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 world 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

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:

- I want to be in control and know all of my passwords
- I am afraid of forgetting my login information

60% 52%

2. We don’t want to be in control

We use the same password with variations

If a hacker gets access to one account, they can wreak havoc on all of them! 91%

We know that using the same or a variation of the same password is a risk; however, do it anyway! 66%

3. We still remember our passwords

We use sentimental information in our passwords

Could guess their significant other’s password 22%

Use sentimental information in their passwords 62%

4. We ignore breaches

We don’t change our passwords in a breach

Don’t change your password in a breach? 52%

Don’t change your password in a breach even after hearing about a breach in the news 22%

5. We underestimate our risk

We think our accounts aren’t valuable enough

Think their accounts aren’t valuable to be worth a hacker’s time 41%

61%

6. We are predictable

Personal information can be easily found by hackers

Personal information can be easily found by hackers on your social media accounts or by doing a quick internet search. 24%

22%

7. We are not using multifactor authentication!

We are using multifactor authentication!

We are protecting our financial and email accounts more than others

We trust biometrics:

We are protecting our financial and email accounts more than others

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

65%

62%

69% 45% 47%

89% 62% 69%

91% 66% 89%