2021 Data Breach Report

North Carolina Department of Justice

Attorney General

Josh Stein

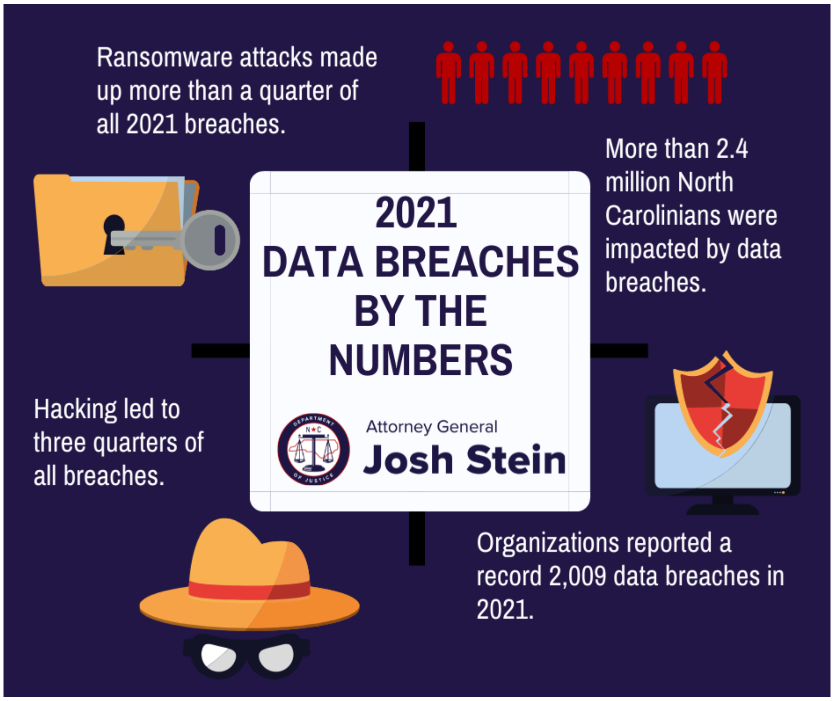
In 2021, the COVID-19 pandemic continued to push much of our world online and criminals looked to take advantage. Many North Carolinians continued to learn, conduct business, access services, and connect with friends and family online. Unfortunately, the more we rely on technology, the more likely we are to experience information security breaches. Our office continues to enforce the law against bad actors and irresponsible companies that jeopardize personal information like bank account, credit card, and Social Security numbers.

Under state law, businesses and government agencies must notify the North Carolina Department of Justice (DOJ) when a security breach occurs. These reports allow our Consumer Protection Division to help protect people who are impacted, inform the public about the scope of this issue, and, if necessary, take action to hold companies responsible for business practices that fail to protect North Carolinians.

In 2021, organizations submitted a record 2,009 data breach notices to DOJ. These breaches put more than 2.4 million North Carolinians' personal information at risk. Since 2005, organizations have reported 10,778 breaches to DOJ.

This report highlights the most common types of data breaches in 2021 and how they compare to previous years. It also shares information on how North Carolinians can protect themselves before and after a security breach. Our office works hard to protect people from data breaches. If you believe you have been a victim of a breach, contact our office at 1-877-5-NO-SCAM or ncdoj.gov/complaint.

Highlights

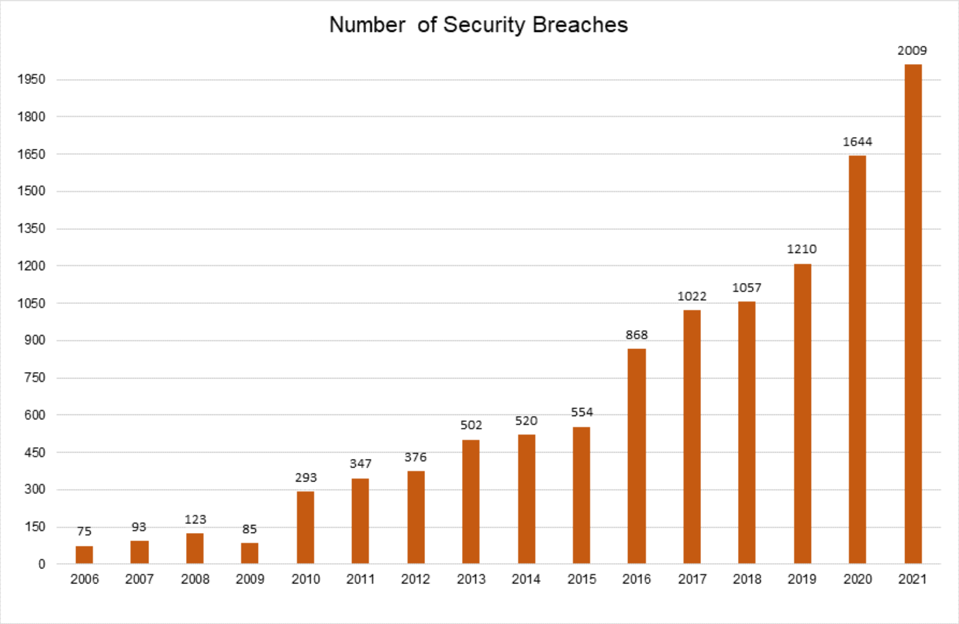

Ransomware attacks made up more than a quarter of all 2021 breaches.
More than 2.4 million North Carolinians were impacted by data breaches.
2021 DATA BREACHES BY THE NUMBERS
Attorney General Josh Stein
Hacking led to three quarters of all breaches.
Organizations reported a record 2,009 data breaches in 2021.

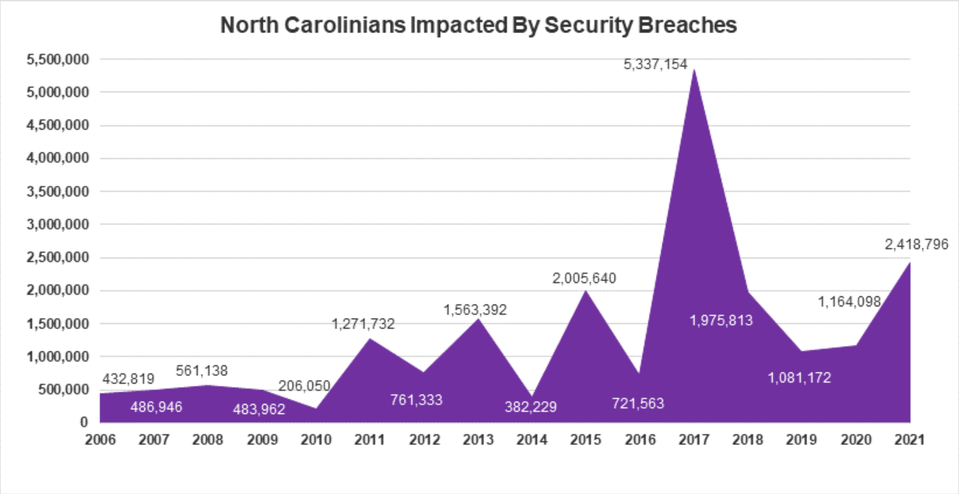
- 2021 marked the 12th consecutive record-setting year of data breaches reported to DOJ. The 2,009 notices represent a 22 percent increase over 2020.
- In 2021, more than 2.4 million North Carolinians were affected by data breaches.
- Ransomware breaches accounted for a record 30 percent of all breaches in 2021.
- Phishing and hacking attacks, the leading causes of ransomware breaches, accounted for nearly 90 percent of all data breach reports in 2021.

Ransomware breaches, when a bad actor locks an organization or individual's data and demands a ransom payment to release it, were a real problem in 2021. These kinds of attacks made headlines across the globe, including the Colonial Pipeline attack that grounded flights at Charlotte Douglas International Airport and caused shortages at gas stations across North Carolina. Ransomware attacks were rampant among reports to our office this year. Attorney General Stein has championed updating our Identity Theft Protection Act to ensure that these type of data breaches constitute a security breach under our state law. This change is critical to protect those affected by ransomware attacks. Attorney General Stein continues to work with the legislature to see these changes signed into law.

Our office took action against organizations that put North Carolinians' data at risk. In March, Attorney General Stein announced a settlement with Retrieval-Masters Creditors bureau, doing business as the American Medical Collection Agency (AMCA), to resolve an investigation into a 2019 data breach that exposed the personal information of more than 7 million people, including 90,055 North Carolinians. The settlement required AMCA to change its business practices to strengthen its information security program or be liable for a $21 million payment. If businesses illegally put North Carolinians at risk of identity theft and fraud, our office will hold them accountable.

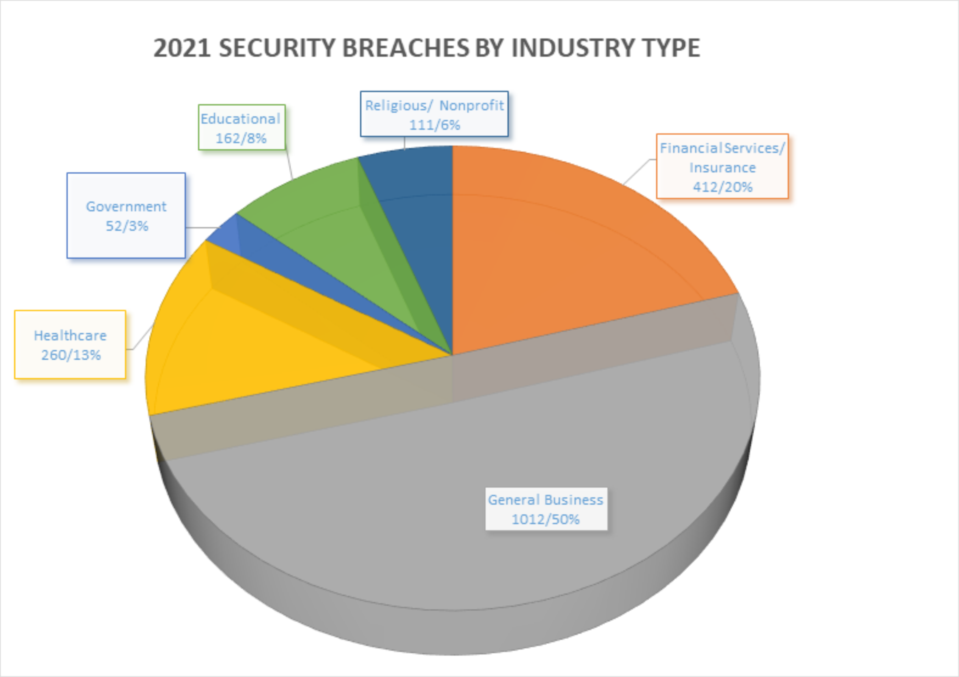
Overview of 2021 Breaches





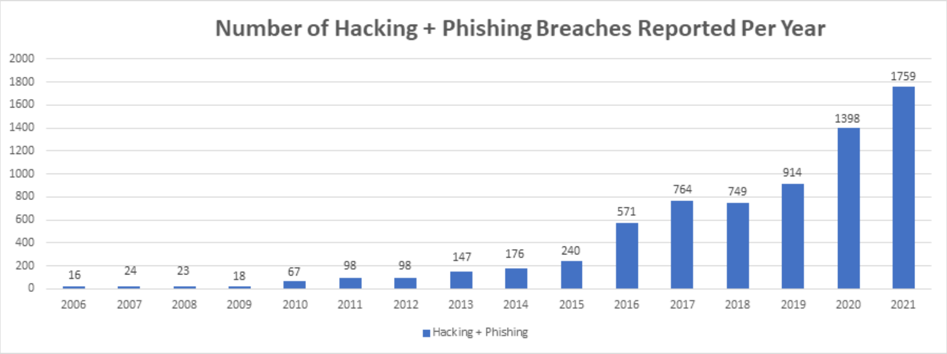
Note: In 2017, Equifax experienced the largest-ever data breach in history affecting nearly 5 million North Carolinians, resulting in a higher number of people having their information compromised that year.

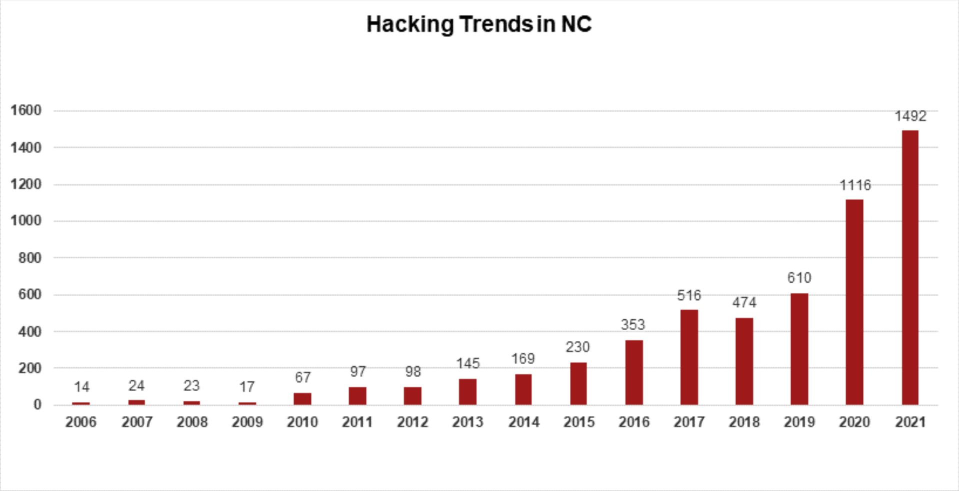
In 2021, people shared information with organizations through their phones, smartwatches, laptops, smart televisions, and many other technologies. Sharing our information is pervasive in our economy and society, which increases the risks to more and more people. The data breaches last year affected more than 2.4 million North Carolinians.

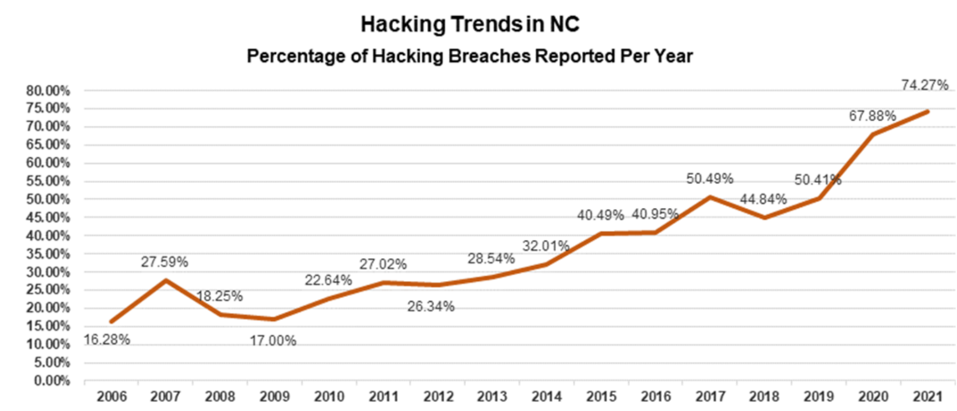


After general business, financial services and insurance organizations represented the largest share of data breach notices. Given the sensitive nature of information shared with financial companies, this data is especially important to protect. Our office continues to work with these organizations to protect people’s data, and we will hold companies accountable if they fail to meet their security obligations.

Hacking and Phishing

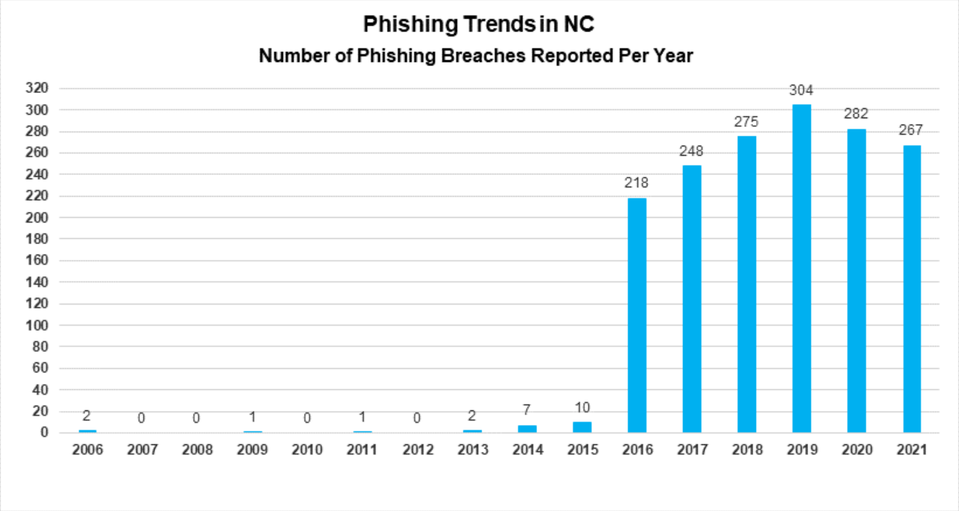






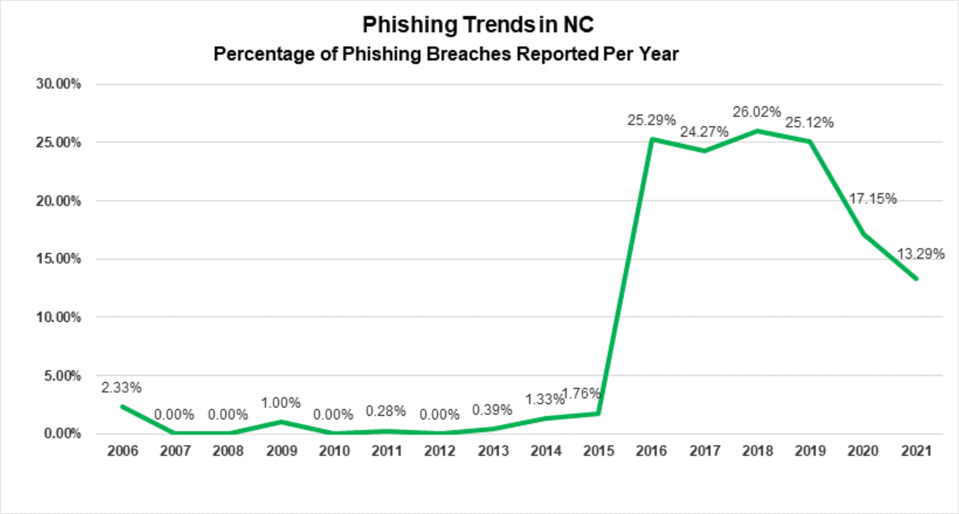
Hacking Trends in NC

Percentage of Hacking Breaches Reported Per Year



Phishing Trends in NC

Number of Phishing Breaches Reported Per Year



Phishing Trends in NC

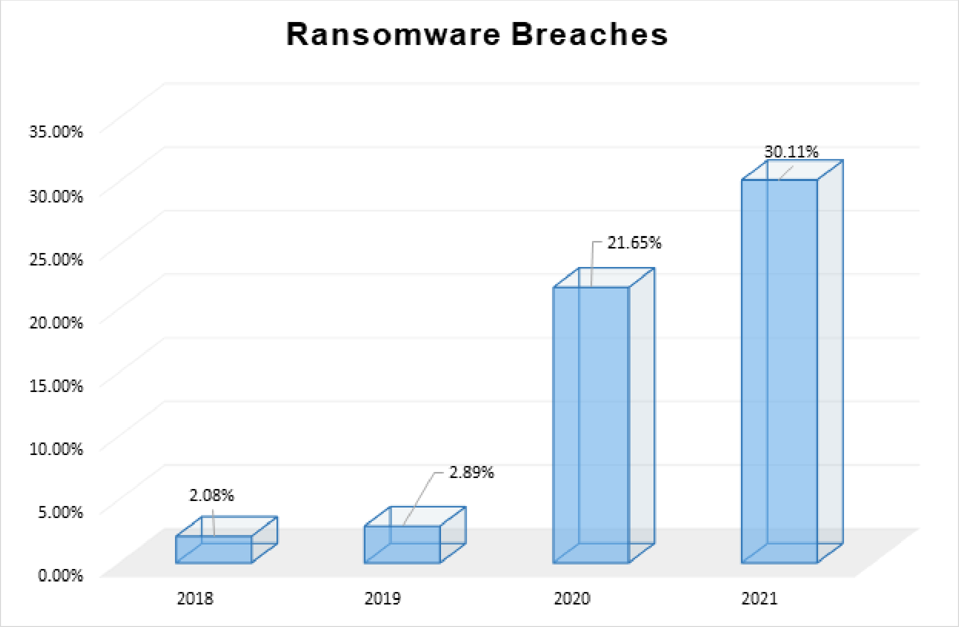
Percentage of Phishing Breaches Reported Per Year

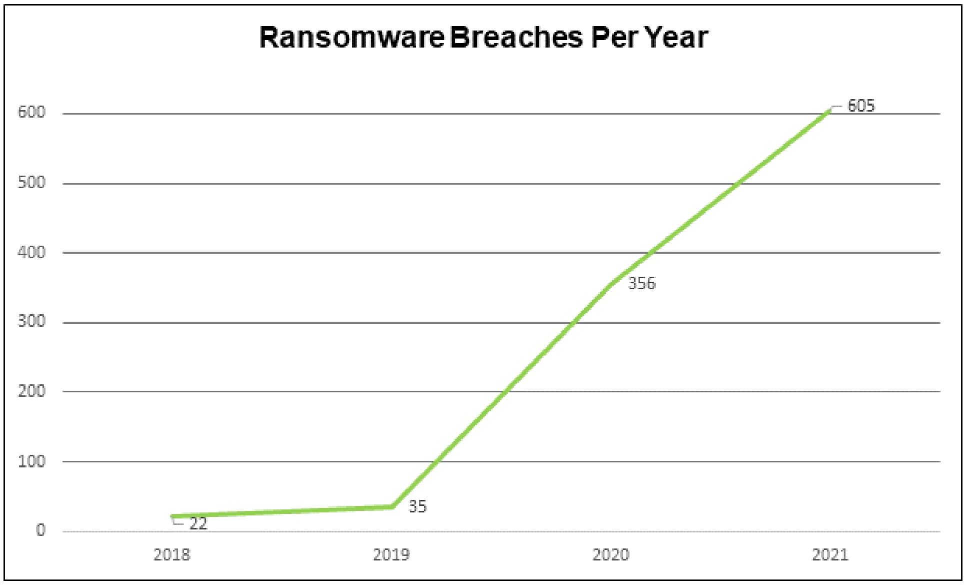
Hackers break into organization's data systems to steal their clients' and employees' personal information. Each year hackers find new ways to bypass security measures. They often employ phishing attacks, fake emails designed to trick users into clicking on malware hidden in attachments or links. Year after year, hacking attacks become more prevalent among reports to our office. Here's how to protect yourself or your organization from these types of data breaches:

- Regularly update your antivirus and security software.
- Don't be fooled by unexpected emails asking you to click a link or download an attachment.
- Don't use email to send and receive personal information.
- Forward phishing emails to the Federal Trade Commission at spam@uce.gov.
- Monitor your financial statements and credit report for irregularities.

If you believe you may have been the victim of a hack, request a free security freeze and contact our office.

Ransomware

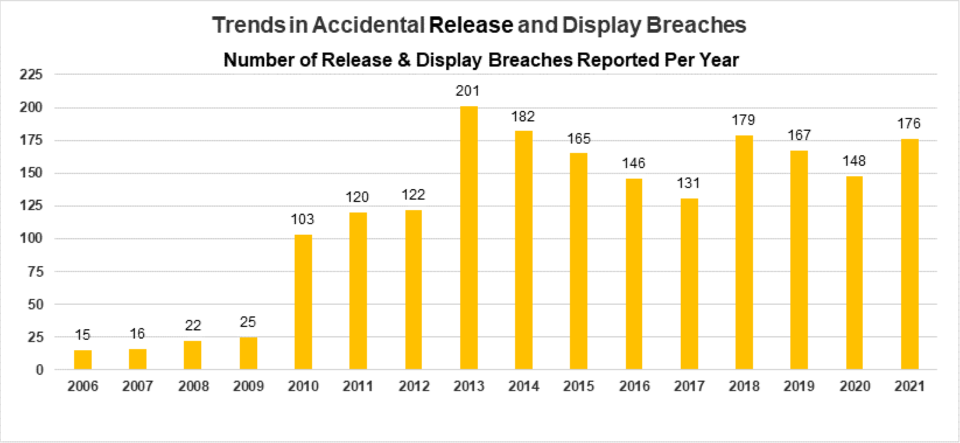


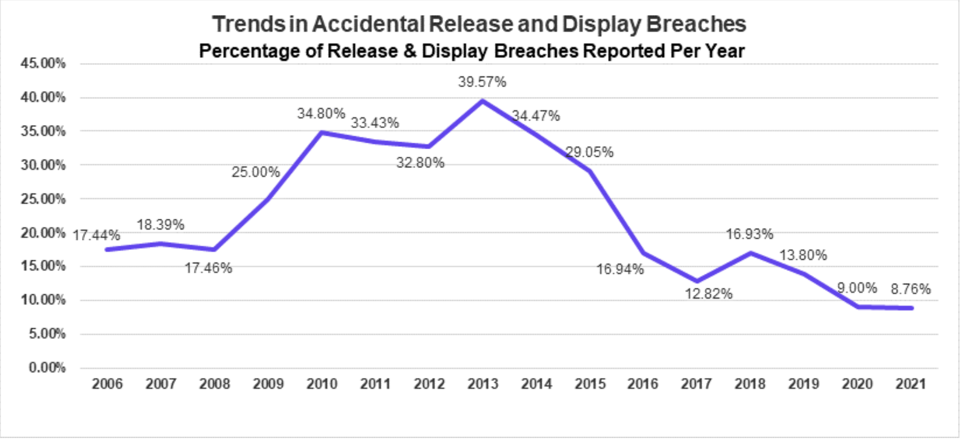


Ransomware attacks represent a growing threat to businesses and people everywhere. This year, our office recorded a record 605 ransomware breaches, a nearly 50 percent increase over last year's record. The attacks made up a record 30 percent of all breaches reported to our office. Follow these tips to protect yourself and your organization from ransomware:

- Regularly update your antivirus and application software.
- Train employees and users on cybersecurity best practices.
- Only conduct business on legitimate websites and software programs.
- Do not click on links unless you are sure they are safe.
- If you think you've been the victim of a ransomware attack, report it to the FBI or the U.S. Secret Service immediately.

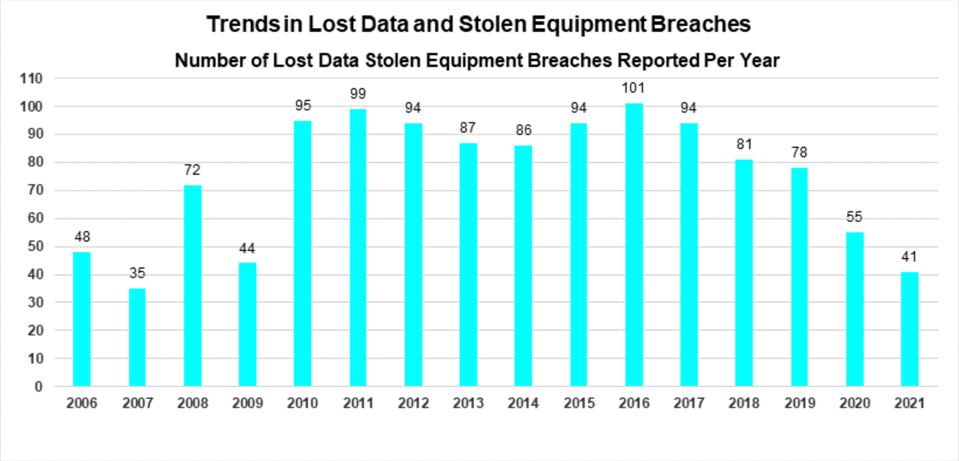
Accidental Release and Display

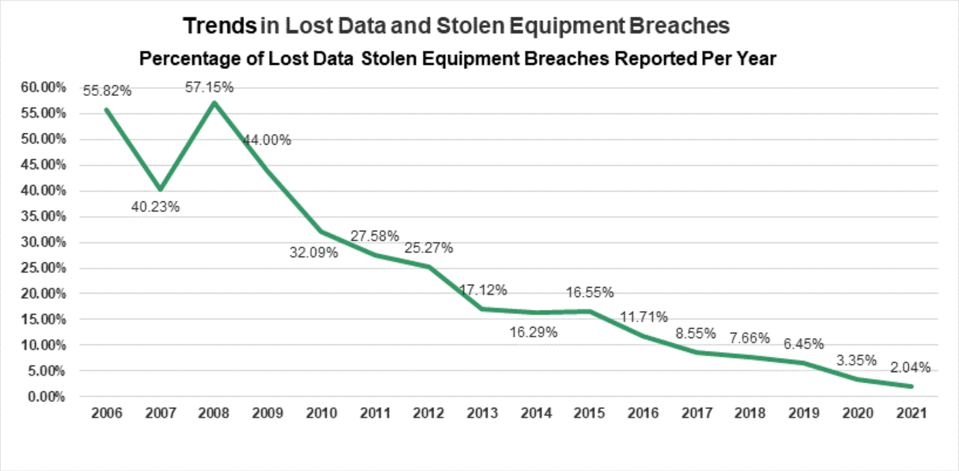




Accidental release and display breaches, when a person or organization accidentally shares data with an inappropriate party that leaves the data vulnerable to abuse, increased for the first time since 2018. However, these breaches represented a smaller share of overall breaches due to the growth in other types of breaches. To avoid these types of incidents, organizations should remind employees to safeguard their passwords and logout of accounts on shared devices, follow appropriate data storage protocols, and delete personal information when sharing data with outside organizations.

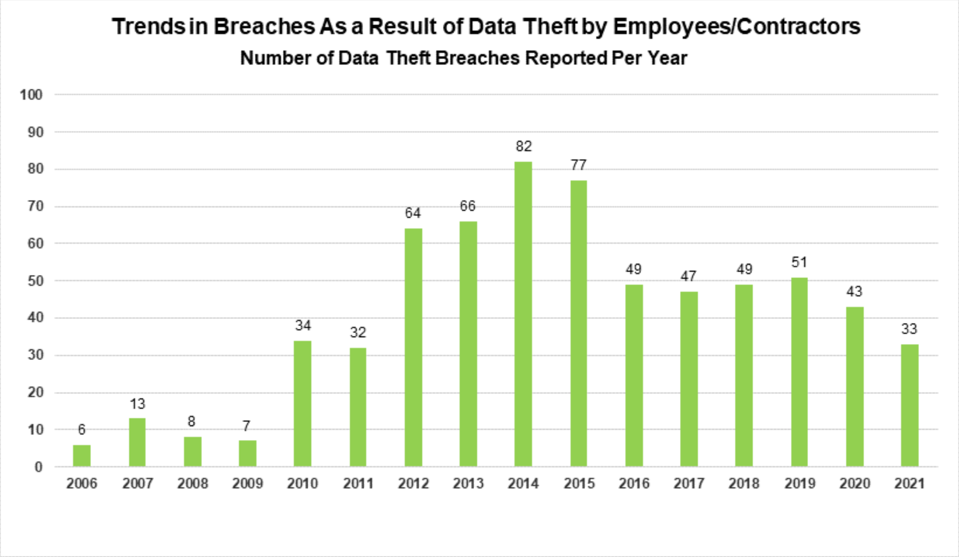
Lost in Transit or Stolen Equipment





Data breaches caused by lost or stolen equipment continued to decline in 2021, with 41 breaches that account for just two percent of all attacks. These breaches occur when data or the devices it is stored on are lost or stolen. To avoid these breaches, organizations should track device inventories and employees should report lost or stolen equipment to their IT department immediately.

Data Theft



Data theft by employees or contractors, the least common breach reported to DOJ, continued to decline in 2021. Organizations can protect themselves from this type of breach by thoroughly vetting employees and contractors before they are hired and restricting access to personal information to only what is needed to perform the job.