Beat: News

LACK OF SECURITY INCREASINGLY FUELING INTERNET DISTRUST

SURVEY: CYBER CRIMINALS, SOCIAL MEDIA

Waterloo, Canada, 11.06.2019, 21:52 Time

USPA NEWS - Waterloo, Canada, 11 June 2019 - In a new survey of internet users around the globe, social media companies emerged as the leading source of user distrust in the internet "" surpassed only by cyber criminals "" with 75% of those surveyed who distrust the internet citing Facebook, Twitter and other social media platforms as contributing to their lack of trust.

While cyber criminals, cited by 81% of those who distrust the internet, remained the leading source of distrust, a majority in all regions (62% globally) indicated that a lack of internet security was also a critical factor.

These and other findings were released today as part of the 2019 CIGI-Ipsos Global Survey on Internet Security and Trust, conducted by Ipsos on behalf of the Centre for International Governance Innovation (CIGI), in partnership with the Internet Society (ISOC) and the United Nations Conference on Trade and Development (UNCTAD).

The CIGI-Ipsos Global Survey, now in its fifth year, is the world´s largest and most comprehensive survey of internet security and trust, involving more than 25,000 internet users in over two dozen countries across North America, Latin America, Europe, the Middle East, Africa and the Asia-Pacific region.

"This year´s survey of global attitudes not only underscores the fragility of the internet, but also netizens´ growing discomfort with social media and the power these corporations wield over their daily lives,"🄯 said Fen Osler Hampson, a distinguished fellow at CIGI and director of its Global Security & Politics program.

In terms of the effects of user distrust, nearly half (49%) of those surveyed who distrust the internet said their distrust had caused them to disclose less personal information online, while 40% reported taking greater care to secure their devices and 39% said they were using the internet more selectively. Conversely, only a small percentage of people reported making use of more sophisticated tools "" such as using more encryption (19%) or using technical tools like Tor (The Onion Router) or virtual private networks (VPNs) (12%) "" to protect themselves online.

"The survey results tell us that people around the world are increasingly concerned about their privacy and security online,"🄯 said Sally Wentworth, vice president of Global Policy Development for the Internet Society. "However, we also see that users aren´t utilizing tools like encryption that can help secure their communications. From keeping messages private to protecting critical infrastructure, encryption is an essential tool for digital security. It´s clear that there is more we can be doing as a community to make it easier for Internet users to secure their communications."🄯

In addition, a digital divide was evident between the world´s developed and developing economies when it came to cryptocurrencies and other new internet frontiers, with those surveyed in Latin America and the BRICS (Brazil, Russia, India, China, South Africa) nearly four times as likely to use or purchase cryptocurrencies within the next year as those in North America, Europe and the G-8.

"Knowledge is power. It´s also a datapoint,"🄯 said Shamika N. Sirimanne, director of UNCTAD´s Division on Technology and Logistics. "The CIGI-Ipsos Survey provides us with compelling evidence to help make decisions, shape policy and channel resources to reduce the digital divide in a way that is safe and still creates opportunities for development. We need more trust if the digital economy is to become a viable development tool for developing nations."🄯

Additional highlights of the 2019 CIGI-Ipsos Global Survey include:

Eight out of 10 (78%) people surveyed are concerned about their online privacy, with over half (53%) more concerned than they were a year ago, marking the fifth year in a row that a majority of those surveyed say they feel more concerned about their online privacy than the previous year.
Fewer than half (48%) believe their government does enough to safeguard their online data and personal information, with the lowest confidence levels in North America (38%) and the G-8 countries (39%).

Citizens around the world are increasingly viewing their own governments as a threat to their privacy online. In fact, more people attributed their growing online privacy concerns to domestic governments (66%) "" a majority in nearly every region surveyed "" than to foreign governments (61%).

While 73% said they wanted their online data and personal information to be stored in their own country, majorities in Hong Kong (62%), Indonesia (58%), Egypt (58%), India (57%), Brazil (54%), and Mexico (51%) said they wanted their online data and personal information stored outside of their country. In contrast, only 23% of North Americans, 35% of Europeans and 32% of those in G-8 countries shared this sentiment.

Less than half of global citizens express at least some degree of confidence that any of the algorithms they use are unbiased, in any context. Confidence was highest in algorithms used for facial recognition systems (47%) and search engines (46%), and lowest in algorithms used for social media news feeds (32%) and predictive policing (34%).

The most common reasons for a lack of confidence in the unbiasedness of algorithms were a lack of transparency, a perception that they are exploitative by design and the absence of a human element from decision-making. By contrast, objectivity, a lack of human emotion to cloud decision-making and the absence of human influence were most frequently mentioned by those who expressed confidence in the unbiasedness of algorithms.

86% said they had fallen for fake news at least once, with 44% saying they sometimes or frequently did. Only 14% said they had "never" been duped by fake news.

Facebook was the most commonly cited source of fake news, with 77% of Facebook users saying they had personally seen fake news there, followed by 62% of Twitter users and 74% of social media users in general.

10% of Twitter users said they had closed their Twitter account in the past year as a direct result of fake news, while 9% of Facebook users reported doing the same.

One-third (35%) pointed to the United States as the country most responsible for the disruptive effect of fake news in their country, trailed significantly by Russia (12%) and China (9%). Notably, internet users in Canada (59%), Turkey (59%) and the United States itself (57%) were most likely to say that the United States is most responsible for the disruptive effect of fake news in their own country, while users in Great Britain (40%) and Poland (35%) were most likely to point to Russia, and users in Hong Kong (39%), Japan (38%) and India (29%) were most likely to blame China.

A majority of internet users around the globe support all efforts by governments and internet companies to combat fake news, from social media and video sharing platforms deleting fake news posts and videos (85%) and accounts (84%) to the adoption of automated approaches to content removal (79%) and government censorship of online content (61%).

Nearly seven in 10 people familiar with blockchain technology believe that it will affect every sector of the economy (68%), that it should be implemented as widely as possible (67%), and that it will have an impact equivalent to the advent of the internet (67%).

One in 10 (12%) admit to accessing the Dark Web, with higher percentages in India (26%), Russia (22%) and Brazil (21%). Two-thirds (66%) of global citizens "" a majority in every country surveyed "" believe that the Dark Web should be shut down. However, this number is down from 71% in 2016.

The 2019 CIGI-Ipsos Global Survey was conducted between December 21, 2018, and February 10, 2019, and involved 25,229 internet users in Australia, Brazil, Canada, China, Egypt, France, Germany, Great Britain, Hong Kong (China), India, Indonesia, Italy, Japan, Kenya, Mexico, Nigeria, Pakistan, Poland, Russia, South Africa, Republic of Korea, Sweden, Tunisia, Turkey and the United States.

Exemption from liability:

Editorial program service of General News Agency: