# In this issue:



---

Dear <first name>,

Welcome to the last cybersecurity newsletter of 2019! It certainly has been a big year for cybersecurity. While we are sure the next decade will bring its own cybersecurity hacks, scams, and frauds—we will likely see new technology to help combat it.

Read on to learn more about the cybersecurity happenings this month including:

- A major department store breach
- How to keep your phone safe at airports
- The setting you must enable for your Ring doorbell
- And much more

## A new decade for cybersecurity

In just a few weeks, we welcome in 2020 and in turn, a new decade. The 2010s were a defining decade for cybersecurity. We saw some of the largest hacks, breaches, and scams make the news over the past ten years. But we have also gotten better with our cybersecurity. The number of institutions offering two-factor authentication has increased. More people are aware of what a phishing attack looks like. And legislation was passed making it easier for everyone (including minor children) to freeze their credit reports.

Of course, as we enter a new decade, new threats will emerge. Technology will continue to advance at a record pace, which brings threats along with convenience. As we enter this new era, let's take a look at how cybersecurity threats advanced over the past ten years and what we think will happen in the future.

**Threats of the 2010s**

1. **Data breaches**

   This past decade has brought us a trend of massive data breaches. Starting in 2013 with the Target data breach that affected over 100 million people, we began to see data being stolen in the millions on a regular basis. For example, we had the Yahoo breach affecting 500 million users. And who could forget the Equifax breach exposing information on nearly 150 million consumers? As we head into 2020, it is likely that everyone's personal information has been exposed over the last ten years, making cybersecurity education more important than ever.

2. **Ransomware**

   Another threat that has made the rounds since 2010 is ransomware—the malware that encrypts all the data on your machine and demands a ransom payment. And while the first ransomware attack allegedly occurred in 1989, we have seen a huge increase over the last ten years. In fact, last year there were an estimated 184 million ransomware attacks compared to just 2,000 in 2017. This, in part, is due to organizations being targeted. It is estimated that one new business falls victim to ransomware every 14 seconds.

3. **Business Email Compromise**

   An influx of phishing emails targeted at businesses emerged in the 2010s. The scam, called Business Email Compromise or CEO Scam, often tricked employees into wiring large amounts of money after receiving an email appearing to be from their CEO. Since 2013, nearly 70,000 companies have been victimized, costing billions in damages.

**Threats looking forward**

1. **Internet of Things (IoT) attacks**

   Towards the end of this decade, we began welcoming more and more smart devices into our lives. Many of us now have connected doorbells, thermostats, and TVs. And while these devices bring a level of convenience, we have also seen cyberattacks launched at these devices' vulnerabilities. In the next decade, it is likely that these attacks will occur more often. Going forward, it is important that we treat these devices as we do our smartphones and computers.

2. **Artificial Intelligence**

   Another technology growing in popularity is artificial intelligence. Many experts believe that hackers will be able to use AI technology to create more realistic scams, including fake videos impersonating a CEO via email or video chat to enable more business email compromise attacks.

3. **Cloud systems**
   Hackers will likely go after cloud systems in the coming years as more and more data is stored in the cloud. This month already saw two ransomware attacks at cloud server vendors that impacted hundreds of businesses using those servers. It will be important going forward to thoroughly vet any cloud system companies you work with.

Each year brings us new cybersecurity threats to defend against—but also brings new ways to fight back. We must all stay vigilant with our cybersecurity plans and adapt when it's indicated. We're looking forward to this new year of cybersecurity vigilance and will continue to keep you updated with the latest news.

## Cybersecurity shorts

**Wawa data breach may affect all 850 stores.** The chain announced a data breach this month exposing customer payment card details. Hackers installed malware that accessed credit and debit card information. It is unknown how many customers were affected at this time. If you have shopped at Wawa this year, be sure to monitor your credit and debit card statements closely.

**Macy's online shoppers beware—your credit card information may have been stolen.** The department store announced a data breach that occurred in October likely affecting thousands of shoppers. Information stolen includes names, addresses, credit card numbers, verification codes, and expiration dates. It is believed that hackers installed malware on the Macy's website to collect this data.

**New Jersey hospital system hit by ransomware pays attackers to unlock medical systems.** Hackensack Meridian Health fell victim to a ransomware attack in early December. The attack resulted in about 100 medical procedures being canceled over 17 hospitals and clinics. Two weeks later, the hospital paid the undisclosed ransom amount saying, "We believe it's our obligation to protect our communities' access to health care."

**Equifax data breach settlement fails federal requirements for fairness and adequacy according to the Center for Class Action Fairness.** The nonprofit says that the settlement does not treat victims equally as it does not account for differences between states such as damage limits. The center also states that consumers' attorneys inflated their legal fees and should be paid $16 million rather than $77 million.

**Robocall mimicking FBI agent drains oncology nurse's life savings.** Nina Belis received a call from an FBI agent saying her Social Security number was stolen and crimes had been committed in her name. The agent then recommended Belis transfer her money into accounts he controlled to protect the funds. She wound up transferring $340,000 before realizing she had fallen for a scam. Read her story here.

**Ransomware attack at IT company cuts nursing homes off from health records,** according to Krebs on Security. The Wisconsin-based company provides cloud data-hosting for more than 100 nursing homes all over the country. It was hit with a ransomware attack that encrypted all the data the company hosts and demanded a $14 million ransom. The owner fears this incident could close her business and seriously affect the health of patients. (A similar attack at a Colorado IT company has affected over 100 dental offices.)

**Over 1 million T-Mobile customers affected by latest data breach.** The company says hackers were able to access information such as name, billing address, phone number, and account number. Affected users were contacted by T-Mobile.

**Travelers, think twice before charging your phone at the airport.** The Los Angeles County district attorney's office is warning of a scam at LAX airport involving fake USB charging stations. Plugging your device into one of these USB charging ports can expose your phone to malware or even lock the device. A power adapter is a much safer charging option when in public.

**Marital identity theft can be one of the most difficult thefts to fight according to many lawyers.** A study done by the National Domestic Hotline found that over half of women who called reported that a partner had put debt in their name through fraud or coercion. In many cases, this ruins their chances of being able to get an apartment on their own. Many police precincts make it difficult to get a police report without divorce documentation—making the fraud difficult to prove.

**Biggest threat to broker-dealers? Cybersecurity** says top Sifma executives. Cybersecurity was a topic of discussion at the Sifma Annual Meeting with chairman James Allen stating, "cybersecurity is the one thing that keeps me awake at night." Sifma believes that all employees should go through cybersecurity training.

**Phishers target small business owners during the holiday season.** Danielle Radin, owner of Mantra Magnets clicked a link in an email inviting her to be a part of a holiday gift guide. Soon after, however, she kept getting notifications that people around the world were trying to access her email account. It turns out that the holiday gift-guide email was a phishing attack. Experts warn that these attacks have become more professional looking, so everyone must closely scrutinize unsolicited emails.

**PR software company exposed data on over 450,000 contacts via an unsecured database**. The information included administrative credentials, assorted documents, and over 35,000 hashed passwords. iPRsoftware's clients include Xerox, Mattel, Nasdaq, and others.

**Brokerage accounts wiped by a simple email scam in New York.** According to reports, a Lithuanian man and a co-conspirator stole hundreds of thousands of dollars from victims after compromising the victims' email addresses and sending wire transfer requests to their financial advisor. Read more here on how to protect yourself from this scam.

**Is your Ring doorbell secure?** The Amazon smart doorbells have been in the news often this month with stories of hacks. The culprit, however, is bad security. Weak passwords have led to many hacks and the doorbell is not set up with two -actor authentication by default. If you own a Ring or other smart doorbell you need to be sure you are using a unique password and that you enable two-factor authentication.

## Software updates

**Adobe:** Updates for Acrobat and PDF Reader were released this month that close over 20 security holes. If you are a Photoshop user, you should update that as well.

**Google:** This might be the first time we warn against an update but do NOT update Google Chrome. The update for Chrome 79 is causing major issues for Android users including data loss. Hold off on updating until a solution is found.

**Microsoft:** Microsoft released over 30 patches this month—including seven for critical bugs. One critical update for Win32k (present in Windows 7-10) is already being exploited. You can read more about the updates here.