Avira Password Security Report

Tidy up your digital life

avira.com

May 2019

Introduction

Technology has become the main theme of the 21st century. It intersects with economy, politics, and science – in fact, it's everywhere in our lives. As new tech emerges, it's to be expected that people become more and more attracted to it, eventually spending most of their time being digitally connected. And with every minute spent in cyberspace, the world generates huge amounts of **digital data**.

Simply refusing to create digital information about yourself is not an option. "Just by virtue of being alive in 2019, you are generating data—both intentionally and unwittingly—that is mined, refined, productized and monetized," stated the Future Today Institute.

"*While the number of data breaches has been increasing substantially in the last couple of months, people tend to take safety measures only when they see their private data is at serious risk*," said **Matthias Ollig, Avira CTO**. "*We know that the main reason for this is related to convenience, which is why we strongly believe performant and easy-to-use solutions that make our digital experiences joyful will protect and secure people in the connected world*."

According to a recent report, out of the **7.7 billion people** on the globe, an estimated **4.4 billion** are **active Internet users** and **3.5 billion** are using some form of **social media**. Not only is that a huge number of connected people, it is also an even larger number of **connected accounts**, and mountains of private data collected about these individuals.

What keeps private information from blowing around cyberspace? Very, very little. For organizations, a growing body of legislation such as GDPR and HIPPA govern how they handle and protect personal data. But, a look at the major leaks of 2018 and 2019 shows that the cybercriminals are simply fusing together data from other legally and illegally collected sources. They have a lot of data to work with.

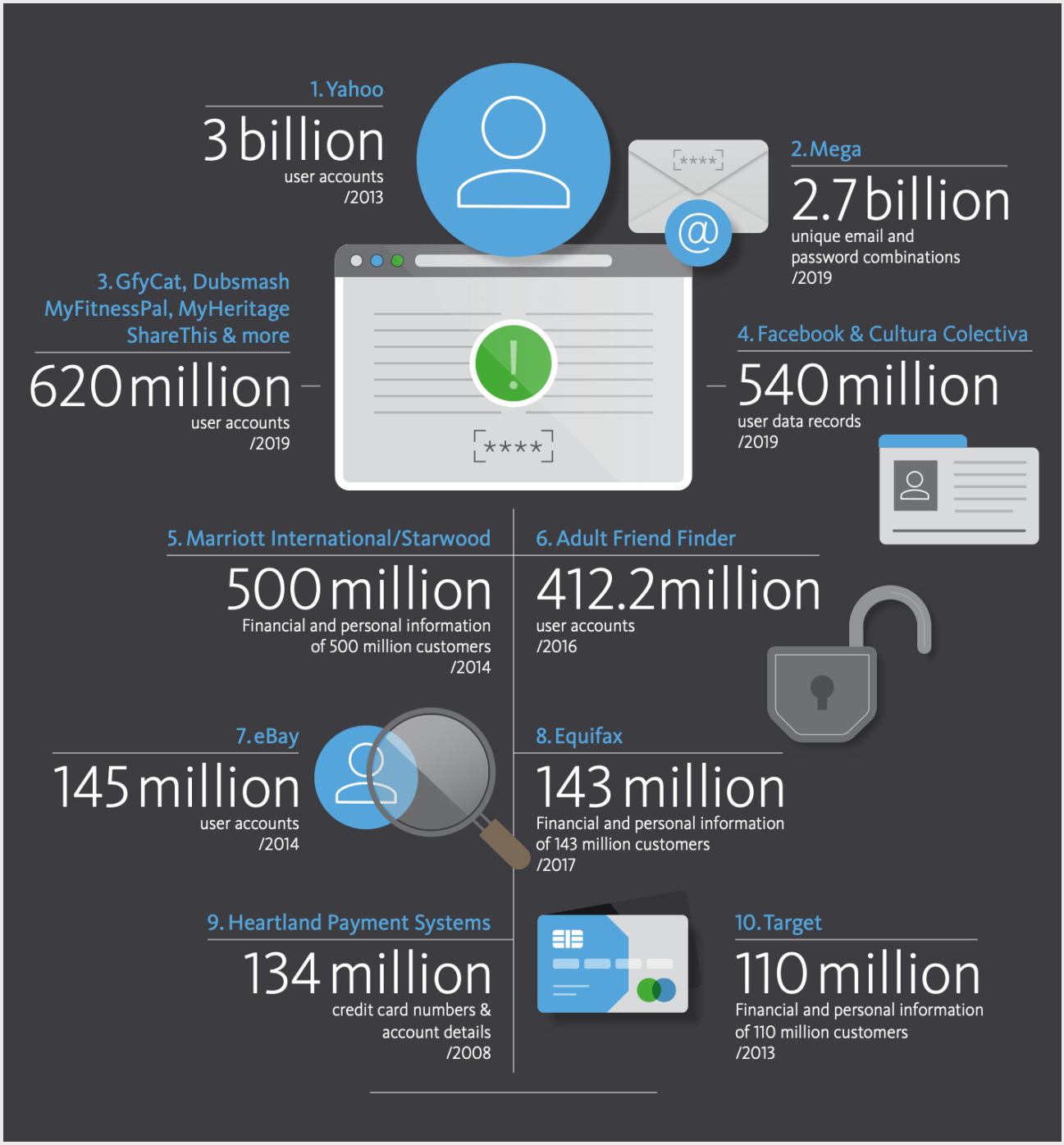
On the personal level, there are a number of steps that can be taken to make accounts more secure. On a technical level, this includes 2FA, use of a password manager, and not recycling passwords and user names between accounts. The problem is that these alternatives are known and ignored.

Think tidy, go for joy

To promote **password and account security**, fearmongering is not the answer. While research shows that consumers often have abysmal security habits (recycled, short passwords) and interest in password managers increases after a major hack, the impact is short-lived.

Joy seems to be a bigger motivator than fear. "*Our research shows that three out of the four major reasons for people to use a password manager were connected to convenience and speed, not security. It's a paradox: use a password manager, have more fun and incidentally, keep your online life much, much more secure*", said **Tim Gaiser, Director Identity Protection**.

Hall of fame:
Biggest data breaches (1)



*Read the full list on https://blog.avira.com

Hall of fame:
Biggest data breaches (2)

Breaches of private data are getting more extensive and more frequent. So far in **2019**, there have been at least four major data breaches, each impacting more than **200 million records**. Worst of all, they are aggregated piles of data from other sources – a sort of digital meatloaf. This data had already been stolen or misplaced and then uncovered only after the fact. It's not even clear where some of this private data originated.

From a non-technical perspective, there are three primary forms of data leaks: hacked, scrapped, and dropped.

- **Hacked** – Hacked lists are when the bad guys directly hack a company and exfiltrate their databases. The bad guys can have different priorities and motives. Nation-state actors tend to be after information, while the traditional black-hat hackers are trying to make money from reselling the lists.

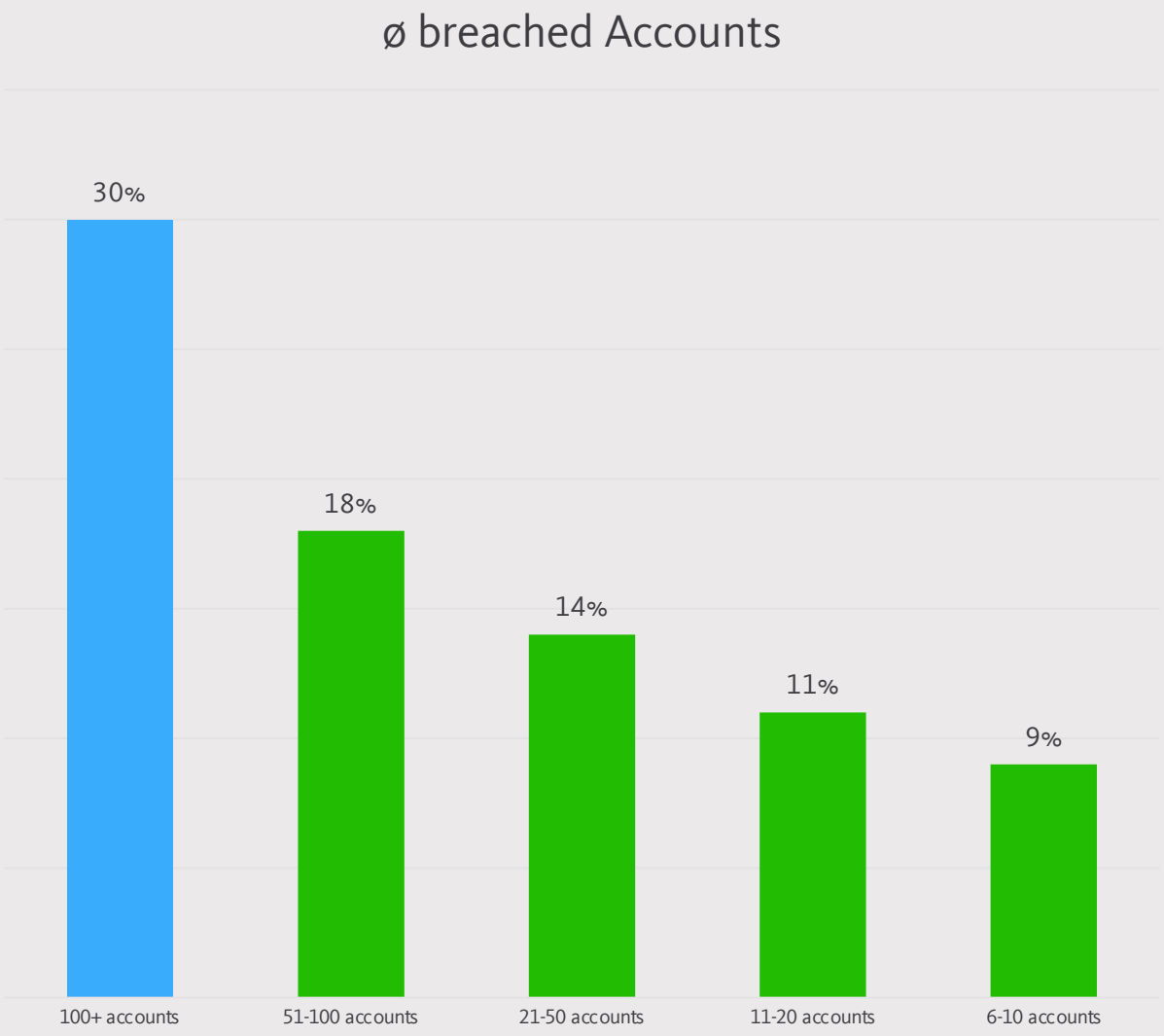
- **Scrapped** – Scrapped databases are assembled with a variety of tools to pry data out of various websites. It's often not clear where the data originates from or whether its collection is legitimate in light of the GDPR. Despite this uncertainty, there can be a lot of personal data in these lists.

- **Dropped** – Dropped databases are simply unprotected lists of data accessible via the Internet. As companies, social media companies, and data brokers compile more information on individual activities and put it into cloud storage, look for these sorts of data breaches to become more common.

The problem is that these are not stand-alone categories. When a black-hat hacker takes data from a company, combines it with other information from a data scrapper, then places it insecurely on an online server where other unauthorized hackers can view it, it fits under all three of the categories. This was the case with the huge Collection #1 (MEGA). It's believed this was a composite database made from other stolen databases. Once compiled, the data was sold and used by a hacking forum for a number of criminal schemes. Collection #1 was only discovered when the hackers stored their lists insecurely on a cloud server.

More accounts, more breaches (1)

The more accounts a person has, the higher the probability that they will be hacked. Studies show that those with 6 to 10 accounts have a 9% chance of a breach – a probability that jumps up to 30% when the number of accounts increases to over 100. The main driver behind the **increase** is the **reusing of account names and passwords** across their online accounts. This makes hacking the accounts of John Doe easy if the account name is going to be JnDough—regardless of whether it is email or the bank – and the shared password is JnB2Gud.



*Data collected by Avira on January 1st, 2019 – March 25, 2019

More accounts, more breaches (2)

We're at a critical juxtaposition of two trends: First, there is a lot of **valuable data** being created and **collected about you**. Every time you do something online – whether this is simple surfing or posting on social media – you're adding to this pile. And it's not just what you do directly, it is also what the army of data trackers and sites are recording about you.

Second, there are a lot of **bad security habits** at the organizational and individual level when it comes to private data. At the top of this list are **weak passwords**, **recycled passwords** across various accounts, **repeated user names**, and **poorly secured databases**.

Put these trends together and there is a wealth of information just sitting there, almost asking to be taken. It's like leaving your wallet in the front seat of a car with the windows down. With these resources within reach, there are armies of hackers – independent and nation-state supported – that are reaching in the window and grabbing it.

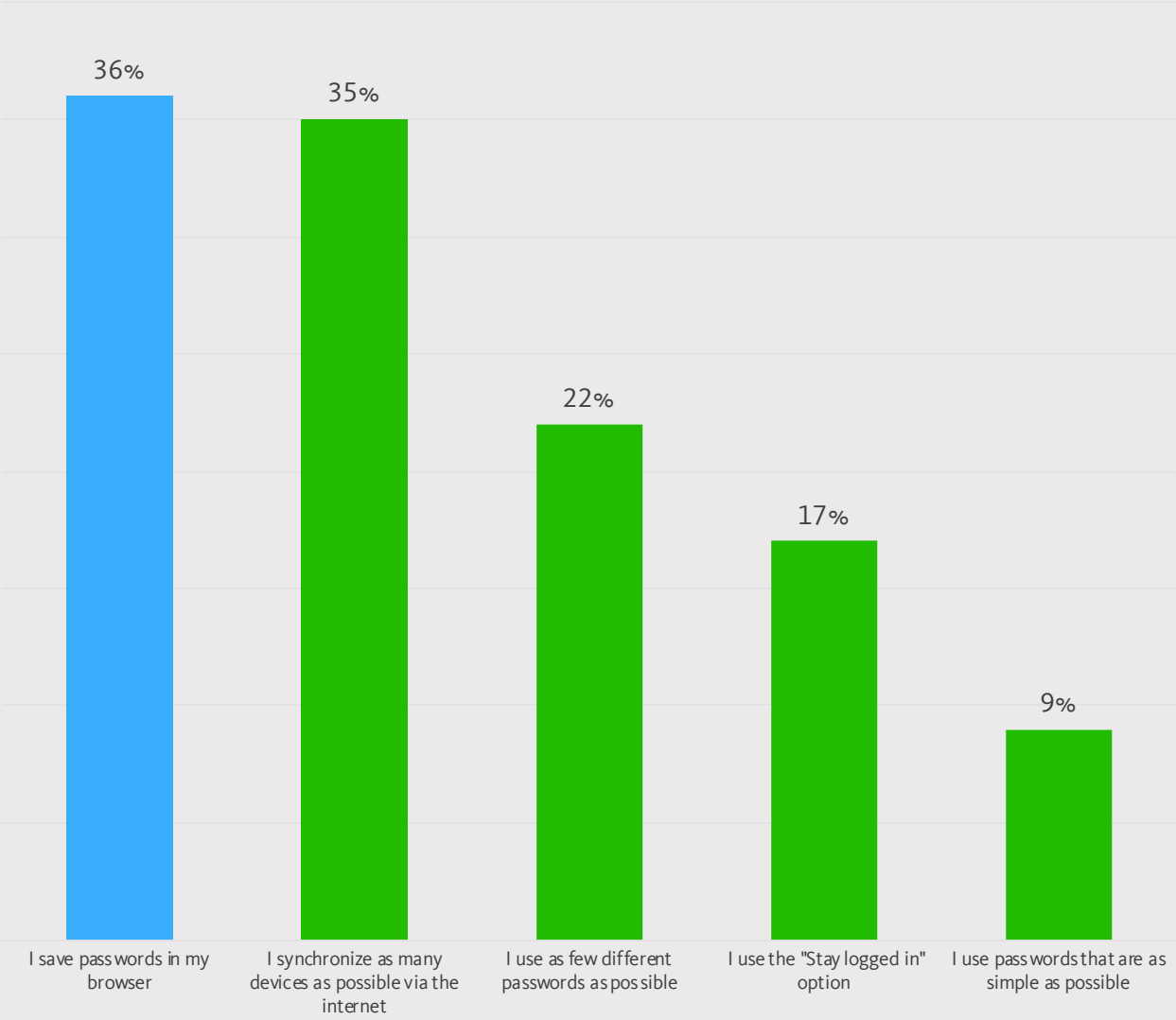
News of these breaches did cause an **uptick in interest in password managers**. As shown by Google Trends, there was an overall surge in people looking up password managers. On a micro level, the news spurred interest in our solution. "*News of these breaches led to up to 60% more installations and up to 20% higher user registrations compared to a normal day*," said **Tim Gaiser, Director Identity Protection**.

"Password management is often practiced on a 'pain avoidance' principle. People pick the shortest, simplest password possible and then reuse it or variations of it across multiple sites. This strategy does reduce the pain and effort involved for hackers. It gives them a clear motivation to try out known passwords across a targeted user's full range of accounts."

Tim Gaiser
Director Identity Protection

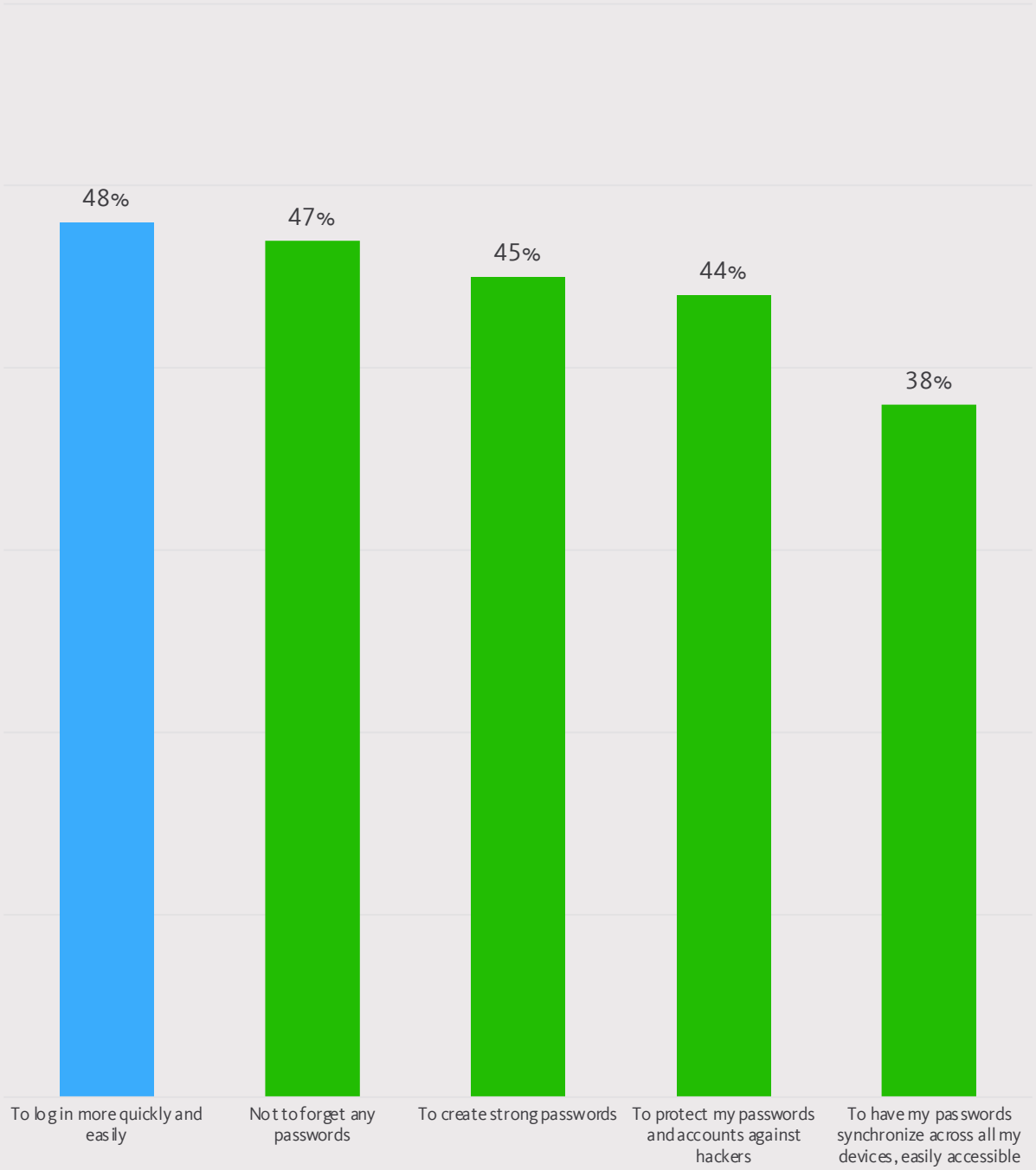
Digital habits

"The survey shows we need to emphasize the fun from using a password manager and the way it makes life easier", Tim Gaiser, Director Identity Protection



*Source: Avira Online Survey (multiple choice option) with 2519 respondents, aged between 20-65 years (US – January – February 2019)

Reasons to use a password manager



*Source: Avira Online Survey (multiple choice option) with 2519 respondents, aged between 20-65 years (US – January – February 2019)

Go from indifference to satisfaction in a month

To see how the **appreciation of password manager** features evolve over time, Avira followed Tim, a **new user** of the Avira Password Manager, over a four-week period. As a bona-fide, 23-year old millennial, he started out with some digital baggage: 30 various accounts with three key passwords slightly amended with additional letters or numbers as required.

Similar to many, Tim believed that using the same or similar password for all online accounts was sufficient to keep his data safe. Tim used 3 similar passwords across 30 accounts. He simply added a number or capital letter to alter them as required. He thought that his passwords were difficult to hack. “I am pretty sure, that nobody is able to hack my accounts, as I use common sense to set them up.”

His initial goals were modest: save time logging into accounts and make life more convenient by not having to reset a handful of passwords every month.

Entering his details at the start took an hour because he forgot some of the account names and the precise passwords. That said, after seeing all of his accounts and passwords in one spot, he was shocked that he had not been previously hacked. “It would have been so easy for someone to have gotten a hold of all my data.” Tim said.

After four weeks, he was a convinced client, using it across his device portfolio of a smart phone and home computer.

“My AHA-Moment when experiencing the auto-fill and auto-save functions in the browser extension... All data is available in no time. I go to a webpage, click on the register or login field and the password manager either saves my data to the dashboard or logs me into the webpage directly.

I can definitely recommend Avira Password Manager to everybody, as it means safety in terms of all your online accounts. I should have used it earlier; it was actually a slap in my face when I saw how risky it was to use the same or similar passwords. ”

*Source: Avira long-term qualitative study (one month)

Tidy up now!

It's time to treat **password management** as a **source of joy** – not as a security tool.

Here are **five suggestions** for using a password manager to experience joy and tidy up your online life:

- **Respect your passwords** - For all the protection they offer, passwords are amazingly under-appreciated. We need them – and we need strong ones. A password manager helps create strong passwords and reminds you when – perhaps unintentionally – a password has been recycled.

- **Stack them neatly** – Many people have passwords everywhere – desk, bulletin board, scattered across a couple devices – or they try to learn them by heart. A password manager lets you neatly organize your passwords and private notes.

- **Get it all within rea**ch – A good password manager goes with you, synching passwords across your device portfolio. This means no longer having to reenter passwords between devices.

- **(Quickly) clean up the other guy's mess** – In case someone else loses your data through a hack or a breach, Avira Password Manager Pro will give you an e-mail alert. Even better, it will help you quickly change the affected passwords, reducing your exposure to someone else's failings.

- **Be secure (of course)** – And yes, a password manager should keep your passwords secure on devices and in the cloud with its military-grade encryption. For even more security, only you know your master password. True password security should start and finish with you.

About Avira

Avira protects people in the connected world – enabling everyone to manage, secure, and improve their digital lives.

The Avira umbrella covers a portfolio of security and performance applications for Windows, Android, MacOS, and iOS. In addition, the reach of our protective technologies extends through OEM partnerships. Our security solutions consistently achieve best-in-class results in independent tests for detection, performance, and usability.

Avira is a privately-owned company that employs 500 people. Its headquarters are near Lake Constance, in Tettnang, Germany, and the company has additional offices in Romania, India, Singapore, China, Japan & the United States. A portion of Avira's sales support the Auerbach Foundation, which assists education, children, and families in need.

For more information about Avira visit www.avira.com.

avira.com