October 16, 2019

American Consumers Recognize Their Role in Preventing Cybercrime, are Bothered by Perceived Inconveniences of Advanced Security

55% of consumers understand they need to do more to protect their personal data; but 59% are bothered by temporary inconveniences of advanced security measures

Only 45% of consumers have received formal cybersecurity training from their employer

BROOKFIELD, Wis.--(BUSINESS WIRE)-- According to the 2019 Cybersecurity Awareness Insights Study released today by Fiserv, most Americans consider themselves at least somewhat informed of cybersecurity threats, yet many fall short at proactively protecting their personal data. Despite this lack of action, more than half (55%) of American consumers understand they need to do more to protect their data, presenting significant opportunity for businesses to reinforce best practices.

Conducted in the summer of 2019 and originally commissioned by First Data, now Fiserv, the study gathered insights from 1,005 Americans ages 18 to 73. The study explores how aware American consumers are of online privacy and security risks, and how they behave when it comes to protecting themselves from cyber threats.

“While cybercrime continues to grab headlines, our study shows that many Americans have not taken action to protect themselves, and the majority say they are bothered by temporary inconveniences brought about by advanced security measures,” said Jay Ablian, Head of Merchant Security and Fraud Solutions, Fiserv. “There is a clear opportunity for businesses to educate consumers and employees to help them understand both the potential impact of inaction and how security measures are designed to protect them.”

Consumer Awareness

The more consumers know, the better they’re able to protect their personal information online. According to the 2019 Cybersecurity Awareness Insights Study, 75% of consumers consider themselves at least somewhat informed of cybersecurity threats. In addition, 55% of respondents understand they should do more to beef up their online security – especially when using social media, online banking, or online shopping.

Despite this, more than half of consumers can be classified as ambivalent, in denial, or oblivious to cybersecurity risks, with only 6% currently taking the steps needed to proactively protect themselves.

Consumer inaction may be driven by perceived inconveniences. To that end, 59% of consumers report they are bothered by temporary inconveniences brought about by advanced security measures that help ensure higher levels of protection.

Consumer Behavior and Data Protection

Although many consumers consider extra cybersecurity precautions a hassle, they are taking some steps to protect themselves. According to the study, dodging inbound phishing attempts is a strong suit of consumers, but additional vigilance around password security is needed:

- The top measure consumers take to protect themselves is refusing to click email links or open attachments from people they don't know, cited by 61% of consumers
- On the other hand, changing passwords is a cybersecurity step 42% of consumers take only if they are required to
- Of consumers surveyed, 33% have a go-to password they modify slightly to meet password requirements, and 20% use names of significant people, places or pets. Neither of these methods is considered a best practice.

Cybersecurity Awareness at Work

Consumers often look to their employer to provide cybersecurity training, but aren't always getting the support they expect. Fifty-eight percent of consumers said their employer sends regular cybersecurity updates, and 45% said their employer offers formal cybersecurity training. Of consumers who aren't provided cybersecurity training, only 9% said their employer has a plan in place to do so.

Employers have a vested interest in cybersecurity awareness, as educated employees can secure their own information and that of the business. Best practices for employers launching their own cybersecurity training include:

- **Emphasize education at work –** Ongoing education about new cybersecurity threats equips employees to recognize them and understand potential implications
- **Encourage lockdown at home –** Employees can secure their home networks, starting with changing all default passwords – especially for internet routers. Those with families can teach children about the dangers of cybercrime
- **Keep information out of the public eye –** Whether on personal or business computers, covering up screens when entering passwords and credentials in public areas helps keep information safe.

Additional Resources

- 2019 Cybersecurity Awareness Insights Study Infographic

About Fiserv

Fiserv, Inc. (NASDAQ: FISV) aspires to move money and information in a way that moves the world. As a global leader in payments and financial technology, the company helps clients achieve best-in-class results through a commitment to innovation and excellence in areas including account processing and digital banking solutions; card issuer processing and network services; payments; e-commerce; merchant acquiring and processing; and the Clover® cloud-based point-of-sale solution. Fiserv is a member of the S&P 500® Index and

the FORTUNE®500 and is among the FORTUNE Magazine World's Most Admired Companies®. Visit fiserv.com and follow on social media for more information and the latest company news.

FISV-G

View source version on businesswire.com:
https://www.businesswire.com/news/home/20191016005304/en/

Media Relations:
Chase Wallace
Director, Communications
Fiserv, Inc.
+1 404-890-2132
chase.wallace@fiserv.com

Additional Contact:
Ann Cave
Director, External Communications
Fiserv, Inc.
+1 678-325-9435
ann.cave@fiserv.com

Source: Fiserv, Inc.