NORTH CAROLINA DEPARTMENT OF JUSTICE

2019 DATA BREACH REPORT

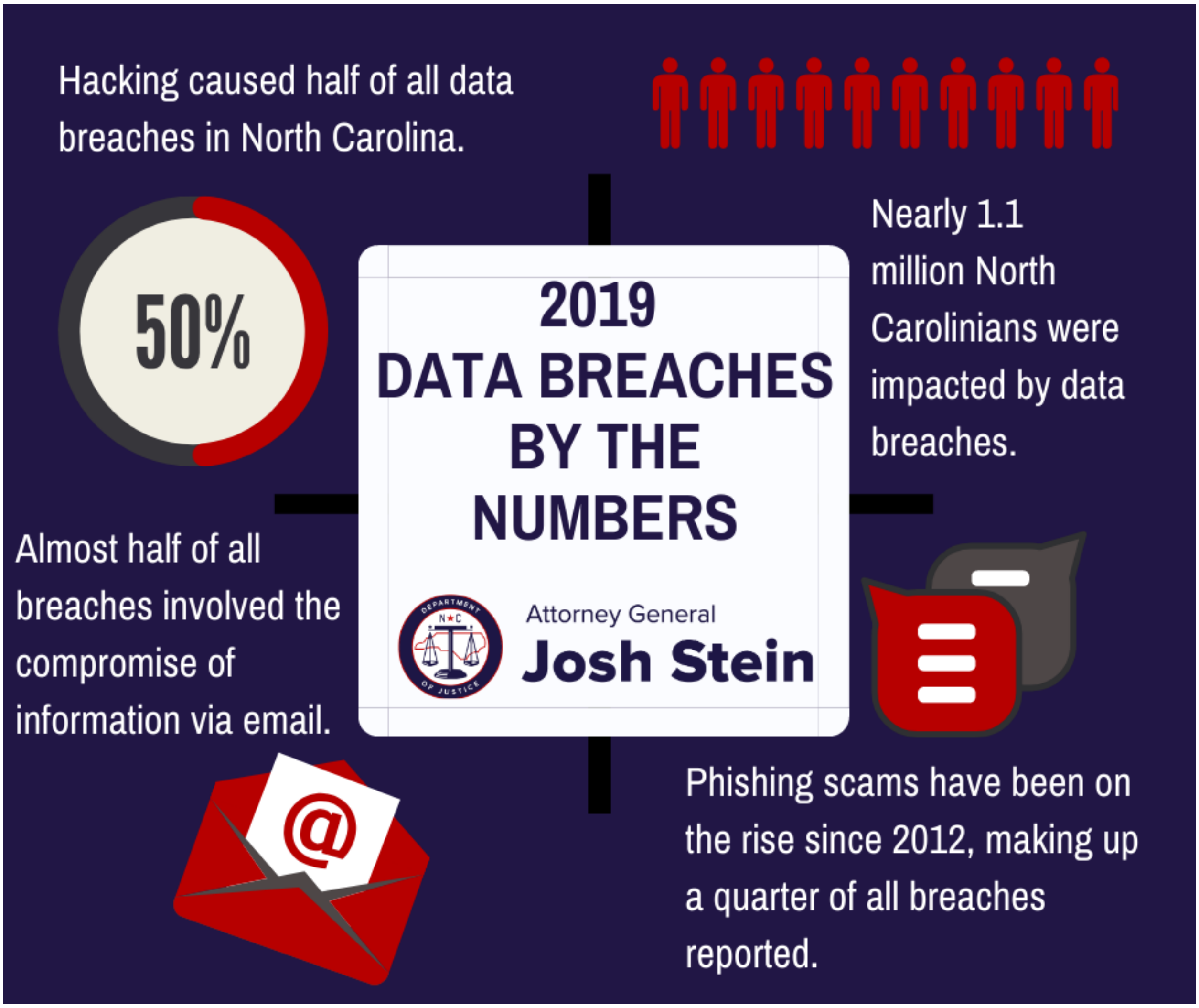
Attorney General
Josh Stein

Executive Summary

Under North Carolina law, businesses and government agencies must notify the North Carolina Department of Justice (DOJ) if a data breach, an unauthorized access or acquisition of records or data concerning personal information, occurs.

In 2019, organizations submitted 1,210 data breach notices to DOJ. These breaches affected nearly 1.1 million North Carolinians.

This 2019 data breach report shares more about the types of data breaches that DOJ was notified of last year and discusses how these breaches compare to previous years. The report also shares more information on what actions North Carolinians should take to protect their information before and after a security breach and the work Attorney General Josh Stein is doing to increase protections for people's personal and financial data.



Hacking caused half of all data breaches in North Carolina.

Nearly 1.1 million North Carolinians were impacted by data breaches.

2019 DATA BREACHES BY THE NUMBERS

Attorney General Josh Stein

Almost half of all breaches involved the compromise of information via email.

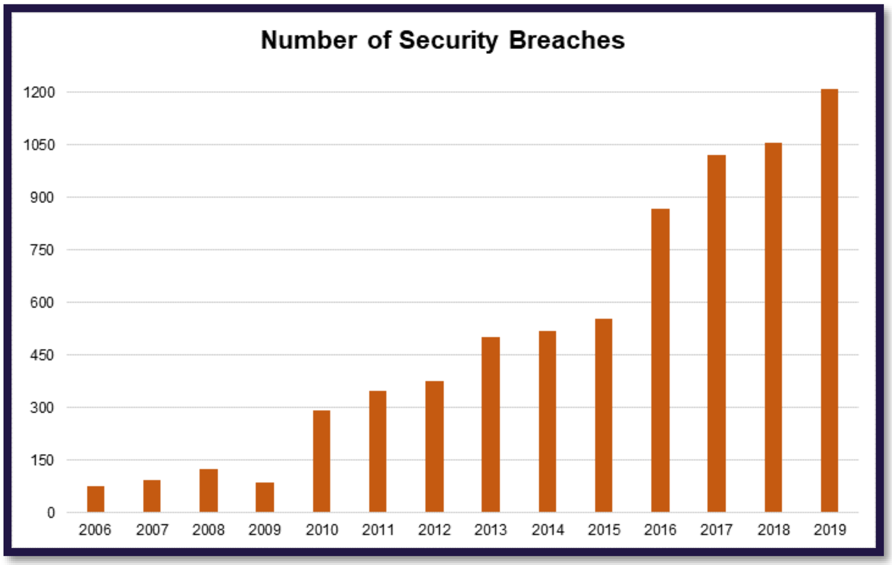
Phishing scams have been on the rise since 2012, making up a quarter of all breaches reported.

Significant Findings:

- In 2019, 1.08 million North Carolinians were affected by data breaches, a 45 percent decrease from the 1.9 million North Carolinians affected in 2018.
- The number of data breaches submitted in 2019 (1,210) were the highest number ever submitted to DOJ.
- Hacking breaches reached an all-time high in 2019, with the 610 breaches related to hacking making up more than half of all reported breaches this year.
- Phishing scams increased by 10 percent since 2018, with 304 breaches reported in the last year.
- Nearly half of all breaches reported involved emails in 2019, up 10 percent from breaches involving emails in 2018.
- Accidental release and display breaches and lost-in-transit and stolen equipment breaches both declined in 2019.

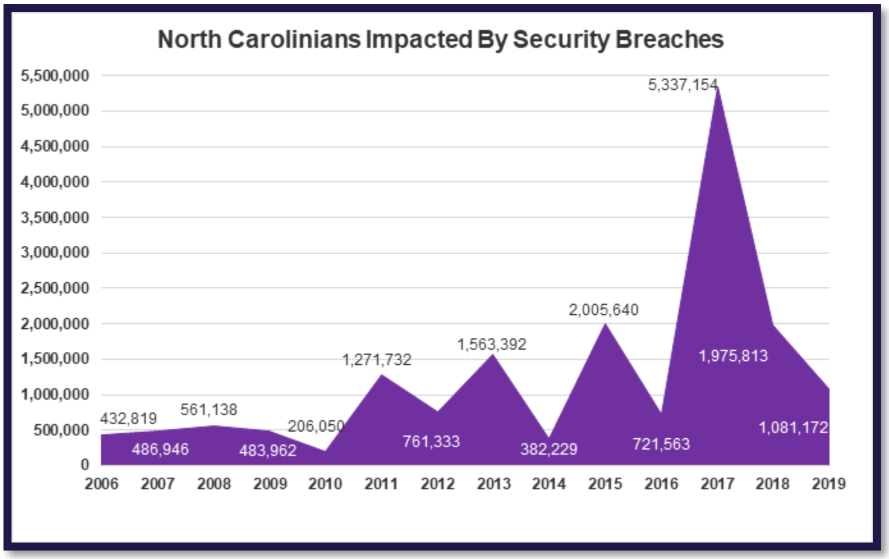
Background

Since 2005, companies and government agencies have reported 7,271 breaches. Nearly 17 percent of all of those breaches were reported in 2019.



Since reporting requirements took effect in 2006, the number of North Carolinians affected by security breaches has more than doubled. That jump is driven by an increase in personal tech devices, online scams, and an increase in the variety and amount of personal information and data that consumers share and companies keep on file.

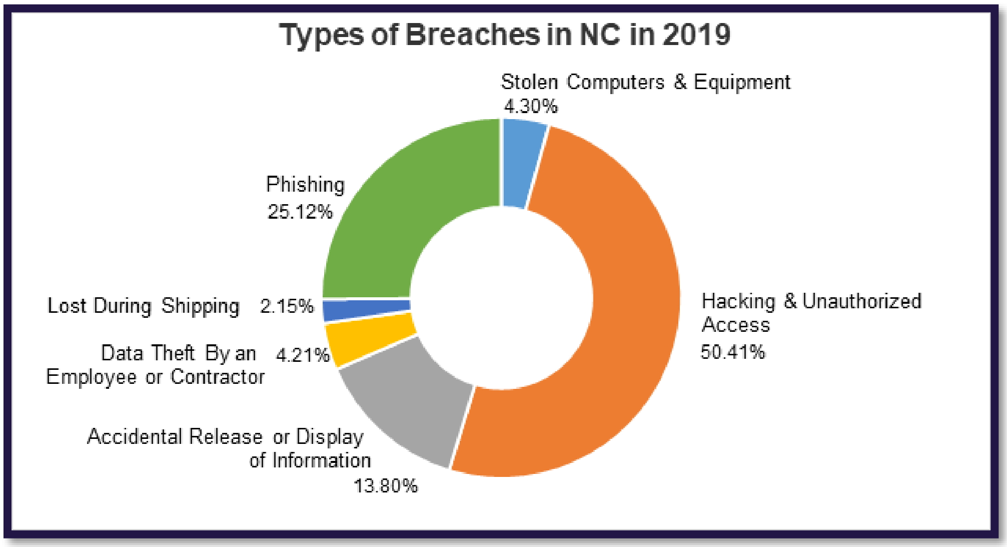
People share a lot of personal information with companies, businesses, and government agencies through phones, laptops, watches, and other devices. But the more information that companies have, the higher the risk for security breaches that compromise consumers' personal data and leave them vulnerable to identity theft, financial fraud, account hacking, and scams.



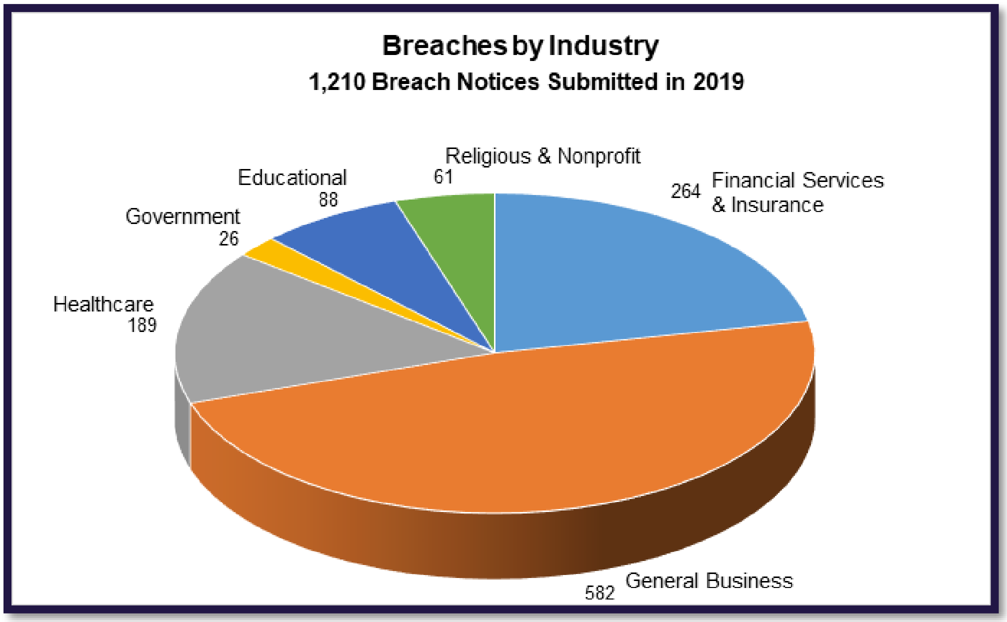
Note: In 2017, Equifax experienced the largest-ever data breach in history, leading to a higher number of North Carolinians having their information compromised that year.

Data Breaches in North Carolina

In 2019, half of all data breaches were caused by hacking and unauthorized access and another quarter were a result of phishing scams. The remaining quarter of breaches were caused by data theft, accidental release or display of information, and stolen and lost-in-transit computers and equipment.



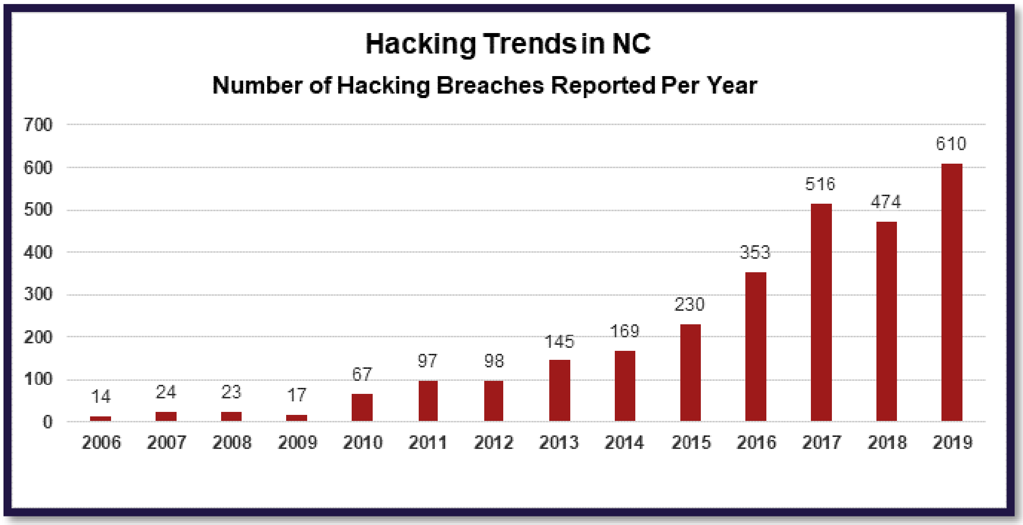
Data breaches were most often reported by general businesses in 2019, followed by financial services and insurance businesses and health care organizations. These three industries saw approximately 85 percent of all the data breaches reported last year.

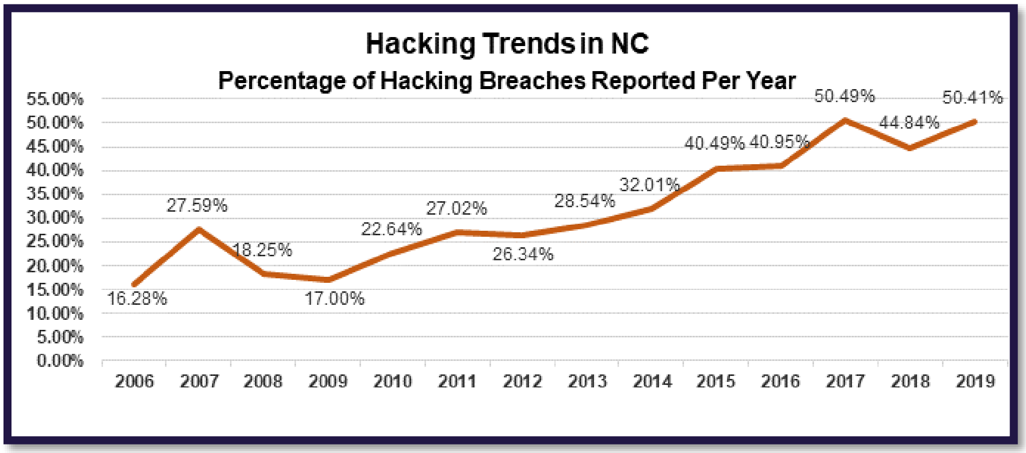


Hacking and Unauthorized Access

In 2019, 610 hacking breaches were reported – more than half of all breaches this year and more than ever before (a 29 percent increase from 2018).

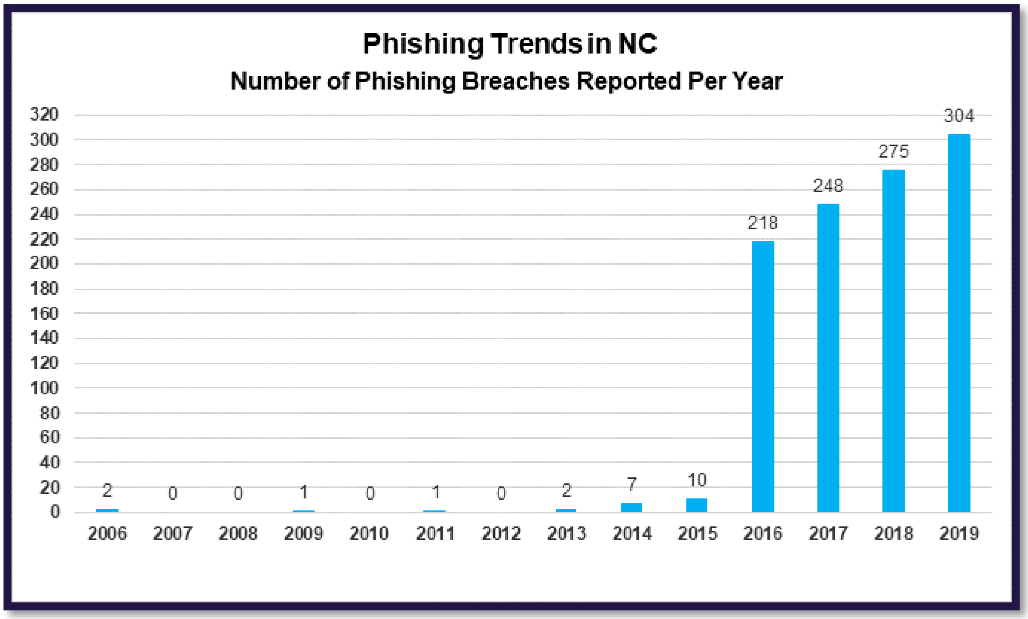
Hackers will search for ways to bypass company security systems to gain unauthorized access to company and consumer data. They can steal that data and use it to commit identity theft and fraud. When companies fail to implement strict security standards and monitor their networks, it is easier for hackers to find a way in and stay undetected for longer periods of time.

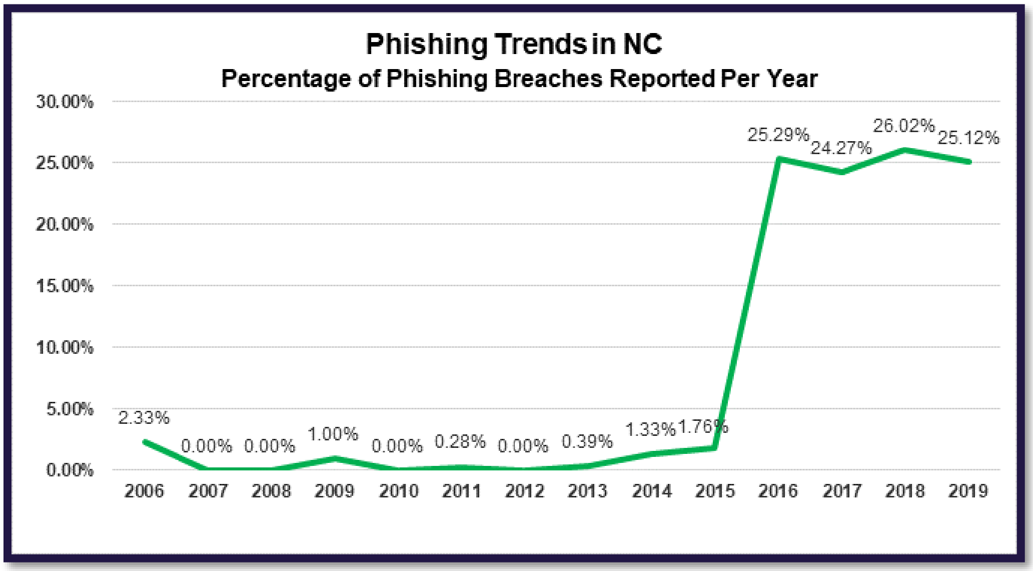




Phishing

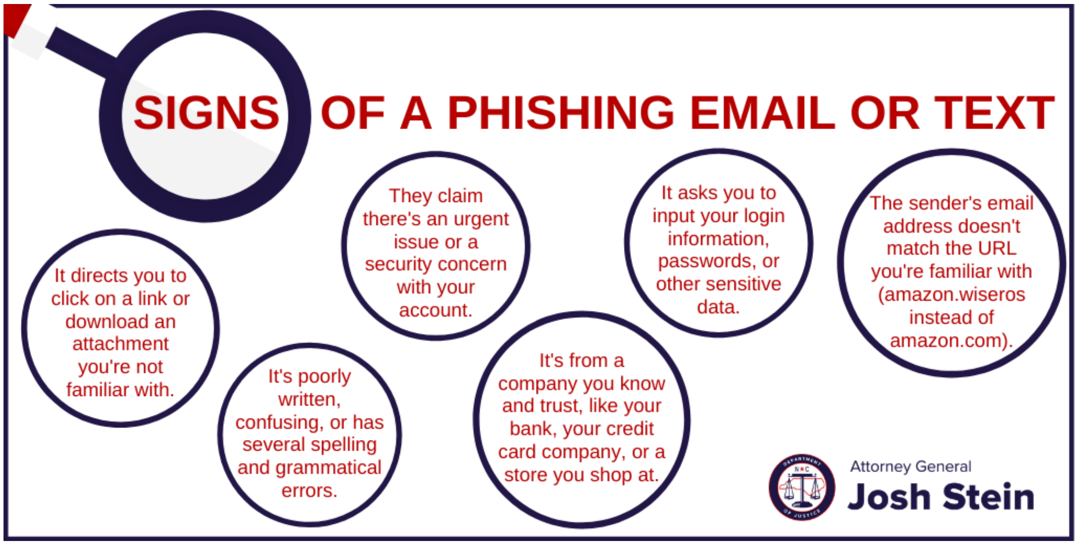
304 phishing breaches were reported in North Carolina last year, an all-time record and a 10 percent increase from 2018. Phishing breaches made up a quarter of all reported breaches in 2019. Phishing scams are successful because the solicitations appear to come from someone you know or trust – your bank, a store you shop at, or a company you have done business with. Often, they claim there's an issue with your account, an important update, or a change you need to make. The message might include additional details that make it look authentic. But the included links will redirect you to phony websites, and by sharing your account information or personal details, you give scammers unauthorized access.





Before you share information, take a minute to review the message. Are you expecting the company to reach out? Is it a question the person would typically ask you? Does it involve sharing personal or delicate information?

If any of these are the case, verify by contacting the sender at a phone number or email you know to be legitimate. Be suspicious of anyone requesting sensitive personal data, such as Social Security Numbers or W2s. Double-check the sender's address to make sure it is legitimate and the URL to make sure it does not send you to a non-secure website. The address bar should include a lock icon and "https".



SIGNS OF A PHISHING EMAIL OR TEXT

It directs you to click on a link or download an attachment you're not familiar with.

It's poorly written, confusing, or has several spelling and grammatical errors.

They claim there's an urgent issue or a security concern with your account.

It's from a company you know and trust, like your bank, your credit card company, or a store you shop at.

It asks you to input your login information, passwords, or other sensitive data.

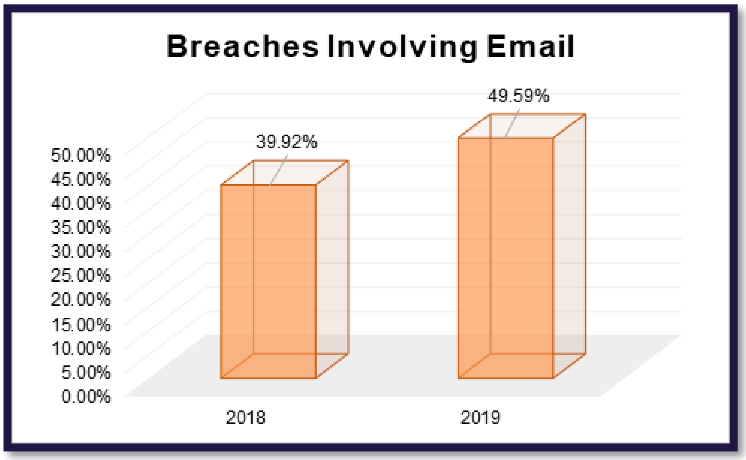
The sender's email address doesn't match the URL you're familiar with (amazon.wiseros instead of amazon.com).

Attorney General
Josh Stein

If you receive what you think might be a phishing email, text, or social media message, report it to the organization the scammer is pretending to represent, and forward a copy to reportphishing@apwg.org (email) or SPAM/7726 (text). You should also file a complaint with DOJ's Consumer Protection Division at ncdoj.gov/complaint and with the FTC at ftc.gov/complaint.

The uptick in phishing and hacking scams means that email accounts are increasingly linked to data breaches. In fact, nearly 50 percent of all breaches reported in 2019 involved email.

To help protect your email account and the data it contains, be careful about the messages you open and the links you click. Be suspicious of any messages that include files or attachments you do not recognize. Make sure your device's security software is up to date, and change your passwords regularly. Use unique, complex passwords and enable additional authentication factors if available.



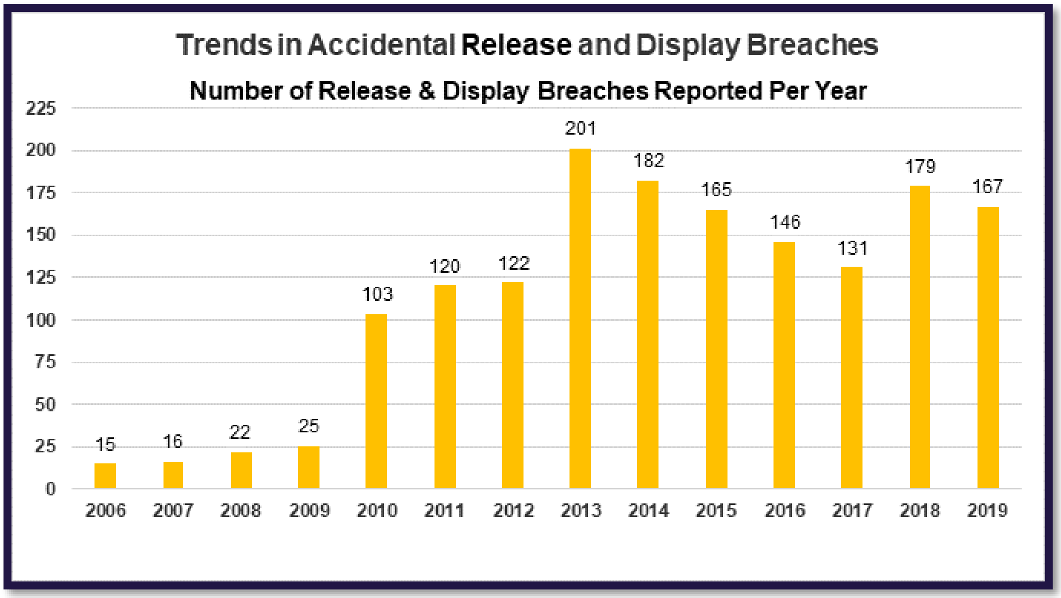
Be careful about sending emails with sensitive information – if a scammer gains access to your account or reviews an email with your sensitive data, you’re vulnerable to identity theft and fraud. Try not to send sensitive information by email, but if you need to, be sure that you’re sending it to only the intended recipient. Don’t get fooled by an auto-populating “To” field or email contacts with similar names. If you’re not careful about sending sensitive data, you may also unwittingly send your or others’ information to the wrong recipient.

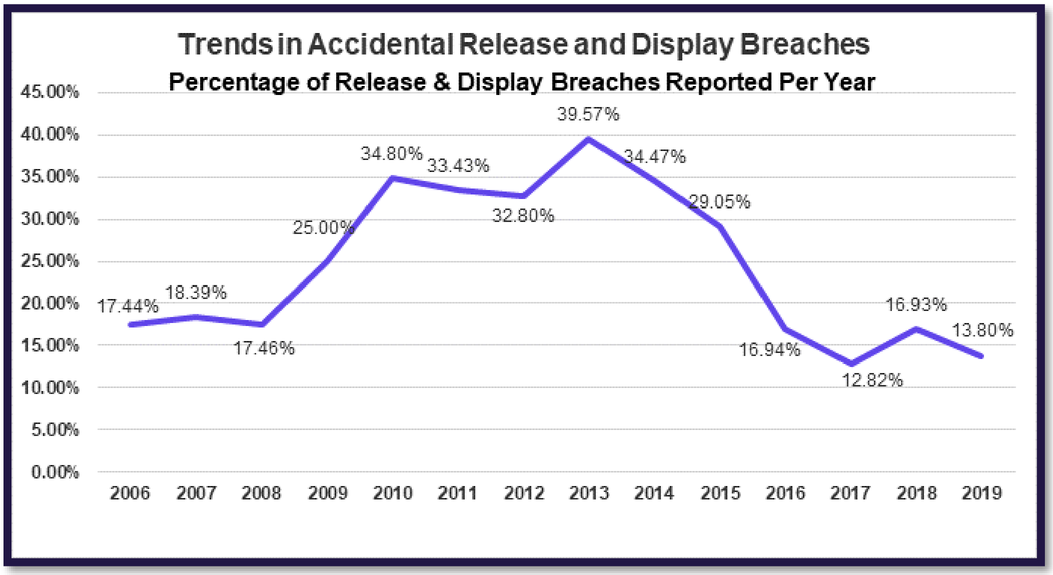
If you are concerned that someone has gained access to your email account or information without your knowledge or permission, report it to local law enforcement immediately. If a corporate email account was hacked, report it to the relevant corporation.

Accidental Release and Display

Breaches caused by accidental release and display dropped 7 percent in 2019. A total of 167 breaches were reported.

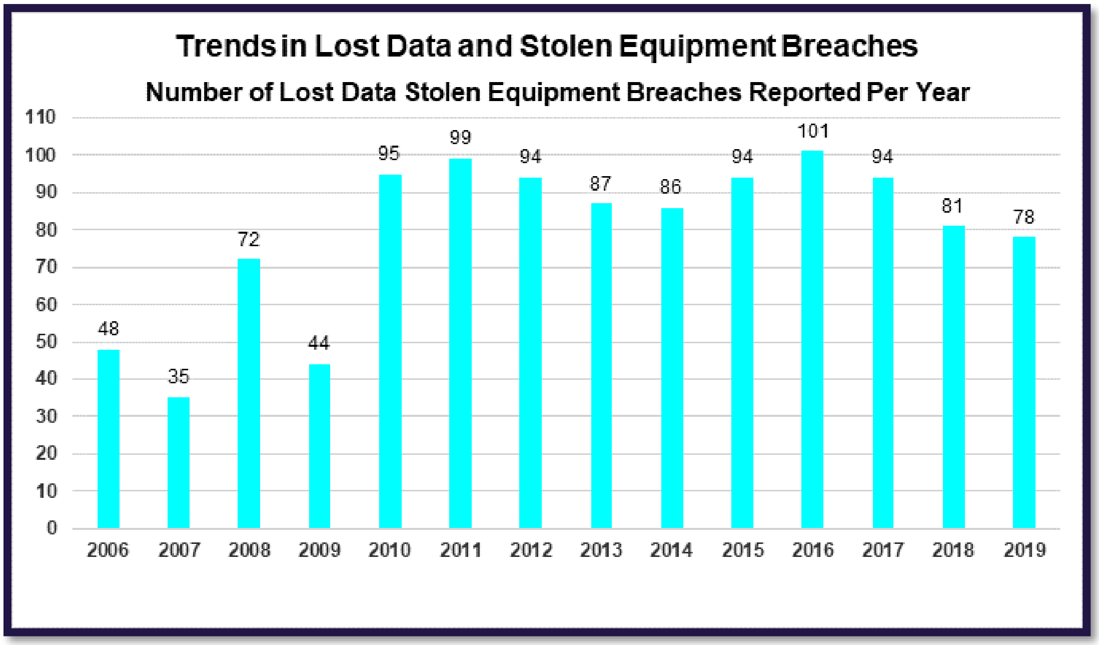
Accidental release and display breaches are the result of human error. For example, employees may store information in the wrong place or without following appropriate protocols, share it with the wrong person, or otherwise mistakenly give away private or confidential data in a manner that leaves it vulnerable to theft.

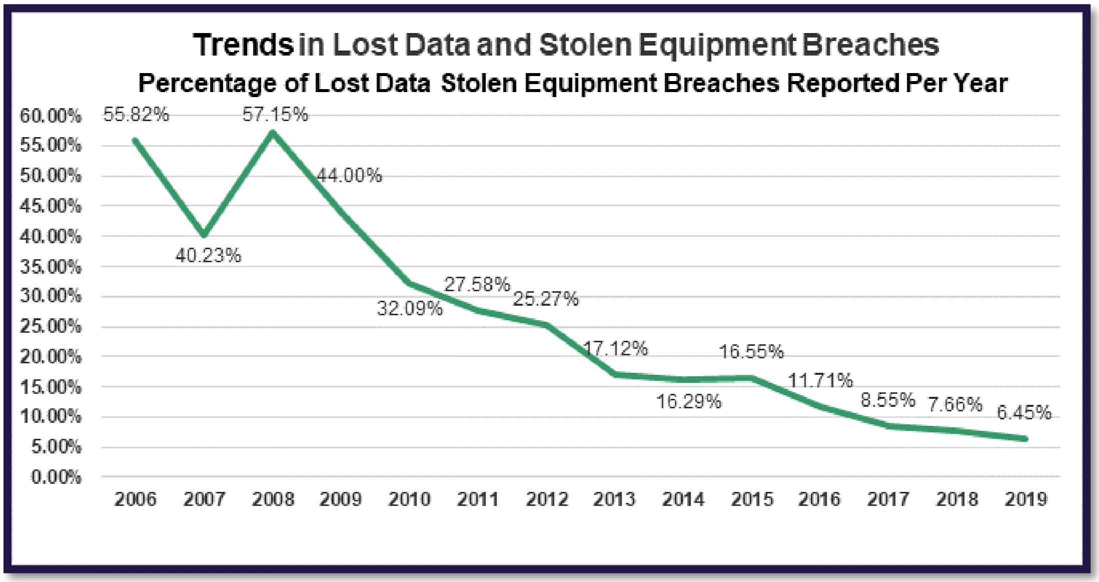




Lost in Transit or Stolen Equipment

Breaches caused by information on equipment that is lost in transit, misplaced, or stolen also continued to drop. 78 breaches were reported in 2019, a 22 percent decrease over the past three years.





Protecting North Carolinians’ Data

In July, Attorney General Josh Sein announced the largest-ever data breach settlement in history with Equifax to address the largest-ever breach of consumer data. The 2017 data breach affected more than 147 million consumers – nearly half of the U.S. population. Compromised information included Social Security numbers, names, dates of birth, addresses, credit card numbers, and in some cases, driver’s license numbers.

Attorney General Stein served on the executive committee of the multistate investigation into the breach, which found that Equifax failed to put adequate security measures in place to protect consumer data, fully patch its systems, and update breach monitoring software.

The $425 million settlement included payouts to the state for consumer restitution and redress. Equifax also agreed to take steps to help consumers protect themselves against identity theft and to address financial and credit issues caused by the data breach.

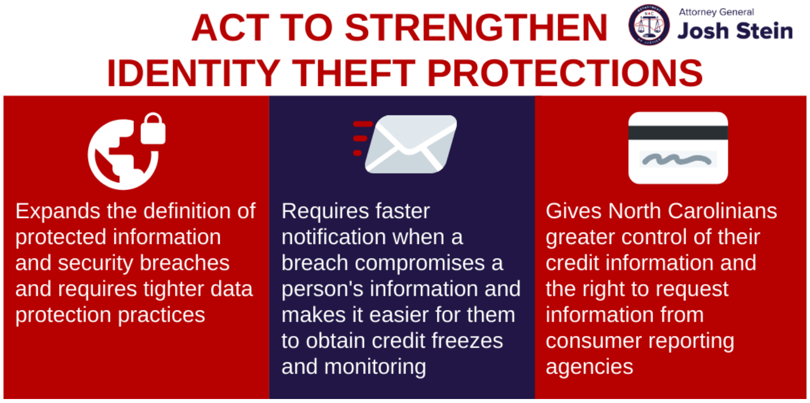
In 2019, our office also reached the first ever multistate settlements involving HIPAA-related data breaches. In May, North Carolina and 15 other states reached a $900,000 settlement with Medical Informatics Engineering over the breach of electronic protected health information of more than 3.9 million individuals. In July, Attorney General Stein and 29 other attorneys general reached a $10 million settlement with Premera over its failure to safeguard information that allowed a hacker to gain unauthorized access to consumers’ data.

Attorney General Stein also urged the Federal Trade Commission to keep its current Identity Theft rules in place, which require financial institutions and businesses that grant credit or issue debit or credit cards to take steps and implement safeguards to detect, prevent, and mitigate identify theft.

Attorney General Stein and representatives from the DOJ have also worked to share information with people across North Carolina through presentations and other outreach about data security, tips to avoid hacking and online scams, and actions to take if your information is compromised. North Carolinians can also learn more about getting a free security freeze to prevent identity thieves from opening new accounts or getting credit in their name if their data is comprised in a breach.

Strengthening North Carolina’s Identity Theft Protection Laws

In 2019, Attorney General Stein and Rep. Jason Saine re-introduced the Act to Strengthen Identity Theft Protections, which is designed to prevent data breaches and protect victims affected by breaches and compromised information. Attorney General Stein will continue to champion stronger data security legislation for North Carolinian consumers in 2020.



ACT TO STRENGTHEN IDENTITY THEFT PROTECTIONS

Attorney General Josh Stein

Expands the definition of protected information and security breaches and requires tighter data protection practices

Requires faster notification when a breach compromises a person's information and makes it easier for them to obtain credit freezes and monitoring

Gives North Carolinians greater control of their credit information and the right to request information from consumer reporting agencies