U.S. Cyber Risk Report Highlights Need for Cyber Resilience and Security Education

April 16, 2020

Annual report underlines the need to improve cybersecurity education during the peak of remote work

WATERLOO, Ontario, April 16, 2020 /PRNewswire/ -- OpenText™ (NASDAQ: OTEX) (TSX: OTEX) released Webroot's fourth annual report on consumer security behavior across the U.S. The report, "A Look at 2020's Most (And Least) Cyber-Secure States" sheds light on the continued need for greater security awareness education nationwide.

"The global COVID-19 pandemic has increased the importance of good cyber resilience habits," said Mark J. Barrenechea, OpenText CEO & CTO. "Our threat Intelligence platform has tracked cybercriminals that create malicous websites mentioning COVID and coronavirus, insert malware into popular video conferencing tools and test users every day with phishing attacks. Both businesses and individuals need to learn about these threats, work with their technology partners and take steps to increase their cyber resilience."

At a time when more people are working remotely than ever before, the report highlights the need to adopt cybersecurity best practices. While most citizens believe they are taking appropriate steps to protect themselves online, almost half (49%) of Americans still use the same password across multiple accounts and only 37% keep their social medial accounts private.

"This is the fourth consecutive year we've seen the same high levels of consumer misunderstanding and general overconfidence when it comes to cybersecurity practices and safety," said Webroot security analyst Tyler Moffitt. "In fact, only 11% of Americans scored an 'A' grade on our index, and no state scored above a 'D'. The need for better cyber hygiene and security education is clear, especially as more Americans work from home."

In order to stay cyber resilient during the pandemic, there are some basic guidelines to follow:

1. Protect devices with antivirus and a VPN
2. Keep antivirus software and other apps up to date
3. Use a secure backup program
4. Create strong, unique passwords (and don't share them) or use a password manager
5. Be extra cautious with links – hover over them to check the full URL or type the website directly into the browser

Explore the full report here.

Read OpenText's response to the COVID-19 pandemic here.

Notable Report Findings:

Almost all (89%) Americans say they're taking appropriate steps to protect themselves online, but there is a general lack of understanding when it comes to cybersecurity.

- Few Americans practice all key benchmark metrics (including using anti-virus software, backing up data and keeping social media profiles private) needed to protect themselves from cyberattacks – the average American scored a 58% on our index (an "F" grade) and only 11% scored 90% or higher (an "A" grade).
- A majority of Americans say they are familiar with malware (78%) and phishing scams (68%), but only about a third feel confident they can explain what malware or phishing is.
- 83% of Americans use anti-virus software and regularly back up their data (80%), but only half know if their backup is encrypted and only 18% back up their data online and offline.
- Almost half (49%) of Americans use the same password across multiple accounts and only 37% keep their social medial accounts private.

Over three-quarters (78%) of Americans who have had their identity stolen have made changes to their online behavior as a result.

- Those who have had their identity stolen are more likely than those who have not to:
- Regularly monitor bank accounts (31% vs. 22%)
- Regularly monitor credit card statements (26% vs. 16%)
- Keep software up to date (26% vs. 16%)
- Regularly check credit reports (25% vs. 15%).
- 73% of employed Americans who have had their identity stolen have looked into the security of their work devices, while 59% of those who have not say the same thing.

Over half (55%) of Americans routinely use their employer-provided work device for personal use.

- 38% consider an employer-provided work device to be their "primary" device for use at home.
- Almost half (48%) have never looked into the security of their work devices, and only a third have taken any steps to improve its security.
- Roughly a quarter (26%) believe their personal devices are more secure than their work devices.

Additional Resources:

- Staying Cyber Resilient During a Pandemic
- Beware of Coronavirus Scams
- 5 Tips for Feeling Your Best in Your Home Office
- Video: 2020's Most (and Least) Cyber-Secure States

About the Survey
Webroot, an OpenText Company, partnered with Wakefield Research to conduct the Webroot 2020 Look into The Most (and Least) Cyber-Secure States survey, which provides insight into the consumer outlook on cyber hygiene. The survey reached 10,000 United States consumers, 200 from each state, and Webroot used the collected data to create a Cyber Hygiene Risk Index. The Cyber Hygiene Risk Index then provided the ability to assess the risks associated with susceptibility to cybercrime in each state, ranking the states to determine the riskiest and least risky states in the United States.

The Webroot® Platform harnesses the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide endpoint protection, network protection, and security awareness training solutions purpose built for managed service providers and small businesses. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals. Learn more at www.webroot.com.

About OpenText
OpenText, The Information Company™, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit opentext.com.

Connect with us:
OpenText CEO Mark Barrenechea's blog
Twitter | LinkedIn

OTEX-G

View original content to download multimedia:http://www.prnewswire.com/news-releases/us-cyber-risk-report-highlights-need-for-cyber-resilience-and-security-education-301041853.html

SOURCE Open Text Corporation

Ashley Stewart, OpenText, 402-910-0140, publicrelations@opentext.com