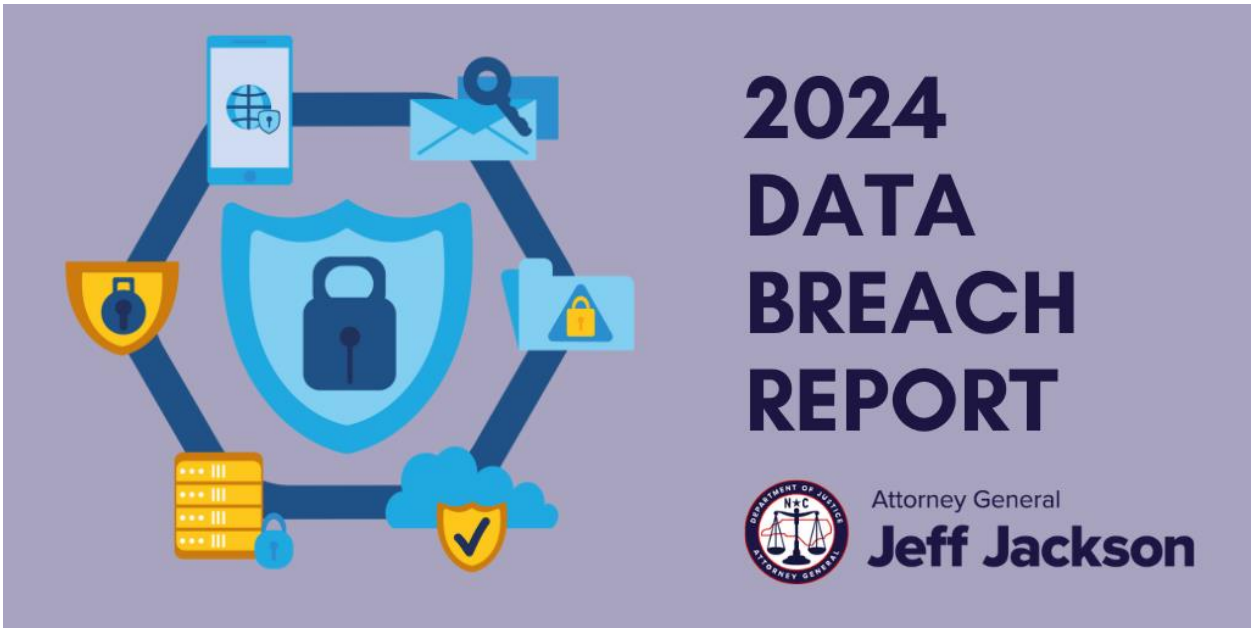


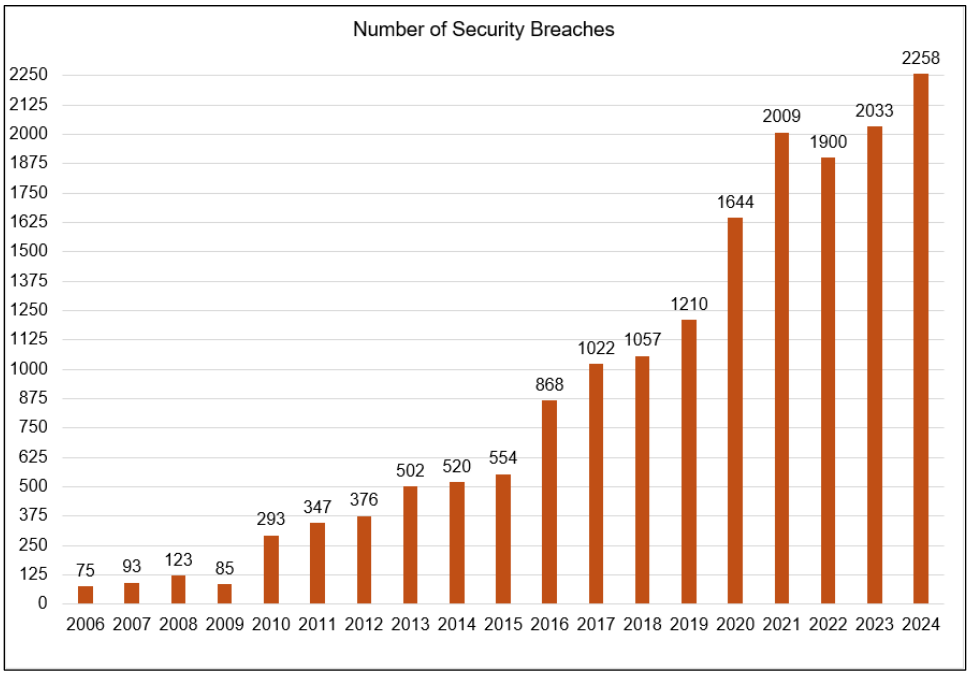
INTRODUCTION

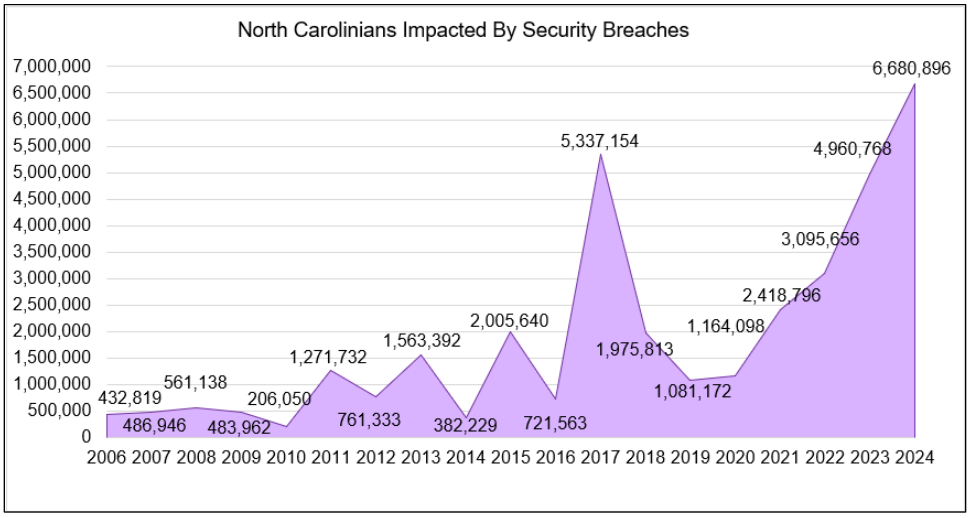
Unfortunately, 2024 was a record-breaking year for data breaches in North Carolina. More than 2,258 businesses, hospitals, government agencies, and other organizations reported data breaches to the North Carolina Department of Justice. Those data breaches also impacted a record-breaking 6,680,896 North Carolinians.

When an organization learns that it's been the victim of a data breach that compromised North Carolinians' information, it has to report that data breach to the North Carolina Department of Justice. Organizations also must share information about how the data was accessed, what type of data was stolen, and how many people were affected by the breach. Businesses are also required to tell us what they're doing to better secure information. Our office reviews that information and might decide to investigate these breaches to determine whether the organization had appropriate security measures in place and took the right steps after the breach was reported to protect information. In some cases, we may take legal action to require companies to do better and provide financial restitution or credit monitoring to North Carolinians.

Unfortunately, because we all transfer so much of our information to various businesses in our daily life, there are a lot of opportunities for a data breach. We use our credit card when we're getting coffee in the morning, we log in to our doctor's office portal to schedule an appointment, we leave our laptop in the car while we're running errands – all of these actions could lead to data being stolen or compromised. Most of us will fall victim to a data breach at some point, so it's important to understand how data can be stolen and what we can do to prevent and respond to a data breach to keep our personal and financial information safe.

This report shares more about the types of data breaches in North Carolina reported to our office and provides tips to protect data breaches. To learn more, visit www.ncdoj.gov/identitytheft.


Number of Security Breaches
2250
2125
2000
1875
1750
1625
1500
1375
1250
1125
1000
875
750
625
500
375
250
125
0
75
93
123
85
293
347
376
502
520
554
868
1022
1057
1210
1644
2009
1900
2033
2258
2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024


North Carolinians Impacted By Security Breaches
7,000,000
6,500,000
6,000,000
5,500,000
5,000,000
4,500,000
4,000,000
3,500,000
3,000,000
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
432,819
486,946
561,138
483,962
206,050
1,271,732
761,333
1,563,392
382,229
2,005,640
721,563
5,337,154
1,975,813
1,081,172
1,164,098
2,418,796
3,095,656
4,960,768
6,680,896
2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024

2024 HIGHLIGHTS

While many data breaches are new spins on the same old tactics, some data breaches happen because hackers learn a new way to target technology.

In 2024, our office received several notices of data breaches that happened through a tactic called **credential stuffing.** Hackers will steal account login information for one website for hundreds of users. Then, they'll take the username and password they stole for one site and try it on several more sites. Because people tend to reuse usernames and passwords, hackers can often gain access to other websites and platforms. The more platforms they can access, the more data they may be able to steal. Then, they try it again for the next person's stolen credentials, and so on, until they've collected many people's financial and personal data.

Credential stuffing is becoming a more common breach tactic, but there's one significant way to help protect yourself from these attacks: practice safe password strategies. Change your passwords regularly, use strong passwords, and don't re-use passwords.

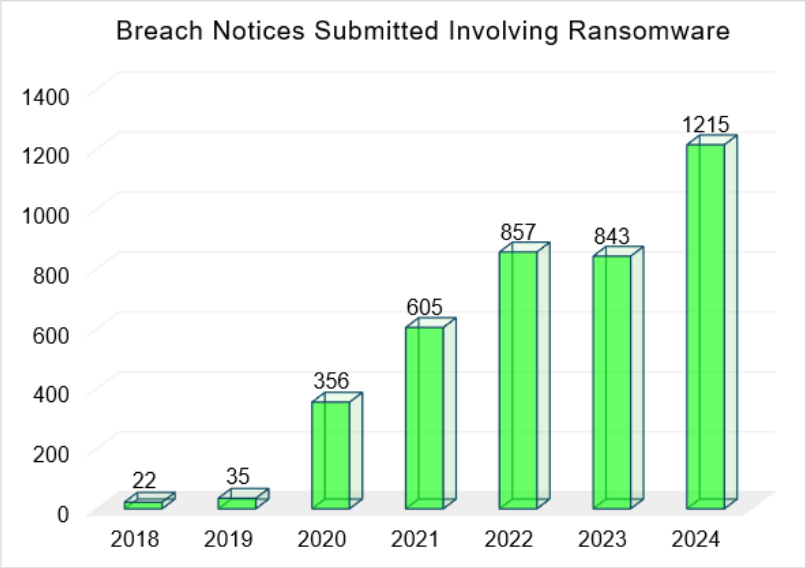
W-2 breaches are also a prominent type of data breach. Hackers will often use phishing emails to target people's tax information, including data contained on their annual W-2 income tax form. Often, those emails look like they are coming from your HR department or benefits manager, so people are motivated to respond and log in. Once they put their information into a phishing site that looks like their organization's financial portal, hackers can access their W-2 information and use it to commit identity fraud. W-2 breaches aren't a new scam tactic, but they are on the rise and often ramp up in the beginning of the year and during tax season.

Ransomware attacks have increased nearly 50 percent since last year and contributed to more than half of all data breaches reported in 2024. Ransomware attacks often start when someone clicks on a link in a phishing email, but they can also happen if a hacker finds a security gap in an organization's data security or installs malware on a network.

CHANGE HEALTHCARE DATA BREACH

In February 2024, Change Healthcare, a major health care company that insurance companies, providers, and patients use to manage insurance claims and payments, detected a ransomware attack in its computer system. The attack reportedly compromised the private health information of approximately 190 million people nationwide – the largest reported health care data breach in United States history. The hackers may have accessed a variety of sensitive personal, health care, and payment information. Change Healthcare has said that there were vulnerabilities in their security measures, including a lack of two-factor authentication, that allowed the attack to occur.

The types of potentially compromised personal information include names, addresses, dates of birth, phone numbers, email addresses, financial and banking information and government ID numbers. The potentially compromised types of health information include health insurance details, diagnoses, test results, medications, imaging records, and care and treatment plans. Our office is continuing to look into this data breach.



To help guard against a ransomware attack:

- Keep your data security software up to date and regularly analyze your security for gaps and holes that a hacker might find. When you find those potential areas for access, address them immediately.
- If you lead a business, make sure you have a plan in place for how you will respond to ransomware attacks – think about who you will need to report it to and what information you'll be able to share with employees and customers to protect their data.
- Train your employees and colleagues to be skeptical of emails and other communications that contain links or downloads. Remind them to report concerns immediately. The faster you know about a potential breach, the faster you'll be to respond.

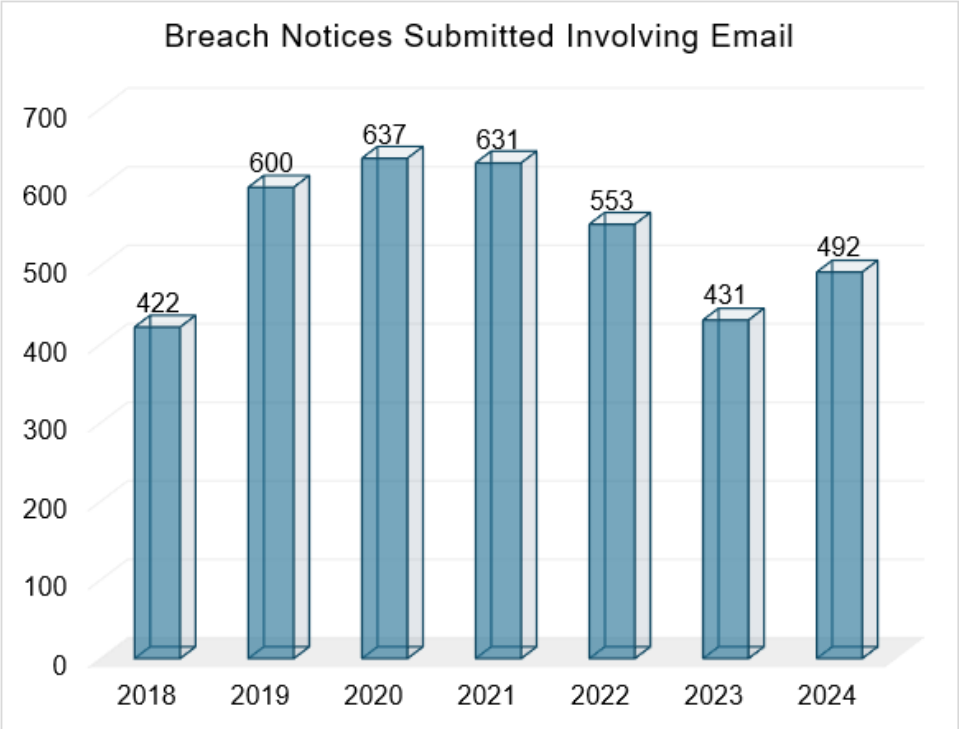
EMAIL BREACHES

Email breaches are on the rise again after having fallen steadily since 2020. An email account is breached if someone gets access to it, or if a hacker uses a phishing or spam email to gain access to your email or your organization's network. We open between dozens and hundreds of emails per day, and scammers know that targeting our email accounts is an easy way to get our personal information.

Help prevent email breaches:

- Implement multi-factor or two-factor authentication on your email accounts so that hackers have a harder time accessing your account and you get notified earlier if someone is trying to gain access.
- Don't share personal or financial data over email. Remember that if a hacker gets access to your email account, they have access to all the information you've sent or received via email. If it's sensitive data, don't share it via email.

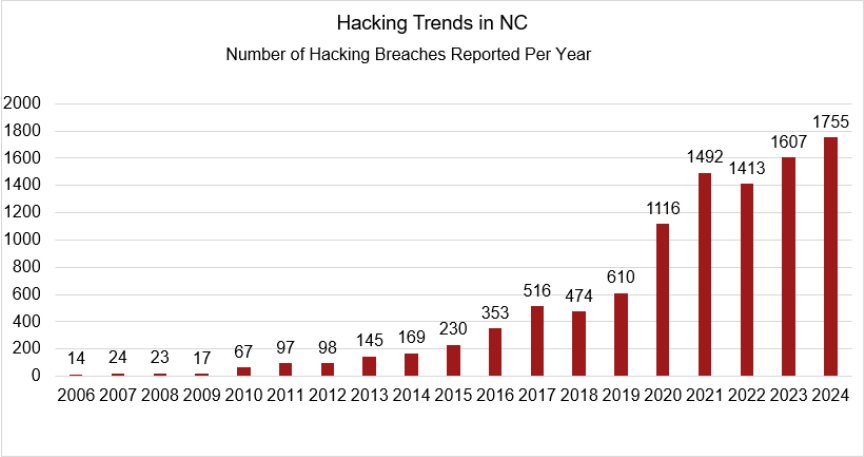
- Examine links or attachments closely before you click on them. If you weren't expecting an email or it's not from a recognized sender, think twice before you click on it.

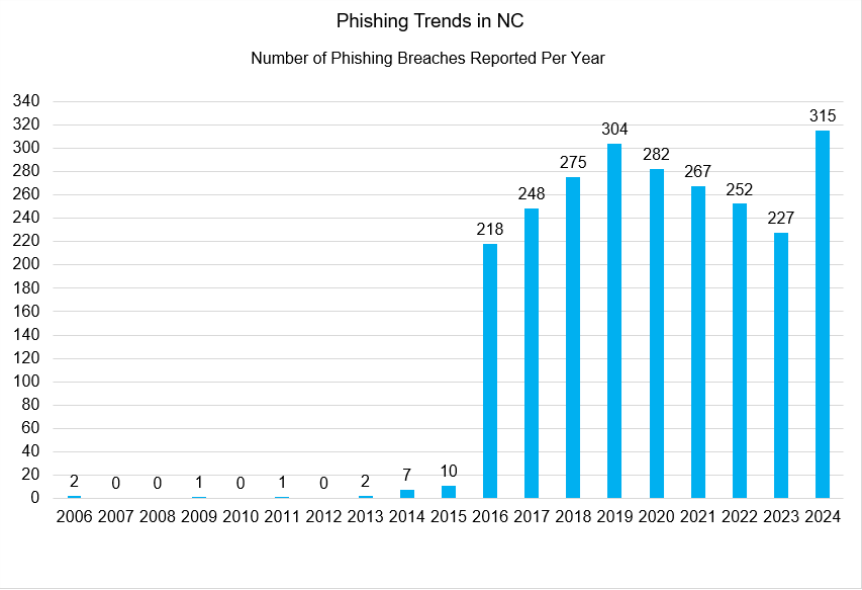


HACKING AND PHISHING

Hacking and phishing scams are the easiest and most common way for scammers and criminals to access people's online data. But in many of these attacks, you have to take a certain action that will allow the hacker access to your system or network – if you can avoid doing that action, the hacker won't be able to access data. So, make sure that you:

- Take a close look at emails before you click on links or download attachments. If something seems off – the sender's email address, uncharacteristic spelling errors, a strange time of day to be receiving an email, or an unexpected email altogether – send it to your IT department or reach out to the sender directly to ask them. It is always better to be safe than sorry.
- When you update antivirus and security software, don't just do it on your laptop. Also take a look at updates for your smartwatch, your TV, your tablet, and smart speakers.
- Use strong passwords and update them regularly.





POWERSCHOOL DATA BREACH

PowerSchool officials are still responding to the PowerSchool hack that occurred in December 2024. PowerSchool sells software products used by schools across the country, including all the public schools in all 100 counties in North Carolina. That means that if you're a parent or a child who is using or has used PowerSchool apps in the past few years, your information may have been compromised. The hacker reportedly obtained data of more than 62.4 million current and former students and 9.5 million teachers – including almost 4 million people in North Carolina – in addition to parents whose information might also have been stored in the app. Hackers gained information including Social Security numbers, medical information, addresses, and phone numbers.

If you're a parent or guardian of a North Carolina public school student or have a student at any private school that also uses PowerSchool, you should take additional steps to set up a security freeze for your child to protect them from identity theft. A child security freeze stops criminals taking out credit in your child's name and protects their Social Security number and other private data.

To put a child security freeze in place, you should contact all three credit bureaus:

- Equifax – Direct Link
  1-800-349-9960
- Experian – Direct Link
  1-888-397-3742
- TransUnion – Direct Link
  1-888-909-8872

You'll need your child's:

- Social Security number or card
- Certified or official copy of a birth certificate
- A driver's license or other government-issued ID copy

You'll also need to provide proof that you have the authority to act on behalf of the child and are their legal parent/guardian - such as a court order, a birth certificate, a Power of Attorney, or a foster care certificate.

Credit bureaus must comply with online or telephone requests for a security freeze within one business day of receiving them, and with mail requests within three business days.

TICKETMASTER DATA BREACH

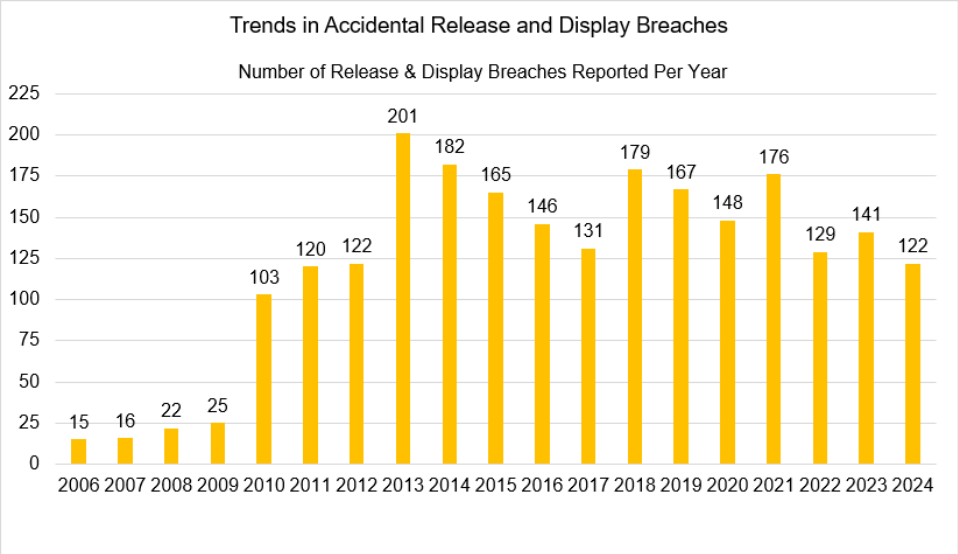
In May 2024, Ticketmaster identified unauthorized activity within a third-party cloud database environment containing Ticketmaster data. The hackers likely accessed and stole information about North Carolinians from that third-party database between April 2, 2024, and May 18, 2024. The compromised information may have included names, contact information, payment card information such as hashed and/or masked credit card numbers, and passport numbers for a limited number of people.

ACCIDENTAL RELEASE AND DISPLAY

Data breaches through “accidental release” have fallen since 2023, which is a good thing. These are unintended instances of sharing information with people who shouldn’t have access to it. If a doctor leaves your medical record open on their laptop and someone walking by reads it, that’s a data breach caused by accidental release.

Take extra precaution to prevent your data from being mistakenly shared with others:

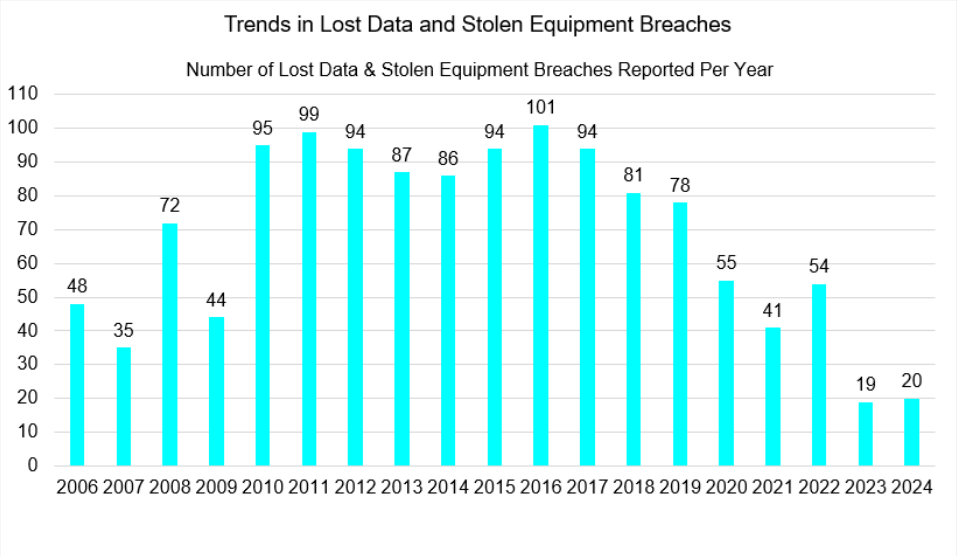
- Double-check who you’re sending information to and what you’re sending – never send more than what is absolutely necessary.
- Sign out of accounts and clear saved passwords, especially if you share a device with others, include your family members.
- If you have confidential data in your office or workstation, make sure it’s secure when you step away or leave for the day.



LOST DATA AND STOLEN EQUIPMENT

We've all lost a device before – it's understandable, but if it falls into the wrong hands, hackers and criminals can use it to wreak havoc. Data breaches caused by lost data or stolen equipment are about as common as they were last year.

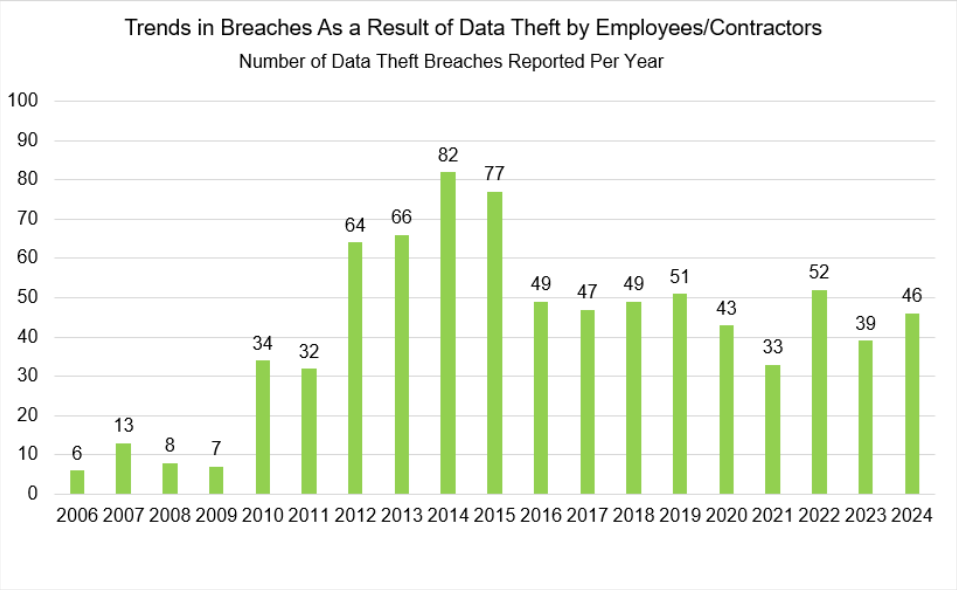
- Make sure you secure your data and devices. If you can, add tracking to your devices so you know where they are even if they get lost or stolen.
- If something is lost or stolen, tell your IT team immediately. Even if it turns up later, your IT team may be able to take action to protect or wipe any confidential data on the device.
- Limit who has access to confidential data and what devices it's stored on. The fewer storage locations for that data, the lower the risk that it's stolen.



DATA THEFT BY EMPLOYEES AND CONTRACTORS

Forty-six data breaches caused by employees or contractors stealing data were reported to our office in 2024. When businesses store personal or financial data for consumers or other people they work with, they have a responsibility to make sure that the people who can access that data are trustworthy and responsible. That includes:

- Limiting access to data to only the people who actually need it. If they don't need it, they shouldn't be able to access it.
- Making sure employees are trained on security practices.
- Installing security software to prevent the unauthorized transfer or download of data.
- Removing access to data for employees after a certain amount of time and when they leave the company.



CONCLUSION

As technology continues to advance, and as we rely on it for more and more functions of daily life, hackers will find new opportunities to steal data or scam people into giving away their personal or financial information. The North Carolina Department of Justice works to keep people updated about the latest data breaches, scams and frauds and provides resources so people can take action if their data is compromised. Learn more at www.ncdoj.gov/internet-safety.