Consumers' Awareness, Behavior and Concerns Around Cybersecurity

How to heighten cybersecurity awareness and protect against cybercriminals who never sleep

Based on the Fiserv 2019 Cybersecurity Awareness Insights Study

First Data is now fiserv.

Table of Contents

About the Insights Study

Fiserv's 2019 Cybersecurity Awareness Insights Study explores how aware American consumers are of online privacy and security risks, and how they behave when it comes to protecting themselves from cyberthreats.

We polled 1,005 U.S. adult consumers ages 18 to 73, all of whom are employed in industries including Education, Manufacturing, Retail, Healthcare & Pharmaceuticals and Information Technology. There was an even number of male and female respondents.

INTRODUCTION

On Your Guard

Consider the following: Nearly every electronic device can be hacked. A new cyberattack occurs every 39 seconds.[1] And by 2024, business losses to cybercrime are expected to exceed $5 trillion – an increase of nearly 70 percent over the next five years.[2]

Yet, a surprising number of U.S. consumers have little awareness of how to defend themselves against a cyberattack. Some never change their passwords and when they do, it's only because they're forced. What's more, many believe neither their employers nor the government do enough to sufficiently protect them from cyberthreats.

The following pages explore U.S. consumers' awareness, attitudes and actions around defending themselves from cyberattack.

1 Security magazine
2 Juniper Research

Presenting Our Cybersecurity Personas

Based on our research, we determined that consumers fall into five broad personality types when it comes to how well they understand cybercrime and how much effort they make to protect themselves.

Some of these individuals flat-out refuse to use a password-protected public Wi-Fi network for sensitive tasks, while others throw caution to the wind, unknowingly putting themselves at risk. Interestingly, more than one-fourth of our respondents would consider being micro-chipped to ensure the ultimate cybersecurity. How about you? In which one of the following groups do you belong?

MEET THE PERSONAS

1% Oblivious Olivia

11% Denial Dan

44% Ambivalent Andy

38% Trying Terri

6% Meticulous Mike

LET US INTRODUCE YOU TO...

OBLIVIOUS OLIVIA: Olivia knows little to nothing about cybersecurity and the risks cybercrime poses. As such, she neither protects herself from it as she doesn't know how, nor does she understand the importance of cybersecurity.

DENIAL DAN: Dan is somewhat aware of the risks of cybercrime but isn't acting to protect himself – perhaps because he thinks, "There's no way that would happen to me."

AMBIVALENT ANDY: Andy is a neutral middle-ground. Although he is aware that cybercrime is a real threat and will protect himself against it when convenient, he isn't worried enough to go out of his way to keep his data safe.

TRYING TERRI: Terri recognizes the dangers of cybercrime and actively wants to protect herself. However, she may not have all the information to stay above cyber threats, but is working to improve.

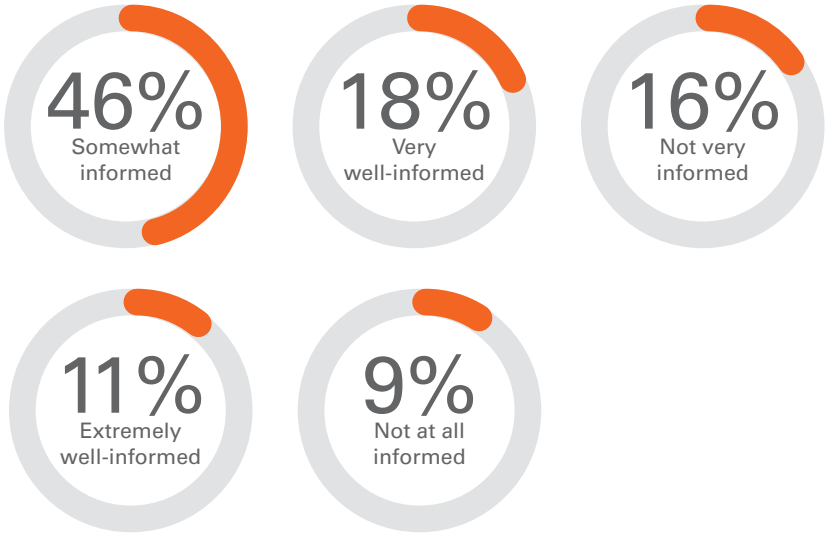
METICULOUS MIKE: Mike recognizes the dangers of cybercrime and has taken the initiative and extra steps to stay educated so he can protect himself effectively.

Consumer Awareness

The saying “Knowledge is Power” rings true when it comes to understanding cybersecurity. The more consumers know, the better they’re able to protect their personal information online. Still, more than half of our survey respondents realize they should do more to beef up their online security. And the top three areas where they feel the most vulnerable? Social media, online banking and online shopping.

IN THE KNOW – OR NOT

When asked how they feel about cybersecurity, one in four respondents considered themselves not very informed or not at all informed.

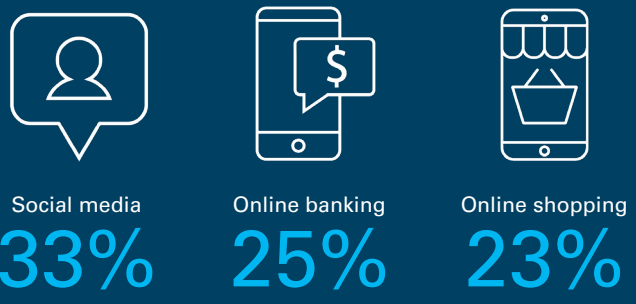


ONLINE SECURITY – A JOINT EFFORT

More than half of consumers (55%) responding say they could do more to protect their personal information online. But they expect businesses to ramp up their cybersecurity strategies, too. Further, 59% are bothered by temporary inconveniences brought about by advanced security measures, even if it means higher levels of safety/protection.

FEELING EXPOSED

Consumers feel most vulnerable to cyber-attacks in these three areas:



CONSUMERS' CREDIT AND DEBIT CARDS LESS THREATENED THAN BEFORE

Although nearly one-third (32%) of this year's respondents have had a personal credit or debit card compromised, the number has dropped since 2017. At that time, nearly three-fifths (57%) of consumers reported a compromise to a credit or debit card.

KEEP OUT

Consumers would be most upset if this personal information was stolen:

Medical record
33%

Mobile phone photos
22%

Salary
17%

Texts
13%

Birth year
8%

GPA
4%

Weight
3%

JUST FOR GRINS

Although there's little room for humor when it comes to talking about cybersecurity and how well-prepared people are to protect themselves online, a little levity seemed in line...

CRACKING THE CODE

Outrageous, controversial behavior? Of celebrities listed, consumers say it would be easiest to crack tabloid talk show king Jerry Springer's password.

Jerry Springer
32%

Lisa Kudrow
17%

Cindy Crawford
13%

Emma Watson
12%

Conan O'Brien
10%

Matt Damon
9%

John Legend
8%

NAME THAT TUNE

Given a list of song titles, here's what consumers say best represents their cybersecurity outlook.

Consumer Behavior

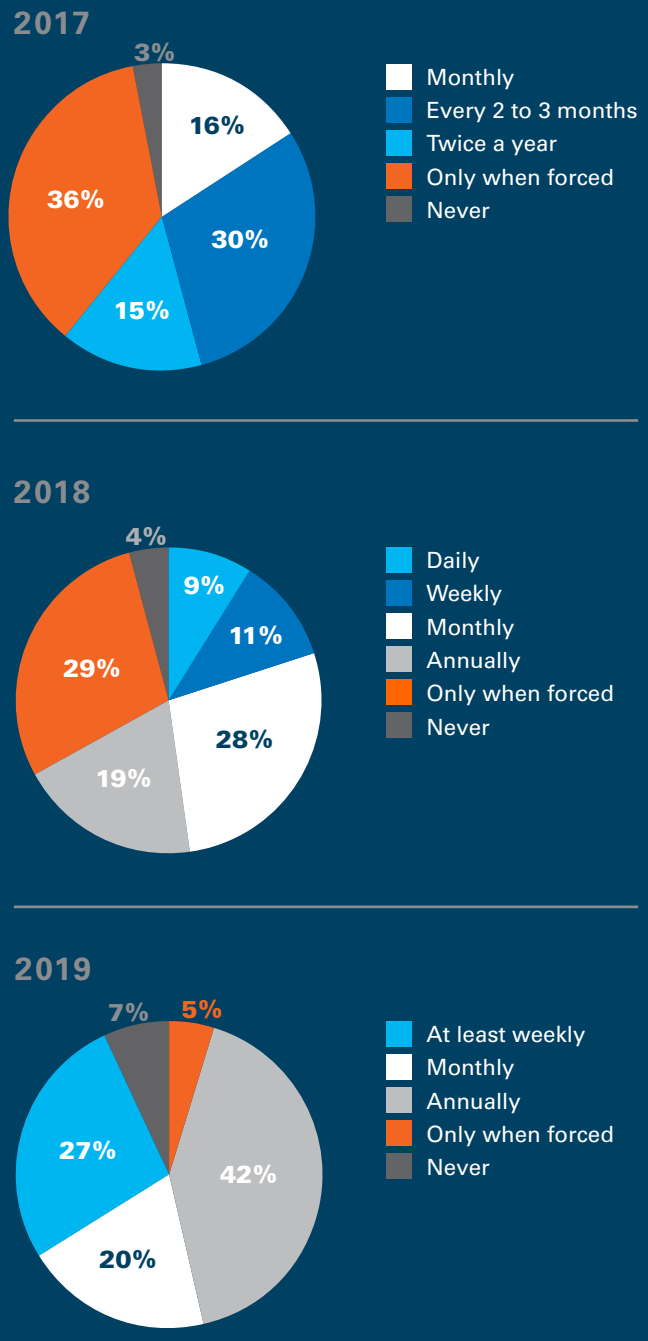
Bothersome or not? Although some consumers consider extra cybersecurity precautions a hassle, others are willing to do what it takes to lock down their personal information online, including changing their passwords monthly.

The majority are savvy enough not to click email links or open attachments from unfamiliar individuals. However, while pet names have often been deemed poor passwords, one-fourth of survey respondents use them anyway.

WHY CHANGE WHAT WORKS?

More than half (52%) of consumers surveyed take steps to decrease their risk of cyber-attack. However, simply changing passwords is a cybersecurity step many don't take unless forced.

The top reason consumers changed their passwords in 2017, 2018, 2019 was they were forced to do so.



HOW PASSWORDS ARE PICKED

Of consumers surveyed, one-third have a go-to password they modify slightly to meet password requirements.

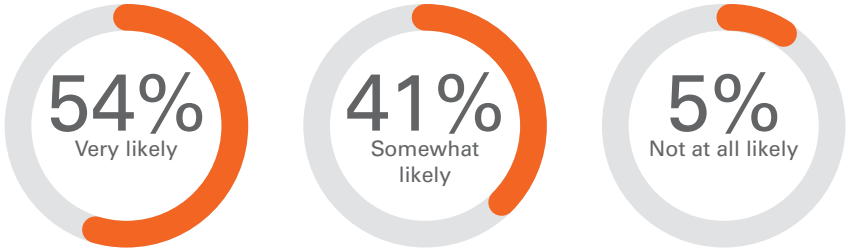
- **4%** "I choose something quick and easy to remember, like 'password' or '1234.'"
- **33%** "I have a go-to password that I modify slightly to the password requirements."
- **20%** "I have a few easy passwords that use the names of significant people/places/pets."
- **25%** I try to come up with random words and use different passwords for different accounts."
- **19%** "My passwords are random combinations of letters, numbers and characters."

USING PASSWORD-PROTECTED PUBLIC WI-FI

Although 19% of consumers would never use a password-protected public Wi-Fi network for sensitive tasks, 28% would. The remaining would only connect to password-protected public Wi-Fi it was extremely urgent (26%) or for tasks such as shopping (28%).

WE'RE NOT GONNA TAKE IT

U.S. consumers won't put up with being hacked on social – 95% would likely delete a social media account if the platform was compromised:



DON'T KNOW NAME? NO WAY

The top measure consumers (61%) take to protect themselves from security breaches is refusing to click email links or open attachments from people they don't know.

- **61%** "I never click email links or open attachments from individuals I don't know."
- **56%** "I set my home and/or personal Wi-Fi networks to private and require password authorization."
- **48%** "I keep my operating system, browser, anti-virus and other critical software up to date."
- **44%** "I don't give out my personal information online."
- **38%** "I avoid autosaving my passwords and manually log into websites and online portals."
- **36%** "I verify the authenticity of requests from companies or individuals by contacting them directly."
- **35%** "I set secure passwords and update them frequently."
- **34%** "I have my bank send text of email notifications following purchases."
- **32%** "I avoid having joint accounts for apps, social channels, services, etc., with my family and friends."
- **8%** "I have not taken any action to protect myself from cybersecurity issues."

WHY CASH COULD BECOME TOP OF WALLET

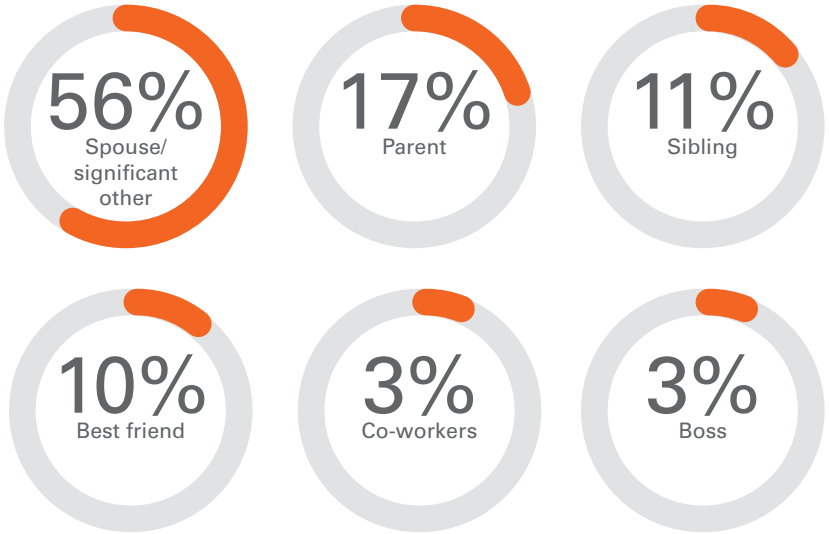
In 2017, 26% of consumers surveyed would continue shopping at a favorite retailer that suffered a security breach but would only pay with cash. In 2019, that number jumped to 40%.

INVASION OF THE BODY CHIPPERS?

The pets can have 'em: Slightly more than one-quarter (27%) of consumers would be willing to be micro-chipped to ensure the ultimate cybersecurity.

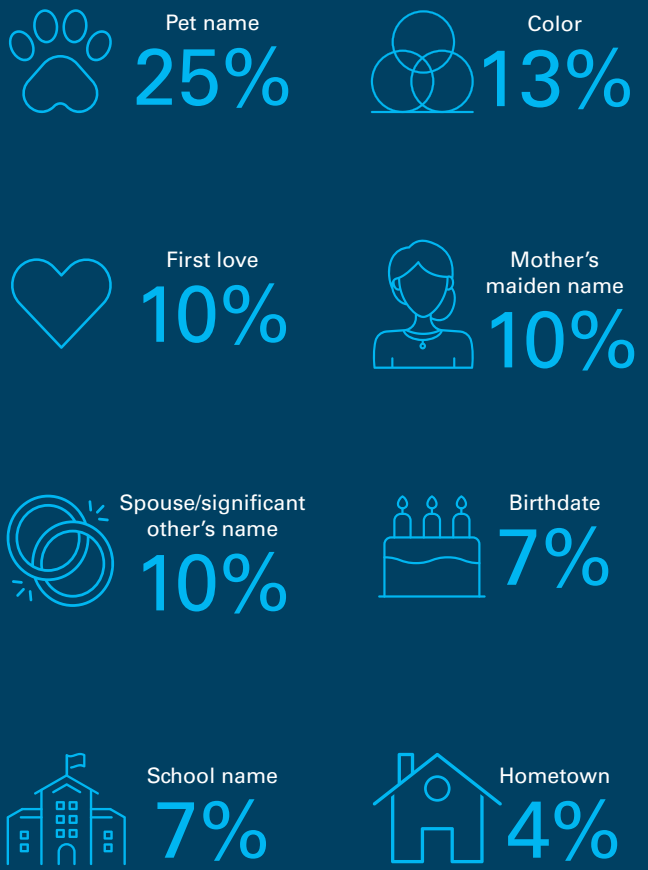
PARTNER TRUSTED WITH PASSWORDS

Not surprisingly, consumers are more likely to trust a spouse or significant other with their online passwords than anyone else.



PEOPLE PREFER PET-NAMED PASSWORDS

Consumers tend to choose easy-to-remember passwords close to their heart. Top choices for passwords include:

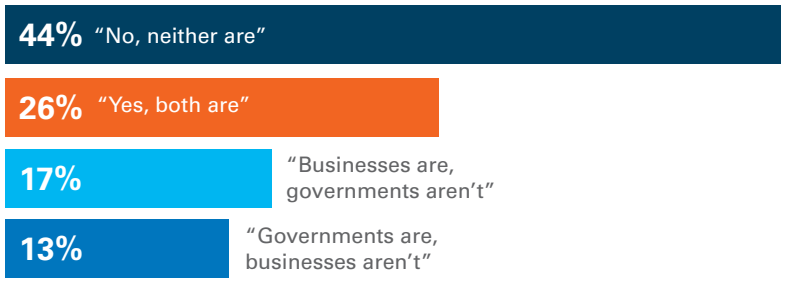


Consumers' Views on How Enterprises Handles Cybersecurity

Although they want heightened cybersecurity measures from businesses and the government, Americans think both groups could do a better job of shoring up their cyber defenses. And while they want and expect their employers to do more to prevent online workplace attacks, less than half say their company offers formal cybersecurity training.

MORE SECURITY MEASURES NEEDED

Nearly 44% of respondents say that neither businesses nor the government do enough to fight cybercrime.



CYBERSECURITY – A NATIONAL TREASURE

Three-quarters of consumers (76%) believe cybersecurity is very important to the nation's security.

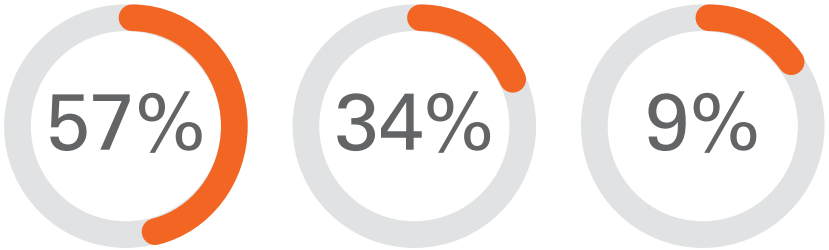
WANTED: HEIGHTENED SECURITY

More than half of consumers (58%) say their company sends regular cybersecurity updates, such as information about the latest scams.

Of the 42% of consumers saying their companies don't, more than half also say their company does not have a plan in place to send out cybersecurity updates or warnings to its employees.

CYBERSECURITY TRAINING: A MUST OR BUST?

Less than half of survey respondents (45%) say their employer offers formal cybersecurity training. Of those that do not have a formal plan in place,



say there isn't a plan in place to begin cybersecurity training

are unsure

say there's a plan in place to begin cybersecurity training

SEEMS SUSPICIOUS? TIME TO TELL IT

Three in four respondents said they would notify IT if they received a suspicious looking email from an unknown sender.

"I would delete it without opening it and immediately notify my workplace's IT personnel."

43%

"I would delete it without opening it, or I would open it and notify my workplace's IT personnel once opened."

32%

"I would open it and then delete it."

12%

"I would open it and then ignore it."

7%

"I would open it and might open any attachments that looked interesting."

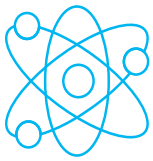
6%

FROM CELEBRITIES TO TV CHARACTERS

We're sure you agree that cybersecurity is serious. We certainly think so, which is why we conduct a fraud- and/or security-related survey each year. Still, we thought we'd toss consumers some silly questions, just to see where their responses landed. Here's what they said…

FITTING THE BAZINGA! BILL

"Big Bang Theory's" Sheldon Cooper, who uses the catchphrase bazinga! to rub a joke in someone's face or when he one-ups a friend, is the fictional character most consumers say best personifies their company's cybersecurity program.



Sheldon Cooper, "The Big Bang Theory"

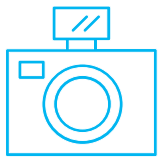
35%

Homer Simpson, "The Simpsons"

23%

Arya Stark, "Game of Thrones"

14%



Olivia Pope, "Scandal"

14%

Mary Richards, "The Mary Tyler Moore Show"

14%

BOSS BEWARE!

More power in the workplace means a larger target on your back. Survey respondents, if forced to hack into someone's account, were more likely to breach their boss than this list of celebrities.

- 31% Your boss
- 17% Kim Kardashian
- 14% Taylor Swift
- 13% Chris Hemsworth
- 13% Kanye West
- 8% Ariana Grande
- 4% Christiano Ronaldo

How Businesses Can Help Their Employees Be More Cyber-Aware – and Secure

And the survey says…consumers want their employers to take an active part in educating them to become more cybersecure. Although some will use their personal time to explore ways to better protect themselves online, many will not. This puts them – and your business – at a greater risk for being breached, as the human element can be particularly difficult to control – nearly one in three security breaches in 2018 involved insiders[1]. For organizations, the goal should be to change your employees from threats to assets by educating them to recognize fraud and security risks.

We can help. As a leader in financial services, Fiserv has deep expertise in preventing and protecting against cybercrime.

We've compiled these three immediate steps you can take as an employer to help your people get smarter about online security.

1 2018 Data Breach Investigations Report

01 SAFETY WHILE YOU WORK

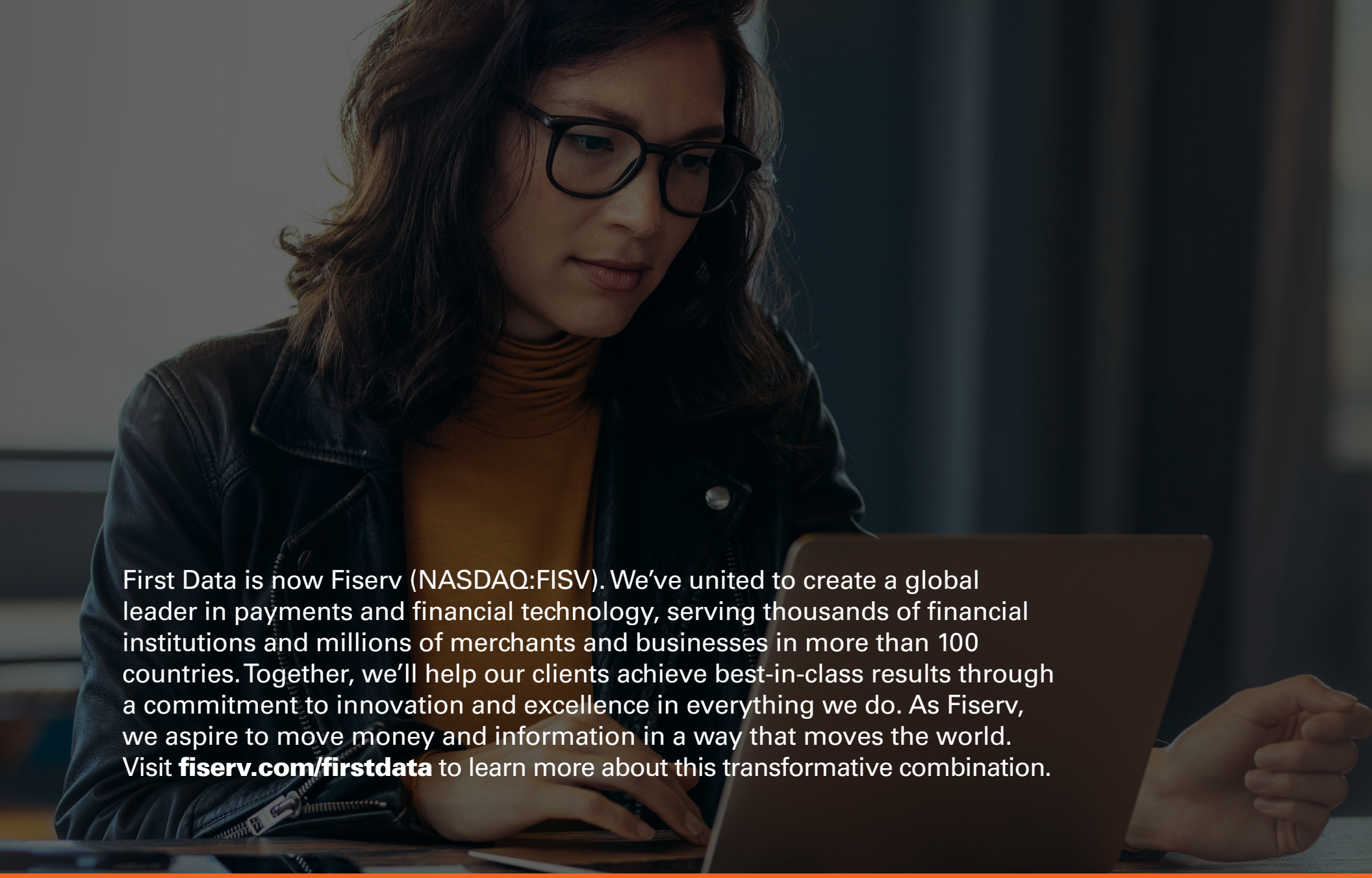
Ensuring company data is protected from the latest cyber security threats is one of the biggest responsibilities your company's IT department bears. Educating your employees on cyber security threats is a best practice followed by companies who issue hardware used outside office walls.

02 LOCK DOWN YOUR HOME

Encourage employees to secure their home network, a good start would be making sure to change default passwords, especially their routers. This helps to protect any data stored or device connected to their home networks. For those that have families, emphasize the importance of teaching them about the dangers of cyber predators, who often target teenagers and young children.

03 KEEPING YOUR ASSETS OUT OF THE PUBLIC EYE

Whether on personal or business computers, educate employees on covering up their screens when entering passwords and credentials in public areas. After all, with mobile device cameras continuing to impress with stronger zoom features and unprecedented pixel rates, you never know who may be watching.



First Data is now Fiserv (NASDAQ:FISV). We've united to create a global leader in payments and financial technology, serving thousands of financial institutions and millions of merchants and businesses in more than 100 countries. Together, we'll help our clients achieve best-in-class results through a commitment to innovation and excellence in everything we do. As Fiserv, we aspire to move money and information in a way that moves the world. Visit **fiserv.com/firstdata** to learn more about this transformative combination.

First Data is now fiserv.