

Psychology of Passwords: The Online Behavior That's Putting You at Risk



As more and more people work, purchase, and socialize exclusively online, hackers are looking to take advantage and steal your personal information. We found that 3250 people from around the world¹ aren't protecting themselves from cyber security risks even though they know they should. Are you guilty of committing these risky behaviors too?

Top 6 Risky Behaviors Making You a Target

1

We use the same password over and over

If a hacker gets access to one account, they can wreak havoc on all of them!

91%

know that using the same or a variation of the same password is a risk; however,

66%

do it anyway!

2

We want to be in control

We think that reusing passwords gives us more control, but it really puts us at risk. When asked why they reuse passwords, respondents said:

60%

I am afraid of forgetting my login information

52%

I want to be in control and know all of my passwords

3

We still memorize our passwords

Can you memorize unique, strong passwords for all your accounts? Only if you're a superhero. If not, you shouldn't be relying on your memory to protect you online.

54%

keep track of passwords by memorizing them

Remembering isn't working:

25%

reset their passwords once a month or more because they forgot them

4

We ignore breaches

If a brand you use is breached, you should change your password.

52%

haven't changed their password in the last 12 months – even after hearing about a breach in the news

5

We underestimate our risk

I'm not a target, right? Wrong. While your credit card number might only get a hacker US \$5 on the dark web², if they steal hundreds of thousands of pieces of data in one fell swoop, it adds up.

41%

think their accounts aren't valuable enough to be worth a hacker's time

6

We are predictable

Personal information can be easily found by hackers on your social media accounts or by doing a quick internet search.

22%

could guess their significant other's password

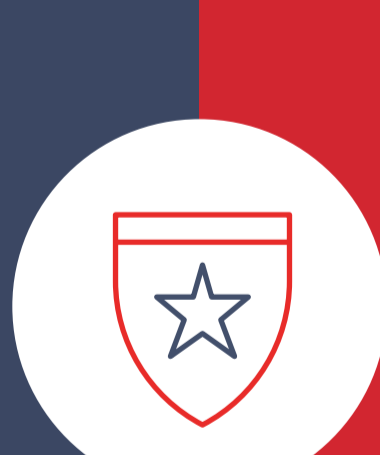
24%

use sentimental information in their passwords

Are we doing anything right?

We are using multifactor authentication!

54% use MFA for personal accounts



But only 37% use it for work accounts

We trust biometrics:

65%

said they trust fingerprint or facial recognition more than traditional text passwords



What is MFA?

Use MFA to add an extra layer of security. After you enter your username and password, MFA requires a second piece of information to login - like a one-time code or your fingerprint.

We are protecting our financial and email accounts more than others

69%

create stronger passwords for their financial accounts and 47% for email

62%

use multi-factor authentication on their financial accounts and 45% for email

¹ Survey respondents were from Australia, Brazil, Germany, United Kingdom, United States and Singapore.

Sources:
² <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/>