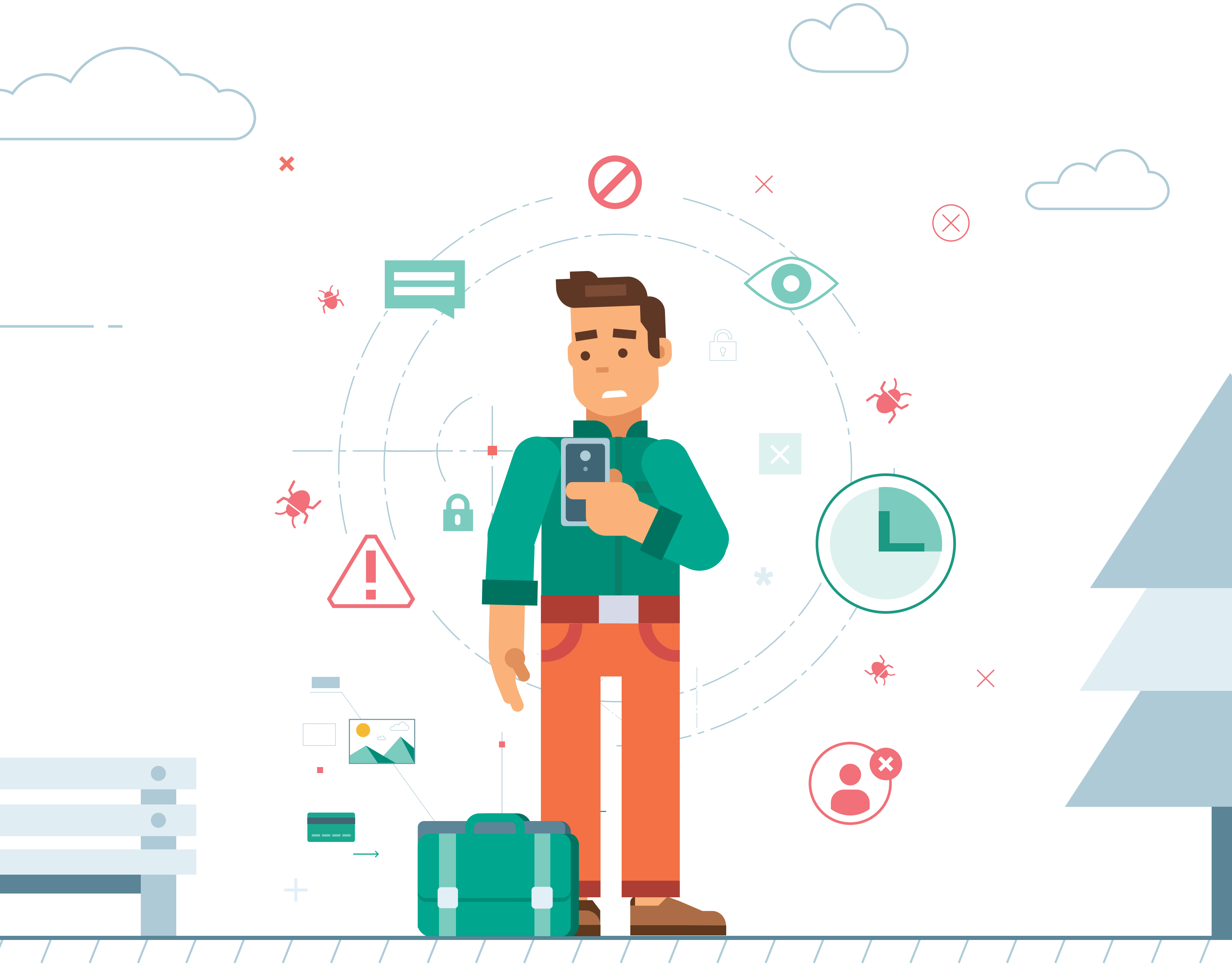


The State of Cyber-Stress

A study on Americans' and Canadians' stress levels and mindsets about cybersecurity.

Introduction

In today's society, stress is so common that it is essentially a state of being for many people, with a recent Gallup survey finding that eight in ten Americans feel stress on a daily basis. Being digitally connected is also a must for most people, as technology is integrated into nearly all aspects of our everyday lives. With digital footprints becoming a way of life for almost every consumer, does the need to be constantly mindful of data security cause "cyber-stress?"

From Target to Yahoo to Equifax, millions of people in North America of all ages and interests have become the victim of a data breach in recent years. With both high-profile breaches and smaller cyberattacks taking place nearly every day, millions more people will be added to the list of those affected in the years to come. Cybersecurity has quickly become top-of-mind for consumers whose personal information of livelihood could be at risk from a breach or cyberattack – and the uncertainty of when the next breach will strike leaves people wondering.

Kaspersky Lab issued a survey to gain insight into the perceptions of consumers in North America regarding cybersecurity, as well as what actions they take to protect their data from online threats. Kaspersky Lab commissioned the research firm Opinion Matters to conduct the survey 2,515 internet users in the United States and Canada. The results of this survey reveal the stress levels of consumers relating to digital security, how they feel about businesses or other people having access to their data, and why some people are more worried than others about a cyberattack.

By identifying consumers' largest sources of cyber-stress, Kaspersky Lab aims to understand what will help people to feel more at ease about the security of their personal data. Through this research, the company hopes to educate both consumers and businesses on the proactive steps to take to avoid or mitigate the impact of a cybersecurity issue, reducing cyber-stress through education and action.

Key findings from the study include:

- The majority of adults – 81 percent of Americans and 72 percent of Canadians – admit that the news of data breaches has caused them stress.
- Nearly half (46%) of 16- to 24-year-olds said they often find it stressful to manage the number of passwords they have, as opposed to just over a quarter (27%) of people aged 55 and over.
- Nearly half of respondents (46%) have experienced at least one cybersecurity issue (e.g. virus, ransomware attack, malicious links or emails) on any of their internet-connected devices in the last five years, including 59 percent of respondents aged 25 to 34 years old.
- Of those that have experienced a cybersecurity issue in the past five years, a third (33%) agreed they often find it stressful protecting all their devices.
- Forty-four percent of respondents underestimated how much a data breach costs an enterprise by at least $300,000, claiming that the cost of this would be $1 million or less.
- People are the least willing to share their personal data with social networking apps, mobile payment apps and banking apps.
- Nearly half of people (49%) from the U.S. and Canada would trust their partner with their username and password for their device(s), and the same proportion would share the answers to their security question(s) with their partner.

Research Methodology

The quantitative study was conducted by research firm Opinion Matters via an online survey in December 2017 of 2,515 adults aged 16+ in the United States and Canada who go online.

Research Findings

The Stressful State of Cybersecurity

With data breaches and cyberattacks making headlines in mainstream news outlets every week, cybersecurity is becoming a topic of conversation as routine as last night's baseball game. According to the Identify Theft Resource Center[1], 1,579 data breaches were reported in 2017– an increase of 45 percent from the previous year, and a record high since this information has been tracked. Many of these breaches included sensitive personally identifiable information (PII), which could put victims at risk for identity theft or bank fraud.

As people increasingly think and talk about cybersecurity, consumers are becoming progressively worried that they will become the next victim of a data breach. When internet users were asked about the stresses that they feel relating to cybersecurity, a vast majority of respondents – 81 percent of Americans and 72 percent of Canadians – said that news of data breaches causes them personal stress.

Data breaches are not the only source of cyber-stress. With the average consumer in North America managing at least 16 username and password combinations[2], choosing secure passwords and keeping track of login information for dozens of online accounts can be quite the headache. For millennials (16- to 24-year olds), who may be conducting more of their daily activities online than their parents or grandparents, protecting all of their online accounts from digital threats can be particularly taxing. Nearly half (46%) of millennials agreed that they often find it stressful to manage the number of passwords they have, as opposed to just over a quarter (27%) of people aged 55 and over.

What is considered Personally Identifiable Information (PII)?

- PII is any data that can be used to identify a specific individual. Includes:
    - Mailing or email address
    - Phone number
    - IP address

- Sensitive PII is information that could result in direct harm to an individual if it is transmitted in unencrypted form. Includes:
    - Medical information
    - Biometric data
    - Bank account numbers
    - Credit and debit card numbers
    - Passport or driver's license information
    - Social Security numbers

Sources[3, 4]

People often think of stress as a reaction to a major life change or strenuous event, like losing a job or becoming from the victim of a crime. However, experts note that it is actually the impact of smaller, ongoing pressures that causes the majority of stress-related illness. According to the American Institute of Stress, chronic stress is that which is caused by "the cost of daily living," such as pressure from work, raising children, or media overload. This is the form of stress that can cause physical symptoms and reduce quality of life, when these everyday aspects are not managed well.

The ongoing anxiety of protecting a variety of devices and data from unknown threats underlies our long-term cyber-stress issues. "Research has shown that it's not the big, acute, one-time challenges that cause the majority of stress-related disease and disorder, but the everyday, nagging, accumulating pressure and tension we feel when we don't have enough capacity to cope with the demands of life," explained Heidi Hanna, Ph.D., executive director of the American Institute of Stress. "Especially when we feel unsafe, out of control, or unable to keep up with the pace of change, something that is inherent in our constantly-connected, digital lifestyle. Advancements in technology provide us with incredible opportunity, but can also quickly cause people to feel lost – and stressed – in a whole new world."

75%
of people say that protecting all of their devices from cyberthreats has caused them some kind of stress.

Kaspersky Lab's survey revealed that for 75 percent of people, protecting all of their devices from cyberthreats has caused them some kind of stress. With the average household containing more devices than people[5], it is no wonder that technology overload is one of the key sources of chronic stress cited by experts. Between data breaches, password management and generally keeping track of a growing number of devices and accounts, cybersecurity is a significant burden for consumers today to bear.

The Reality of Online Threats

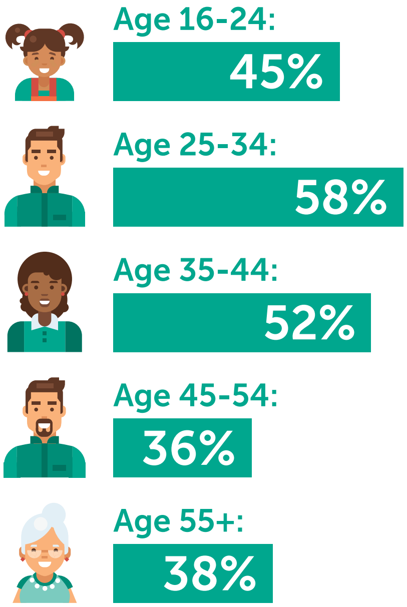
Being stressed about cybersecurity may seem superfluous to those who are especially tech-savvy or who have not been personally impacted by a data breach. However, the reality is that fears about becoming the next victim of a cyberattack are not unfounded. Many consumers are experiencing cybersecurity issues affecting their personal devices, including malware infections, ransomware attacks or having accounts breached.

Kaspersky Lab found that nearly half of survey respondents (46%) have experienced at least one cybersecurity issue in the last five years, including 58 percent of respondents aged 25- to 34-years old. Looking at some of the biggest data breach headlines of the past five years, it is unsurprising to see a high percentage of people impacted by cybersecurity issues. In addition to high-profile breaches, such as Equifax and Verizon – in the last year alone – consumers also became the target of a number of massive fraud scams that affected everyday applications, such as the Google Docs phishing attacks or ransomware-laced spam emails that appeared to be sent from Dropbox.

Becoming the victim of a cyberattack can be a stressful experience that can add to the anxiety people feel around cybersecurity. A third of people surveyed (33%) claim that they often find it stressful protecting all their devices when they have experienced a cybersecurity issue in the last five years. With new cyberattacks and scams already barraging consumers in 2018, protecting devices and data from these threats is a stressor that doesn't appear to be going away anytime soon.

While falling victim to a cyberthreat can be a wake-up call to start paying attention to online security, Kaspersky Lab's research also found that a small portion of people do not learn from their mistakes. Fourteen percent of Americans and six percent of Canadians admitted to having experienced four or more cybersecurity issues in the last five years. While in some cases this may be due to sheer bad luck, such as having data compromised through numerous third-party breaches, experiencing such a high frequency of cyberattacks may signal a failure to take precautions to protect devices.

Percentage of people by age group who have experienced at least one cybersecurity issue in the last five years:



14% of Americans and 6% of Canadians admitted to having experienced 4 or more cybersecurity issues in the last 5 years.

Turning Away from Technology?

For some consumers, the stress stemming from a cyberattack on a personal device or news of a data breach may prompt them to download security software. However, in response to increased levels of cyber-stress, some consumers have lost trust in the companies and technologies with which they share their data. When asked about which industries they would trust to protect their data (such as finance, healthcare or education), Kaspersky Lab found that more than one-in-five survey respondents (22%) would not rely on any sector. This figure rose to 32 percent of people over the age of 55 who claim that they do not have confidence in any sector to protect their data.

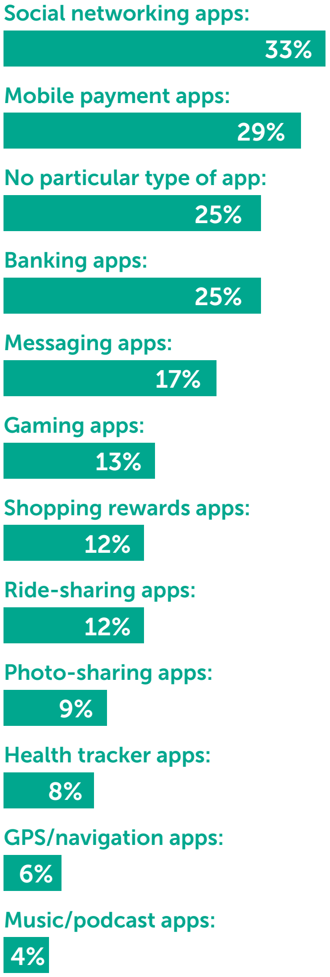
News of point-of-sale (PoS) breaches, such as those at Chipotle, Hyatt Hotels and Forever21, may be one of the reasons that consumers are feeling wary about sharing data, particularly with retail companies. Recent research found that in 2017, businesses experienced a significant increase in cyberattacks involving vulnerabilities in PoS systems[6]. In light of this news, 19 percent of survey respondents indicated that they least trust the retail sector when it comes to protecting their data.

"Companies who are involved in a breach often face brand abandonment, as people feel let down by an organization they felt safe and connected with, regardless of the actual cause of the disruption," said Heidi Hanna, Ph.D., executive director of the American Institute of Stress. "On the other hand, brands who are able to instill a sense of safety, compassion, and consideration for consumer security are able to build brand loyalty quickly, and contribute to a decrease in collective stress levels as communities feel safer together."

Another reason that consumers may be losing confidence in businesses to keep their data safe is a lack of knowledge about the effect of negligent cybersecurity practices on an enterprise. Kaspersky Lab research found that nearly half of consumer respondents (44%) underestimated how much a data breach costs an enterprise (businesses with more than 100,000 employees), assuming that the cost would be $1 million or less. In reality, the average cost of a data breach in North America is $1.3 million for enterprises, according to a separate Kaspersky Lab survey conducted in 2017.

While consumers may be more trusting of certain sectors, such as technology or banking, to protect their data, they could still be wary of the technology that these companies offer to its customers: apps. When asked which kinds of mobile apps they would trust the least with their data, 32 percent of respondents said that they would be least likely to trust social networking apps. This was closely followed by mobile payment apps (29%) and banking apps (25%), showing that no industry is immune from the impact that cyber-stress has on its customers.

Types of apps people would be least likely to trust with their data:



Finding Security in Friends and Family

Although consumers' stress related to sharing personal data with companies or technology is on the rise, many people are still finding refuge in a familiar source – friends and family. Kaspersky Lab found that a relatively large proportion of people are still willing to entrust sensitive data to the people closest to them, even though this could pose substantial privacy risks. Nearly half of survey respondents (49%) would trust their partner with their username and password for their devices, and the same percentage would trust their partner with the answers to their security questions. While this behavior may seem harmless, as there is no risk of data being leaked in a breach or compromised by hackers, another recent Kaspersky Lab study showed that sharing unrestricted digital access with a significant other could come with risks of its own. The report[8] found that 21 percent of people have admitted to spying on an ex-partner through an account to which they had access, such as social media or email, revealing one potential security risk of sharing passwords with a partner.

For younger internet users, a parent may fill the role of a secure confidant, with 45 percent of respondents aged 16- to 24-years-old stating that they would trust their parents with their username and passwords to their devices. The younger demographic was also more likely to entrust their data to a friend, with 19 percent of respondents aged 16 to 24 stating that they would share their online account or app login details with friends, compared to just seven percent of the general population.

Sharing device passwords or online accounts with family, friends and partners may seem like a safe option for many consumers. However, as these third parties are less invested in the information saved on these accounts, they may not feel as responsible for its security. Therefore, sharing sensitive digital data with others, even if they seem trustworthy, can be a dangerous habit.

Who would you trust with your personal data?

	Username(s) and password(s) for my device(s)	My online account or app login details	My credit / debit card(s) details
My partner	49%	48%	51%
I wouldn't trust anyone with my personal data	26%	28%	29%
My parent(s)	26%	26%	26%
My children (aged over 18 years old)	16%	15%	14%
My password manager	7%	7%	5%
My friend	7%	7%	4%
My children (aged under 13 years old)	6%	6%	4%
My children (aged 14 - 17 years old)	5%	4%	3%
Other	2%	2%	2%
A third party app	2%	2%	2%
My employer	2%	2%	2%

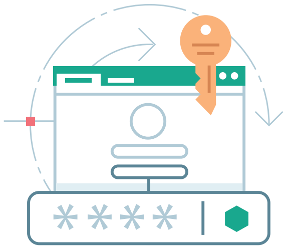
Conclusion

With data breaches, cyberattacks and online scams making news and impacting millions of people in North America every year, consumers are increasingly cognizant of cybersecurity threats. However, many are still unaware of how to fully protect themselves and their devices in the face of these complex threats, leading them to become stressed about the potential exposure of their data. With a lack of proper knowledge and tools to secure their digital lives, consumers are instead attempting to alleviate their cyber-stress by avoiding the companies and technologies that appear to be at fault for these cyber incidents.

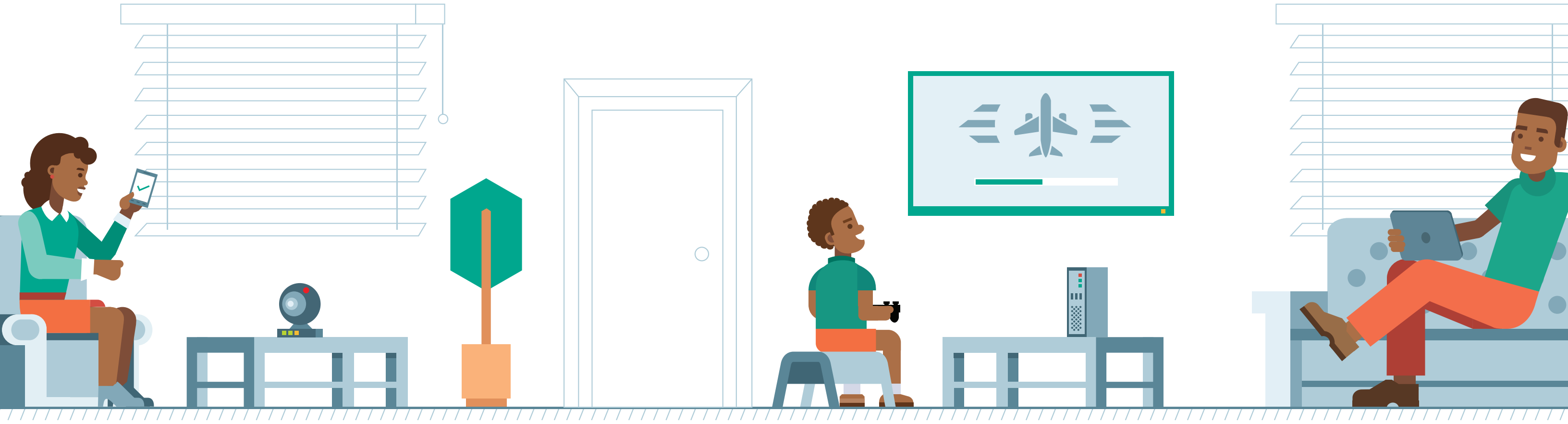
Instead of allowing themselves to be plagued by cyber-stress, consumers should feel empowered to learn more about cybersecurity best practices and the tools that will help them secure their data. Additionally, businesses in the security community should share their resources and information on the latest digital threats with consumers, opening up a dialogue about how consumers can proactively take control of their own security.

Staying informed about emerging online threats, installing reliable security software across all devices and taking note of cybersecurity best practices can give consumers peace of mind that they have done everything possible to secure their data. In the event their personal data is compromised in an incident that is out of their control, they will also have better understanding how to mitigate the negative effects of a breach.

By taking proactive steps to learn more about cybersecurity and implement solutions to protect devices, consumers can avoid becoming the next victim of a cyberattack. While many sources of 21st century stress show no signs of abating, cybersecurity has the potential to become a source of empowerment rather than frustration. Through education and action, consumers can understand how to embrace and utilize technology safely – instead of allowing it to add to the daily stress in their lives.



Leveraging security technologies like password management software or anti-spam email filters can help consumers to steer clear of common online security issues.



Cybersecurity Best Practices

✓ **Install an antivirus solution on all your devices, including PCs, Macs, smartphones and tablets.**

- Antivirus software safeguards consumers from malware, ransomware, phishing scams and more. Kaspersky Lab offers a number of robust security solutions for home users, designed to protect consumers from the latest cyberthreats.

✓ **Use strong passwords that are different for every account.**

- Passwords should be six characters or more and should include a mix of uppercase and lowercase letters, numbers and symbols. Store passwords securely using a password manager, and activate two-factor authentication when possible.

✓ **Make sure all apps and programs are kept up-to-date with the latest software patches.**

- Cyberattacks often take advantage of bugs or security flaws in older versions of software programs and devices, so set your devices to automatically install updates.

✓ **Keep track of third-party applications that have access to your personal data.**

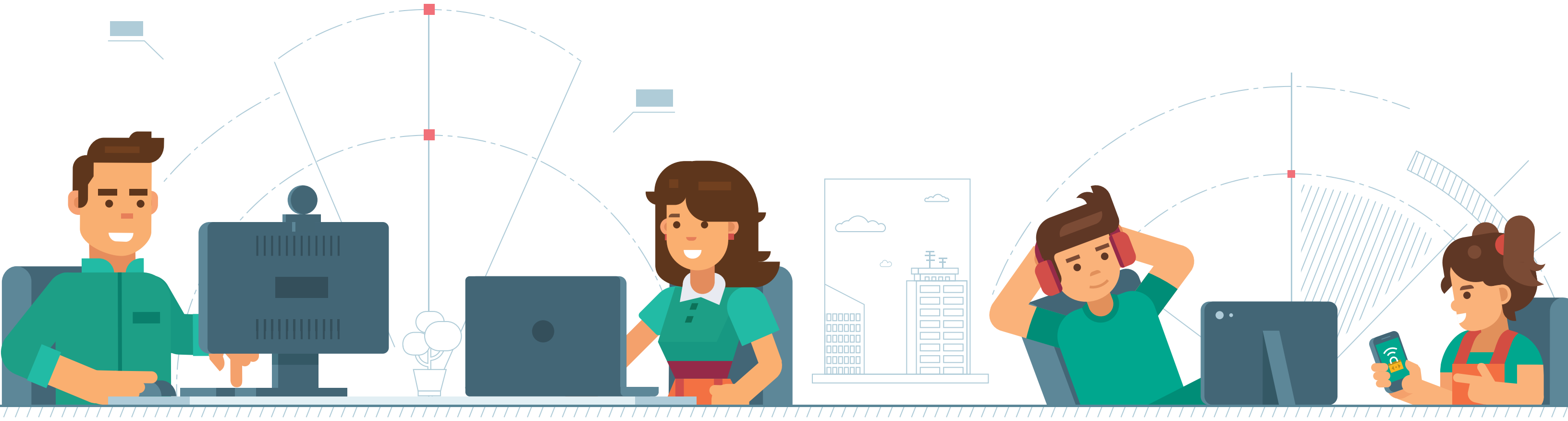
- Regularly take inventory of the applications that have permission to access data on your device or social networks, and delete apps or accounts that you no longer use.

✓ **Consider installing parental control software on your children's devices.**

- Combine software with other practical measures, such as keeping computers in family areas and educating children about potential cyberthreats, to keep kids safe online.

✓ **Pay attention to cybersecurity headlines in the news.**

- If a breach should happen at a company where you have data stored, the company should reach out and provide information regarding their remediation efforts and any next steps. As a customer, you can also contact the company directly yourself, in addition to checking your accounts to confirm if your data has been compromised.



About Kaspersky Lab

Kaspersky Lab is a global cybersecurity company, which has been operating in the market for over 20 years. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them. Learn more at www.kaspersky.com.

1. "2017 Annual Data Breach Year-End Review"
2. "New Kaspersky Password Manager Offers Secure Storage for Payment Data and Documents"
3. "Handbook for Safeguarding Sensitive Personally Identifiable Information"
4. "Definition: Personally identifiable information (PII)"
5. "Kaspersky Lab latest home solutions address security issues for the modern household"
6. "Businesses Beware: Holiday Season Revenues at Risk from DDoS and POS-Vulnerabilities"
7. "Kaspersky Lab Survey: Cyberattacks Cost Large Businesses in North America an Average of $1.3M"
8. "Connected Love: Privacy in Relationships and the Boundaries of Personal Space"

Learn more about cybersecurity: **www.securelist.com**

www.usa.kaspersky.com
#truecybersecurity

Kaspersky Lab, Inc.
500 Unicorn Park, 3rd Floor Woburn, MA 01801 USA
Tel: 866-563-3099 | Email: corporatesales@kaspersky.com