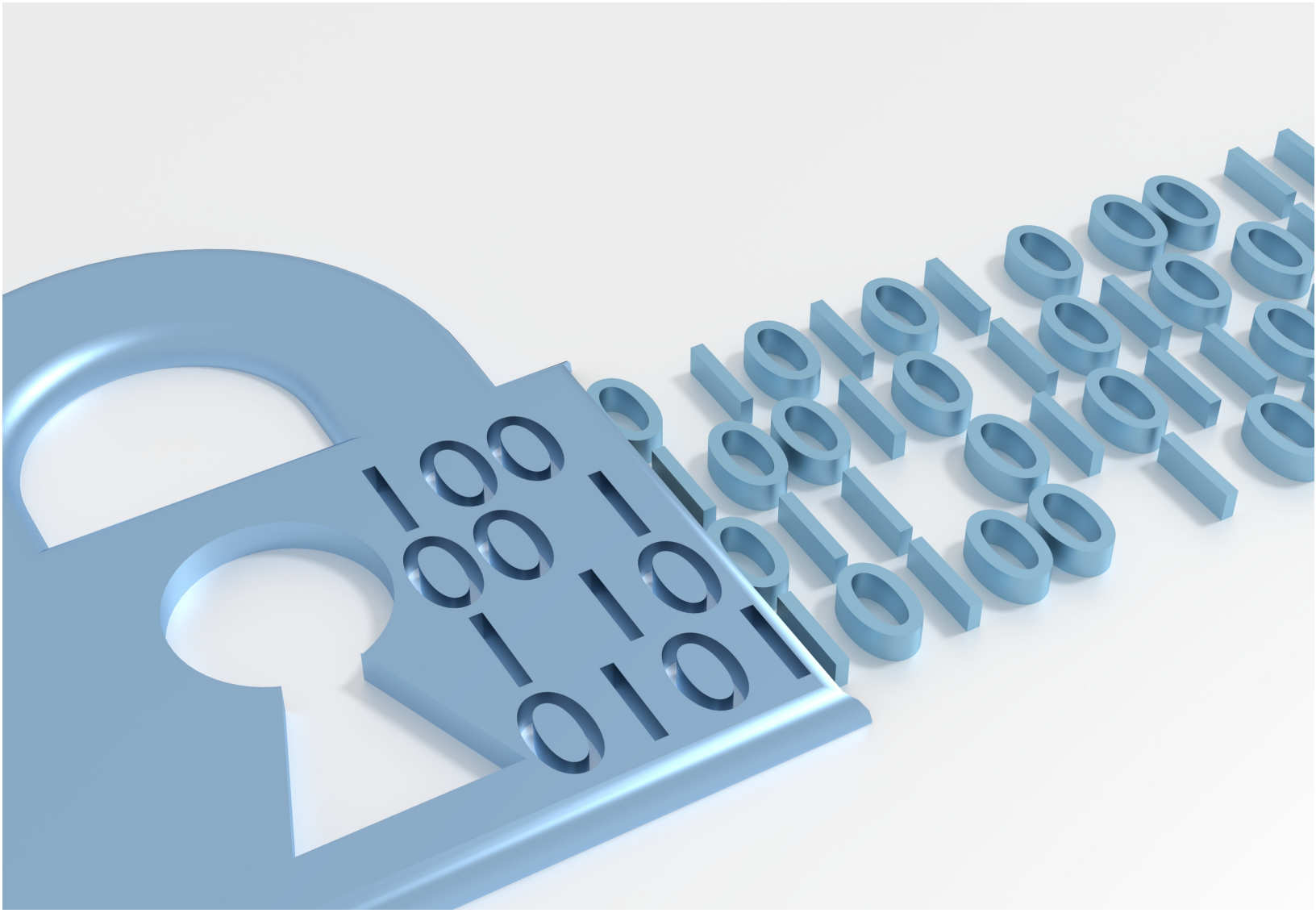
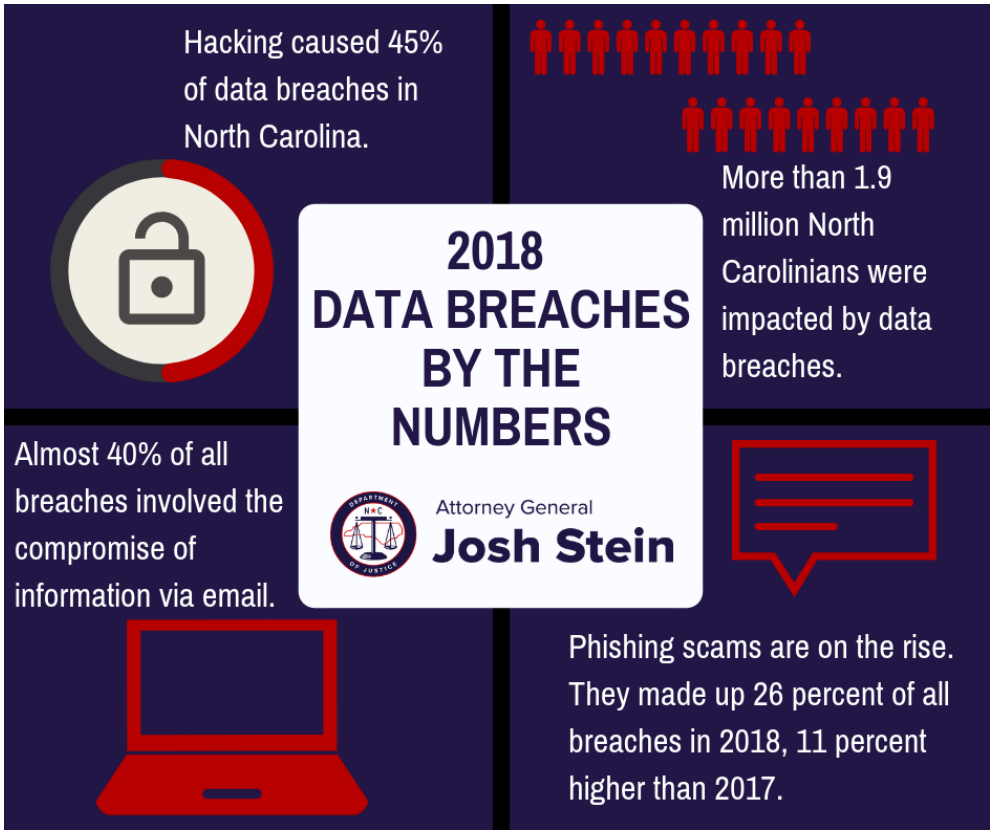
North Carolina Data Breach Report 2018



Attorney General Josh Stein
North Carolina Department of Justice

Executive Summary

Between January 1, 2018, and December 31, 2018, organizations reported 1,057 data breach notices to the North Carolina Department of Justice. These breaches affected more than 1.9 million North Carolinians. This report discusses the types of data breaches that occurred in our state last year and shares how consumers can protect themselves before and after their information is compromised. It also details enforcement actions Attorney General Josh Stein has taken and legislation he's proposed to better protect people's personal information.



Significant Findings:

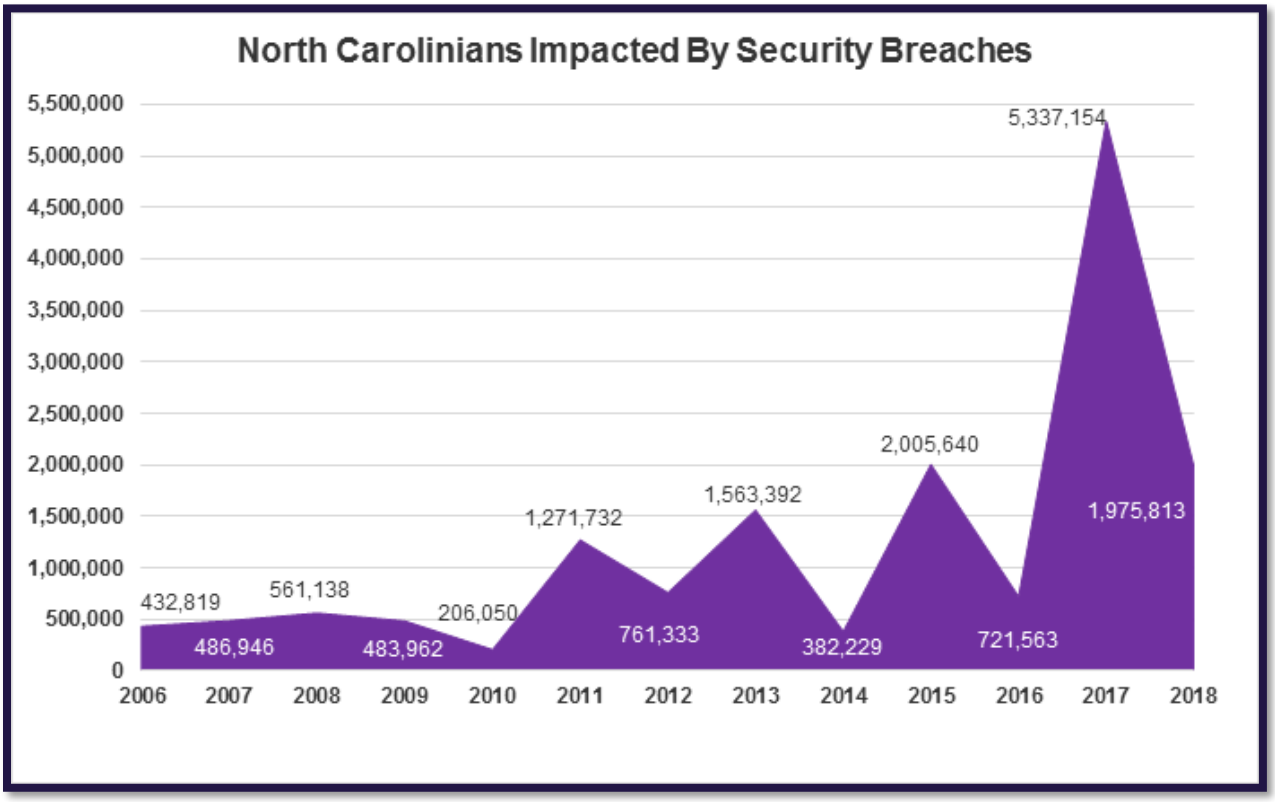
- Phishing scams made up 26 percent of all breaches in 2018, up nearly 11 percent since 2017 and 2,650 percent since 2015.
- Accidental release and display breaches increased in 2018, after a steady decline since 2013.
- The 474 hacking breaches reported in 2018 marked an 8 percent decline since 2017. Hacking breaches in 2018 were 1,960 percent higher than a decade ago.
- In 2018, more than 1.9 North Carolinians were affected by data breaches, a 63 percent decrease from the 5.3 million North Carolinians affected by data breaches in 2017. In 2017, an estimated 5 million North Carolinians were affected by the Equifax breach, one of the most significant security breaches in American history.
- More data breach notices were submitted in 2018 than in 2017. The 1,057 data breach notices submitted in 2018 were 3.4 percent higher than the number of notices submitted in 2017.

Background

Businesses and state and local governments are required under the Identity Theft Protection Act to report all security breaches to the North Carolina Department of Justice. Since this law was passed in 2005, businesses and government entities have reported 6,061 data breaches. Data breach notices in 2018 represent 17 percent of all data breaches reported in the last 13 years.

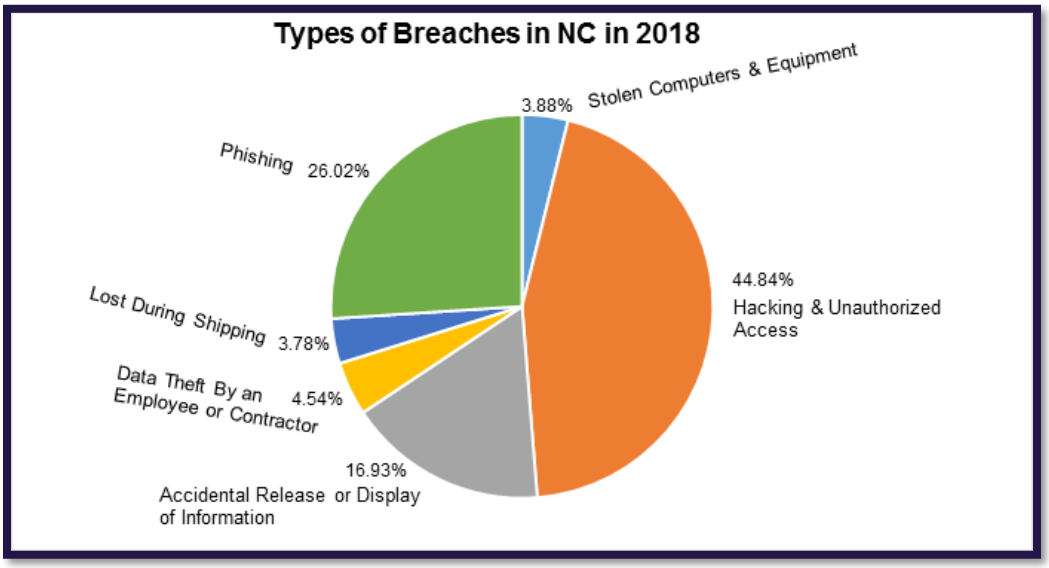
Over the past 10 years, the number of North Carolinians impacted by security breaches has increased by more than 250 percent. The increase in security breaches is a combined result of the near-universal access to technology from personal devices, an upswing in online scams, and the amount of consumer personal information and financial data that companies keep.

Breaches that compromise people's personal information or financial data can have serious repercussions on people's privacy and well-being. They leave customers at risk for identity theft, financial fraud, additional online scams, and lasting credit damage.

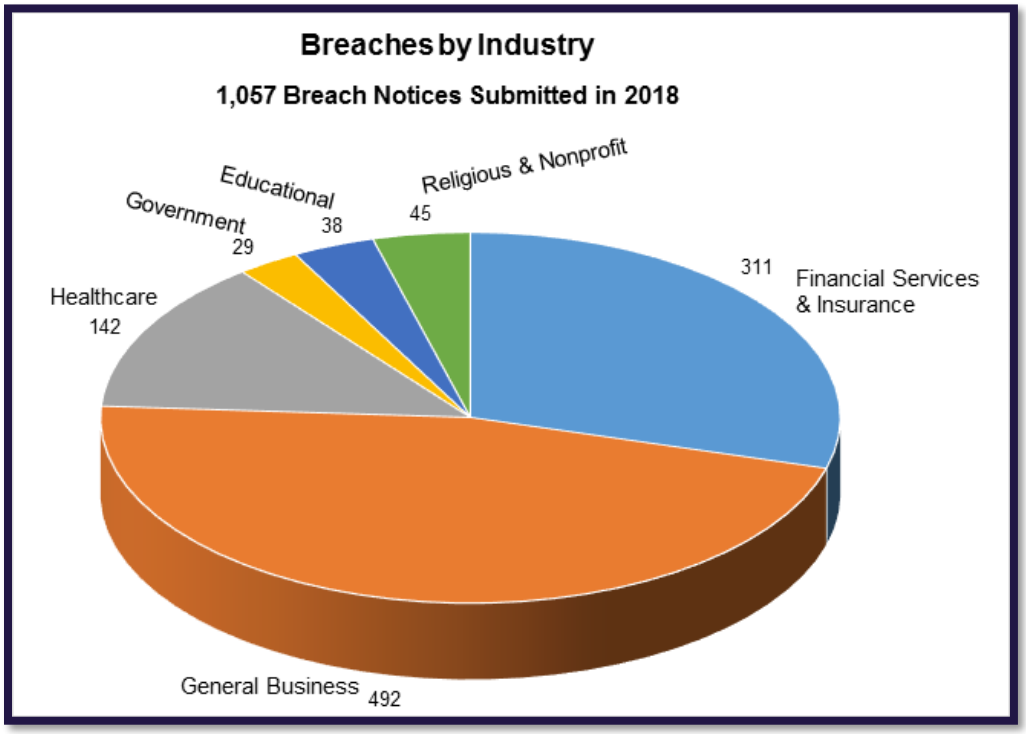


Data Breaches in North Carolina

Personal data can be exposed or stolen in different ways. In 2018, hacking and unauthorized access made up nearly half of all reported breaches. Data can also be exposed through phishing, accidental release or display of information, data theft, stolen computers or other equipment, and loss of personal data while it is being transported between locations.

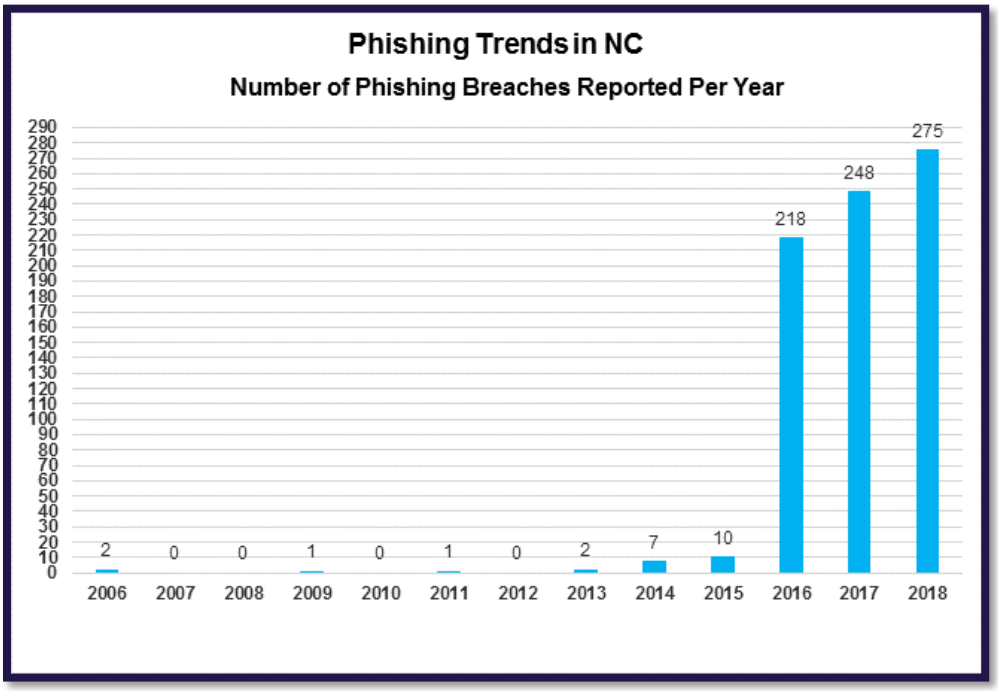


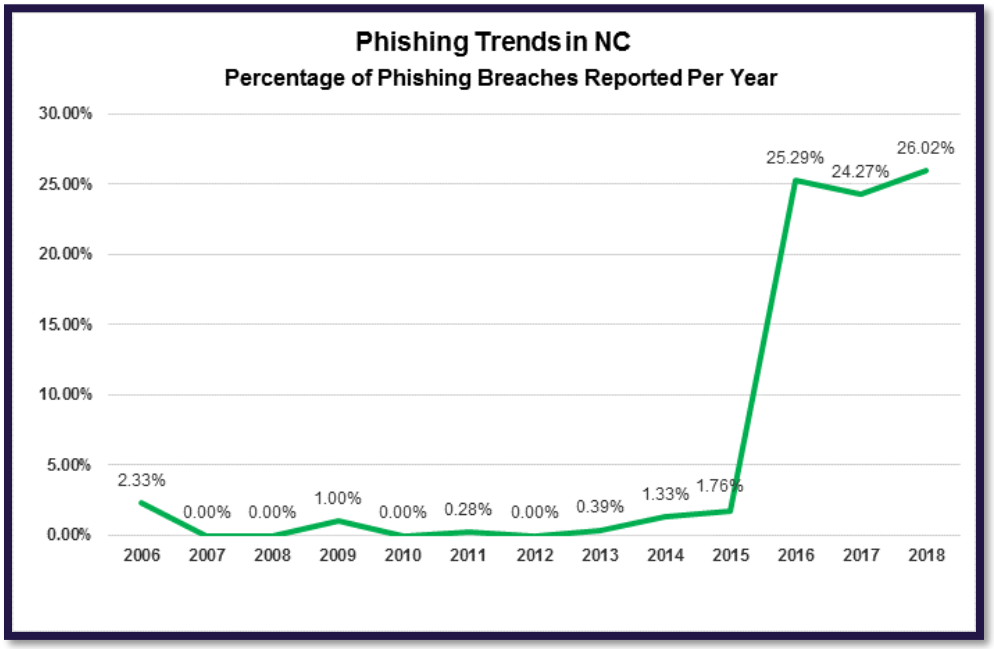
Data breaches involving businesses and financial services and insurance companies made up more than three-fourths of all reported data breaches in 2018.



Phishing

A record number of phishing breaches were reported in North Carolina last year. The 275 breaches reported in 2018 mark a nearly 11 percent increase from 2017. Phishing occurs when scammers try to steal your personal information, or trick you into sharing it with them, by sending you fake emails or text messages. These messages will appear to be from legitimate companies or individuals, and will link to a website that resembles a legitimate organization's website. If you log in, the scammers will have access to your login credentials and may be able to access your email account, financial accounts, or personal information.





Always verify via phone any email requests to send personal information (W2s, for example) with the person who appears to be requesting the information before sending. Search the internet to get the correct phone number.

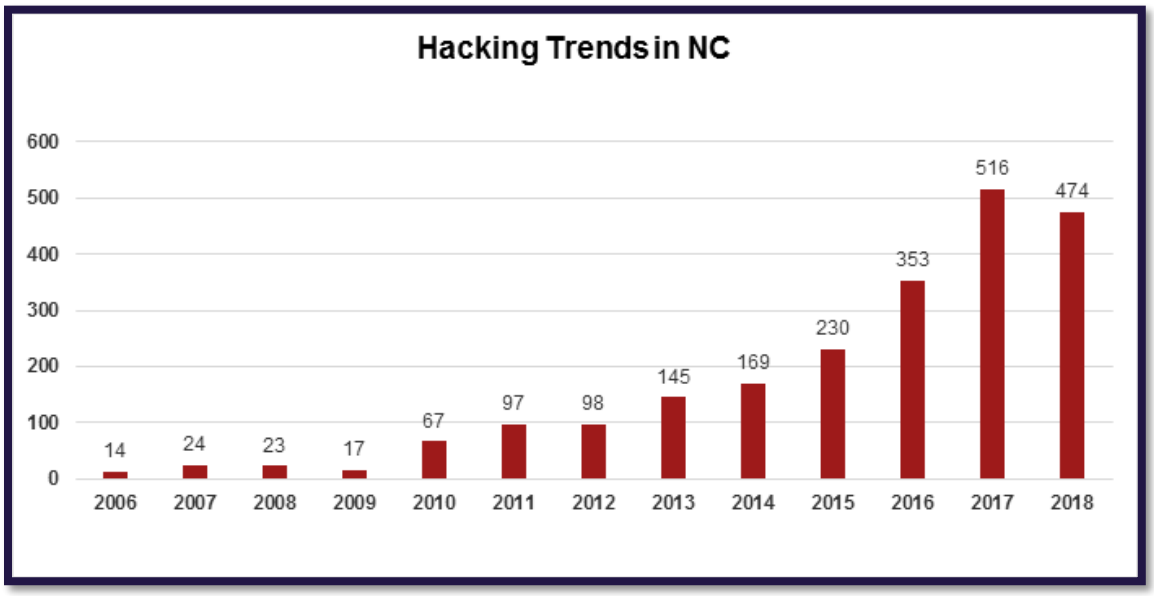
Report phishing to the real business or organization the scammer claims to be from. Also forward phishing emails to the Federal Trade Commission at spam@uce.gov.

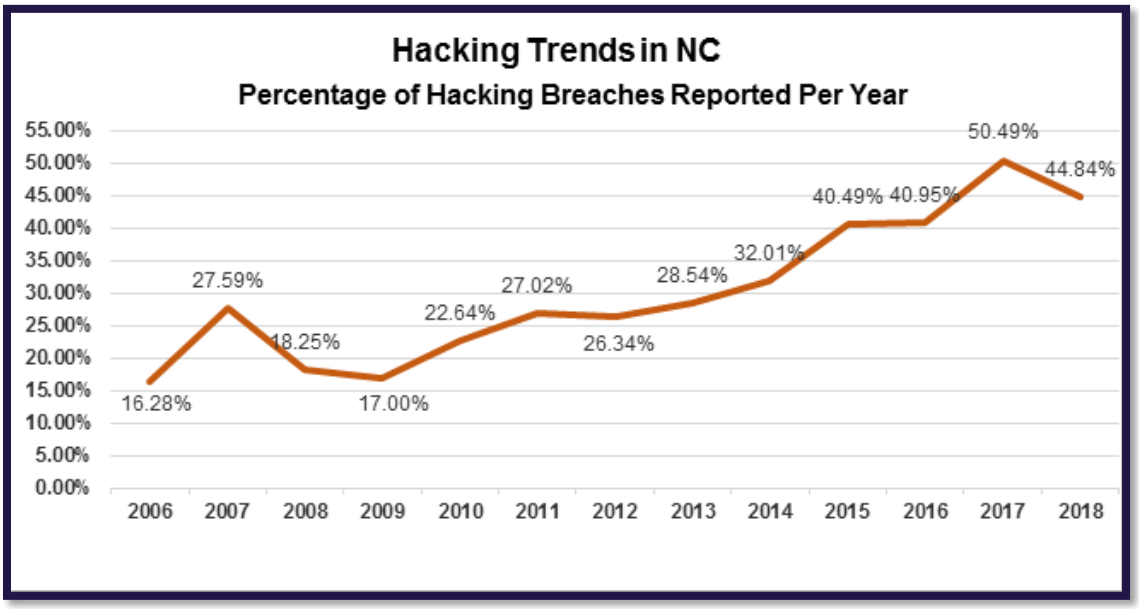
If you do respond to a phishing email, contact your bank and your credit card company immediately. If you think you may be a victim of identity theft, contact NCDOJ for help at ncdoj.gov/complaint or 1-877- 5-NO-SCAM.

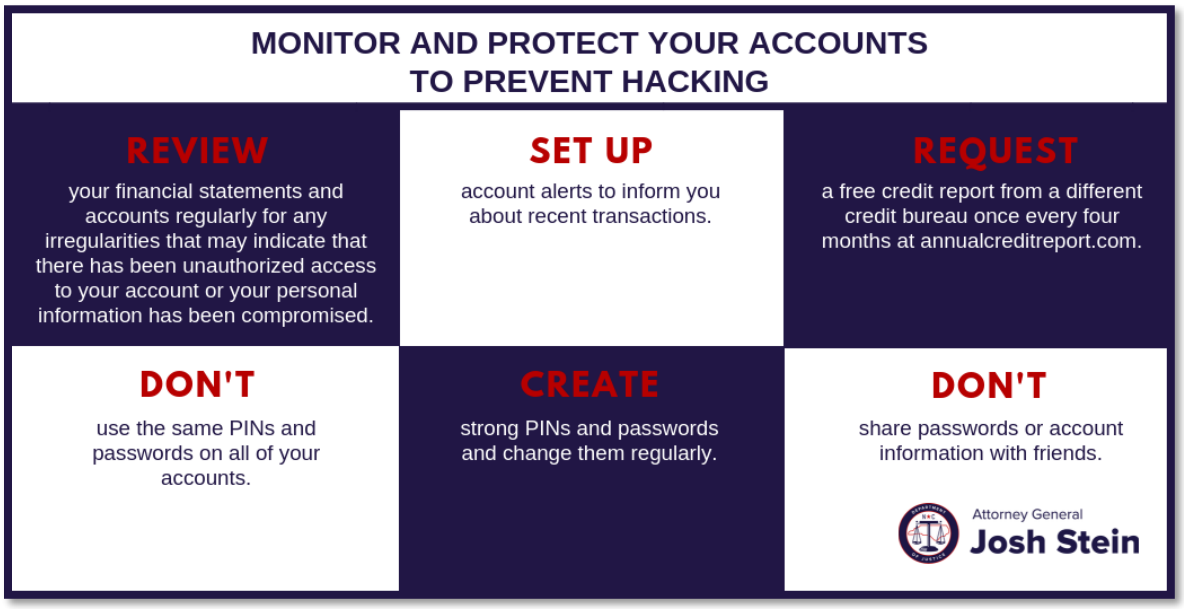
Hacking and Unauthorized Access

Hackers look to exploit weaknesses in the security of various systems to gain unlawful access to personal information that is being stored or transmitted electronically. Businesses, financial organizations, educational institutions, and government organizations all store consumers' personal information on internal systems. If these systems don't have the proper security protections in place, or fail to comply with established security standards, hackers can access and steal information. They can sell or use that information to commit identity theft and financial fraud.

The DOJ received 474 reports of hacking in 2018, a 1,960 percent increase from the reports of hacking a decade ago. For two consecutive years, hacking breaches have made up nearly half of all data breaches reported to the DOJ.





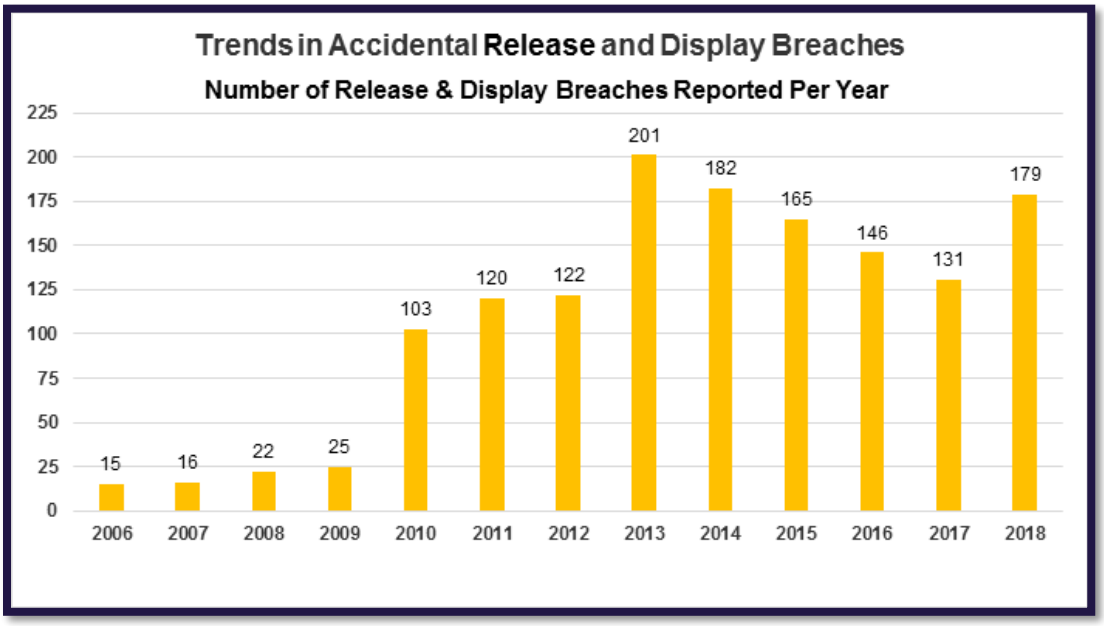


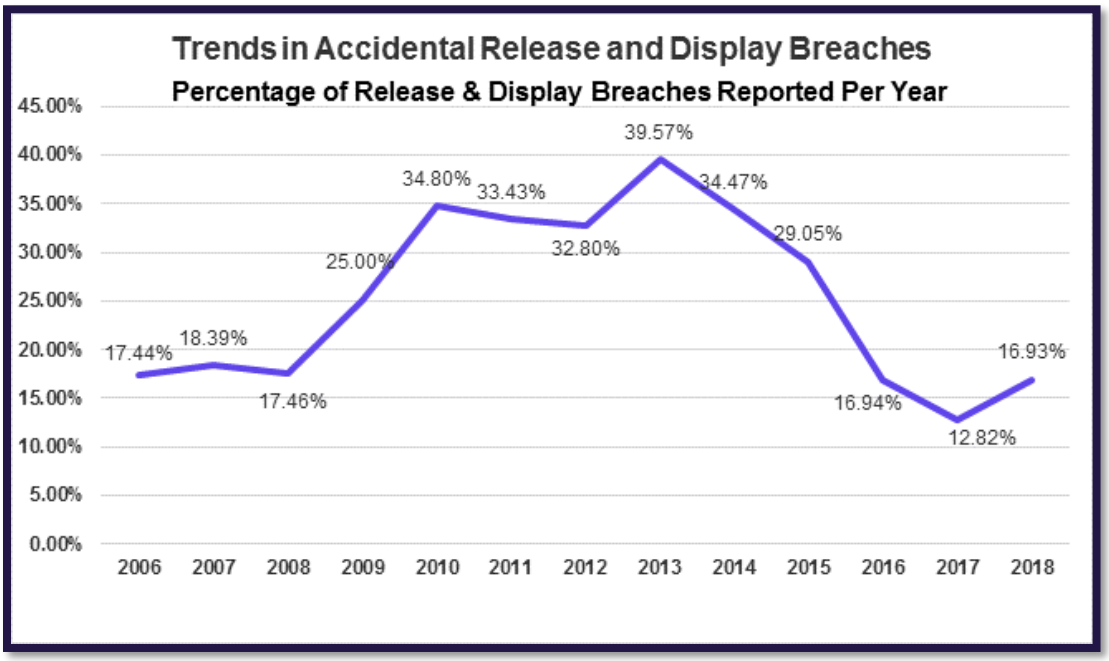
If you suspect that there has been unauthorized access to your accounts, report it to local law enforcement.

Accidental Release or Display

There were 179 accidental release and display breaches reported to the DOJ last year, up 36 percent since last year.

Accidental release or display of personal information is often the result of carelessness or human error. This can happen in a number of ways – an employee may store information online without the appropriate security measures, share it with the wrong individual in person, online, or through mail, or leave it in a place where others may be able to see it.

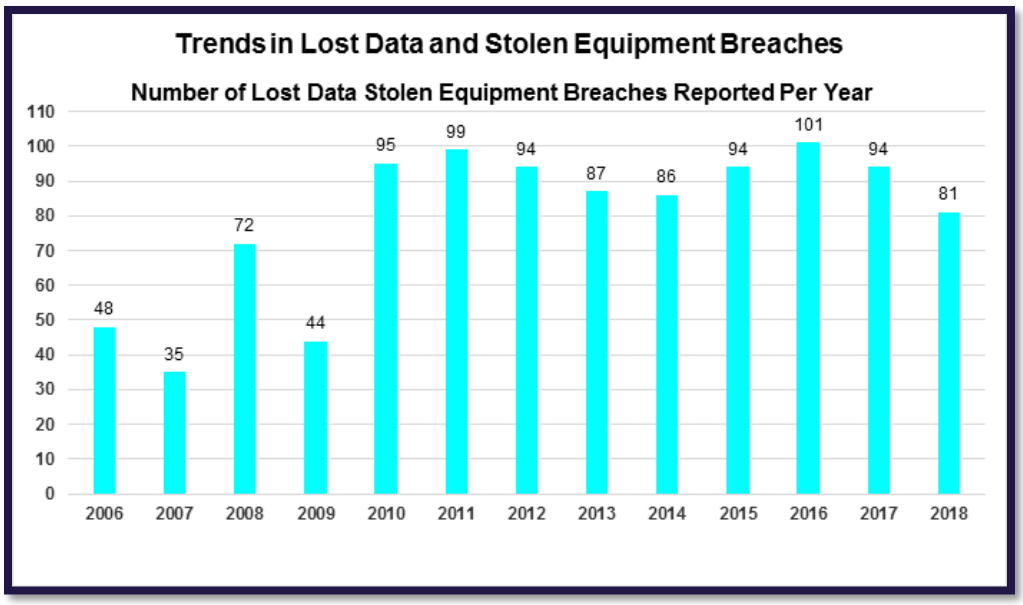


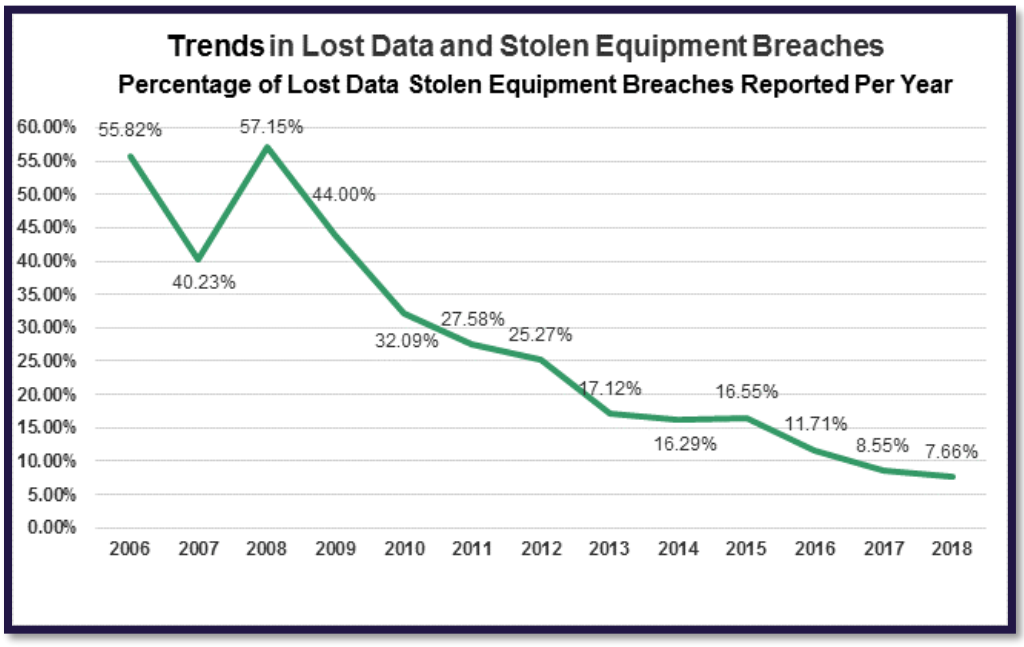


Lost-in-Transit or Stolen Equipment

Data breaches can also occur if equipment or files that contain personal information are lost, misplaced, or stolen. This is a higher risk when information is contained on portable technology equipment, including flash drives and laptops.

In 2018, 81 data breaches involving lost data and stolen equipment were reported to the DOJ, down nearly 14 percent since 2017.





Discussion

In 2018, 1,057 data breach notices were submitted to the Department of Justice, a 3.4 percent increase from 2017. These breaches involved the exposure of or access to different types of personal information and financial data, compromised through a variety of breaches.

North Carolina's data privacy laws are already strong, but they can be stronger. That's why Attorney General Stein partnered with North Carolina Representative Jason Saine, who introduced the Act to Strengthen Identity Theft Protections in 2018. They will champion the bill again in 2019.

The Act to Strengthen Identity Theft Protections would:

- Update the definition of a security breach and protected information and tighten data protection rules for companies.
- Increase the tools available to consumers to monitor and protect their credit in the event of a security breach.
- Give consumers more control of their personal credit information.

Read more about the legislation here.

In addition, Attorney General Stein took several actions in 2018 to hold companies responsible when consumer data was exposed. He joined a bipartisan coalition of 37 attorneys general to demand answers from Facebook about the company's business practices and privacy protections. As a result of this ongoing investigation, Attorney General Stein learned that Facebook shared the data of more than 2.5 million North Carolinians with Cambridge Analytica and other third-party organizations.

Attorney General Stein demanded additional answers from Facebook and Google after they both announced significant data breaches in October. Facebook announced that 50 million of its accounts were hacked, and Google announced a security breach to its Google+ network.

Attorney General Stein reached a $148 million multi-state settlement with Uber over a data breach that affected drivers. North Carolina received $3,661,800.27 and Uber agreed to strengthen its corporate governance and data security practices to help prevent a similar occurrence in the future. Also in 2018, Attorney General Stein and 11 other states filed a federal data breach lawsuit related to HIPAA, the first time state attorneys general have joined together to pursue a HIPAA-related data breach case in federal court.

Attorney General Stein spoke up on federal actions that would change how law enforcement and states are able to investigate data breaches. He urged Congress to pass the Clarify Lawful Overseas Use of Data (CLOUD) Act to give law enforcement officials access to American consumer data stored by American companies on foreign servers so they can bring criminals to justice. The CLOUD Act became law in March. Attorney General Stein also pushed back on federal legislation that would preempt state data breach and data security laws, making it harder for states to enforce data breach notification requirements and respond to data security threats.

Finally, Attorney General Stein and his office made more than 55 presentations in 2018 to groups sharing the tips included in this document as to how to protect personal information, as well as what steps to take if their information has been compromised. Consumers should regularly check their credit reports to see if anyone has taken out loans in their name. Additionally, placing a security freeze is the most effective tool to protect one's credit. To learn how to get your free credit report and how to freeze your credit, visit ncdoj.gov/identitytheft.

Conclusion

Attorney General Stein and the North Carolina Department of Justice's Consumer Protection Division work to ensure that companies better protect their customers' personal information and are held accountable when they fail to act responsibly.

We also work to educate North Carolinians about new scams and frauds that may compromise their information and how to respond in the event of a data breach. Consumers should take steps to protect their information from exposure by monitoring accounts, protecting passwords and other private data, checking their credit regularly, and getting a security freeze when appropriate.

For more information on security breaches in North Carolina, tips for protecting your data, and data breach report forms, visit the North Carolina Department of Justice online at www.ncdoj.gov/identitytheft.