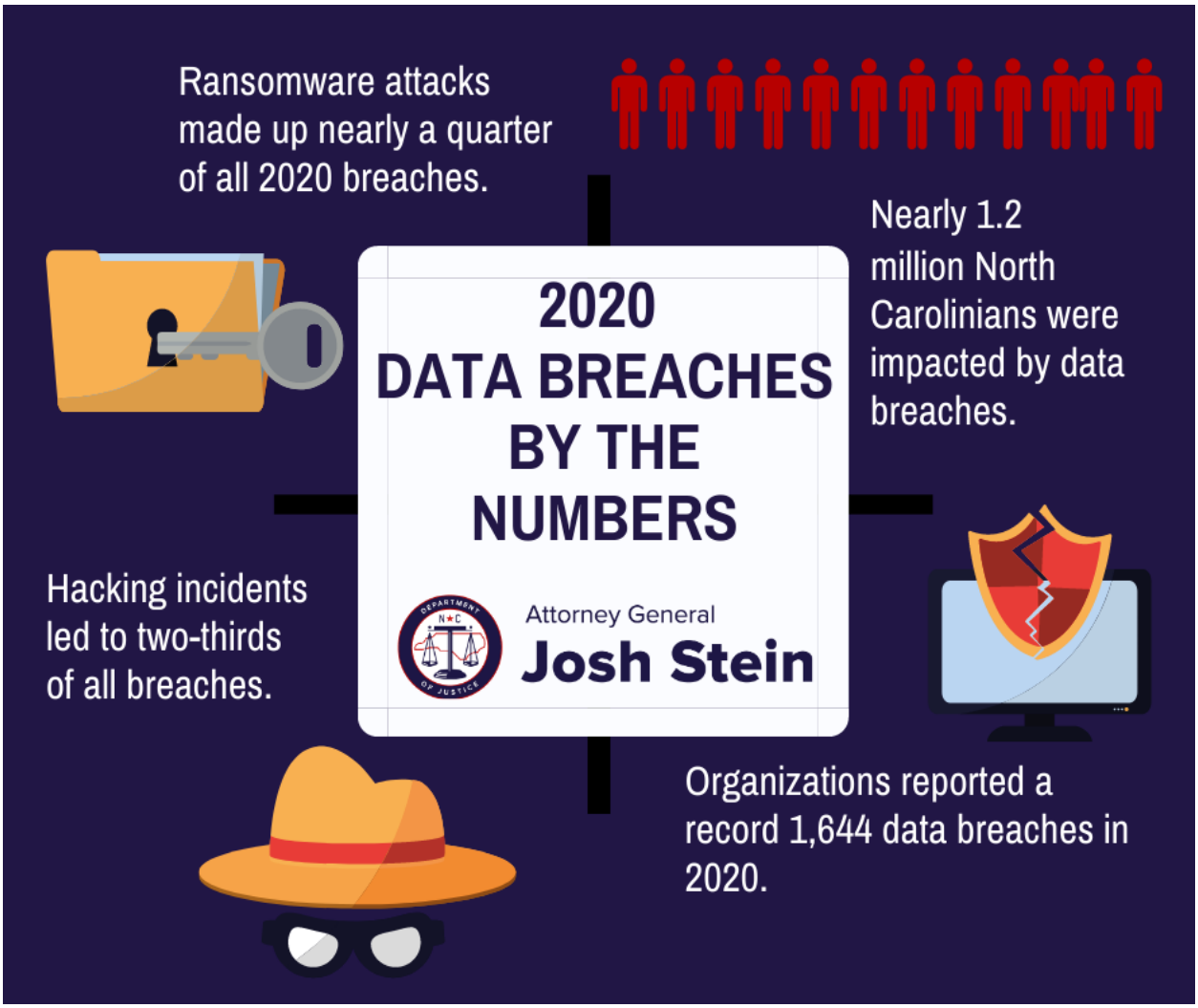
EXECUTIVE SUMMARY

In 2020, practically our entire world moved online. The coronavirus pandemic dramatically increased the extent to which we use technology. For most of the past year, many of us have relied almost exclusively on digital tools to continue to work, do business, access services, learn, and stay in touch with loved ones. The increased use of technology to share information imposes an even greater responsibility on businesses, digital platforms, and government agencies to protect our personal and financial data. When companies fail to do so, they leave people's information – including their bank account, credit card, and Social Security numbers – vulnerable to security breaches.

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 North Carolinians.

In 2020, organizations submitted 1,644 data breach notices to DOJ. These breaches put nearly 1.2 million North Carolinians' personal information at risk.

This report highlights the most common types of data breaches in 2020 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.

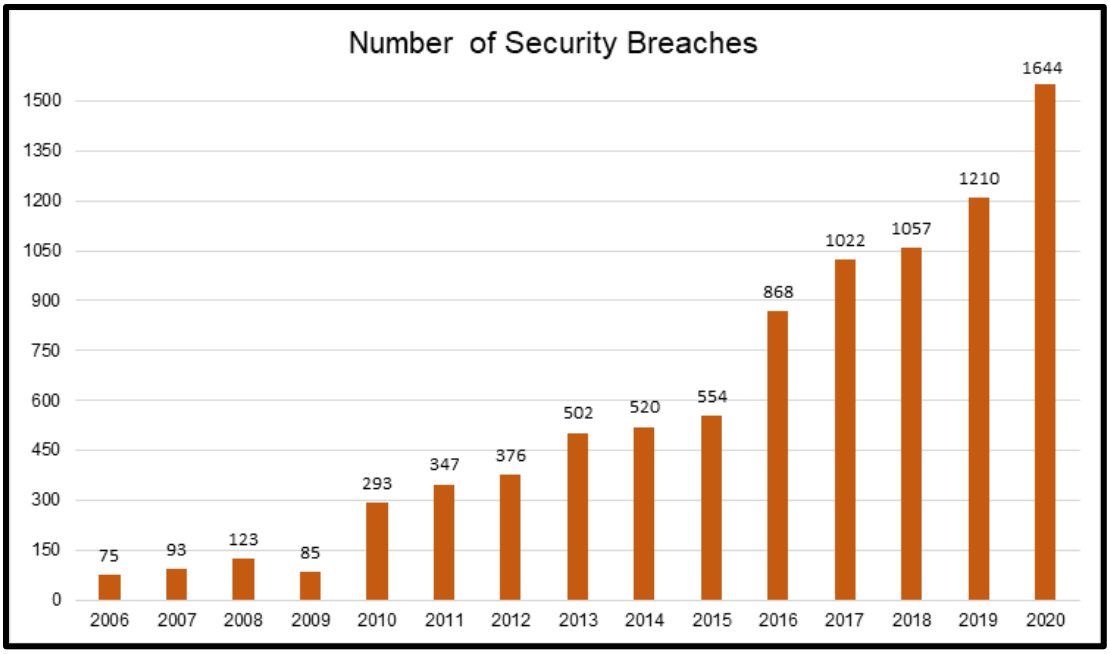


Highlights

- 2020 marks a record number of data breach notices submitted to DOJ. The 1,644 data breach notices submitted this year represent a 36 percent increase from 2019.
- In 2020, nearly 1.2 million North Carolinians were affected by data breaches.
- Ransomware breaches accounted for 22 percent of all breaches in 2020, more than an 18 percent increase from the year before.
- Email breaches made up nearly 40 percent of all breaches in 2020, about a 10 percent drop from 2019.

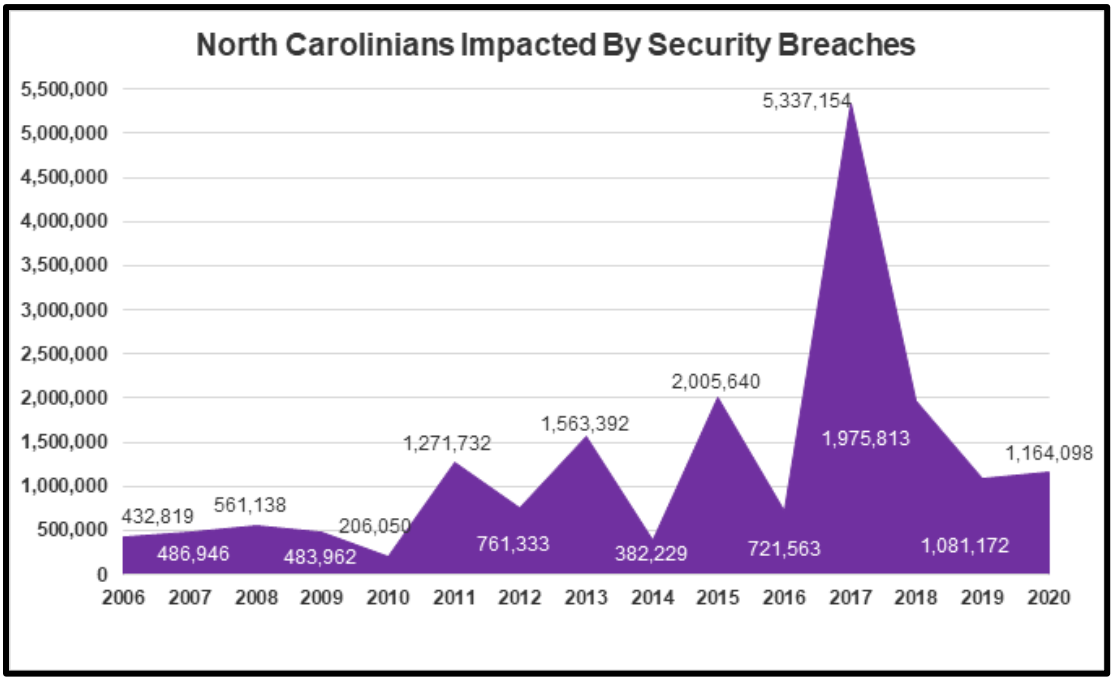
Background

Since 2005, organizations have reported 8,769 data breaches to DOJ. The 1,644 data breaches reported in 2020 marked 434 more reported breaches than 2019, the largest year-to-year increase on record.



As North Carolinians battled the health and economic effects of the COVID-19 pandemic in 2020, hackers and fraudsters looked to take advantage. These breaches affected nearly 1.2 million North Carolinians.

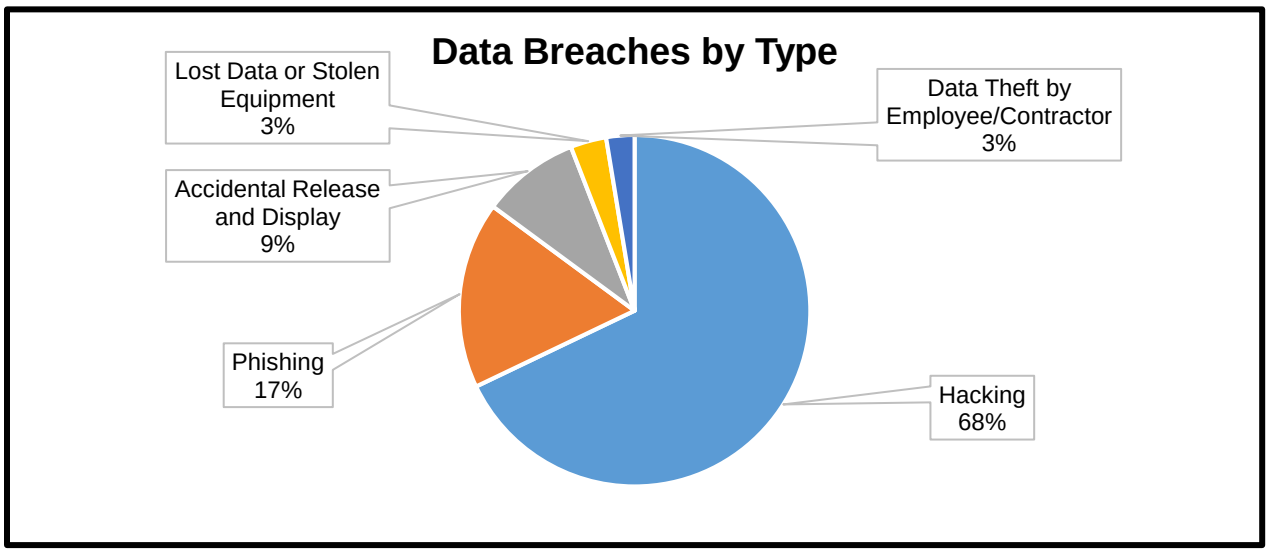
People share personal information with companies through phones, laptops, watches, and other technology. The more information that companies have, the higher the risk for security breaches.

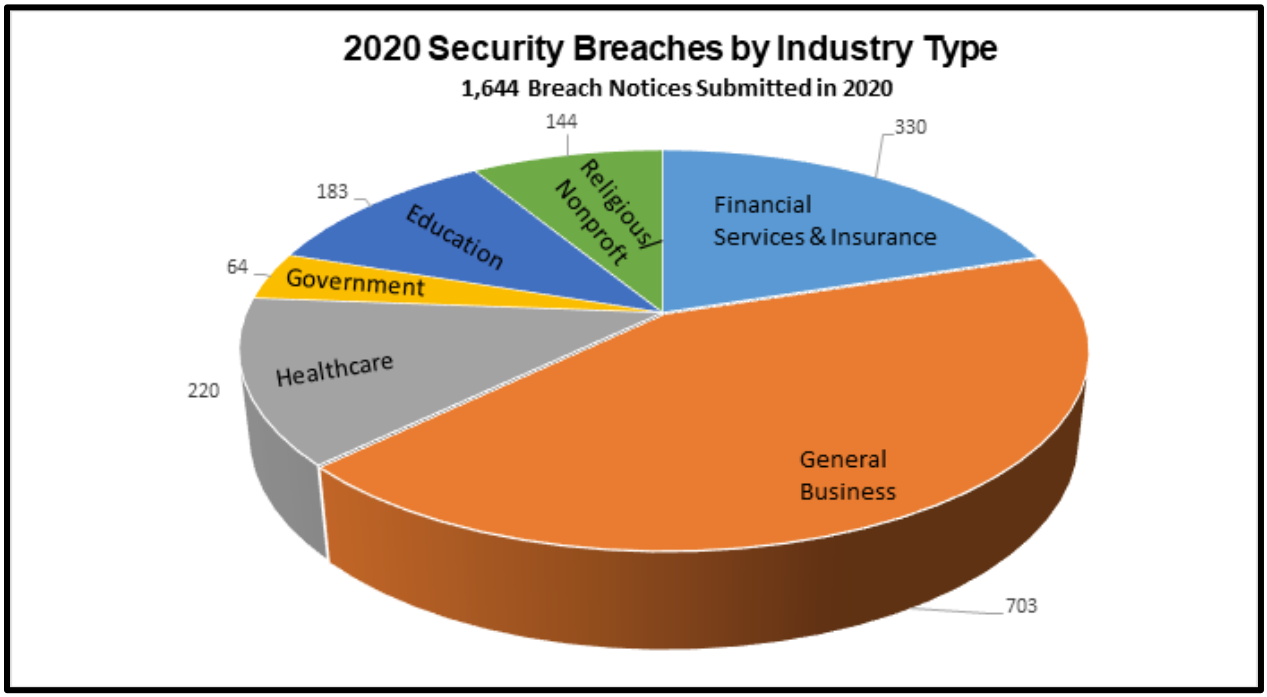


Note: In 2017, Equifax experienced the largest-ever data breach in history affecting nearly 5 million North Carolinians, resulting in a higher number of people having their information compromised that year.

Overview of 2020 Breaches

Hacking accounted for the majority (nearly 70 percent) of data breaches in 2020, an increase of 80 percent in hacking breaches since 2019 and 135 percent since 2018. Phishing and accidental release of information accounted for nearly a quarter of 2020 breaches, and stolen equipment and data theft by an employee or contractor made up less than five percent of breaches.

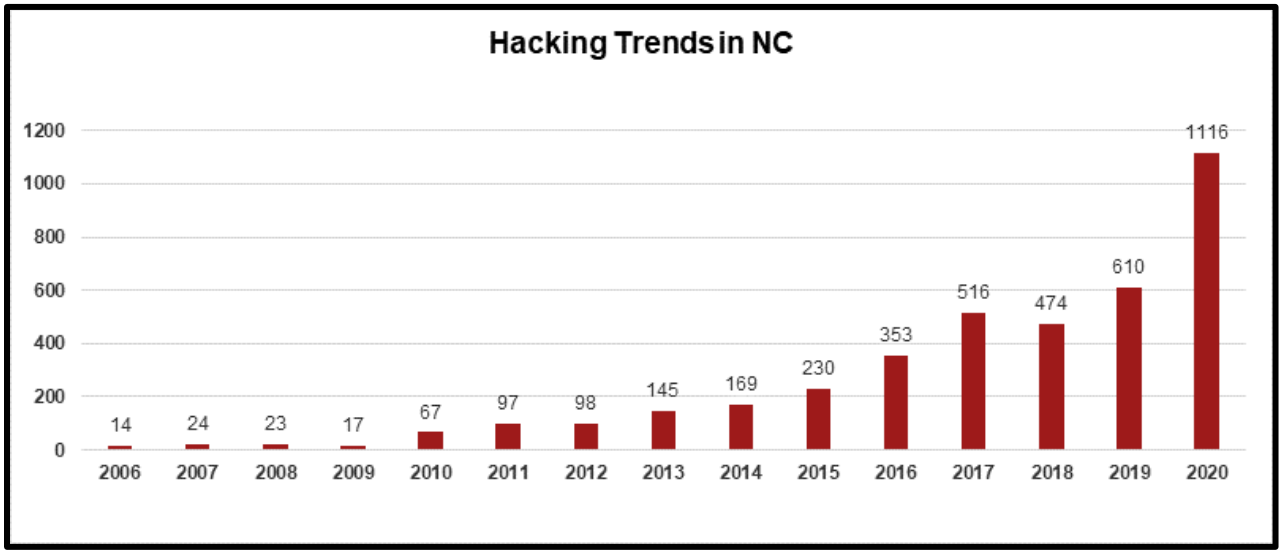


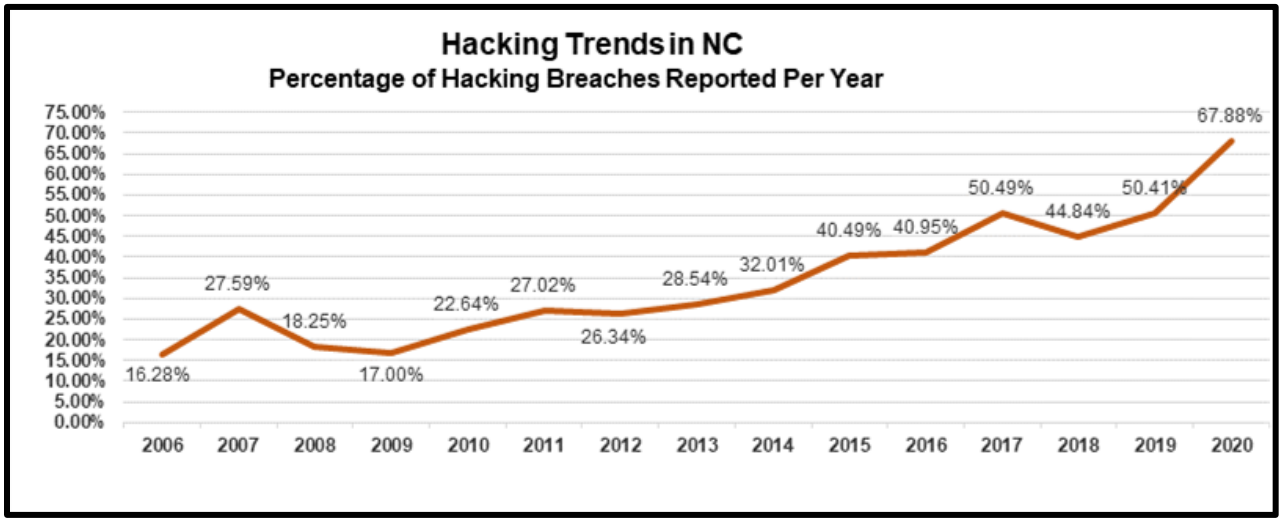


HACKING

Hackers gain access to North Carolinians' personal and financial information by breaking into an organization's internal electronic systems. As technology progresses, hackers get even more efficient at exploiting weaknesses in security systems. These breaches are especially damaging because sometimes, organizations may not even know they have been the victim of a hack.

Hacking accounted for the majority of security breaches reported last year in North Carolina. The 1,116 security breaches caused by hacking represent an all-time record in the state, and more than an 80 percent increase since last year. For the third year, these breaches make up the majority of those reported to DOJ.





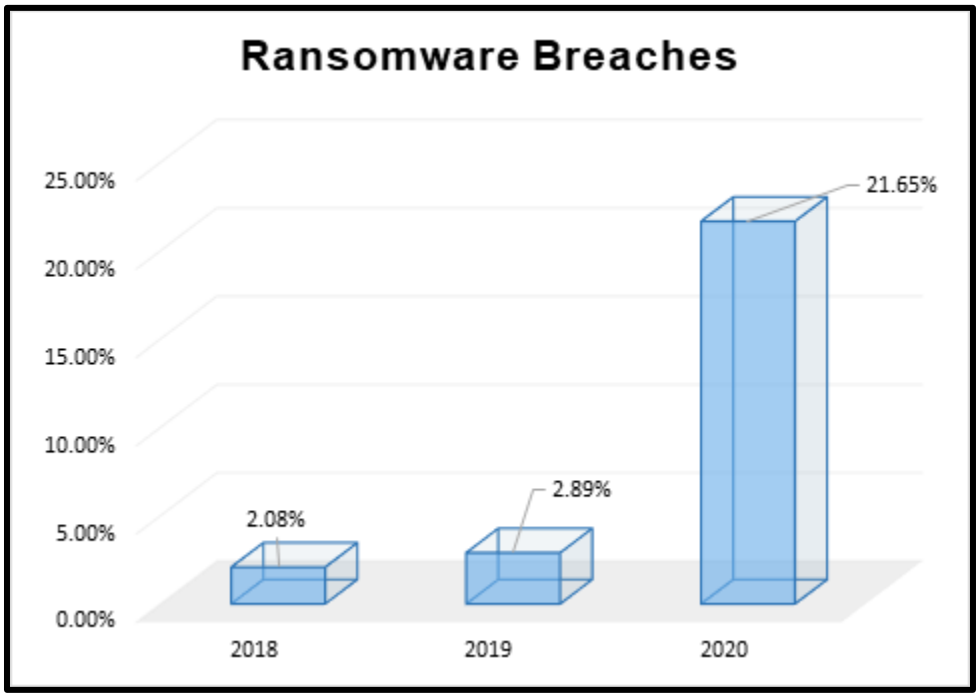
The best way to prevent from falling victim to a hack is to follow these tips:

- Keep the security software on your devices up to date.
- Beware of phishing emails that trick you into clicking on attachments that give the criminals access to your computers.

- Be careful about what information you share with organizations online, and only disclose private information like Social Security numbers, banking numbers, or birth dates if absolutely necessary.
- Monitor your financial statements for irregularities and request a free credit report at annualcreditreport.com.
- If you believe you have been the victim of a hack, request a free security freeze and contact our office.

Gaining Access through Ransomware and Email

Ransomware-related breaches jumped dramatically in 2020, making up more than 20 percent of all breaches that were reported to our office. Ransomware can refer to many types of malware, including viruses and other types of unauthorized digital programs that hackers can use to gain access to a device or network, and then encrypt and hold the data available for ransom in exchange for money. Even if a person or business pays the ransom, they may not always be able to recover their data, and the financial impact can be overwhelming.



One significant driver of ransomware attacks in 2020 was the Blackbaud attack, which was linked to 214 of the 356 ransomware breach notices. Blackbaud is a cloud services vendor that works with many schools, universities, non-profit organizations, and health care systems. While the extent of the breach is still being determined, data compromised includes bank account information, Social Security numbers, and other identifying details.

Here are some ways to guard your data and networks against ransomware:

- Keep your anti-virus and other malware software updated.
- Back up your data regularly.
- Make sure you only conduct business on secure networks and through legitimate URLs.

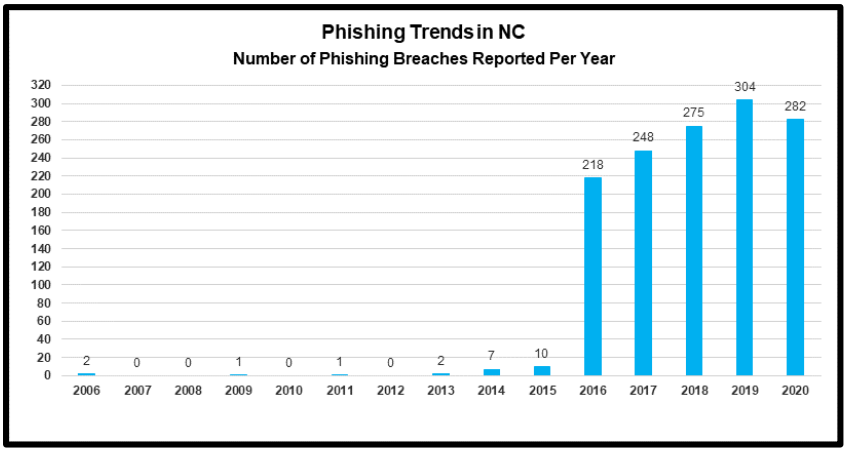
- Conduct a risk analysis of your network and security systems and conduct your own hacking attempts to find any security gaps.
- Patch any vulnerabilities in your security system as soon as you identify them.
- Allow only approved, verified programs and software to run on your computer and networks.
- Ensure that anyone who has access to your network has been trained on best practices in cybersecurity and knows what to do if a hacking or ransomware incident occurs.
- Do not click on attachments in phishing emails.

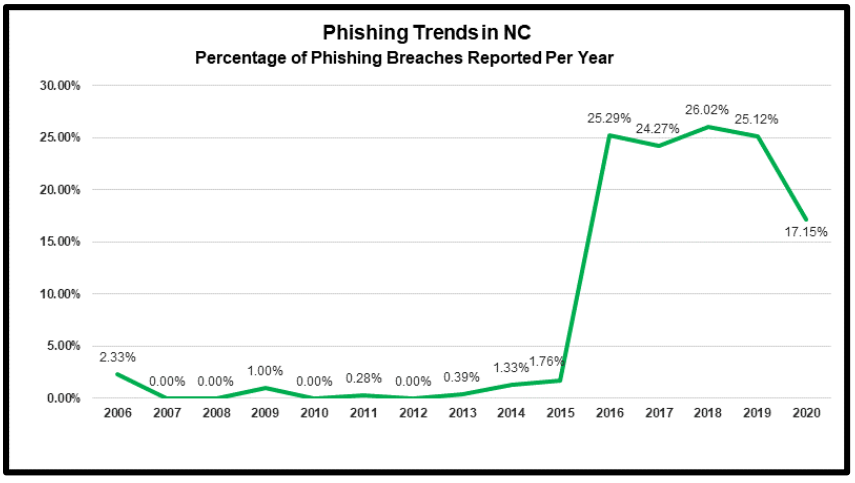
If you think you've been the victim of a ransomware attack, report it to the FBI or the U.S. Secret Service immediately. Learn more about ransomware attacks here.

PHISHING

Phishing attacks occur when criminals try to trick victims into clicking on a link or replying to phony emails or text messages. Phishing attacks can appear legitimate – the message may look like it comes from an email address or person you know or a company you do business with. But these attacks give criminals access to the information on the networks or computers they infiltrate.

Almost 300 breaches caused by phishing attacks were reported to our office last year, and phishing breaches continue to remain a threat to people's online security.





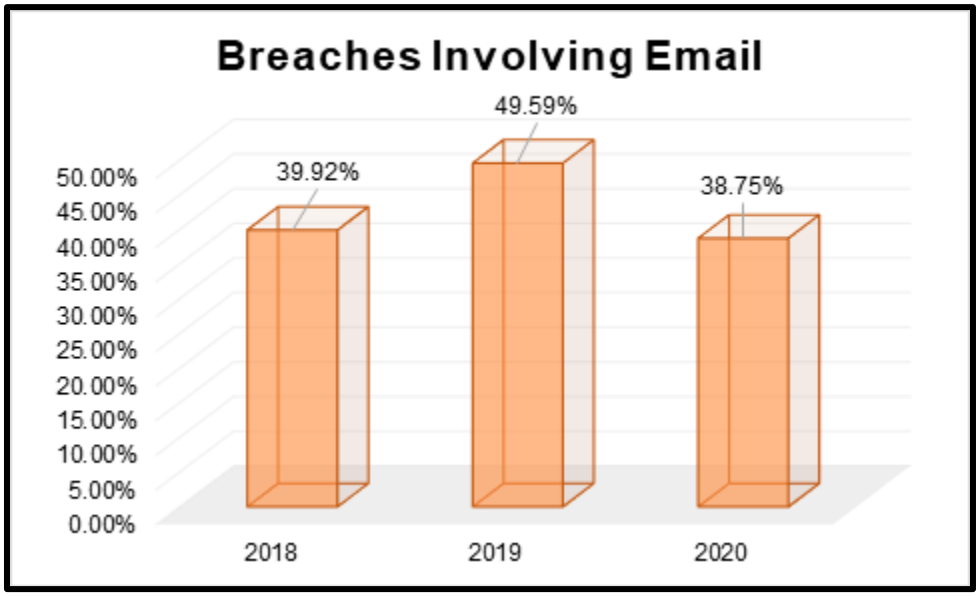
Email Breaches

Breaches involving email continued to stay high in 2020, making up nearly 40 percent of all reported breaches. Email breaches occur when the security of someone's email account is compromised. People's data might be breached through email with a phishing scam, but they may also inadvertently give people access to their email or have weak password and verification measures that make it easier for others to gain access.

If you receive what you think might be a phishing email, text, or social media message, don't respond, click on links, download attachments, or input any information.

Report the message by forwarding a copy to or filing a complaint with:

- The organization the scammer is pretending to represent
- reportphishing@apwg.org (email) or SPAM/7726 (text)
- DOJ's Consumer Protection Division (ncdoj.gov/complaint)
- FTC (ftc.gov/complaint)

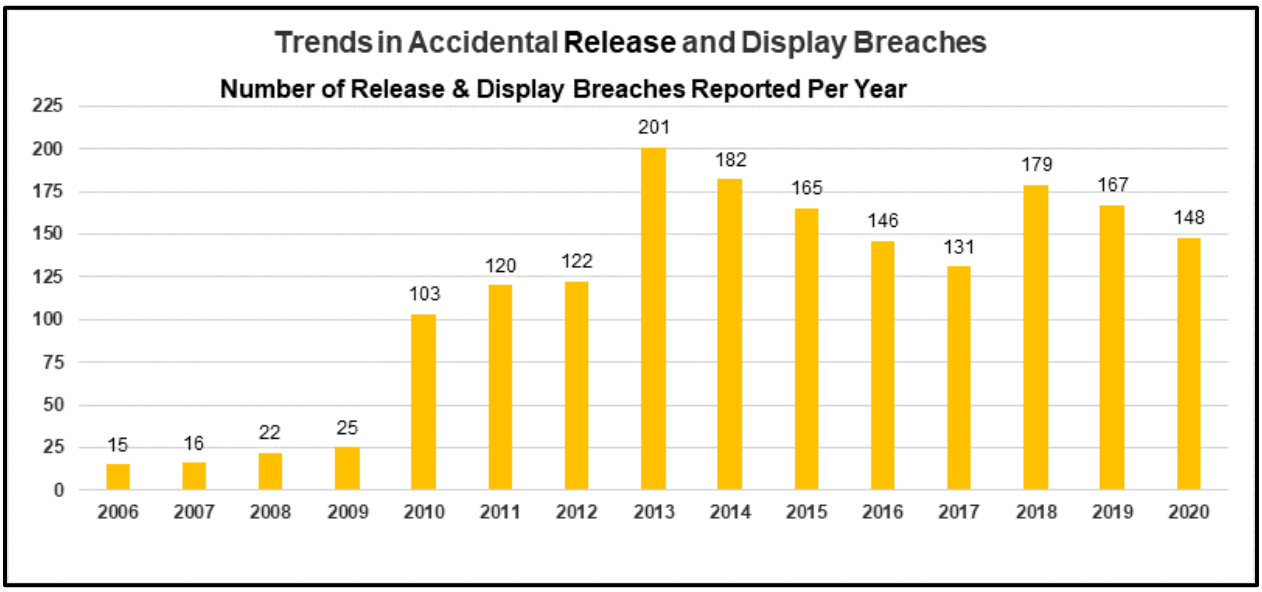


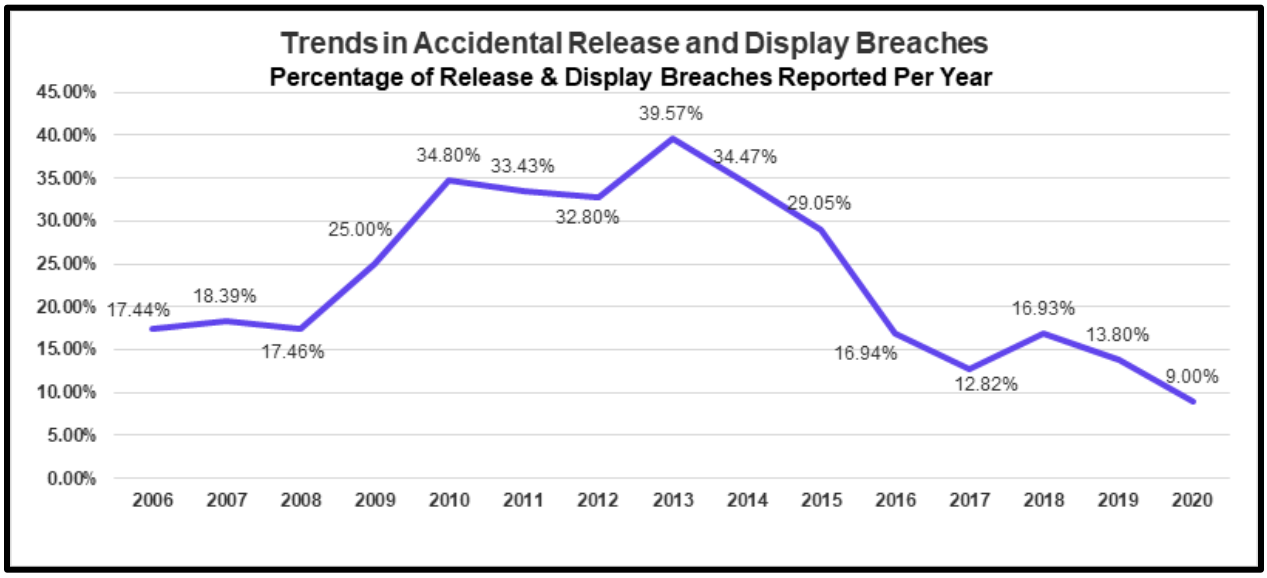
You can reduce the risk of being a victim of a phishing email by taking these steps:

- Make sure your passwords are strong, and don't share them with others.
- Check to see what authentication measures are available on the email platform or digital device you're using.
- Never send sensitive personal information via email that others could have access to if your email account is compromised or the recipient's email account is compromised.

Accidental Release and Display

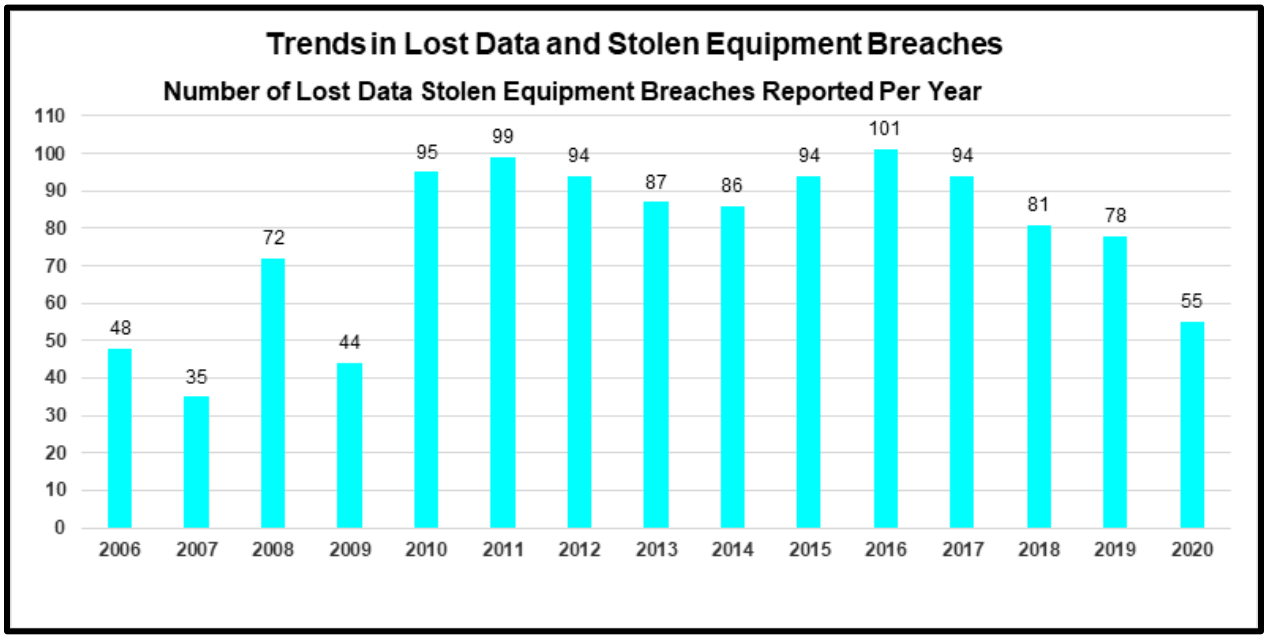
Accidental release and display breaches continued to drop in 2020, an 11 percent decrease to 148 breaches. Such breaches are often the result of vulnerable security practices that make it easier for data to be compromised. A business or government employee might not appropriately secure data they are responsible for safeguarding, leave their passwords or other verification information in places where others can access it, or make other mistakes that lead to people's information being left unprotected.

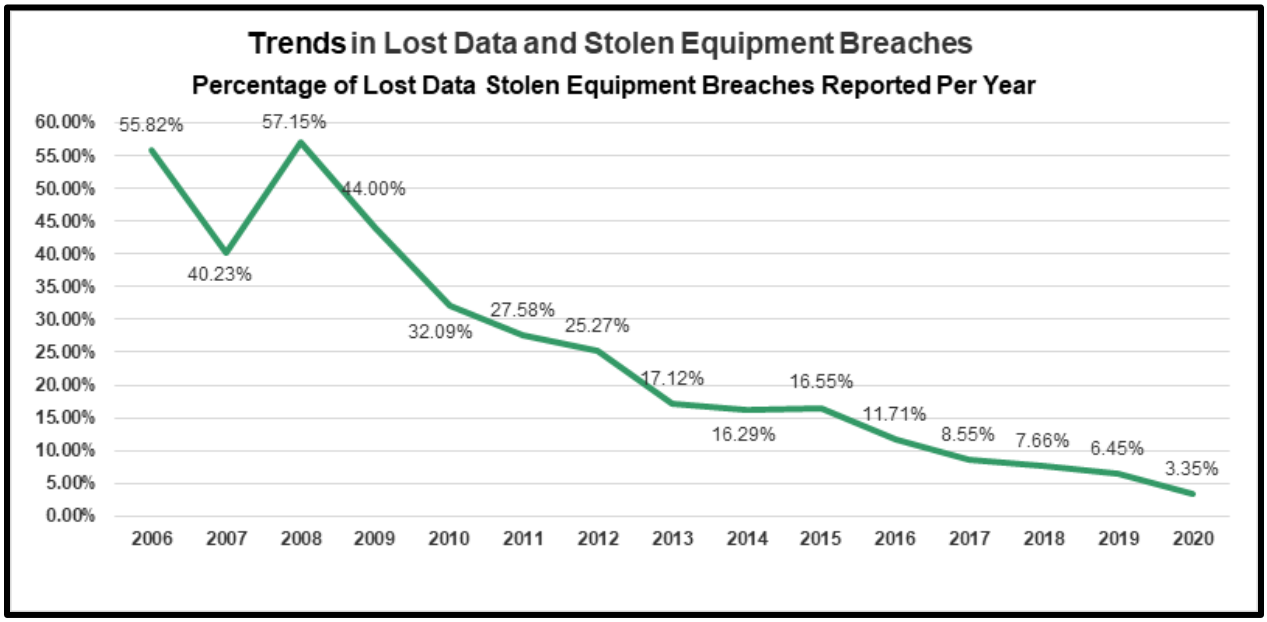




Lost in Transit or Stolen Equipment

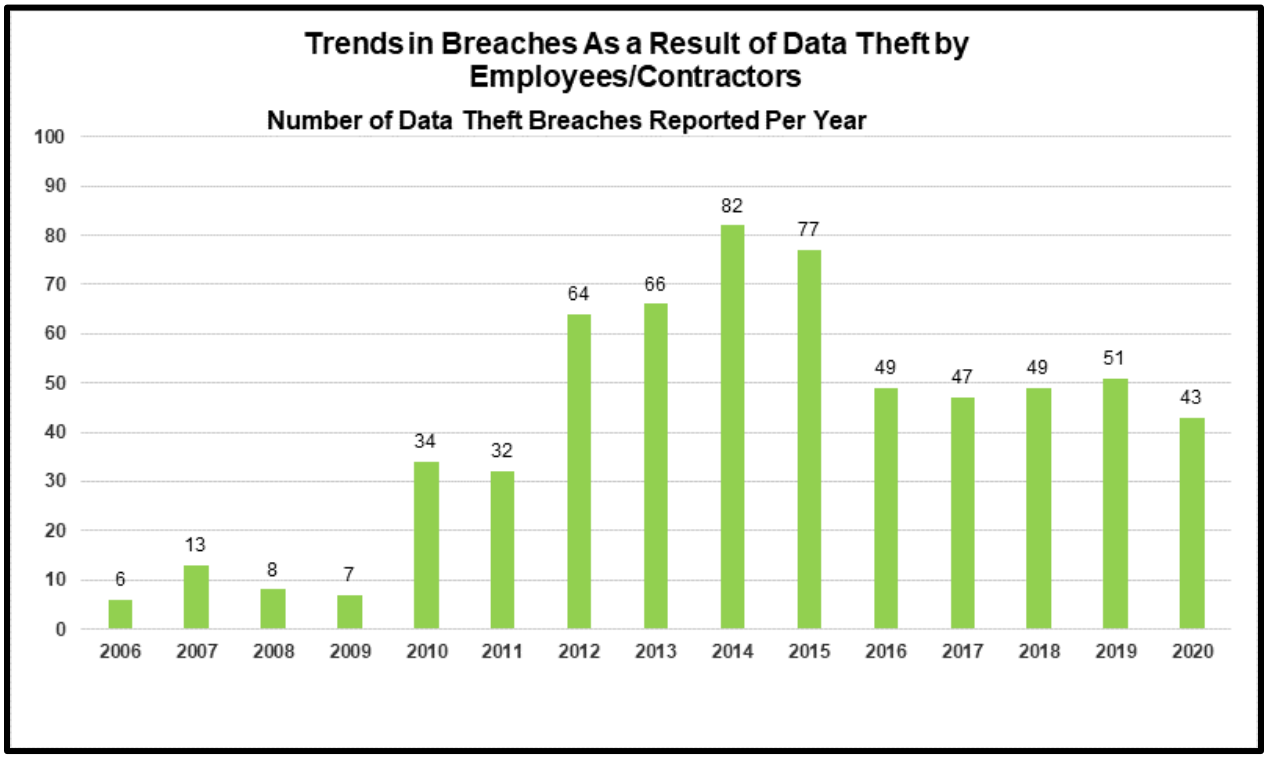
Data breaches caused by equipment lost in transit or stolen are at their lowest level in a decade – only 55 such breaches occurred this year, down nearly 30 percent from 2019. These breaches occur when data or the devices it is stored on is lost, misplaced, or stolen.





Data Theft

Data theft by employees or contractors is consistently one of the smallest causes of a breach. In 2020, only 43 breaches – approximately 2.6 percent – of all breaches were caused by employee data theft.



Protecting North Carolinians' Data and Privacy

Attorney General Stein cares deeply about protecting your personal information and will aggressively enforce state law on violators. He and the Department of Justice won several data-breach related settlements in 2020. In September, he announced a $39.5 million multistate settlement with Anthem over a 2014 data breach that compromised the information of 78.8 million individuals, including 775,606 North Carolinians. The information compromised included names, dates of birth, Social Security numbers, health care identification numbers, home addresses, email addresses, phone numbers, and employment data. Under the settlement, North Carolina will receive $401,172.38 and Anthem has also agreed to a series of steps to strengthen its security practices going forward.

In November, Attorney General Stein won a $17.5 million multistate settlement against Home Depot to resolve an investigation over a 2014 data breach that exposed the financial data of approximately 40 million Home Depot customers. The breach occurred when hackers gained access to Home Depot's network and deployed malware on its self-checkout point-of-sale system.

Attorney General Stein also won a $2.4 million multistate settlement with Sabre Corporation over a 2017 data breach of its hotel booking system. The breach exposed the data on approximately 1.3 million credit cards.

In October, Attorney General Stein won a $5 million judgement against Community Health Systems over a data breach that affected approximately 6.1 million people. At the time of the data breach, CHS owned or operated six hospitals in North Carolina, and 59,527 North Carolinians had their names, birthdates, Social Security numbers, and addresses exposed.

Attorney General Stein also took steps to further protect North Carolinians' privacy online. In December, after leading a multistate investigation into Facebook, he sued the company alleging that it used its monopoly power to buy and bury competitors and cut services to other companies. These actions ultimately harm people by reducing privacy protections for consumers.