Avast® Data Protection Survey Report

April 2017 | by Avast® Software

Contents

Intro and Methodology A

A Introduction

We look at how Avast users from across the globe value and protect their online data

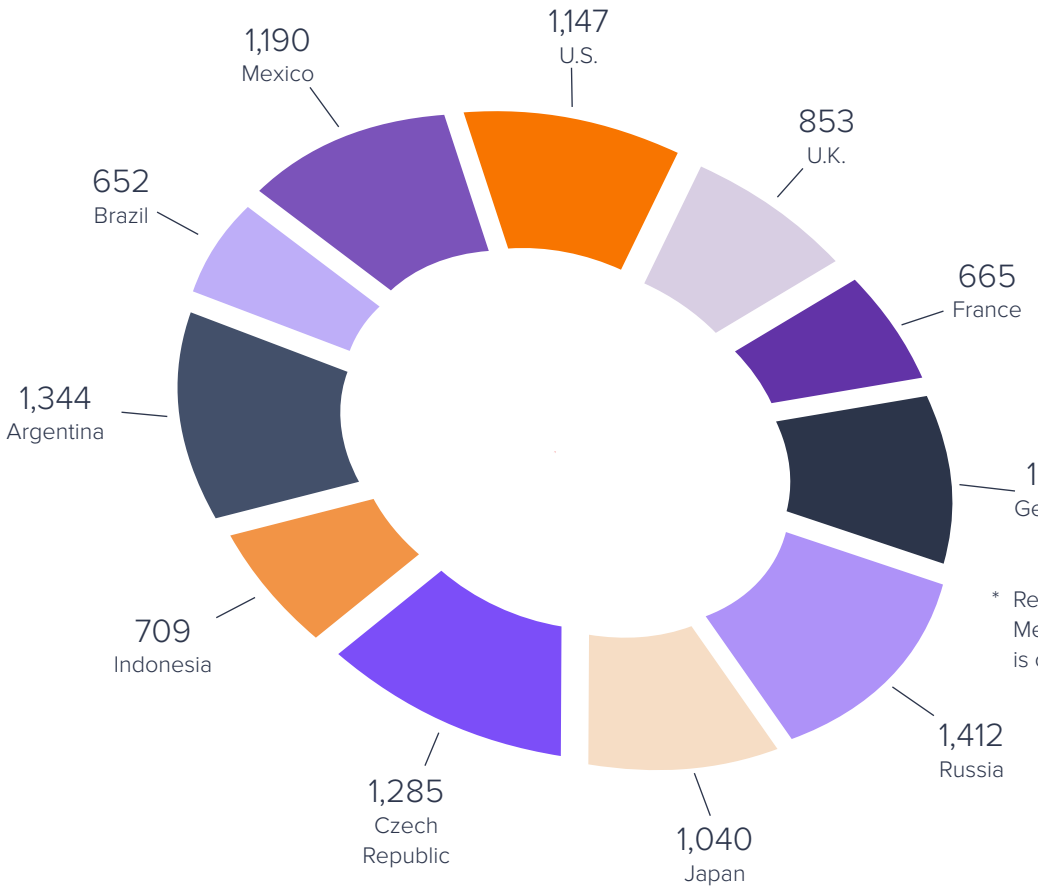
In a survey conducted among 11,417 Avast users worldwide, Avast gauged people's views regarding the value of their data stored in online accounts like email, shopping and social networking sites, and their habits when it comes to protecting their data.

The results show that, while many respondents view their data as having actual financial value, they aren't taking proper measures when affected by a data breach.

Methodology

- Online survey
- Respondents: Avast PC users
- Time frame: December 2, 2016 – January 27, 2017

Participants per country



* Report, including data for Mexico, Argentina, and Brazil, is coming soon.

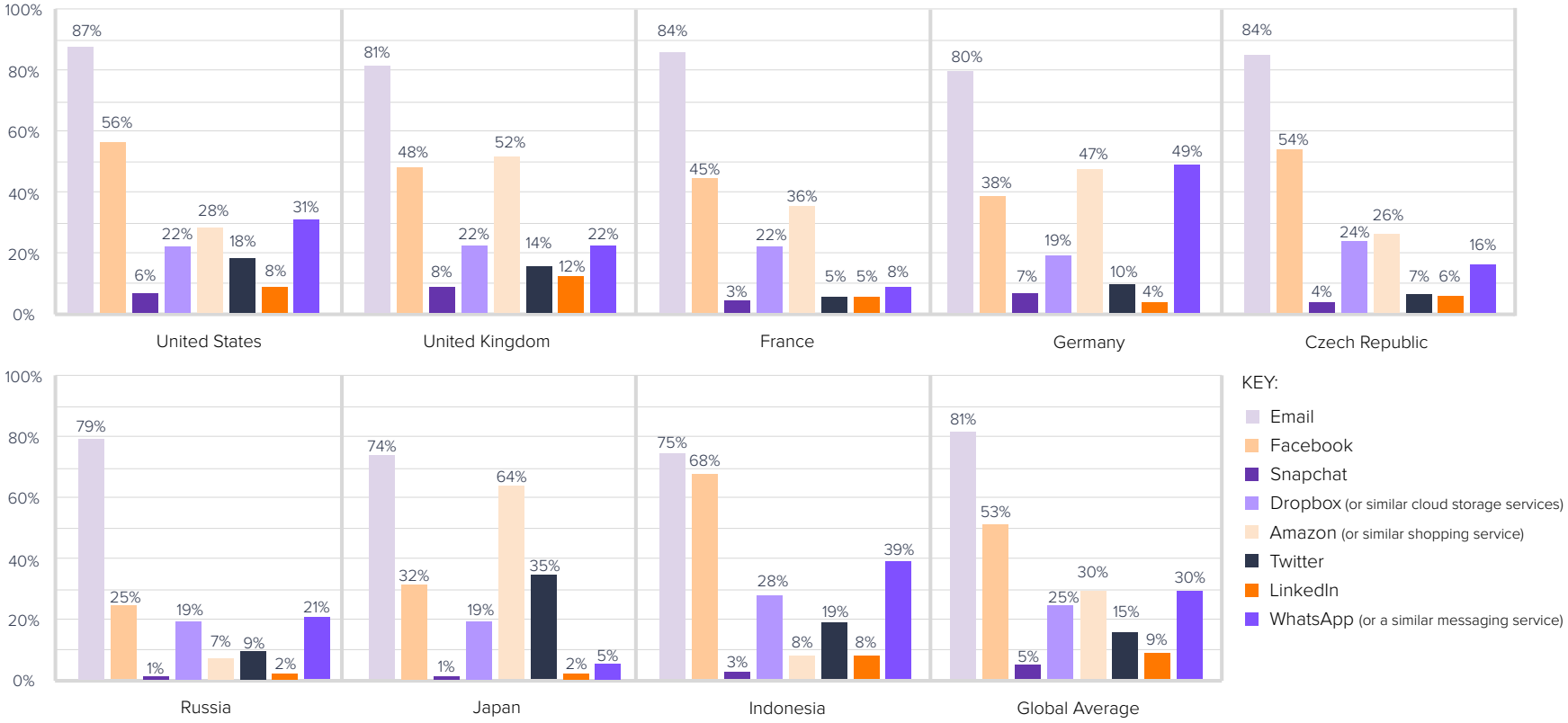
The Value of Data B

B The value of data

Email and Facebook are the most used online services

The majority of global respondents have an email account and use Facebook. Japanese respondents use shopping sites like Amazon the most (64%) compared to respondents in other countries, and messaging services, like WhatsApp, are more popular in Germany and Indonesia than in other regions.

Which services do you use?

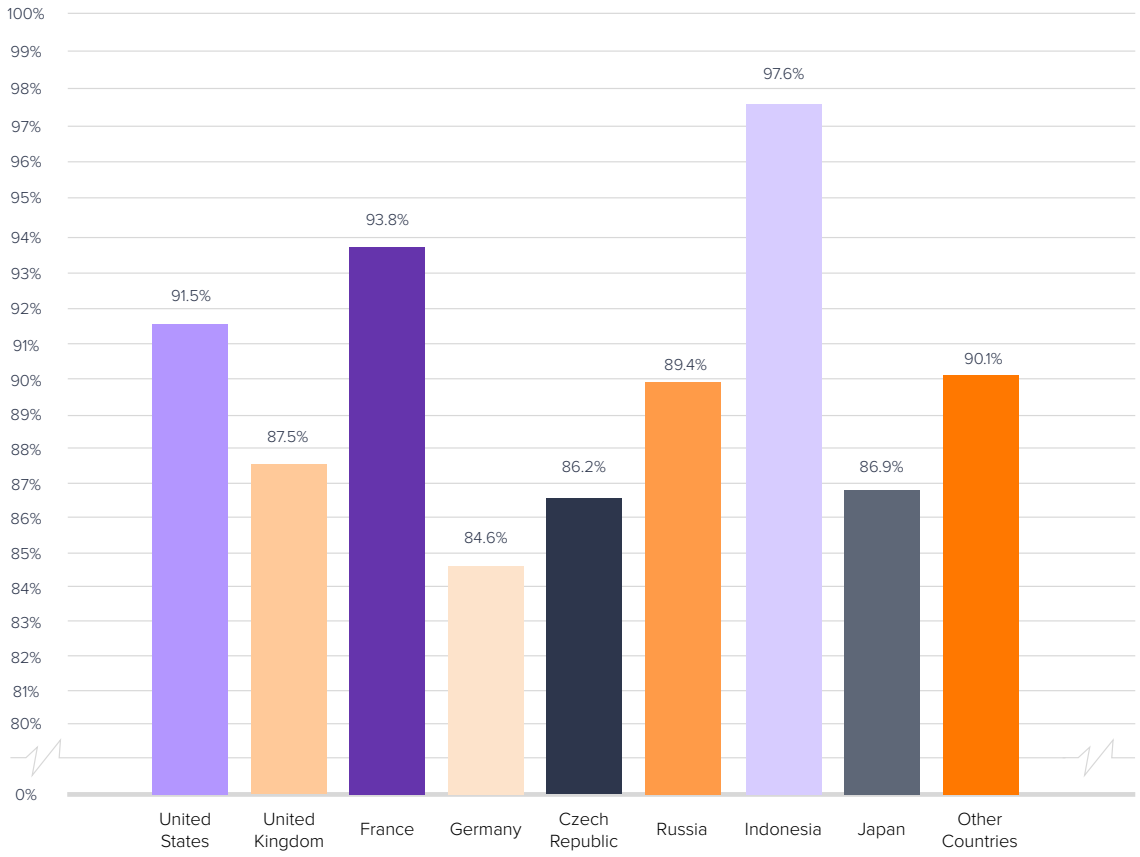


B The value of data

People value the data stored in their online accounts

When asked how much they value their data in general, nine out of ten respondents in most countries responded that the data in their online accounts is valuable to them.

Yes, the data in my online accounts is valuable to me

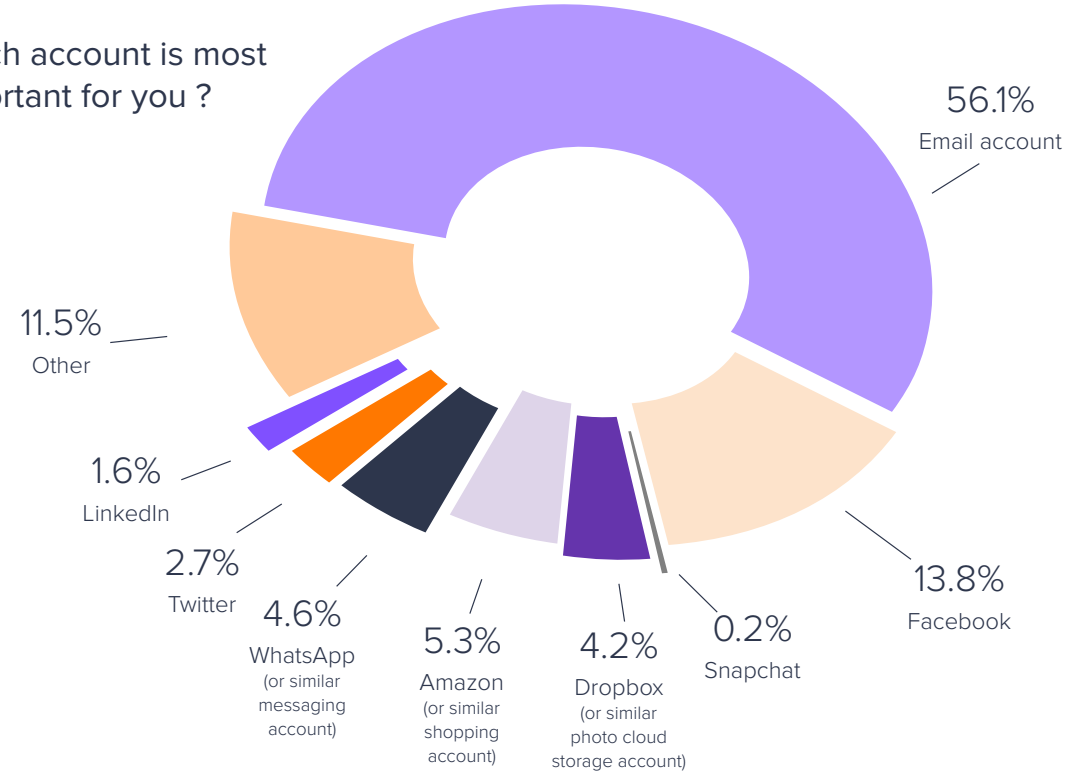


B The value of data

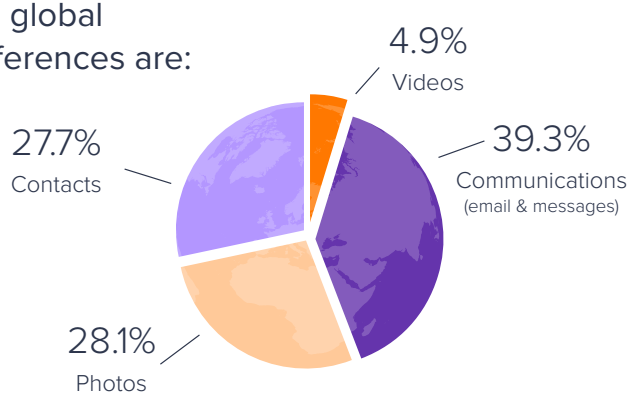
Email is more valuable to people than Facebook and messenger apps

In all regions, close to or more than half of respondents rate their email account as their most important online account. Facebook comes second, with a global average of only 13.7% who said the social network is most important to them. On a global average, less than 10% said shopping sites or messenger apps are most important to them, and less than 5% said their photo cloud storage account, WhatsApp, Twitter or LinkedIn accounts are most important to them.

Which account is most important for you ?



The global preferences are:



The top four valuable pieces of data, financial information excluded, are nearly the same in all countries. Videos were rated least important, and in all countries, with an exception of Czech Republic and Japan, communications like emails and messages were ranked by the highest number of people as their most valuable piece of data. In Czech Republic, photos were ranked as most valuable by one-third of respondents, and communications, like emails and text messages were ranked second (28.5%). In Japan, contacts were ranked as most valuable by two out of five respondents, and communications were ranked second (29.2%).

B The value of data

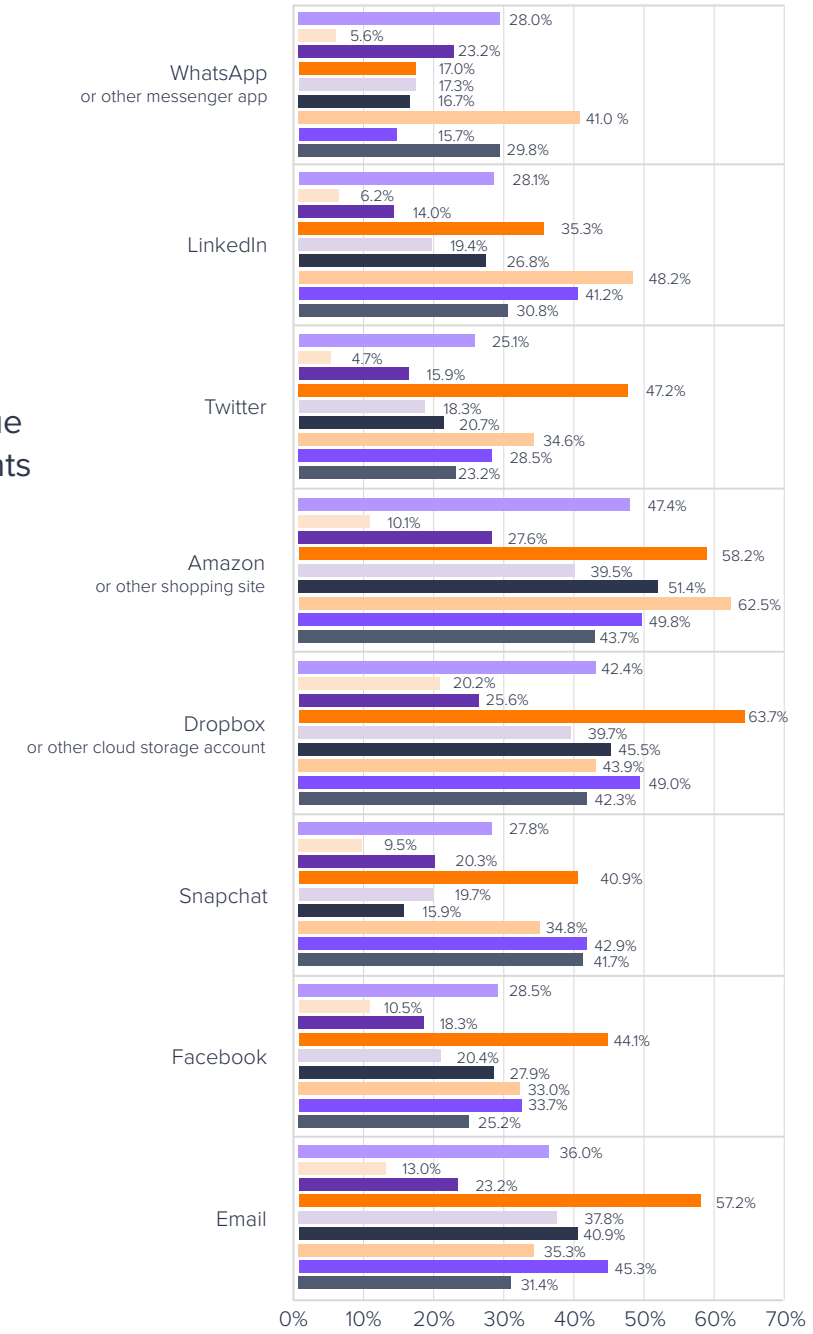
People value the sensitive data stored in their Amazon and Cloud storage accounts the most

We asked respondents how valuable their email, social media and shopping accounts, and the data stored on them, are for them. On average, nearly half of the respondents across all countries said the account details and data stored in their Amazon accounts is worth $100 or more, followed by 42.4% who said the data stored on their Dropbox or other cloud storage account is worth at least $100 or more.

In reality, account information, including user name, password, and credit card details, are sold for just $2 or less on the dark web, depending on the Bitcoin exchange rate.

As user data is currently being traded for very little on the dark web, it is more important than ever that people take the right measures to protect their data.

How much value do your accounts have for you? $100 and more



Online Security and Protection C

C Online security and protection

Peoples' confidence in online data security is low

Although many users feel their data is valuable, they do not take the appropriate actions to protect themselves. The majority of respondents said they are not confident that their online data is secure. Japanese respondents are most suspicious when it comes to the security of their online data with about four out of five respondents saying they are not confident that their data is secure, while the majority of British and Indonesian respondents are confident their data is secure.

Nearly half of the respondents worldwide said they were a victim of a data breach, or they are not sure if they have been affected by a data breach. In a worldwide comparison, U.S. users have been affected by data breaches the most, according to their responses.

Users are not confident that their personal data is secure

66.6% Russia
83.8% Japan
42.9% Indonesia
69.6% Germany

45.2% United Kingdom
62.3% Czech Republic
54.6% United States
57.2% France
61.7% Global average

C Online security and protection

Nearly 40% of people do not take action after learning they have been the victim of a cyber attack

In the past years, there have been many data breaches that have affected customers worldwide, for example, eBay customers, or the Yahoo data breach that affected one billion of its users last year. On average, less than 20% of global respondents said they have been a victim of a data breach, however 28.9% aren't sure if they have been affected. The majority said they have not been affected.

The U.S. is the country where most respondents said they have been affected by a data breach, with more than a quarter claiming so. Another 23.6% of Americans said they aren't sure if their data was included in a breach. The reason for the high number of respondents saying they have been affected by a data breach could be a result of U.S. laws that require an entity to notify their customers of a breach. In both Russia and Indonesia, three out of ten respondents are unsure if they have been affected by a data breach.

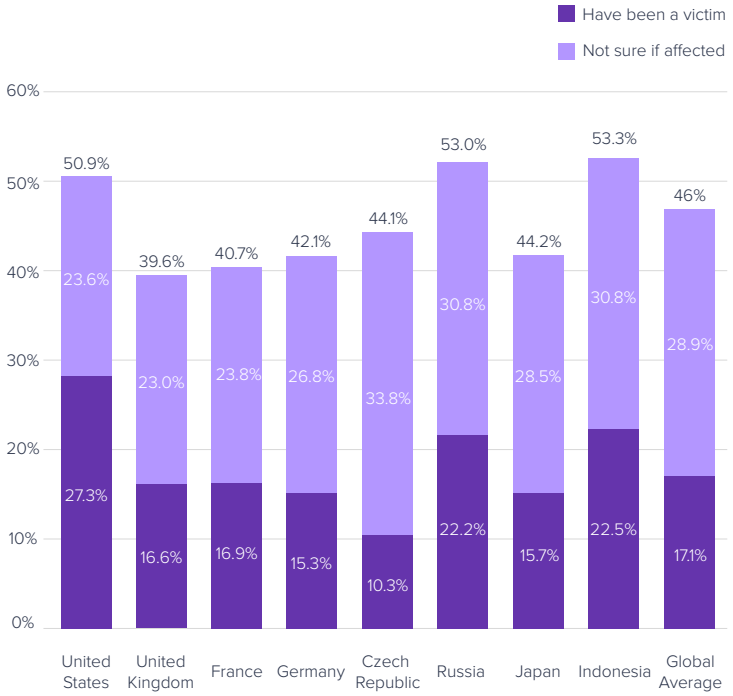
Although many have been affected by a data breach, most do not take proper measures to protect themselves. Many do not take action after their accounts were hacked.

In our survey, we found out that in all countries a third or more of the respondents never took action to change their password after a breach happened. The actual number might be higher, as some may not like to admit in a survey that they did not act responsibly. Out of those who said they changed their password on a website that was hacked, the majority did not change their password for other sites that required one.

This is a problem, as cybercriminals often use credentials obtained from a data breach to gain access to other accounts, as many people use the same credentials for multiple accounts.

Leaked databases typically are either sold or posted for free download on the dark web, so further criminals can abuse the data. Databases often show up on the dark web years after a data breach happened. It is, therefore, crucial for people to change their passwords for all the services they use on a frequent basis.

Have you been affected by a data breach?



C Online security and protection

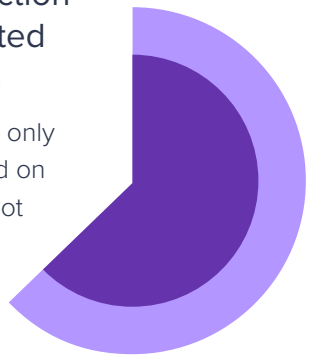
Nearly 40% of people do not take action after learning they have been the victim of a cyber attack

Often, services hash their customers' passwords, meaning clean password versions will not appear in leaked databases, but rather an encrypted version. This is a good way of protecting customers, however, the individuals are responsible for their security as well.

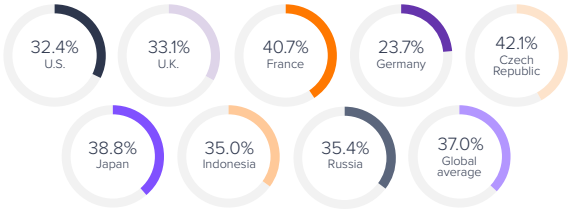
If a password is simple and, for example, only contains letters, a few characters and no special characters or numbers, hackers can easily guess the password. There are lists of the most frequently used passwords that hackers can use to hack their way into an account.

Only 63% took action after being affected by a data breach

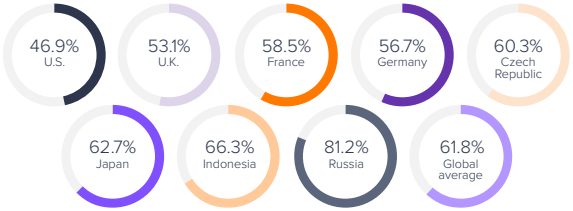
61.8% who took action only changed the password on the affected website, not on other sites where they used the same password.



Many never took action to change password

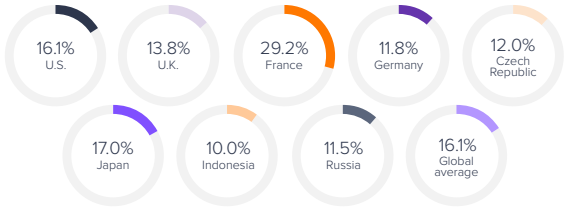


Many changed password for hacked website but not for other sites



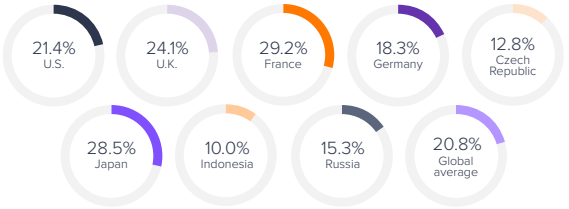
Important for businesses and website owners is that one out of five people (20.8%), globally, said they shut down their account after they found out about a data breach, and 16.1% claimed they never returned to the site that was affected.

Some never returned to hacked site



These numbers are certainly higher than the reality, as a 2016 report of the Ponemon Institute shows that the customer churn rate after data breaches grows by an average of 2.9%. However, we take this as an indicator that many are frustrated when it comes to data breaches. We assume that the results also include respondents that were affected by several data breaches, and chose to shut down or never returned to one of the sites that was breached, but not all of them.

Some shut down account with this service



C Online security and protection

Most people use a mix of letters and numbers to make their passwords stronger

Many leave their online accounts vulnerable to being hacked, by not using strong passwords. There are several ways people can ensure their passwords are strong. Globally, the majority of respondents use a mix of letters and numbers. The second most popular method to create a strong password is the use of eight characters or more, however only half of the users use this method.

Methods users use globally to make their password stronger

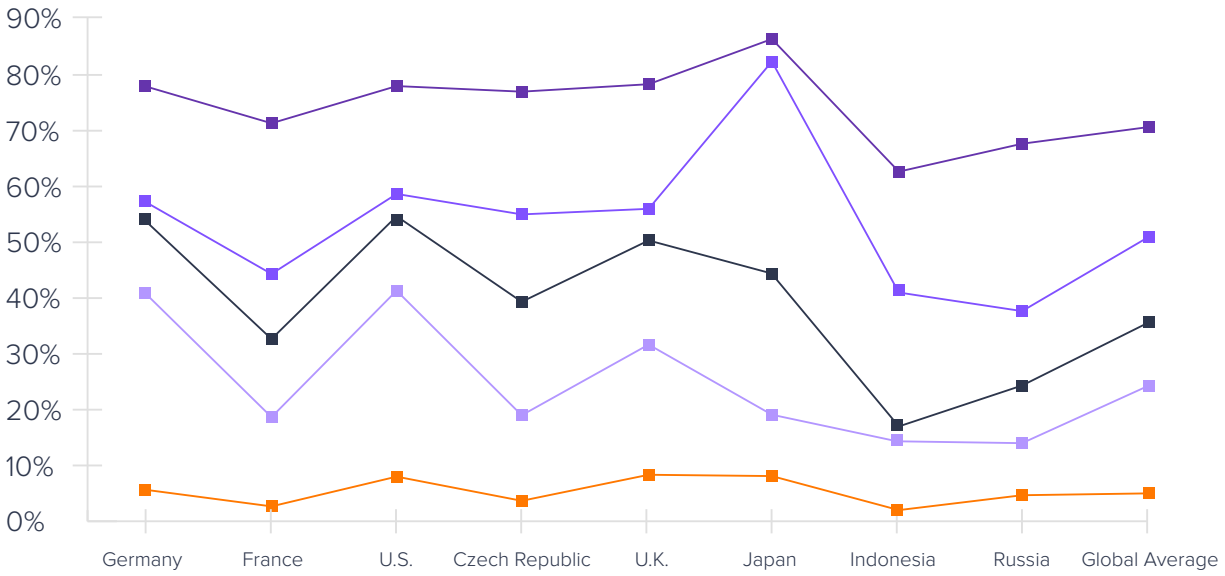
5.1% Use a password manager

24.1% Use special characters

36.1% Use upper & lower case characters

51.4% Use eight characters or more

71.8% Use a mix of letters & numbers



Global numbers show similar preference across different countries

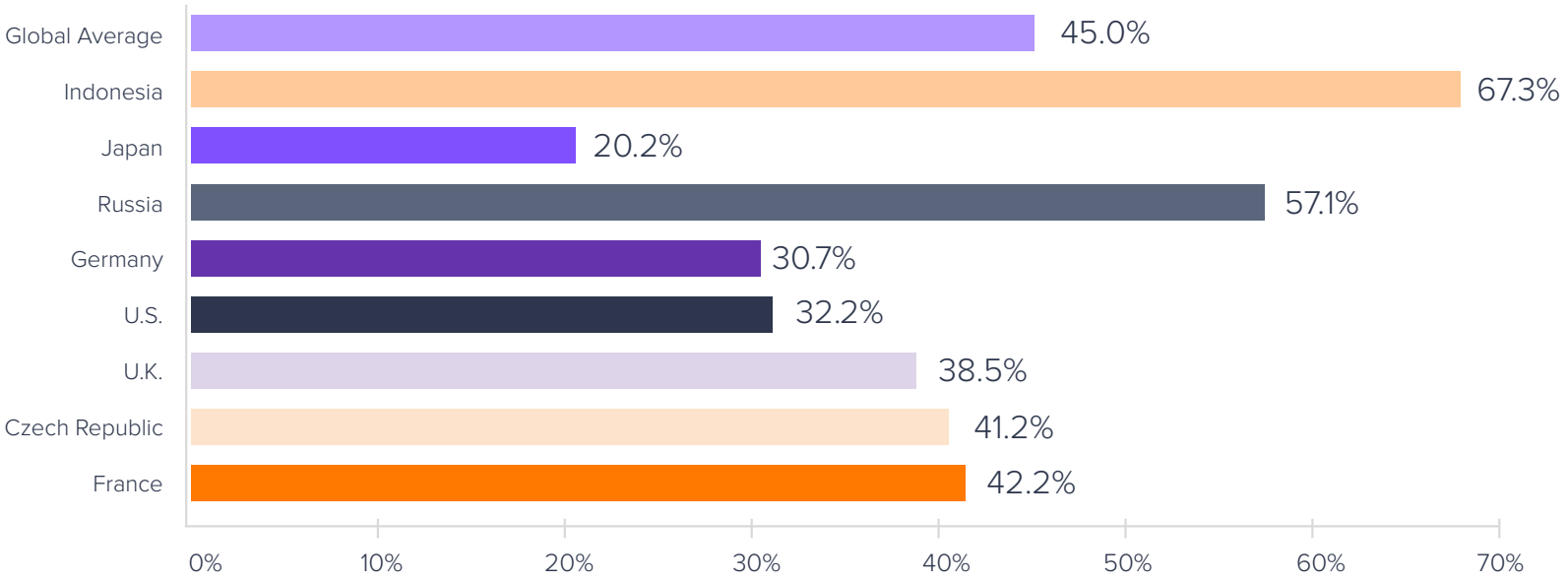
KEY:
- Use a password manager
- Use special characters
- Use upper & lower case characters
- Use eight characters or more
- Use a mix of letters & numbers

C Online security and protection

Most people use a mix of letters and numbers to make their passwords stronger

Many users only use one method to strengthen their passwords, which is not enough to protect themselves from hackers, and brute force attacks. Also, Avast numbers show that about 80% of users store passwords in their browser, which is not secure. Passwords stored in the browser can be accessed by software installed on the computer.

On global average, 45% use weak passwords



Conclusion and Contacts D

D Conclusion

Information is currently the most valuable commodity. Via email alone, people share financial information, photos, videos, personal messages and sensitive documents. Attackers are aware that this information is valuable to the people, and making it an ideal asset for them to abuse, and there are many ways an attacker can abuse the contents of emails, for example, by making them public, and blackmailing the victim.

Our report shows that many people don't trust that their data is secure online. Stolen data is being traded on the dark web for much less than what the people think it is worth. These are good reasons for them to take action and protect their data.

One way is to use complex passwords, always and everywhere, even for their smart TVs or thermostat at home. Another way to manage and create complex passwords is a password manager, like Avast Passwords. In the new version of Avast 2017, Avast Passwords has been redesigned for PCs, Macs, and mobiles, making passwords even easier to manage and keep our users safe. Users' passwords are stored securely in one convenient location, locked behind a master password.

When unlocked, and when the accompanying browser add-on has been installed, Avast Passwords auto-fills the user's login information any time they try to access their protected accounts.

When upgraded to premium, which is only available for PC users, Avast Passwords automatically notifies users whenever any of their account credentials are found to be leaked on the internet, and also allows users to unlock their desktop passwords from their phones. www.avast.com

Contact Information

email: pr@avast.com