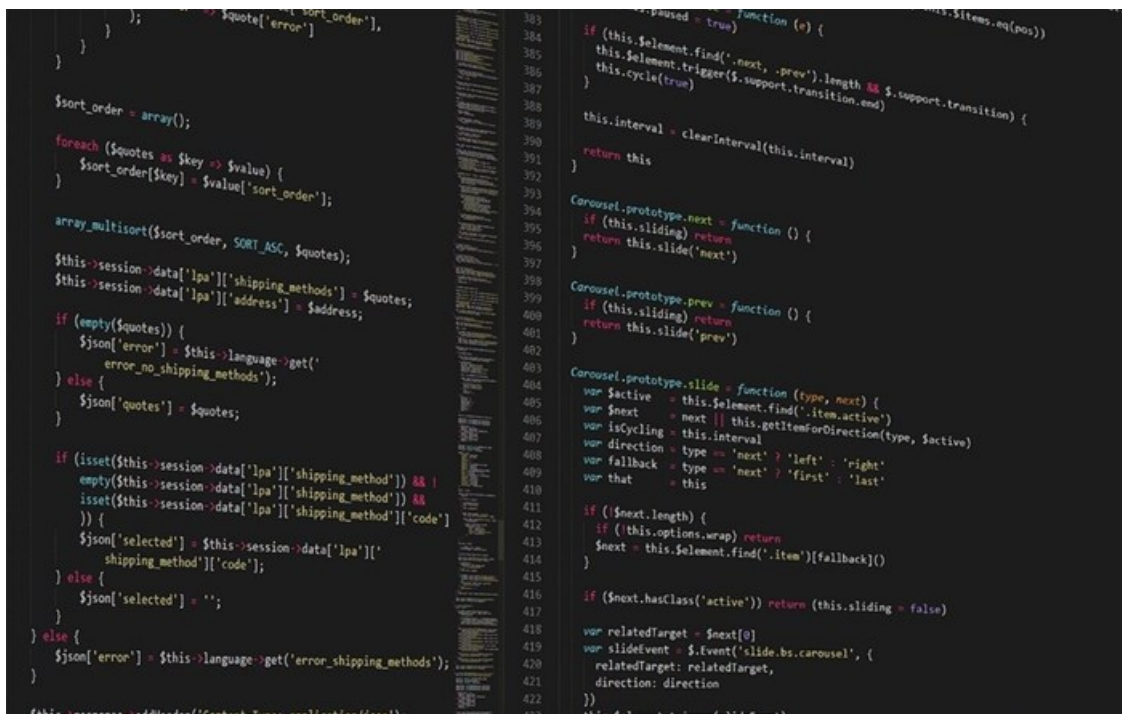# Study shows people and organisations don't fully trust anyone with their online data

From cybercriminals to their own government, employers and even family, people worry about who could access their online life.

A new study of mid-size businesses and consumers reveals that many are confused and lack trust when it comes to the privacy and security of their online data and behaviour. The research, which covered six countries in Europe and North America, found that people worry that hackers, their own and foreign governments, employers and even friends and family might want to access their online data, and how to stop them.

The independent study, commissioned by Kaspersky Lab with the data analysis undertaken by Applied Marketing Research, surveyed 600 mid-sized companies with IT security professionals as well as 6,000 consumers with security software installed on their devices, split equally across France, Germany, Italy, Spain, the UK and the US.

Source: pixabay.com

The top unwelcome intruders were, not surprisingly, cybercriminals, with 45% of businesses and 47% of consumers worried about protecting their online data from malicious attack. But this is followed closely by wanting to protect it from their own government (36% and 33% respectively), and foreign governments and companies (30% and 26%). As many as one in three (29%) business respondents have concerns about their employer getting to their online data, while a quarter (26%) of consumers worry about their family snooping.

Concerns and fear

These concerns extended to cybersecurity, where there was widespread confusion about the information cybersecurity providers could access. Many respondents worry that their provider might gather their online data, opinions, location or browsing habits and then share this information with foreign entities. However, the vast majority (87% of businesses and 82% of consumers) trust their security provider to behave ethically in the collection and use of their data.

These results suggest that the current cybersecurity landscape has created for both businesses and consumers an environment of fear, uncertainty and doubt that has left many struggling to trust anyone at all online.

click to enlarge

Commenting on these findings, Anton Shingarev, VP of public affairs at Kaspersky Lab, said, "These research results are indeed amazing. They provide further evidence that technologies and software are a black box for many companies. They don't know how they work, what's inside, what data is collected or how it's stored. As a result, they don't trust vendors. I believe this to be unacceptable, and, as an industry, we need to ensure that people understand exactly what we do and what kind of things a security provider would never do. "

"This should be accompanied by an ongoing commitment to building resilience and security into our products, and to proving their trustworthiness through transparency and accountability. All this is embedded in our Global Transparency Initiative, a program designed to help rebuild trust in information security."

Key findings

Other findings of the research include:

- Privacy appears to be considered a fundamental right for everyone: 46% of businesses and 51% of consumers believe a cybersecurity provider should not automatically have to share a user's private data with the government in matters of national security, but that it should depend on the circumstances.

- The research also suggests that other things matter more to business and consumers than a company's country of origin: 55% of businesses and 66% of consumers say their government should do business with the company that offers the highest quality products or services, even if it is a foreign company. Surprisingly, this rises to 82% and78% respectively when it concerns areas crucial to national security.

Commenting on the findings, Dr. Milton Mueller, a professor at Georgia Institute of Technology School of Public Policy, Internet Governance Project, added, "This survey addresses the nexus between nationalism, national security and trust in internet service providers. There are surprising findings regarding consumer and business attitudes towards the role of governments in cybersecurity.

For example, it was fascinating to see how many consumers believe that their government should use the best vendor for national security-related capabilities regardless of what country it is from. It was also interesting to see that consumers are more likely to fear their data will be interfered with by their own government than foreign governments."

For more, visit: https://www.bizcommunity.com