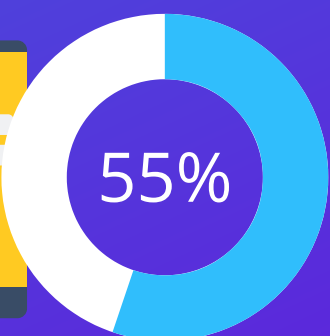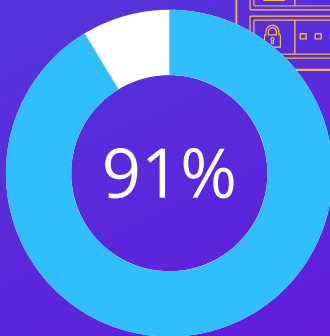# Online User Behavior
Perceptions vs Reality

Users are more worried about cybercrime statistics but fail to follow through with protecting their assets
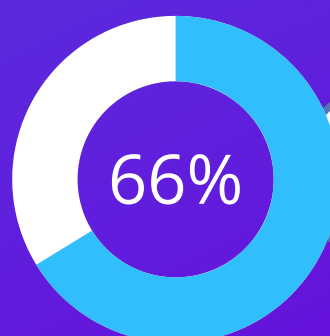
People aren't protecting themselves from cyber security risks even though they know they should.

55%

55% of people are worried about criminals accessing their data[1]

91%

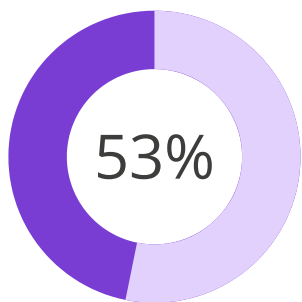91% say that they know using the same or a variation of the same password is risky[2]...

66%

...while 66% will always or mostly use the same password or a variation[2]

Sources:
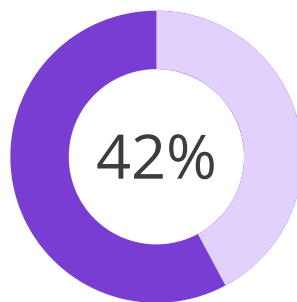[1]ENISA Threat Landscape Data Breach 2020
[2]LastPass Psychology of Passwords: The Online Behavior That's Putting You at Risk 2020

Password behavior

53%

In the last 12 months

53% of respondents haven't changed their password in the last 12 months even after hearing about a breach in the news

42%

Easy to remember

42% of respondents say that having a password that is easy to remember is more important than one that is very secure
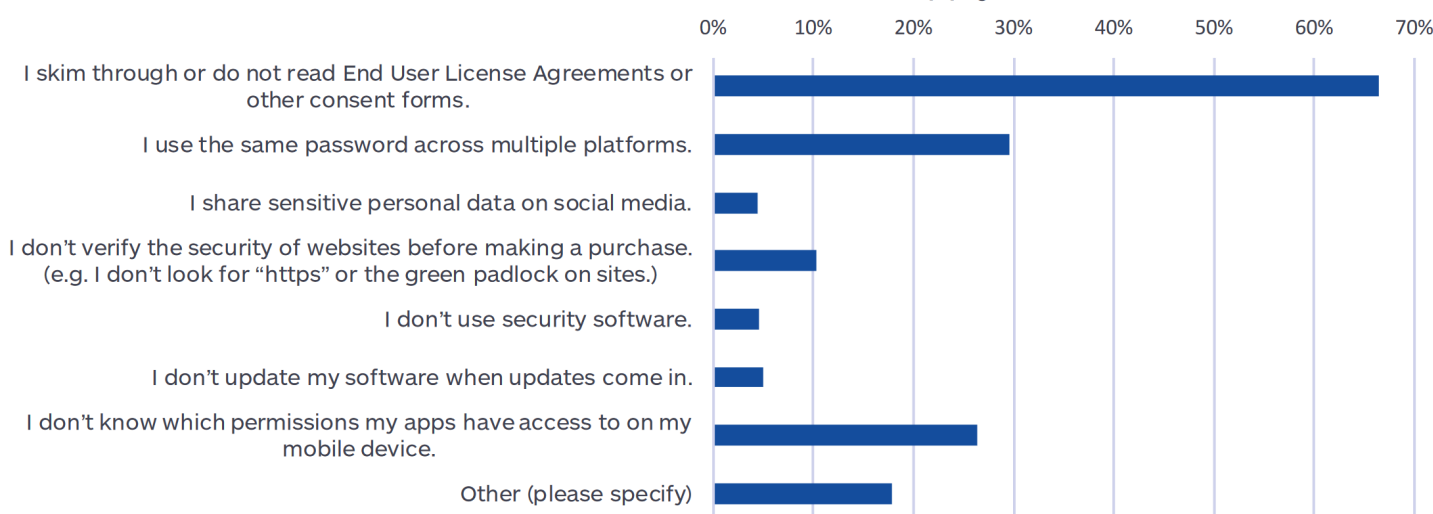
Source:
LastPass Psychology of Passwords: The Online Behavior That's Putting You at Risk 2020

SECURITY HUBRIS

Perceived confidence in privacy practices is higher than reality.

Because users follow many of the perceived-as-easier security tactics, they believe themselves safe, even while ignoring other important security measures that appear difficult.

What are some cybersecurity best practices that you do **not** follow? Please select all that apply.

	0%	10%	20%	30%	40%	50%	60%	70%
I skim through or do not read End User License Agreements or other consent forms.								
I use the same password across multiple platforms.								
I share sensitive personal data on social media.								
I don't verify the security of websites before making a purchase. (e.g. I don't look for "https" or the green padlock on sites.)								
I don't use security software.								
I don't update my software when updates come in.								
I don't know which permissions my apps have access to on my mobile device.								
Other (please specify)								

Source:
Malwarebytes Labs "The Blinding Effect of Security Hubris on Data Privacy 2019

"This kind of behavior is what criminals want users to do. It makes it easy to steal the credentials from one source and use them elsewhere. Using a password manager is a great solution for this problem"

Malwarebytes Labs "The Blinding Effect of Security Hubris on Data Privacy

Sources

300+ Terrifying Cybercrime and Cybersecurity Statistics (2021 EDITION) (www.comparitech.com)
ENISA Threat Landscape 2020 - Data Breach (www.enisa.europa.eu)
Psychology of Passwords: The Online Behavior That's Putting You At Risk 2020 (www.lastpass.com)
The Blinding Effect of Security Hubris on Data Privacy 2019 (www.malwarebytes.com)