

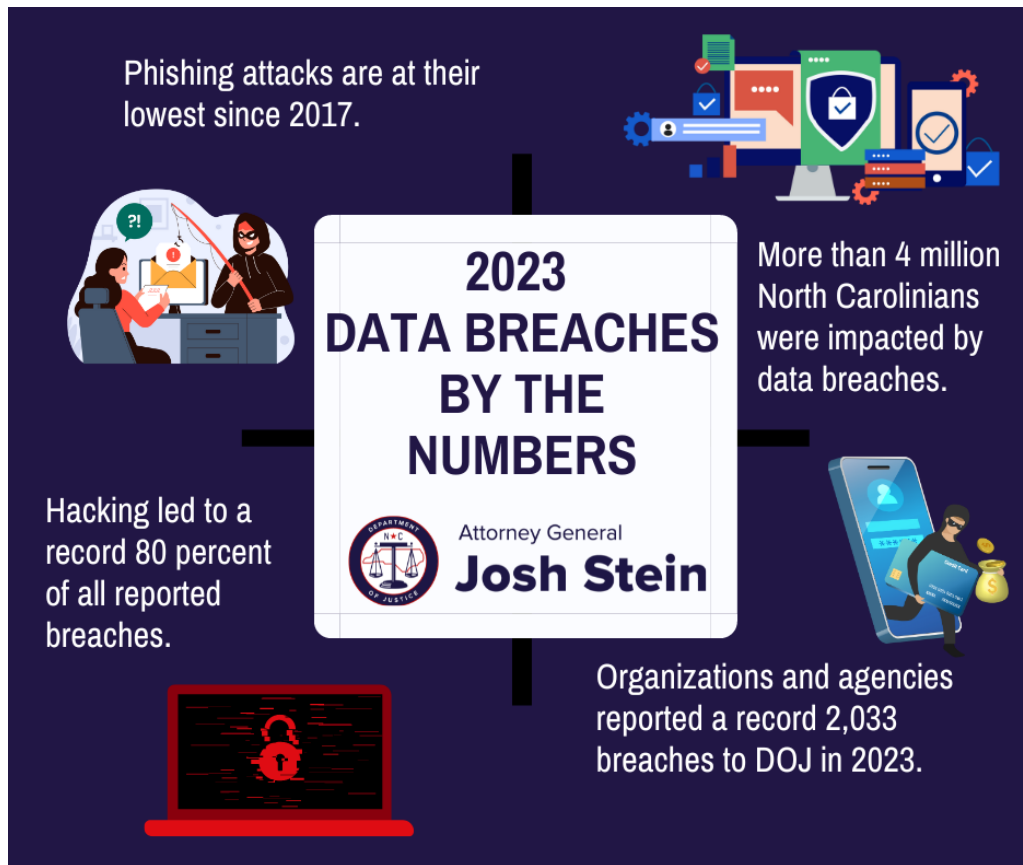


In North Carolina, businesses and organizations that fall victim to a data breach are required to report the breach and the information that was compromised to the North Carolina Department of Justice. The Department of Justice educates North Carolinians about data breaches, how to protect their data to prevent a breach, and what to do to safeguard information if a breach happens. The annual data breach report recaps the types of data breaches reported to our office in 2023, and how we can all take steps to protect our data.

The Department of Justice also investigates certain data breaches to determine when a company is at fault because it failed to properly secure customer data or notify customers after a breach. In some cases, we may take legal action to hold these companies responsible, win back money for North Carolinians, and make sure that companies strengthen their business practices to protect against future data breaches.

For more information on how to protect your data and how to respond if your data has been compromised, visit www.ncdoj.gov/identitytheft.

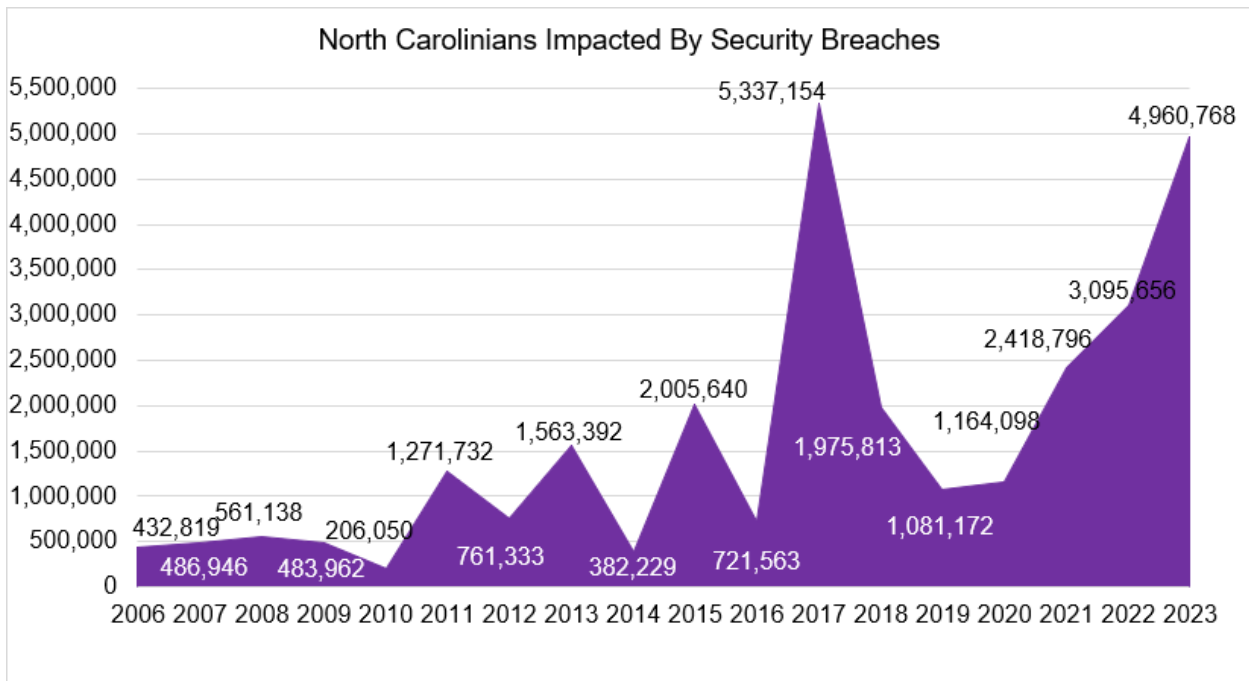
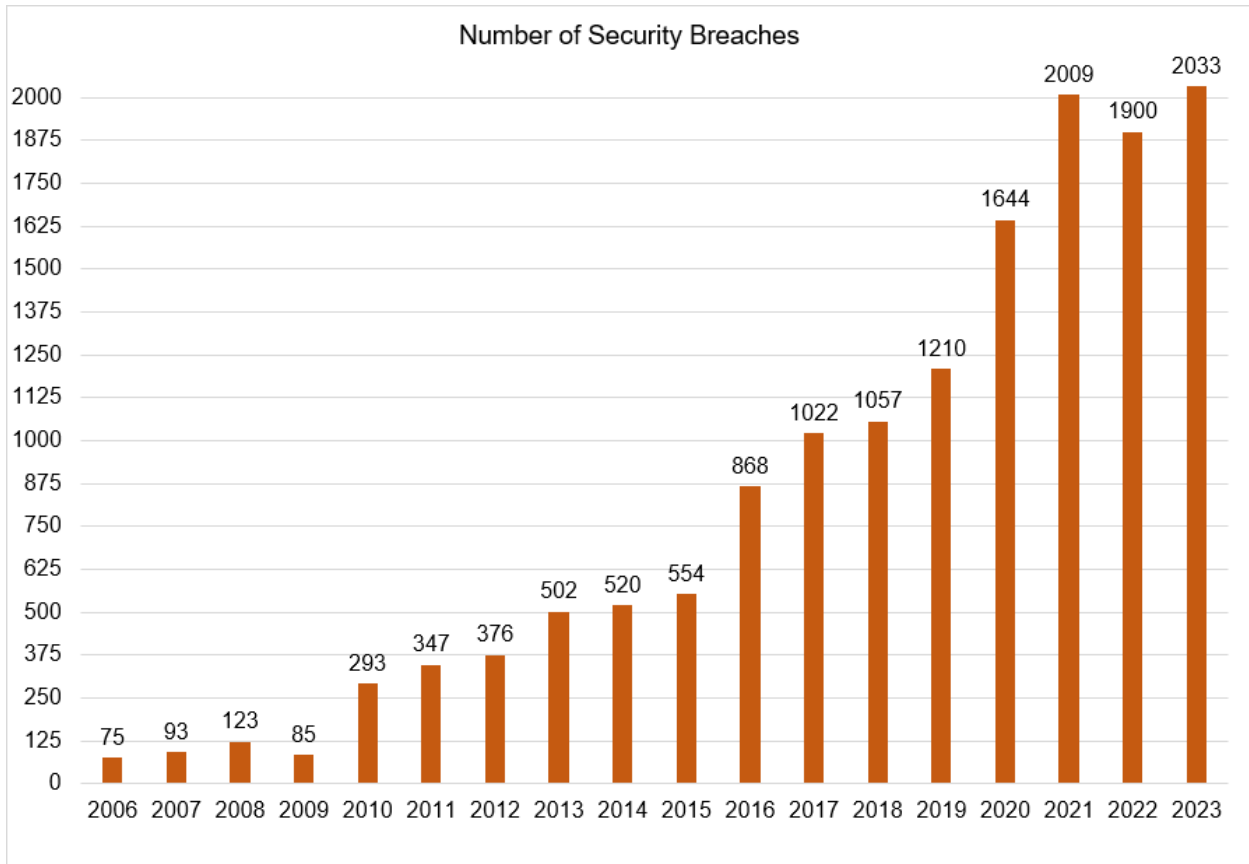
HIGHLIGHTS



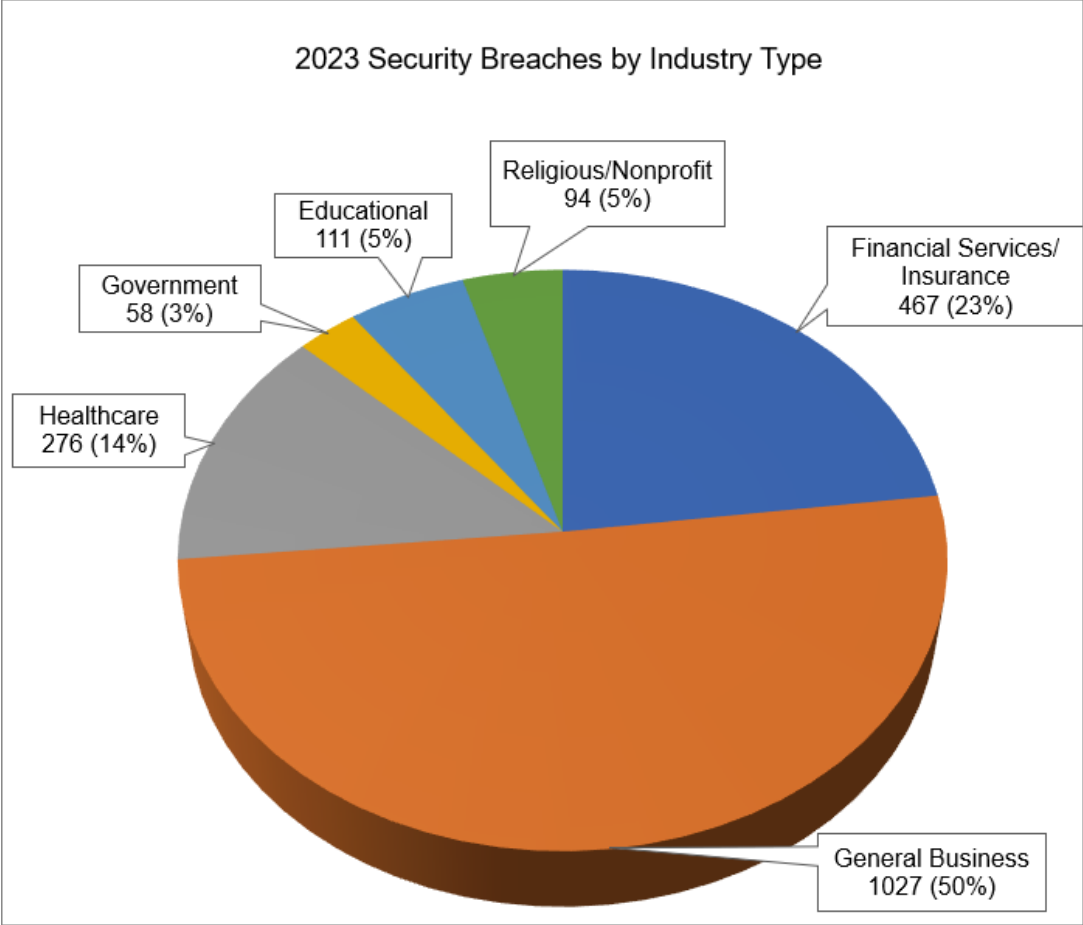
- Businesses reported a record 2,033 data breaches to the Department of Justice in 2023, the highest number of breaches ever reported to our office.
- More than 4.9 million North Carolinians were affected by data breaches – the second highest number of people impacted in a single year, second only to the 5.3 million North Carolinians affected in 2017 (largely as a result of the Equifax breach).
- Hacking-related breaches were at a record high, causing 80 percent of all reported breaches.
- Phishing, ransomware, and breaches involving email were all down in 2023.

OVERVIEW OF 2023 BREACHES

In 2023, DOJ received 2,033 data breach notices from organizations. The breaches impacted more than 4,960,768 North Carolinians, the second highest number of people impacted ever and more than those impacted in 2022. Since 2006, businesses have reported 14,711 data breaches that impacted 24,446,261 people in all.



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

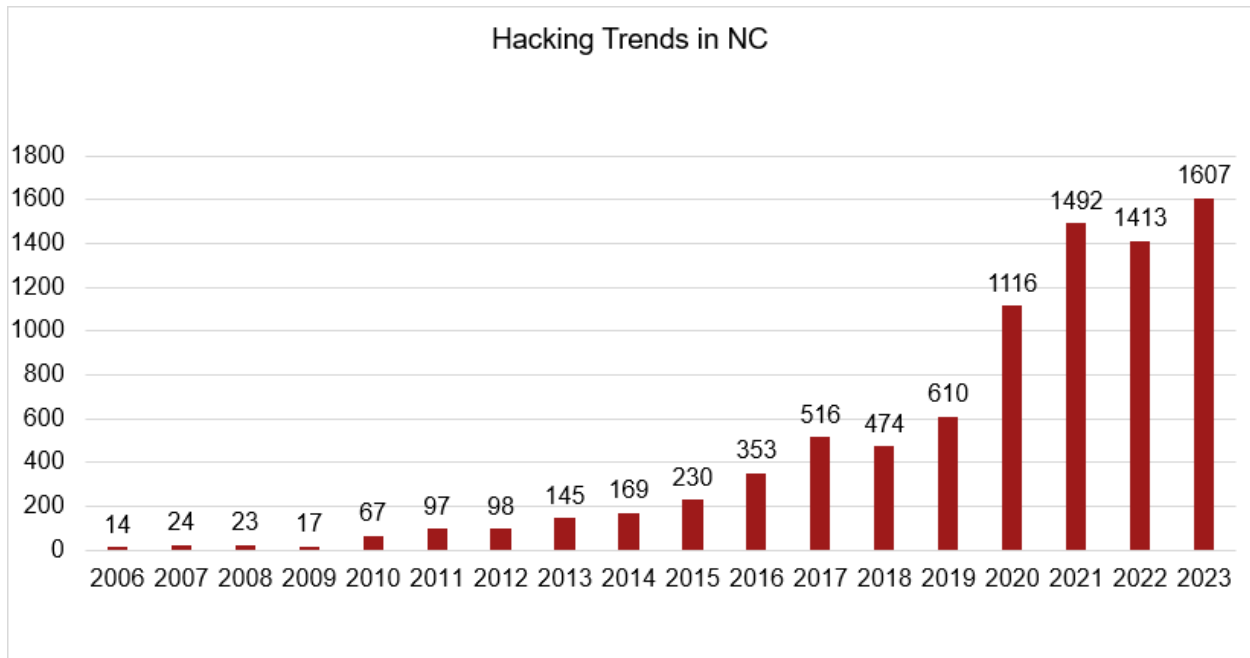


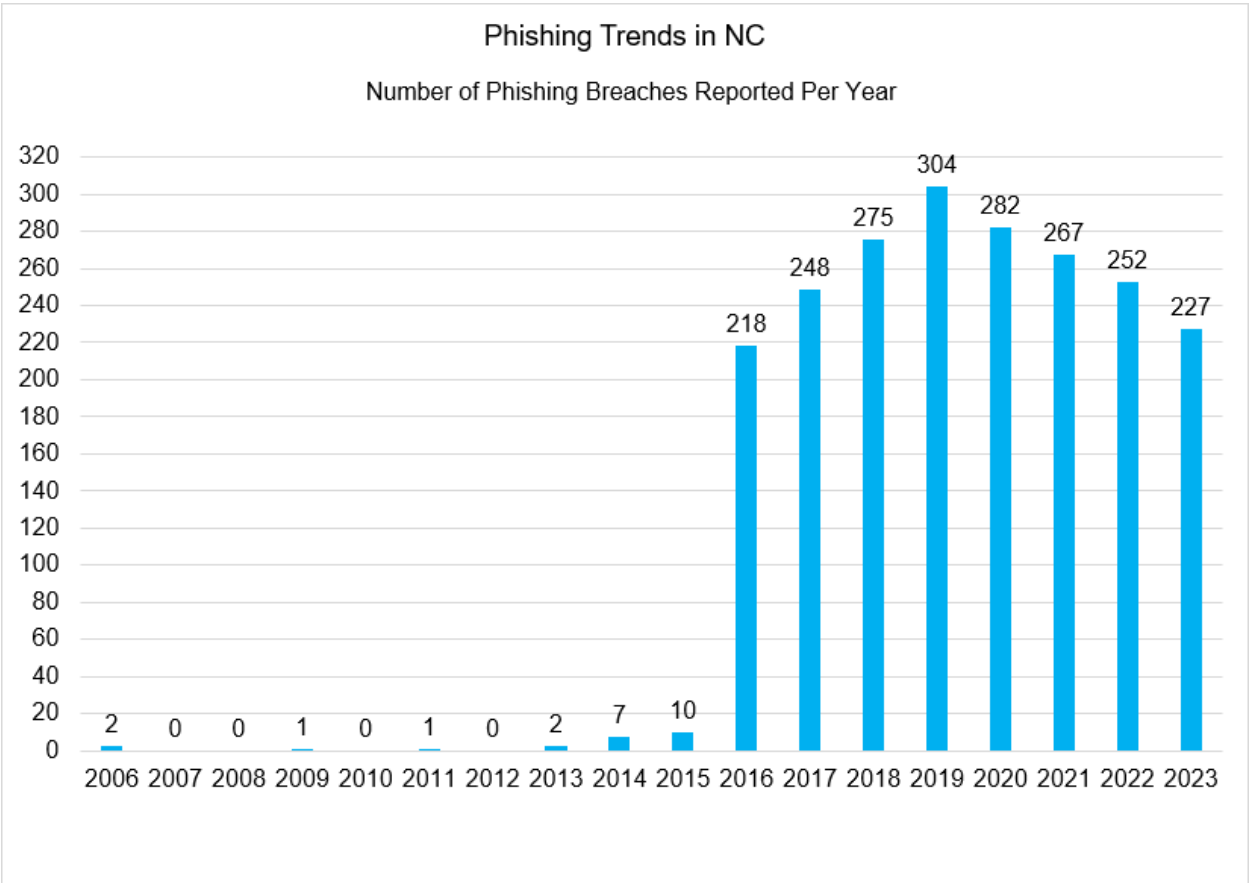
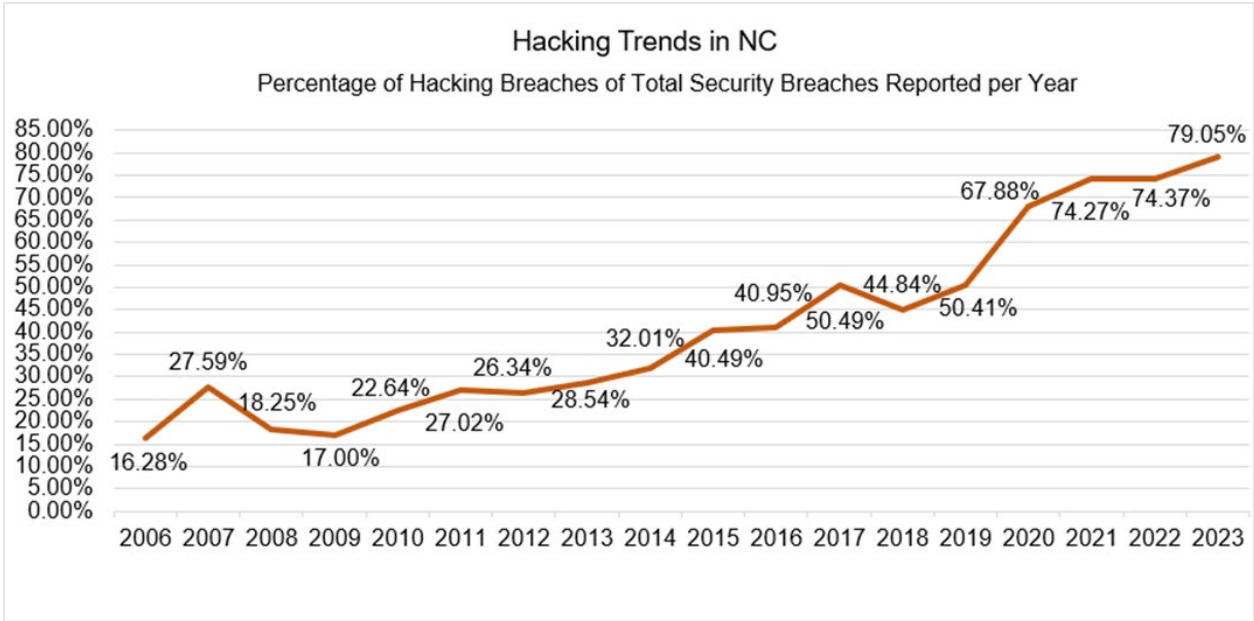
Similar to 2022, general businesses, financial services and insurance, and health care-related organizations reported the most breaches to our office in 2023. Often, these types of industries collect and maintain many kinds of personal information, making them prime targets for hackers. The Department of Justice has been working to encourage organizations to better protect people’s data by revisiting and revising security policies. When companies have access to North Carolinians’ information, they must take reasonable precautions to keep that information safe.

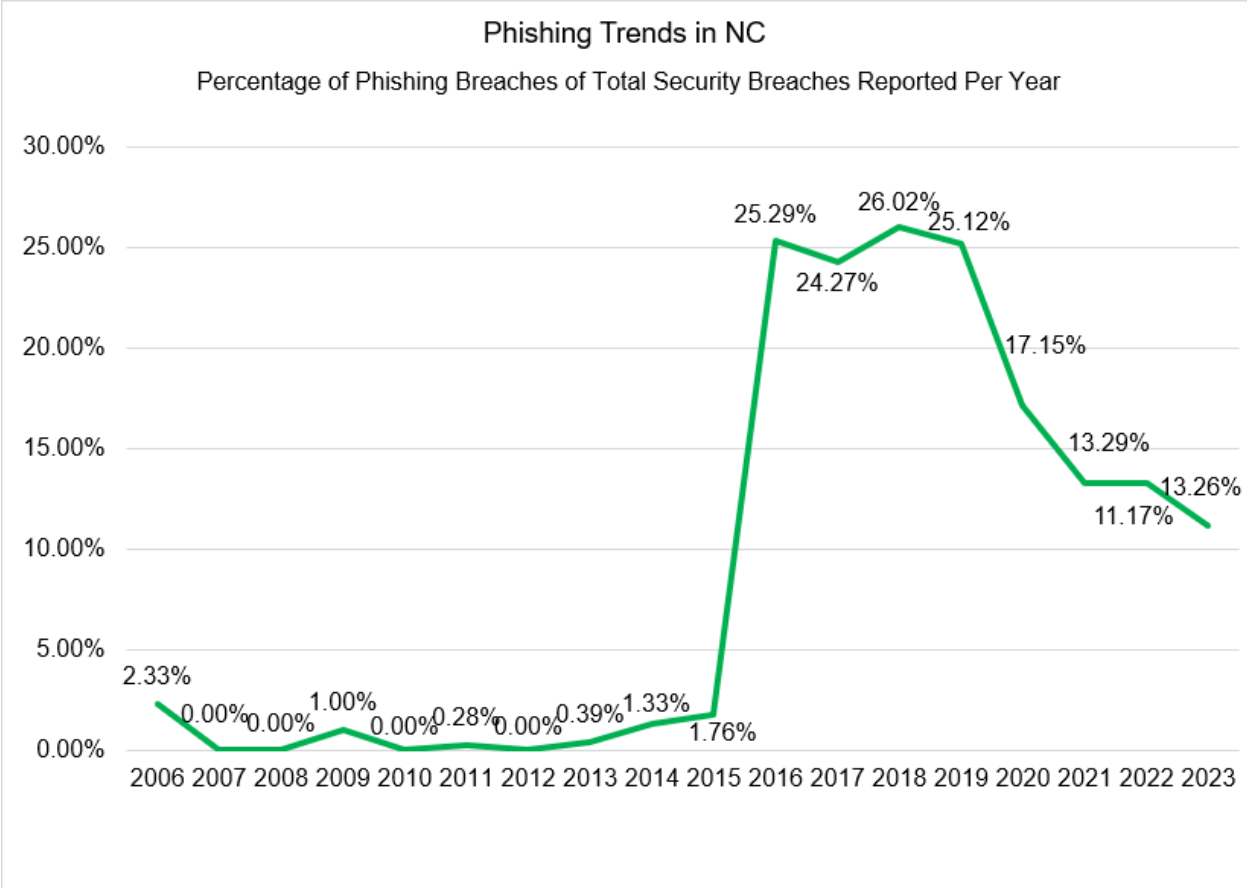
HACKING AND PHISHING

We often hear of hackers who break into an organization's data systems to steal people's personal information and other stored data. Hackers try to break into security systems using several different tactics – they can send you a phishing scam email, employ a ransomware attack on devices or networks, or gain access to your security information and password to login as you. Make sure that you are taking the following security precautions to avoid a hacking or phishing attack. Many hacking-related breaches and ransomware attacks start with a phishing attempt via email, text, or phone call.

- Regularly update your antivirus and security software on your phone and computers. Don't forget about your other smart devices, such as watches, TVs, and tablets.
- Don't open emails, click links, or download attachments from unverified senders.
- Examine an email closely before you act – do the email address, the subject and content, and the attachments or links seem authentic? Are they coming from people you know and email addresses you recognize? If you're not sure, contact the company or person directly to ask.
- Use strong passwords and change your passwords and security questions regularly.
- Use different passwords for your various accounts and websites so if one is compromised, it won't give someone access to other accounts.
- Don't use public Wi-Fi to make purchases, access your bank accounts, or log into any websites that have personal information. Public Wi-Fi networks are not secure, so they're much more susceptible to hackers.
- Forward phishing emails to the Federal Trade Commission at spam@uce.gov.
- If you believe you may have been the victim of a hack, request a free security freeze, contact our office, and monitor your credit report and bank accounts for errors and irregularities. To learn more, visit www.ncdoj.gov/securityfreeze.





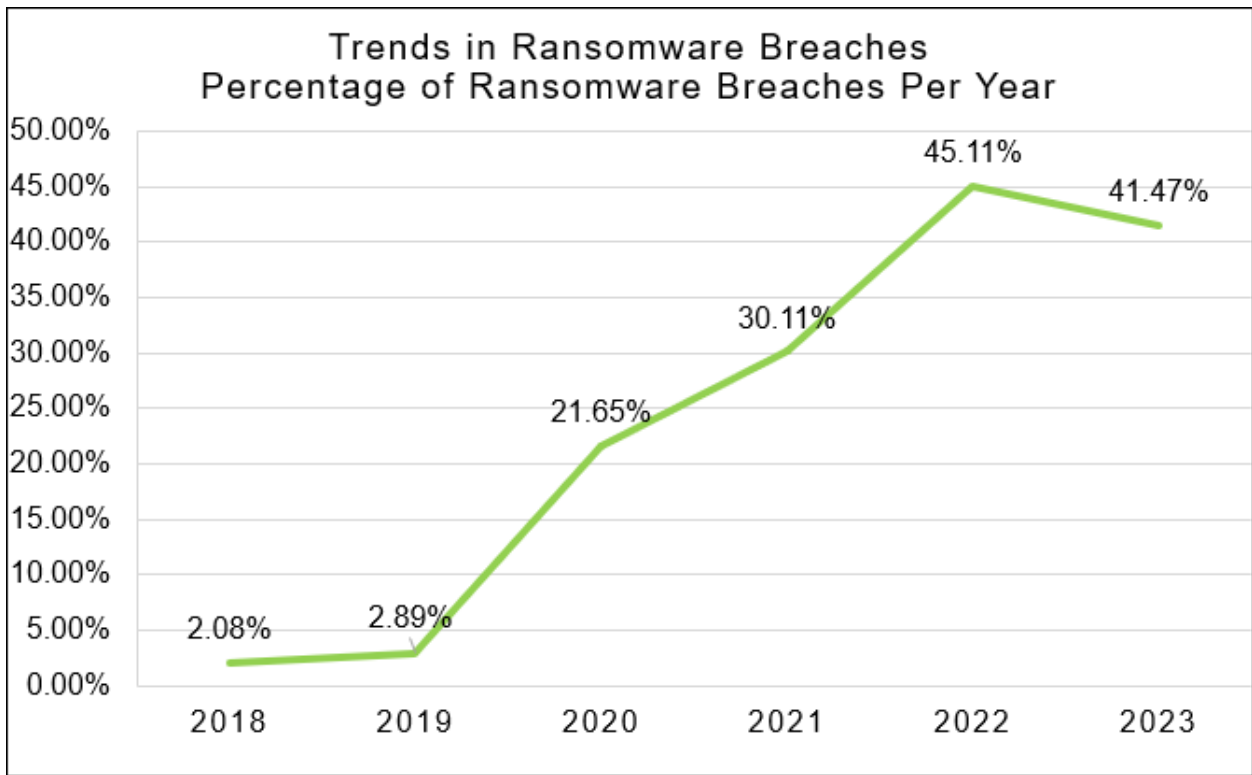
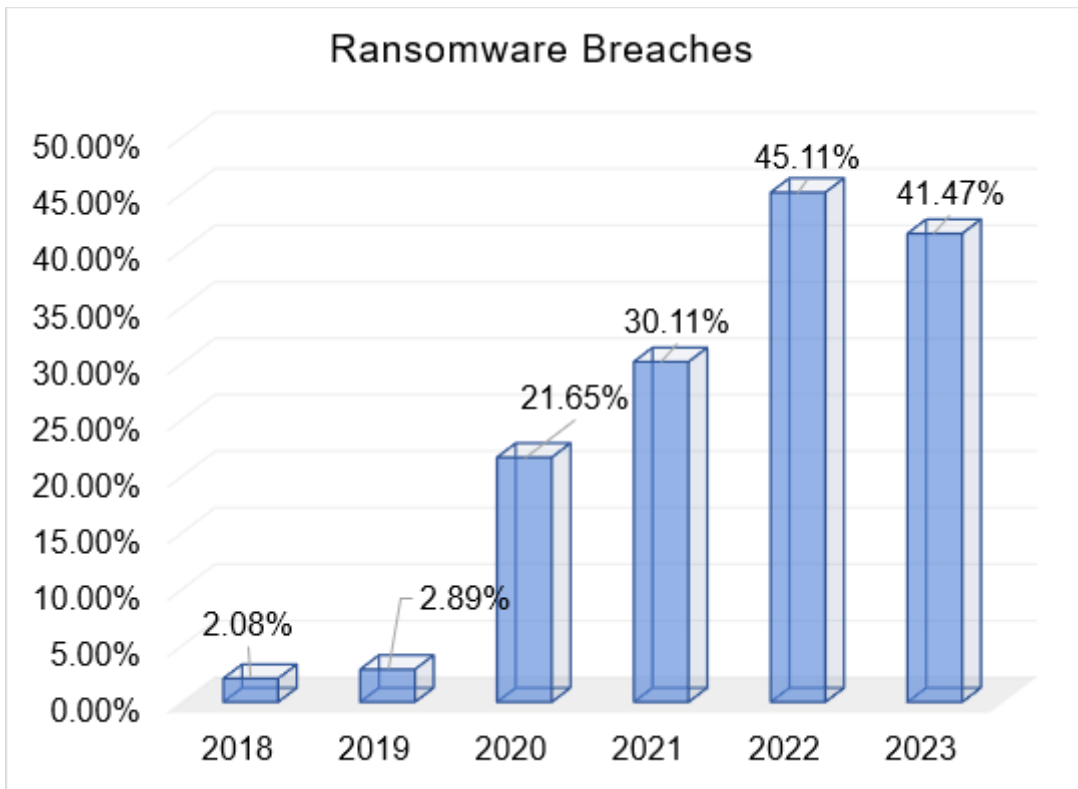


RANSOMWARE ATTACKS

Ransomware attacks reported to our office dropped from 2022; however, ransomware attacks remain a threat to organizations and people across the state. In 2023, our office received 843 data breaches caused by ransomware. Many ransomware attacks start with a phishing attempt so that the hacker can gain access to your device and your network.

Here are some tips to prevent a ransomware attack:

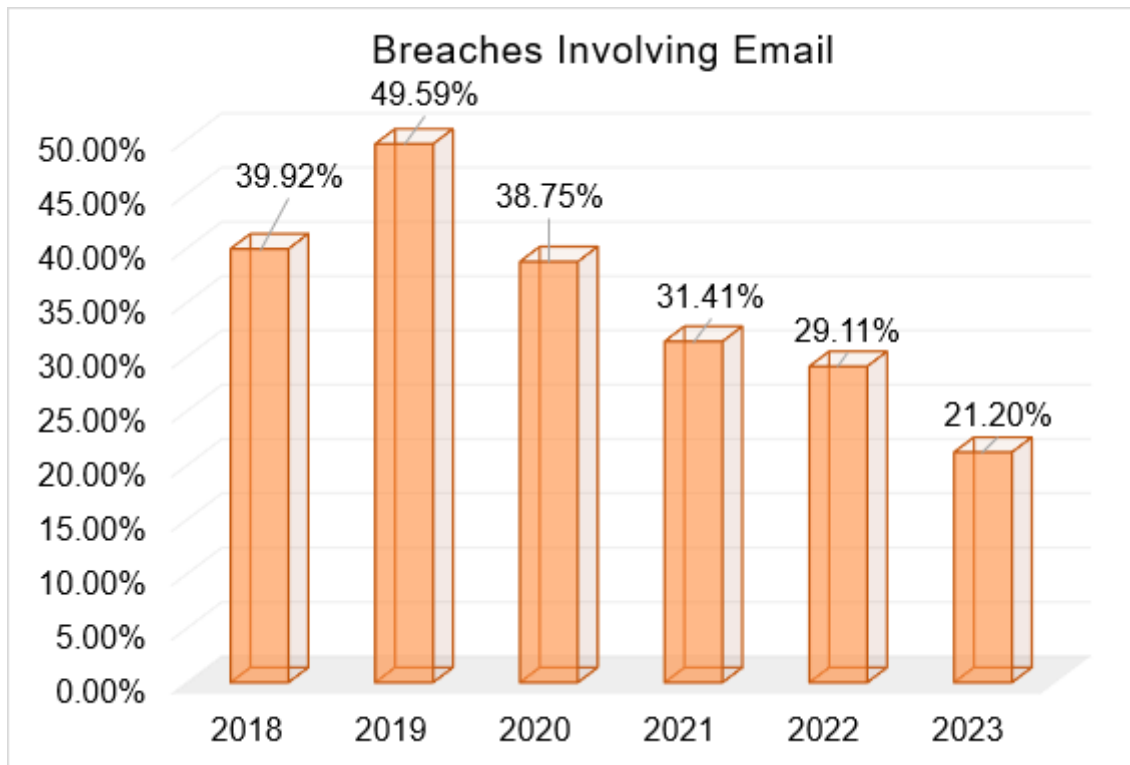
- Train employees and users on cybersecurity best practices regularly.
- Only conduct business on legitimate websites and software programs.
- Have a plan in place for how you or your organization will respond to a ransomware attack. Make sure to include a plan on how to properly notify employees, customers, or other people whose data you store.
- Maintain software and security practices so that they are up to date.



EMAIL BREACHES

We have seen a steady decrease in email breaches reported to our office. Email breaches include misdirected emails that contain personal information, phishing access into email accounts, and any other unauthorized access. Protecting your emails is important not only for yourself, but also helps protect your organization and other people's information. If a hacker gets access to an email account, they can get access to a company's network.

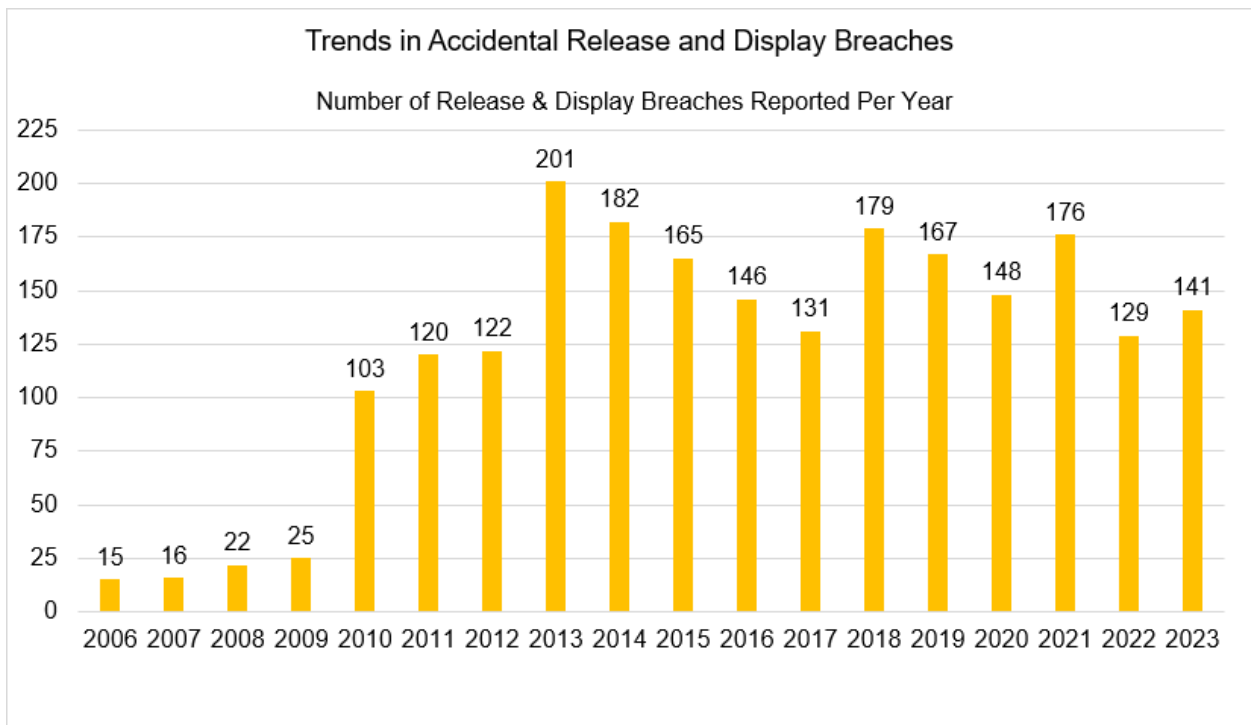
- Keep your passwords creative and make sure you are not using the same password for multiple accounts.
- Limit the exchange of personal information over email. If a hacker gains access, it will reduce the amount of information they are able to compromise.
- Always be skeptical of links and attachments sent in emails. Before you click on them, confirm that they were sent from a credible source.
- Use multifactor authentication to better protect your accounts and make it harder for hackers to break in.



ACCIDENTAL RELEASE AND DISPLAY

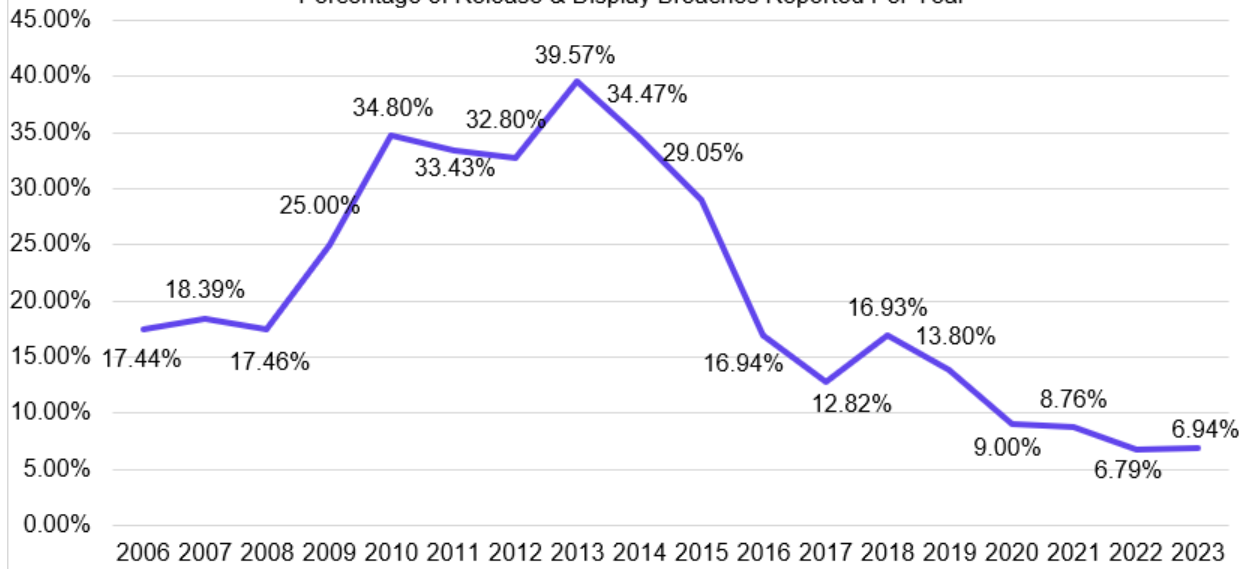
Data breaches can occur through accidental release or display when someone forgets to log out of their account, leaves a digital file on a shared desktop, or emails information to the wrong recipient, among other things. Accidental release and display incidents are up slightly since 2022. Many of these situations can be avoided if we secure our information.

- Log out of accounts on shared devices, and when you save information, make sure you're saving it to the right file and server.
- Double-check recipients and information before you send emails or messages.
- Don't save passwords on shared devices, and don't share passwords with other people.
- Make sure your digital workspace is as secure as your office – protect anything that is confidential, so you don't accidentally share it.



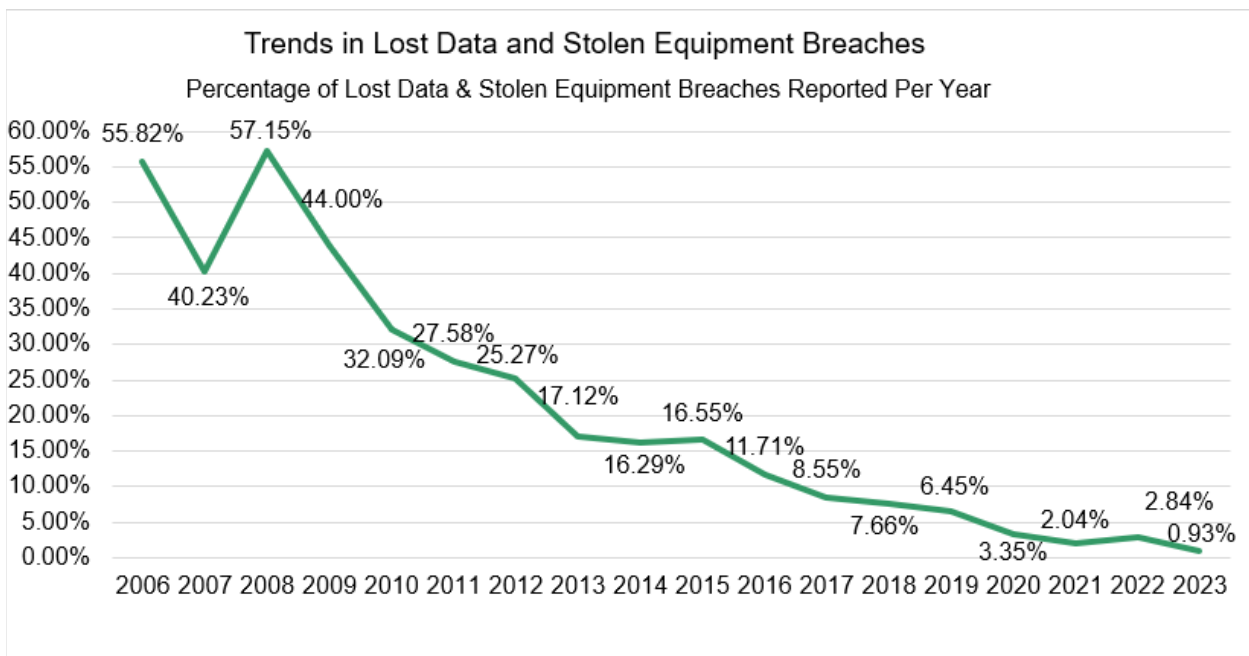
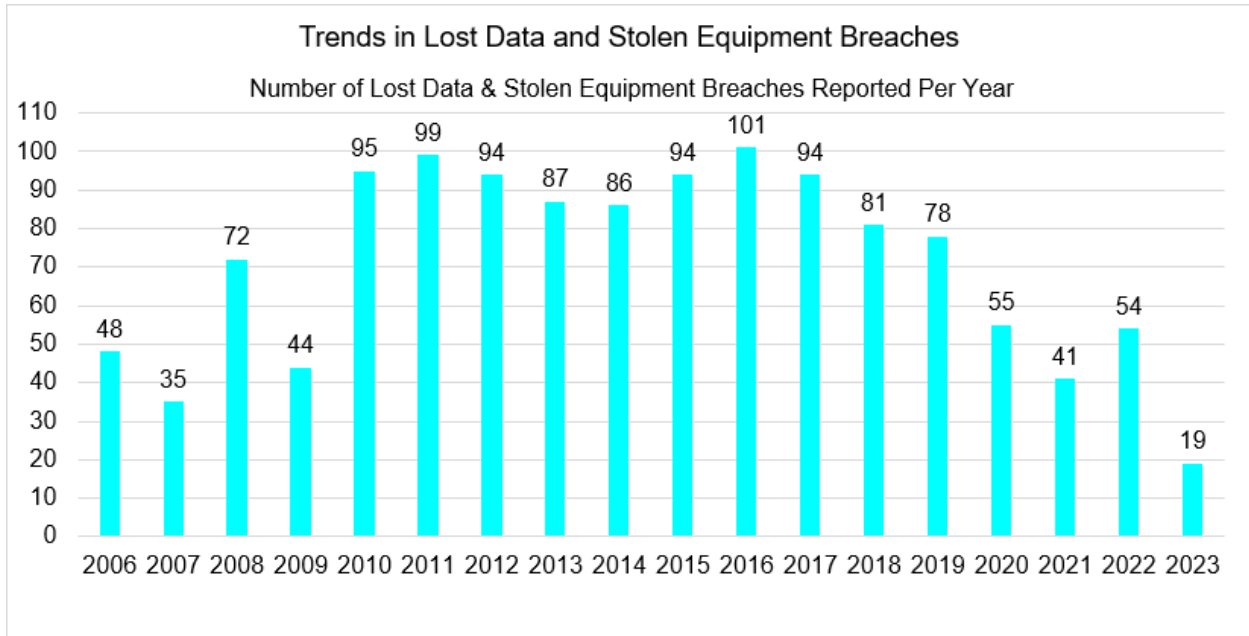
Trends in Accidental Release and Display Breaches

Percentage of Release & Display Breaches Reported Per Year



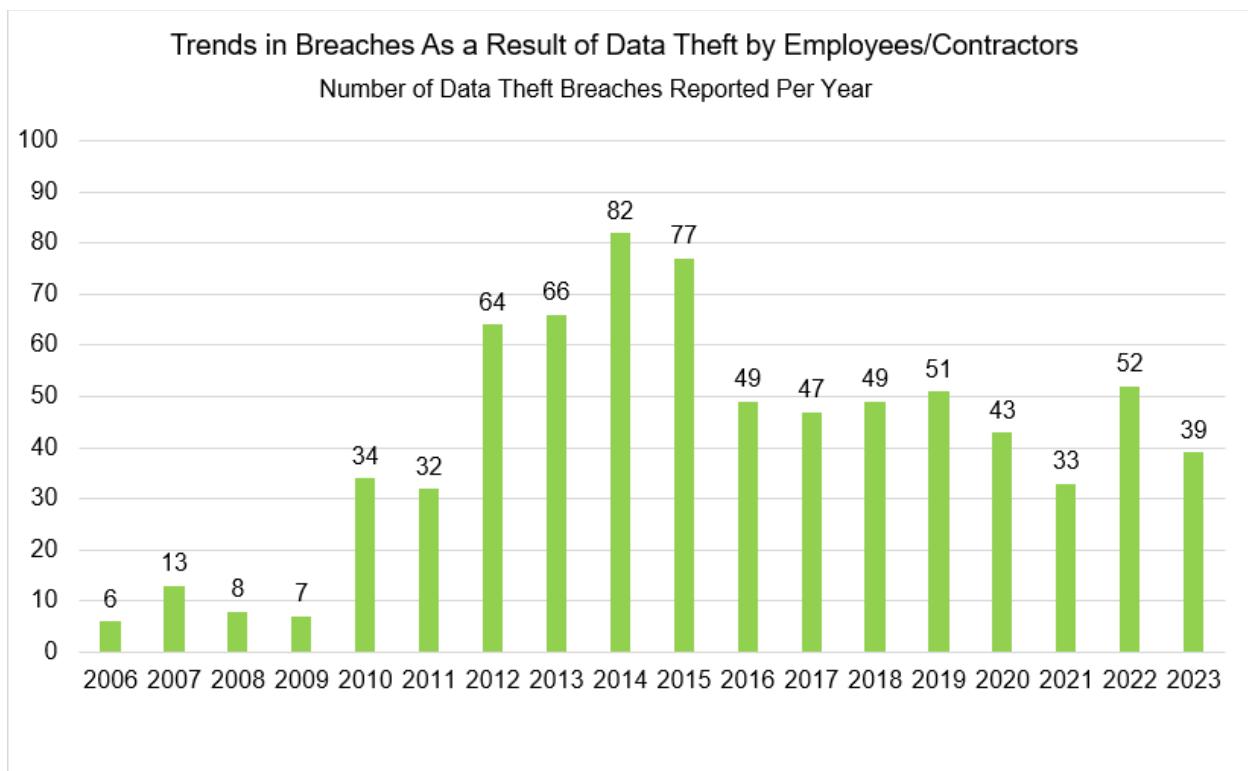
LOST AND STOLEN EQUIPMENT

The number of breaches caused by lost data and stolen equipment were at their lowest since data breaches began being reported to our office 18 years ago. That's great news and means that people are being careful about protecting devices and equipment that have sensitive data on them. People should always store devices with confidential information in locked, secure areas where unauthorized people can't get to them. Employees should act quickly to report stolen or lost devices quickly to their IT team, and businesses should have a plan in place to delete data remotely or otherwise track and retrieve stolen devices.



DATA THEFT BY EMPLOYEES OR CONTRACTORS

Data theft by employees or contractors dropped since 2022, but can be especially frustrating when it happens because the data is stolen by people who had the appropriate access to it. Businesses should make sure that employees and contractors only have access to the data they need and no more. When dealing with sensitive data or private information, employers should carefully review potential hires for any concerns. And when employees separate from a company, their employers should act quickly to remove their access to data.



SETTLEMENTS

Attorney General Stein and our office's Consumer Protection Division are committed to protecting North Carolinians' personal information. We will not hesitate to act if an organization fails to properly secure data or notify people of a breach in a timely manner.

In October, Attorney General Stein reached settlements with the companies Blackbaud and Inmediata for their lack of security practices to secure North Carolinians' data and personal information. Blackbaud settled for \$49.5 million for its deficient data security practices and response to a 2020 ransomware attack that exposed the personal information of millions of people across the United States. The North Carolina Department of Justice received 313 security breach notices related to the Blackbaud ransomware attack, which impacted 78,697 North Carolinians. North Carolina will receive \$1,181,270, and that money will go toward protecting consumers. Inmediata settled for \$1.4 million for exposing the protected health information of approximately 1.5 million consumers over almost three years. North Carolina will receive \$27,870 from the settlement.

YOUTH ONLINE SAFETY

Our kids are spending more and more time online, and while the digital world can be beneficial, it can also have damaging impacts. Middle school students spend about five and a half hours and high school students spend on average eight and a half hours online a day. Research has linked the increased amount of time on social media platforms to mental health damage and increased risk of self-harm and suicide. Social media can also expose children to content that depicts abuse and disturbing sexual images, which can warp their understanding of healthy and safe relationships.





In October, Attorney General Stein and 41 other bipartisan attorneys general sued Meta, which owns Facebook and Instagram, for allegedly designing their social media platforms to hook children and teenagers and deceiving the public by claiming that these platforms were safe and suitable for young users. Attorney General Stein is also leading a bipartisan group of state attorneys general investigating TikTok over concerns that the company unlawfully provided and promoted its platform to children.

Attorney General Stein has been visiting North Carolina schools to share his family tech agreement, a DOJ guide to help start conversations between children and caregivers about online safety and responsible internet use. The agreement, available in English and Spanish, can be downloaded [here](#).

IT TAKES A WHOLE FAMILY TO BE SAFE ONLINE

FAMILY TECH AGREEMENT


The internet can be a dangerous place, and it's important for us all to be safe online. Below are some helpful internet principles to consider with your family.

- 1 I WILL NOT TALK TO STRANGERS ONLINE.**
Direct messaging is only allowed with people we already know.
A trusted adult must approve who we message and our friends list. 
- 2 I WILL BE CAREFUL ABOUT THE INFORMATION I SHARE ONLINE.**
The things we do on the computer and other devices are not secret or confidential.
I will think twice before I share information with others or post it online, and I will never share personal details, financial information, or inappropriate content. 
- 3 I WILL COMMUNICATE WITH MY FAMILY AND STAY SAFE.**
If I see or hear something online that makes me feel scared or sad, I will tell someone. 
- 4 I WILL FIND A BALANCE WITH SCREEN TIME.**
I will have a good balance between screen time and spending time offline. 

Student's Signature

Parent/Guardian's Signature

Date





Attorney General

Josh Stein



Attorney General Josh Stein and the North Carolina Department of Justice work to protect the people of North Carolina.

For a more detailed family contract and to learn more, visit ncdoj.gov/internet-safety.

TIPS TO STAY SAFE ONLINE

- 1** Start a conversation about internet safety.
- 2** Set up parental and security controls.
- 3** Consider setting limits and alternatives to screen time.
- 4** Keep devices in common spaces, especially overnight.

ARTIFICIAL INTELLIGENCE

We heard a lot more about artificial intelligence (AI) in 2023. Some of the ways artificial intelligence can be used is exciting and promising – but we know that with any new technology, scammers will always find a way to use it to commit fraud and steal from hardworking people. That’s why Attorney General Stein has been leading nationwide efforts to put artificial intelligence protections in place. He led a bipartisan group of attorneys general urging Congress to study how artificial intelligence technology may be used to exploit children and create deep fake content that harms children. He also encouraged Congress to pass legislation to put protections in place to prevent such child exploitation.

Attorney General Stein also sent a letter to federal regulators advocating for stronger protections for AI testing, transparency, data privacy, and government oversight of AI use in high-risk situations. As AI increasingly becomes a part of our lives, we must act now to make sure bad actors can’t use it to harm North Carolinians.