KASPERSKY lab

Cyber-Stress, Refreshed

A study on the causes and evolution of Americans' and Canadians' stressors relating to cybersecurity and personal data protection

Introduction

Stress is one of the most prevalent health issues facing society today. Especially in North America, people of all ages are harboring considerable stress in every aspect of their lives. The source of this stress can range from anything including personal pressure and family issues, to money problems and job challenges. One relatively new source of stress, however, is the anxiety that many people feel in relation to technology, including social media, device overload, and in particular, cybersecurity.

In May 2018, Kaspersky Lab released "The State of Cyber-Stress," a study examining the stress levels of consumers in the U.S. and Canada in regards to cybersecurity and data breaches. The research findings revealed a key trend: both Americans and Canadians were feeling unprecedented levels of stress about protecting their devices and personal data from online threats.

In fact, the vast majority of adults – 81 percent of Americans and 72 percent of Canadians – admitted that the news of data breaches caused them stress. With events such as the colossal Equifax data breach of 2017 likely weighing on many survey participants' minds, the study also found that stress levels rose among those who had recently experienced a cybersecurity incident affecting their personal data or devices. Overall, the study identified cyber-stress as a key issue for many consumers in North America, and furthermore, revealed that many people were lacking the proper knowledge and tools to feel secure in their digital lives.

One year later, Kaspersky Lab is revisiting the issue of cyber-stress to determine how consumers' attitudes may have changed over time. In this year's report, we measured how consumers' feelings of cyber-stress have changed, whether increased knowledge of the technology industry has any impact on stress levels, and how cyber-stress influences the way people behave online.

Key findings from the study include:

- In relation to cybersecurity, 75% of people surveyed said that the number of passwords they have to manage causes them stress, while 68% said news of data breaches is a source of stress.
- In the last year, more than one-in-four people (28%) said they were informed by a company, or noticed themselves, that their data had been compromised in a breach or cyberattack.
- Over half of respondents (52%) classified themselves as a 'beginner' or 'basic' in terms of cybersecurity knowledge, and an additional 11% said that they do not understand what cybersecurity is or how it could apply to them.
- For those who rated their knowledge of cybersecurity as 'expert,' 86% said that news of data breaches causes them stress, as opposed to only 44% of those that said they had no knowledge of cybersecurity.
- Over half of people surveyed (51%) would be willing to share their personal data with their significant other but just 11% would be willing to share their personal data with a digital password manager.
- Nearly a third (30%) of people use the same passwords for all or most of their online accounts.

Research Methodology

The quantitative study was conducted by research firm Opinion Matters, via an online survey in December 2018 of 2,567 adults (aged 16 or older) in the United States and Canada who go online.

Research Findings

The Stressful State of Cybersecurity

Cybersecurity has continued to climb the ranks as a trending news topic, with a number of major stories bringing the industry to the forefront of headlines around the world throughout the last year. News stories around Facebook privacy concerns, the massive Marriot data breach, the rollout of GDPR and more erupted throughout 2018, bringing continued attention to the role of data security and privacy in our society.

Kaspersky Lab's survey found that consumers are continuing to recognize cybersecurity as an important topic in their daily lives. The research found that 68 percent of people in the U.S. and Canada said that in relation to cybersecurity, news of data breaches causes them stress. Furthermore, three-quarters of people (75%) said that they are stressed by the number of passwords they have to manage. These statistics demonstrate that consumers are taking note of news stories around data breaches, cyberattacks and password management, and are reacting with concern.

Notably, consumers' current stress levels regarding data breaches are slightly lower than observed in Kaspersky Lab's May 2018 report on "The State of Cyber-Stress," which found that 76 percent of people were stressed by news of data breaches. One plausible explanation for this discrepancy is the sheer number and size of breaches that were reported in 2017 – a record-high year for data breaches, with 1,579 total incidents. Comparatively, 2018 saw a slight decrease in data breaches, with 1,244 in total.[1]

This year's survey found that cyber-stress is more than just a hypothetical; many consumers have faced a cybersecurity incident in their personal lives. These incidents are extremely stressful, and in fact, are one of the most anxiety-provoking scenarios that a person can face today. When presented with a variety of common stressful scenarios, two-thirds of respondents (66%) ranked having their bank account compromised, which can happen due to fraud or a breach, as one of the top stress-inducing incidents. A bank account compromise ranked as more stressful than losing a job (chosen by 46 percent of people) or being in a minor car accident (chosen by 20 percent of people).

Overall, these results draw a key conclusion: cybersecurity-related stress and anxiety is as prevalent as ever, and shows no signs of slowing down. While reviewing some of the factors that influence stress levels for different groups, some patterns emerged that may help provide a resolution for what we can do to combat cyber-stress.

What's causing our stress?

Why are Americans and Canadians so severely stressed about cybersecurity? While frequent news of data breaches and cyberattacks is certainly a factor, we looked deeper into the survey data to discover what influences certain groups to be at a higher risk of experiencing cyber-stress.

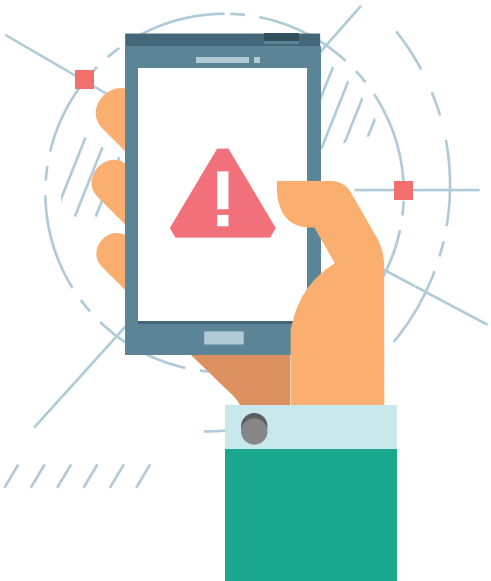
First, it is evident that people in North America are putting a lot of personal stake in technology. Over three quarters of respondents to Kaspersky Lab's survey (76%) agreed that they are very reliant on technology in their personal lives. This comes as no surprise, with recent research finding that Americans check their smartphones 52 times a day on average[2]. Today, the vast majority of people have no problem using their phone at work, while out shopping, when watching TV, during conversations with family and friends, or even when eating at a restaurant.

52%

said that they would class themselves as a 'beginner' or 'basic' in terms of their understanding of cybersecurity.

Despite this strong dependency on technology, many consumers still do not feel that they have a solid understanding of the intricacies of their phones, computers and other digital devices. Especially when it comes to cybersecurity, there still seems to be a significant gap between how often consumers use their devices, and how much they know about the dangers to which these devices can expose them. In Kaspersky Lab's survey, less than a quarter of respondents (23%) said that they had a formal education in an IT discipline. Furthermore, over half of respondents (52%) said that they would class themselves as a 'beginner' or 'basic' in terms of their understanding of cybersecurity.

Even more worrisome, a small cohort of people appear to be falling substantially behind the standard learning curve. When asked about their level of cybersecurity knowledge, one-in-ten respondents (11%) said that they do not understand what cybersecurity is or how it could apply to them.



Unfortunately, cyber-threats are now a reality for everyone, regardless of knowledge level. In the last year, 34 percent of Americans and 23 percent of Canadians have been informed by a company, or noticed themselves, that their data was compromised in a breach or cyberattack. These numbers are only expected to rise, as companies struggle to catch up with the pace of technology.

How do the experts feel?

Cyberattacks don't discriminate. Even some of the world's most knowledgeable cybersecurity experts have become the victim of a data breach or faced a cyberattack. For those who consider themselves to be in the top tier of cybersecurity expertise, we wanted to examine how cyber-incidents make them feel. Are they worried about the security of their personal data, or do they feel at ease when it comes to cybersecurity, knowing that they have the tools and knowledge to protect themselves in the face of a cyberattack?

Interestingly, Kaspersky Lab's research showed a reverse correlation between cyber-stress and level of cybersecurity expertise. Of those who self-identified as cybersecurity experts, 86 percent said that news of data breaches caused them stress. Conversely, for people who said that they had no knowledge of cybersecurity, just 44 percent were stressed by news of data breaches. Furthermore, over half of respondents (55%) who classed their knowledge of cybersecurity as expert completely agree that being faced with a data breach or cyberattack is inevitable. Only 14 percent of respondents with no cybersecurity knowledge believe this to be true.

"My concern about data breaches is less about a specific incident, and more focused on the fact that data breaches are now routine in a world where many people use the same login credentials across multiple sites, leaving all their accounts exposed through a single breach," said David Emm, principal security researcher, Kaspersky Lab Global Research and Analysis Team. "As you would expect, I take steps to secure the devices I use, secure my online accounts and avoid behavior that puts me at risk. But some things are out of my control – I can't do anything to ensure that an online provider takes effective measures to secure my data."

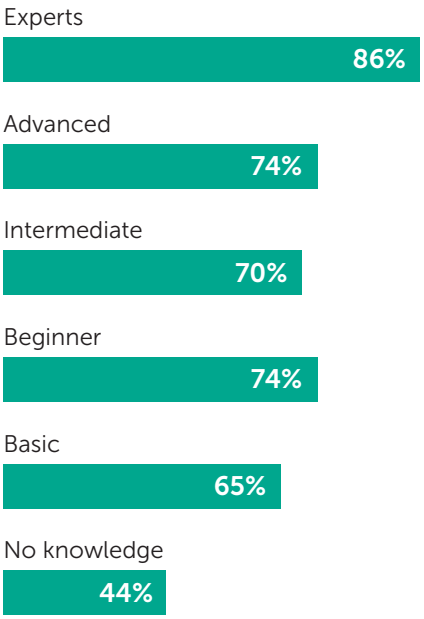
"My concern about data breaches is less about a specific incident, and more focused on the fact that data breaches are now routine in a world where many people use the same login credentials across multiple sites, leaving all their accounts exposed through a single breach."

- **David Emm**, principal security researcher, Kaspersky Lab Global Research and Analysis Team

The survey found that experts are also more likely to notice when their own personal data has been compromised. Two-third of experts (67%) said that they are aware that their data was compromised in a breach or cyberattack in the last year. However, only 20 percent of people with basic cybersecurity understanding said that their data was breached within the last year. Once again: cyberattacks don't discriminate, and it's unlikely that experts are actually being breached more often. This difference is likely due to experts being more aware of cybersecurity issues, and therefore, paying attention to when their data is at risk. If consumers do not notice indicators of a breach, or if they are not tuned in to cybersecurity news, they may never even realize that their data is no longer secure.

"The brain is hardwired with a sensitivity to perceived threats in our environment," said Heidi Hanna, Ph.D., executive director of the American Institute of Stress "When we work in an industry or situation where we have to be constantly focused on real or potential danger, we can become hypersensitive to stress. Over time, this can contribute to breakdown and burnout."

Who is stressed out by data breach news?
(By level of cybersecurity expertise)



How cyber-stress impacts our actions

People react to stress with a variety of different emotions, ranging from anxiety to anger to distrust. These responses can also vary widely based on the specific stressor. So, what are the most common psychological responses to cyber-stress, and how is it impacting the way that people interact with technology?

Generally, as cyber-stress becomes more widespread, many people seem unsure of whom to trust with their personal data. Many seem skeptical of relying on technology to keep their data safe. In Kaspersky Lab's research, just 11 percent of survey respondents said that they would be willing to share their personal data with a password manager program. Cybersecurity experts are slightly more trusting of this specific technology, with 26 percent responding that would share their data with a password manager. As a comparison, more than half of respondents (51%) said that they would be willing to share their personal data with a significant other.

There also seems to be a high level of concern, particularly among Americans, about sharing personal data with the government. Just 13 percent of U.S. respondents said that they would be willing to share their data with the government. In Canada, this number rises to 30 percent – still, a relatively small percentage.

Unfortunately, it does not appear that stress around data security has led the majority of people to improve their personal cybersecurity habits. For example, nearly a third of respondents (30%) said that they use the same passwords for all or most of their online accounts. This is an especially bad habit among Gen Z; for those aged 16 to 24, this rises to 44 percent who use the same password for all or most of their accounts. Even those who consider themselves to be cybersecurity experts are not making smart security choices. Fifty-one percent of experts said that they use the same passwords for all or most online accounts, significantly higher than the general average.

Re-use is widely known to be one of the most risky password behaviors. It can put users at risk for credential-stuffing attacks. Credential-stuffing has been to blame for many notable security incidents of late, impacting well-known brands like Reddit, Dunkin Donuts and HSBC.

What is Credential-Stuffing?

Credential-stuffing is when attackers use unencrypted username and password combinations that have previously been leaked in a breach to try and hack into accounts that may use the same login information. Re-using usernames and passwords across multiple online accounts can put users at risk of having their data breached through this attack method.

Although a number of people admit to poor security practices, such as password re-use or forgoing a PIN on their device, the majority still fail to see the error of their own ways. Nearly three-quarters of people (73%) completely or somewhat agree that they have good cybersecurity habits. However, this false sense of security may lead some groups to adopt a lax attitude towards proactive protection. Less than a quarter of people use a security solution on all their devices, including just 17 percent of Generation Z.

A number of statistics revealed further evidence of a disconnect between people's perceived security knowledge and their actions. For example, the survey showed a significant level of confusion about what to do after a data breach. The largest percentage of respondents (51%) said that if they faced a breach, they would change the password for all of their accounts – not just the account that was impacted. However, responses to this question varied widely; some said they would await instructions from the organization responsible, while others would contact a knowledgeable friend or family member, alert the authorities or deactivate the breached account.

Facing our cyber-stress: The good and the bad

It is clear that cybersecurity experts and beginners alike are all experiencing significant levels of stress about data breaches, password management and other IT security topics. However, while stress often has a negative connotation, cyber-stress in itself is not necessarily a bad thing. In fact, some amount of stress can actually be beneficial for a healthy life.

"Good stress," known as eustress, can help motivate, build resilience, and encourage growth, according to psychologists[3]. In regards to cyber-stress, this means that those who have a healthy level of stress about cybersecurity are more likely to take steps to protect their devices and data.

"People still tend to assume that stress is bad for us, when it is actually intended to help us fuel positive change," said Heidi Hanna, Ph.D., executive director of the American Institute of Stress. "This study reinforces that fact by demonstrating what happens when we have just enough stress or focused attention on something that matters to us, but not so much that we feel overwhelmed or out of control. Stress is good at showing us what we care about – if we didn't care, we wouldn't feel stressed. As long as we use the energy and information that stress provides to take positive action, like educating and empowering ourselves, stress is our friend instead of our enemy."

However, once cyber-stress rises to a certain level, the negative effects start to outweigh the positive. Security experts appear to be the group most likely to experience unhealthy levels of cyber-stress, with 86 percent reporting that they feel stressed by news of data breaches, and more than half believing that facing a cyber-threat is inevitable. As they feel more pessimistic about cybersecurity, these experts seem to be failing to take the basic precautions to protect themselves from threats, such as using secure passwords.

"I think it's important to adopt a mindset of 'informed paranoia' in everything, from not automatically holding doors open at the office for those I don't know, or locking my computer when leaving my desk, to using strong passwords and securing confidential data," said David Emm, principal security researcher, Kaspersky Lab Global Research and Analysis Team. "I find that it's best to approach security like housework – it's not a one-time transaction, but rather an ongoing process."

"People still tend to assume that stress is bad for us, when it is actually intended to help us fuel positive change. As long as we use the energy and information that stress provides to take positive action, like educating and empowering ourselves, stress is our friend instead of our enemy."

- **Heidi Hanna, Ph.D.,** executive director of the American Institute of Stress

Key Takeaways

By taking simple steps to have a stronger personal level of cybersecurity, consumers at each stage of the knowledge spectrum can keep their cyber-stress manageable and healthy. Here are a few of Kaspersky Lab's top tips for proactively maintaining a secure lifestyle, to avoid becoming over-burdened with cyber-stress:

- ✓ **Use strong passwords that are unique for every account.** Find a system that works for you, which will help you to come up with a different secure password for every online account. This could be storing login information in a password manager, or using a word association technique like the one recommended by Kaspersky Lab experts for creating passphrases.
- ✓ **Secure your device with a PIN or password.** A surprising number of people do not lock down their smartphones with a simple PIN or password. This can help to protect your personal information from outsiders if your device is lost or stolen.
- ✓ **Use a VPN when connecting to public Wi-Fi.** A VPN can encrypt all data sent over public Wi-Fi, ensuring that third parties cannot view or intercept your personal information. For those that are often using devices on the go, in airports, coffee shops or hotels, a VPN is a must-have.
- ✓ **Consider a security solution that can protect your personal data.** Less than a quarter of people (24%) use a security solution on all of their devices. Reliable security software can protect you from malware, ransomware, phishing, spam and more, while also offering features that can enhance your online life, like a password manager and parental control components.
- ✓ **Learn about cybersecurity and online privacy.** Ignorance may be bliss, but more knowledge of cybersecurity threats and best practices will help you reduce the impact of a breach or cyberattack if you face one in the future. Here are some resources that can help you get started:
  - National Cyber Security Alliance: https://staysafeonline.org/stay-safe-online
  - InfoSec Institute: https://resources.infosecinstitute.com
  - FTC Consumer Information: https://www.consumer.ftc.gov
  - Kaspersky Daily Blog: https://www.kaspersky.com/blog
  - Kaspersky Resource Center: https://usa.kaspersky.com/resource-center

The best kind of cyber-stress is that which encourages action. Paying attention to cybersecurity news and understanding the real dangers posed by today's cyber-threats is essential for staying protected. Being at either end of the cyber-stress spectrum – either lacking any level of stress whatsoever, or being overwhelmingly aware of cybersecurity issues – is not conducive to positive action. Overall, a healthy level of concern about data breaches, cybersecurity and privacy can help motivate people to take the right steps towards having a more secure online presence.

About Kaspersky Lab

Kaspersky Lab is a global cybersecurity company, which has been operating in the market for over 21 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. The Identify Theft Resource Center, "2018 End-of-Year Data Breach Report"
2. Deloitte, "Global mobile consumer survey"
3. *TIME Magazine*, "How Some Stress Can Actually Be Good for You"

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

usa.kaspersky.com
#truecybersecurity

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