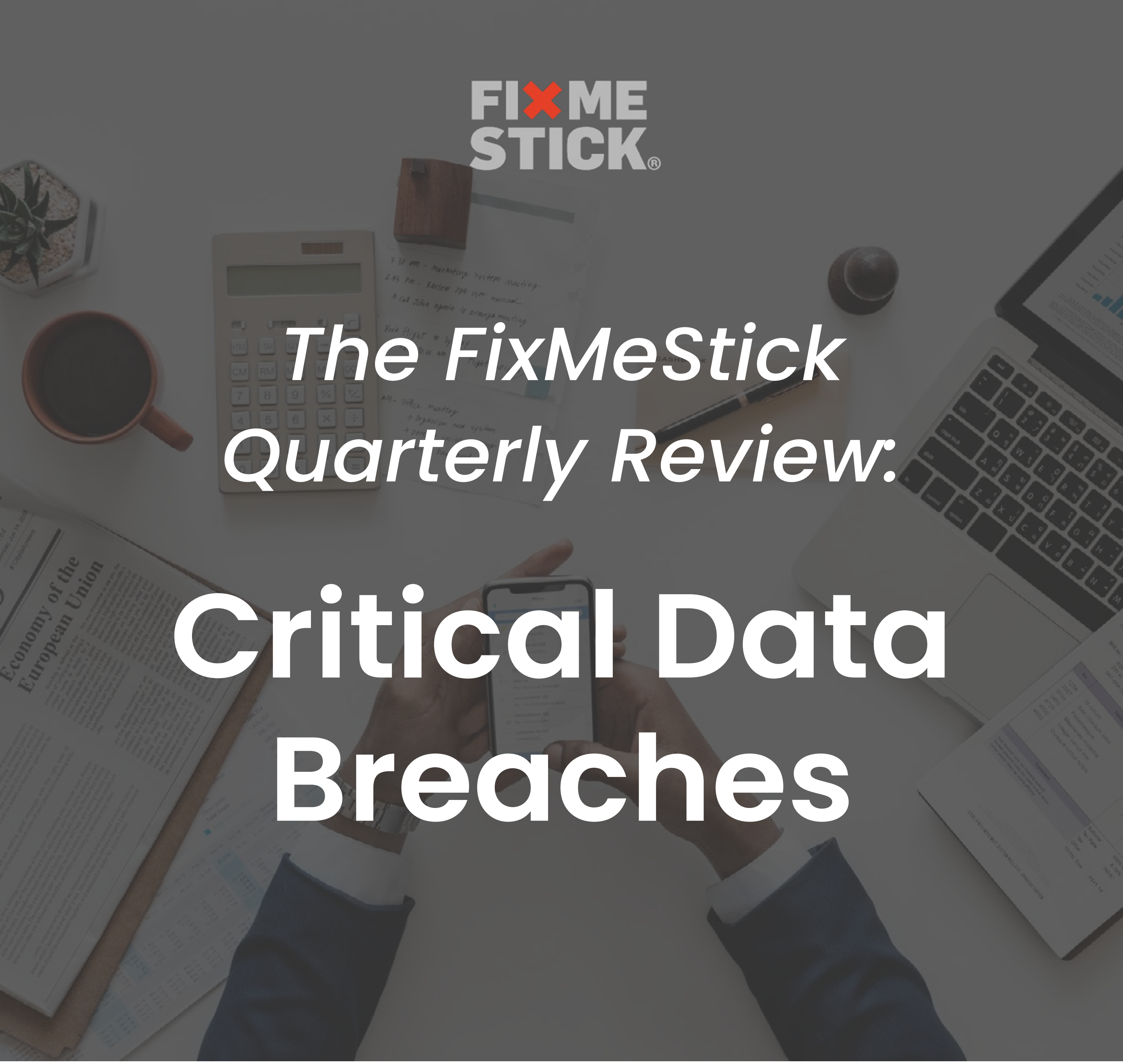

FIXME STICK®

The FixMeStick Quarterly Review:

Critical Data Breaches

2019

4 FACTS YOU NEED TO KNOW ABOUT DATA BREACHES

It seems data breaches are happening every other day. We wanted to **simplify the conversation** and provider our readers with our insights into the **data breaches from the first quarter of 2019.** This review is meant to arm our FixMeFans with an easy-to-follow guide of the digital threat landscape of today, and the best tips and tricks to reduce fallout after a data breach.

Below we isolate the most critical data breaches we've seen this year, and present a timeline of events, key trends in cybersecurity threats today, and the lessons we learned (so that you don't have to learn the hard way)! **Here are our 4 main findings:**

1

Passwords and email addresses have been the most commonly exposed pieces of information in 2019's data breaches.

2

Cloud based storage sites are presenting an increased threat to data privacy.

3

There have been almost **50 significant data breaches** or data breach announcements in the first 3 months of 2019.

4

Healthcare providers, health Insurance companies, and **third-party sites/applications** remain top targets for cyberattacks.

5 KEY DATA BREACH STATISTICS

4.4 billion is the amount of active internet users in the world.[1]

10% of cyberattack groups use malware to disrupt company operations.[2]

56% of data breaches in the first half of 2018 were targeting social media platforms.[3]

$3.86 million is the average cost of a data breach.[4]

30% of all companies have over 1,000 sensitive folders open to the public.[5]

1. https://www.statista.com/statistics/617136/digital-population-worldwide/
2. https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-executive-summary-en.pdf
3. https://www.itweb.co.za/content/G98YdqLxZZNqX2PD
4. https://www.ibm.com/downloads/cas/861MNWN2
5. https://www.varonis.com/2018-data-risk-report/

TIMELINE OF EVENTS

Jan. 17th: MEGA (a cloud-based storage site)

In a shocking discovery, a security researcher found a database on MEGA which contained **773 million email addresses** *and* **22 million unique passwords** *collected from previous data breaches.*

Jan. 23rd: Alaska Department of Health & Social Services (DHSS)

In a vicious cyberattack an Alaska's Division of Public Assistance, the social security numbers, date of birth, addresses, income, and health information of more than **100,000 people** *were exposed.*

Feb. 11th: Various Online Entities

Almost **620 million online account details,** *mainly emails and passwords, were revealed to be for sale on the Dark Web. Sites like Coffee Meets Bagel, 500px, Whitepages, and MyHeritage were main targets.*

Feb. 18th : MediCall (Sweden)

It was discovered that a Swedish company left **2.7 million recorded calls** *available on an unencrypted server, exposing personal medical histories, phone numbers, and social security numbers of millions of Swedes.*

Mar. 6th: Health Alliance Plan

A ransomware attack on a third-party server that hosts the private medical information of the Michigan-based health insurance company left **120,000 patients'** *claim information exposed.*

April 2nd: Facebook

Through two third-party applications that hold Facebook data, Cultura Colectiva and At the Pool, more than **540 million data records** *including Facebook IDs, passwords, user activity, and photos were exposed.*

FIXME STICK®

4 LESSONS WE'VE LEARNED FROM DATA BREACHES IN 2019

1 Passwords are a key first step in protecting your personal data.

Having a unique, hard-to-crack password for all your accounts can lessen the fallout of a data breach.
FixMeTip: Regularly update your passwords, or use the password saver in your browser if you're having trouble remembering your login credentials. Check out our handy guide to creating a strong password here!

2 A clean computer makes your devices more secure.

Malware is evolving as an increasingly popular vessel for cybercrimes. Having an up-to-date antivirus program acts as a preventative measure against breaches while the FixMeStick virus removal devices locates and eliminates existing threats that snuck past your antivirus.

3 Responsible digital citizens come out ahead.

Staying up-to-date on the latest cybersecurity threats and data breaches means that you can make good decisions regarding the companies you give your personal information to, and the tools you keep in your digital toolbox. The FixMeStick newsletter and blog are great places to start!

4 Well-maintained online accounts are the way to privacy.

Pay attention to the information you are sharing online with applications, digital platforms, and companies. Check for new privacy settings available and learn about your options. Not using an account or application anymore? Delete it to reduce the chances of becoming a data breach victim!

Looking for more cybersecurity news and tips?
Remember to check out our blog here:
fixmestick.com/blog