SECUREAUTH

2020 STATE OF IDENTITY REPORT

CREDENTIAL CARELESSNESS

SECUREAUTH CONDUCTED the research using an online survey among 2,000 general population consumers in the U.S. Data was collected between March 16 and March 21, 2020. With nearly 50% of survey respondents currently in the U.S. workforce, the survey provides an objective data set with respect to the security and privacy habits consumers apply in both their personal and professional lives.

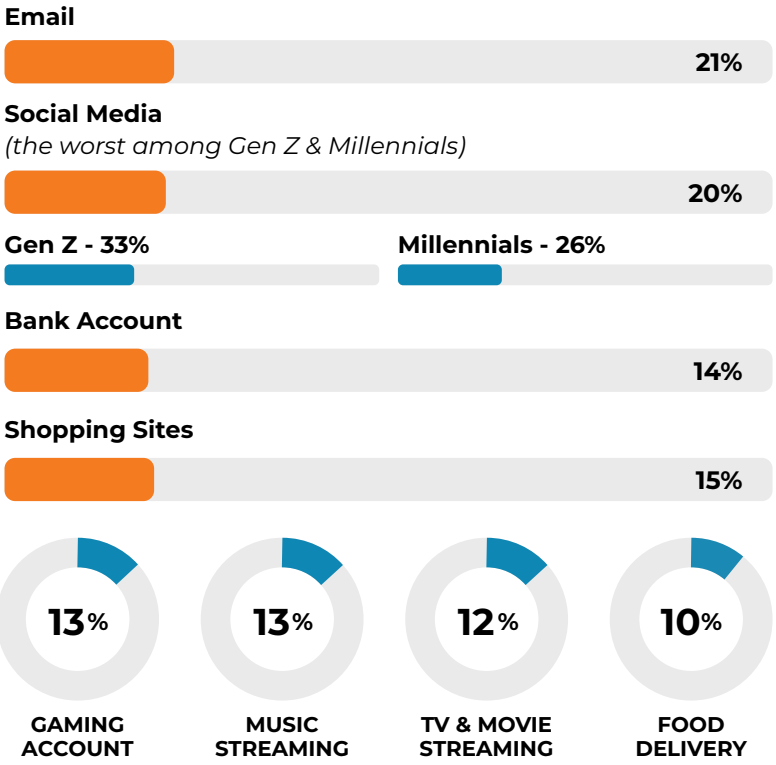
SECUREAUTH

No matter how much cyber experts preach, bad password habits are always going to be a large problem for our personal and work lives

Among those who are using the same password for more than one account, most are using it across 3-7 accounts (62%) --- and 10% say they are using the same password across 10+ accounts.

The blurred lines between work and personal passwords

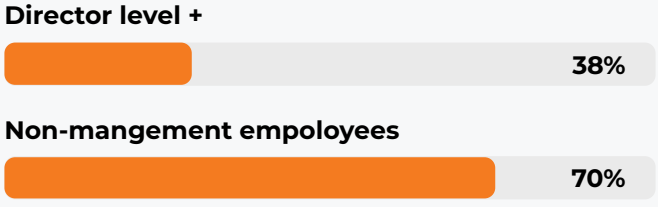
44% of people have admitted to **using their personal passwords at work.**

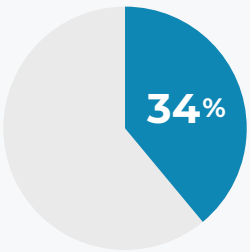


Why? Because people are predictable due to truly unique passwords being a headache to remember.

In the workplace,

management is even worse than junior staff at password hygiene. Only 38% of those in leadership positions **say their work passwords are unique.**





Password
123456789
Admin
Qwerty123
Abc123
Iloveyou
123123

34% of employed people in a director level + role admit to having used one of the most common passwords.

It's important to remember, sharing is NOT caring when it comes to passwords

Streaming service accounts have the most shared passwords or login credentials, followed by gaming accounts and mobile phone passwords. The type of account with the least shared credentials/passwords are work email accounts, but even still, 34% have shared their work email password.

Account Type	Spouse/Partner	Boyfriend/Girlfriend	Parents	Friends	Co-workers	Never Shared
Phone passcode	35%	11%	8%	9%	3%	41%
Phone fingerprint or face ID	12%	8%	5%	5%	1%	46%
Social Media	22%	8%	4%	8%	2%	55%
Banking	41%	5%	9%	4%	2%	56%
Personal Email	36%	6%	7%	9%	4%	59%
Work Email	15%	5%	5%	5%	6%	66%

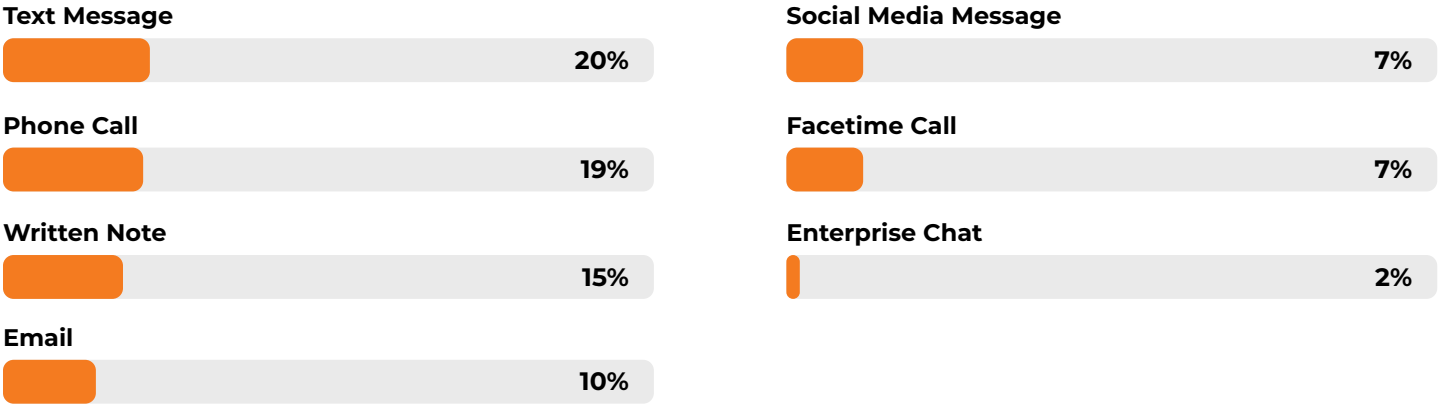
As relationships move from dating to marriage, password sharing increases as much as 4x for most services

Nearly twice as many people will share their bank account password with their spouse (41%) as their social media password (22%)

Most consumers are sharing passwords in ways that are easily hacked

A text message is the most common way in which people share a password, with 20% of consumers saying they share a password this way.

Ways consumers are sharing their passwords



The future of identity lies in biometrics, but more education must be done to increase appetite and willingness among average consumers.

Currently, fewer than 1 in 3 consumers

say they are comfortable sharing various forms of their biometric data with either a company they purchase goods and services from, or the government.

Despite high levels of discomfort when specifically asked about biometrics, data shows they're already using biometrics in multiple contexts

51% of consumers are **already using biometrics**

Consumers are willing to share their biometric data to save time

13% will share to save 30 sec or less.
12% will share to save 5 min.
10% will share to save 10 -30 min.

Ways consumers are using biometrics

The SecureAuth Approach

Organizations no longer need to compromise security for ease of use. SecureAuth enables a layered approach to access management enabling the strongest security without disrupting users. The SecureAuth Identity Platform is the best solution to ensure people attempting to access your valuable resources are, in fact, who they say they are, protecting against cyber criminals with malicious intent.

SECUREAUTH

“It’s important to remember, even if passwords are encrypted, hackers can use brute force against them and find out what they are. Ultimately, the victim will have no advanced warning which is why passwords need to disappear and an elevated form of continuous authentication needs to be implemented.”

- Bil Harmer
CISO & Chief Evangelist, SecureAuth