently in circulation:

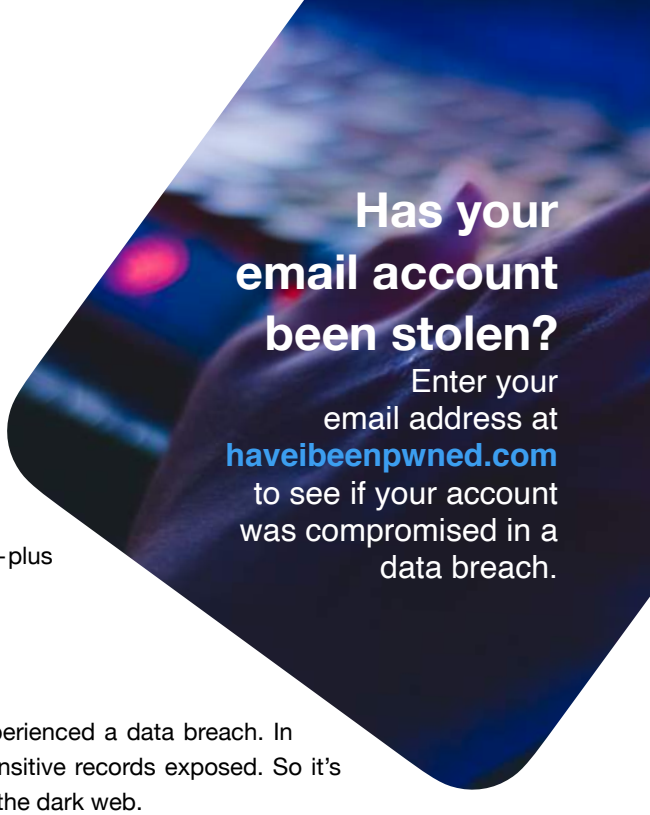
"I am well aware that [REDACTED] is your pass words. Lets get right to point. Neither anyone has paid me to investigate you. You may not know me and you are probably thinking why you're getting this e-mail?

I installed a software on the adult videos (pornographic material) web-site and do you know what, you visited this website to have fun (you know what i mean). While you were viewing videos, your web browser began working as a Remote Desktop that has a key-logger which gave me accessibility to your display and also cam. Just after that, my software gathered every one of your contacts from your Messenger, Facebook, as well as email. After that I created a double video. 1st part displayed the video you were viewing (you've got a nice taste haha), and next part shows the recording of your cam, yeah its you."

From here, the scammer usually asks for payment via Bitcoin to stop the circulation of the "video" content.

And the scam works—a lot of the time (Winder, 2020).

How would they know your username and password?



Despite the threatening language, you may initially be skeptical if you receive a threat like the one above.

But then, how could this person have gotten your contact information—plus they know your username and password?

There are several reasons.

First, it's possible you work for or are a client of a company that has experienced a data breach. In 2019, there were 1,473 data breaches in the US, with over 164 million sensitive records exposed. So it's not uncommon your email account may have been stolen and uploaded to the dark web.

Encryption options for different types of data

In a years-long study of more than **742 million passwords** that were revealed in numerous data breaches, Turkish researcher Ata Hakçil found that:

- The most popular password (123456) appeared more than 5.3 million times, or one out of 138 entries
- There were only 169 unique passwords—pointing out how often people use obvious passwords
- Only 12% of all passwords contained a special character, like punctuation

Of the top 100 worst passwords—and outside of number combinations—Hakçil also found certain word categories (Wagenseil, 2020):

- **Names:** ashley, michael, daniel, charlie, jessica, jordan, thomas, michelle, nicole, joshua, andrew, hunter and jennifer
- **Things:** dragon, princess, monkey, computer
- **Sports:** football, baseball, soccer
- **Trends:** pokemon, superman, starwars
- **Other words:** sunshine, lovely, master, killer, shadow, f***you

How to make your password hard to hack

Most websites require you to create the usual 6-to-8 digit password with the usual capitals, lowercase letters, numbers and symbols.

Using that formula, your password may come out to be something like PassW0rd01! But that's not really a secure password.

Here's why: hackers and the algorithms they use have been trained to know how to swap out the number zero for "O," "A" for "@" and so on. As such, the password above is plain text to the seasoned hacker.

Instead, aim for a password that is simple, but far longer than the usual eight digits.

As an example: let's say your favourite show is The Big Bang Theory. Making this your password could appear as ilovethebigbngtheory, with the "a" removed in the word "bang." In doing so, this not only makes the password longer than required but there is an additional level of complexity that is harder for hackers to crack (because of the nature of the sentence structure, the missing letter etc.).

Let's take it a step further. In instances where special characters can be represented by actual spaces, a simple yet highly secure password could be "I Love the Big Bng Theory Very Much." Again, no special characters are used other than spaces—but the length and mathematical complexity make it even more secure.

Ironically, making your password simple can actually make it harder to hack.

How secure is your password?

Go to **www.security.org/how-secure-is-my-password** and plug it in to check.

Use a password manager

In addition to changing your password, use a secure platform like LastPass, Dashlane, or Keeper.

Also known as password managers or password vaults, these types of platforms manage all your passwords in one place—usually with a primary password to access your account. They also help you create and remember your passwords, making sure none of them are repeated.

The benefit is that you can finally move away from using one password for all your cloud and other activities.

By randomizing all passwords—and adding length and even sometimes weird structures—along with enabling a password vault to secure them, this adds yet another layer of security to the mix.

Conclusion

Data breaches and scams are unfortunately here to stay, but you can help protect yourself by being more strategic about your passwords—and hopefully preventing a cyber criminal from using one exposed login to access your data elsewhere.

Meanwhile, don't let the scammers intimidate you. If you find yourself receiving any type of suspicious email, simply Google it—chances are you'll get confirmation that it's a scam almost immediately. And then, if you haven't done so already, change up your passwords using the tips above.

By creating new habits for today's digital age, your cyber resiliency will increase greatly—keeping the bad guys at bay.

References

Editorial Board. (2020, July 10). *Make time for password security.* Retrieved from https://www.post-gazette.com/opinion/editorials/2020/07/10/Password-protection-security-123456-privacy/stories/202007100005

Osborne, Charlie. (2020, November 18). *The worst passwords of 2020 show we are just as lazy about security as ever.* Retrieved from https://www.zdnet.com/article/the-worst-passwords-of-2020-show-we-are-as-lazy-about-security-as-ever/

Wagenseil, Paul. (2020, July 6). *These are the latest world's worst passwords—don't use any of them.* Retrieved from https://www.tomsguide.com/news/worst-passwords-2020

Winder, Davey. (2020, July 24). *Got An Email From A Hacker With Your Password? Do These 3 Things.* Retrieved from https://www.forbes.com/sites/daveywinder/2020/07/24/got-an-email-from-a-hacker-with-your-password-do-these-3-things-sextortion-scam-cybercrime-advice/?sh=1931de57160c