NORTH CAROLINA
DEPARTMENT OF JUSTICE

2022 DATA BREACH REPORT

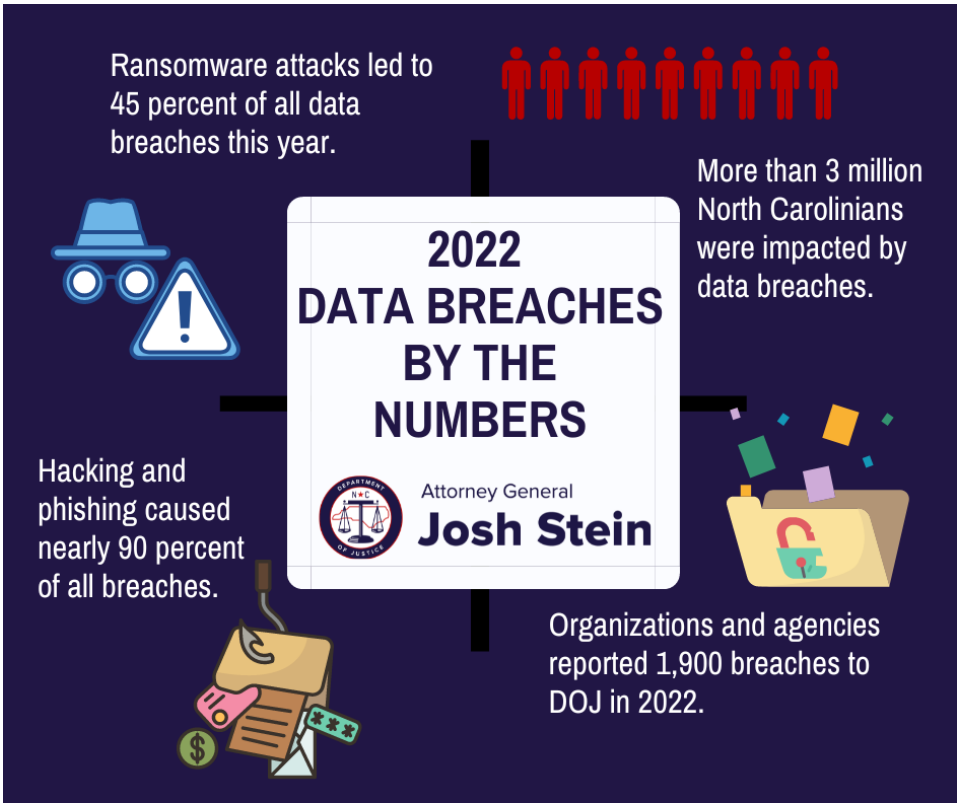
Attorney General
Josh Stein

At the North Carolina Department of Justice, we work to protect North Carolinians from scams and fraud. Scammers are always looking for new ways to get your money or your personal information. Unfortunately, the more time each one of us spends online, the more our information is at risk. We work, manage our bank accounts, shop, go to school, and connect with friends online. We leave our data and passwords in the hands of online platforms, companies, and government organizations. We put our trust in these entities.

Those organizations have a responsibility to keep our data safe and to minimize any damage when our information is compromised. In North Carolina, businesses and government agencies are required by state law to report security breaches to the Department of Justice. This annual data breach report breaks down the security breaches reported to our office in 2022, and where those breaches stand in comparison to years before. We're also sharing information you can use to prevent security breaches and keep your information secure.

For additional resources to protect your identity and data, or to report a scam or fraud, contact our office at 1-877-5-NO-SCAM or visit www.ncdoj.gov.

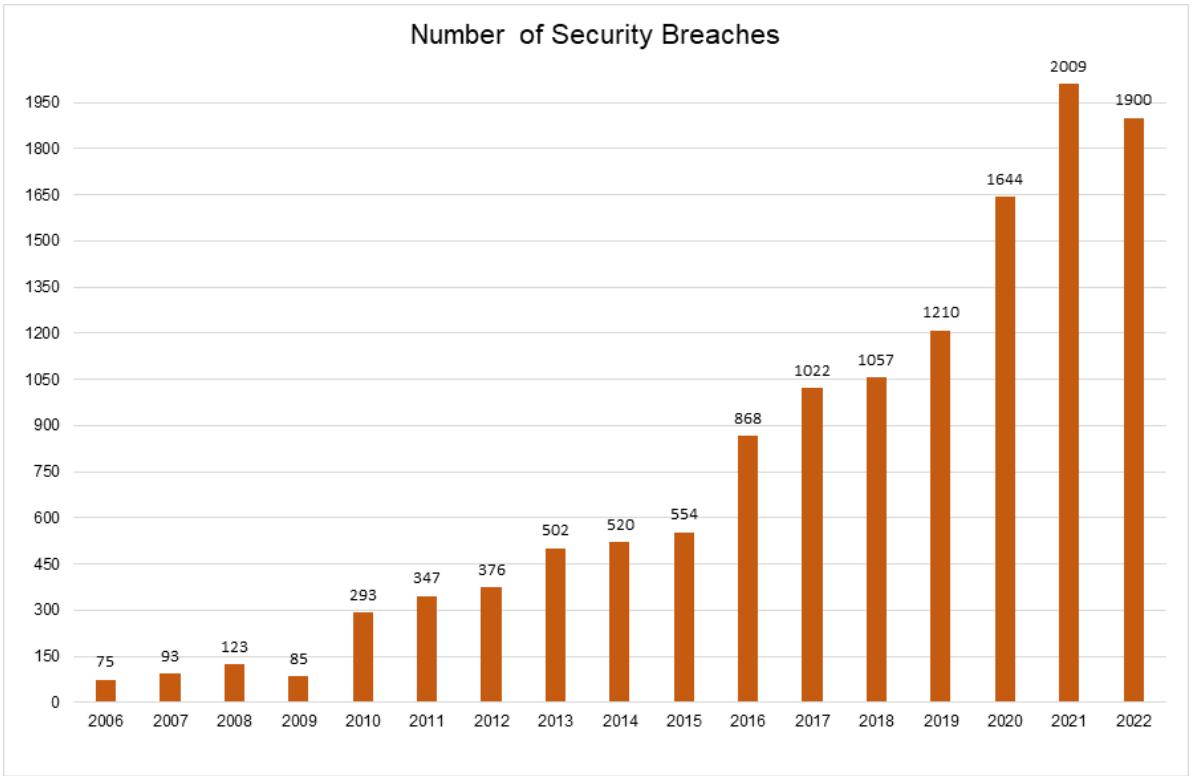
HIGHLIGHTS

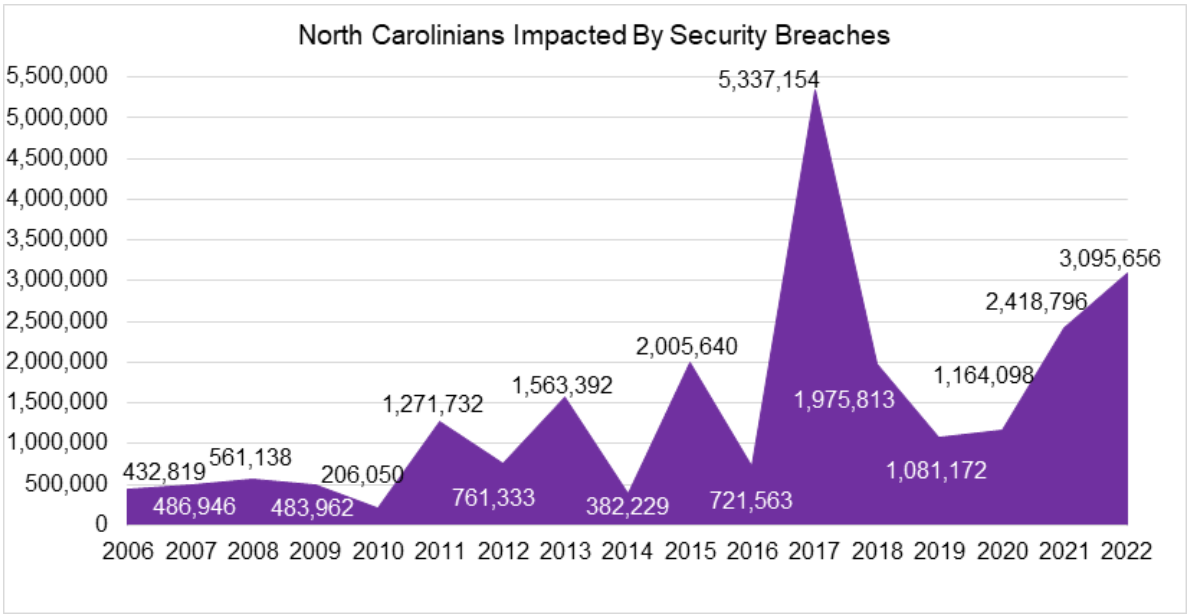


- The number of security breach notices (1,900) dropped for the first time since 2009.
- More than 3 million North Carolinians were victims of security breaches last year. This is the second highest number of people impacted by breaches in a single year, second only to 2017 when the Equifax data breach affected nearly 5 million North Carolinians.
- Ransomware breaches are continuing to skyrocket. This year, they made up 45 percent of reported breaches.
- Phishing and hacking caused the majority of breaches – nearly 90 percent, for the second year in a row. Criminals often use phishing and hacking scams to infect systems and networks with ransomware.

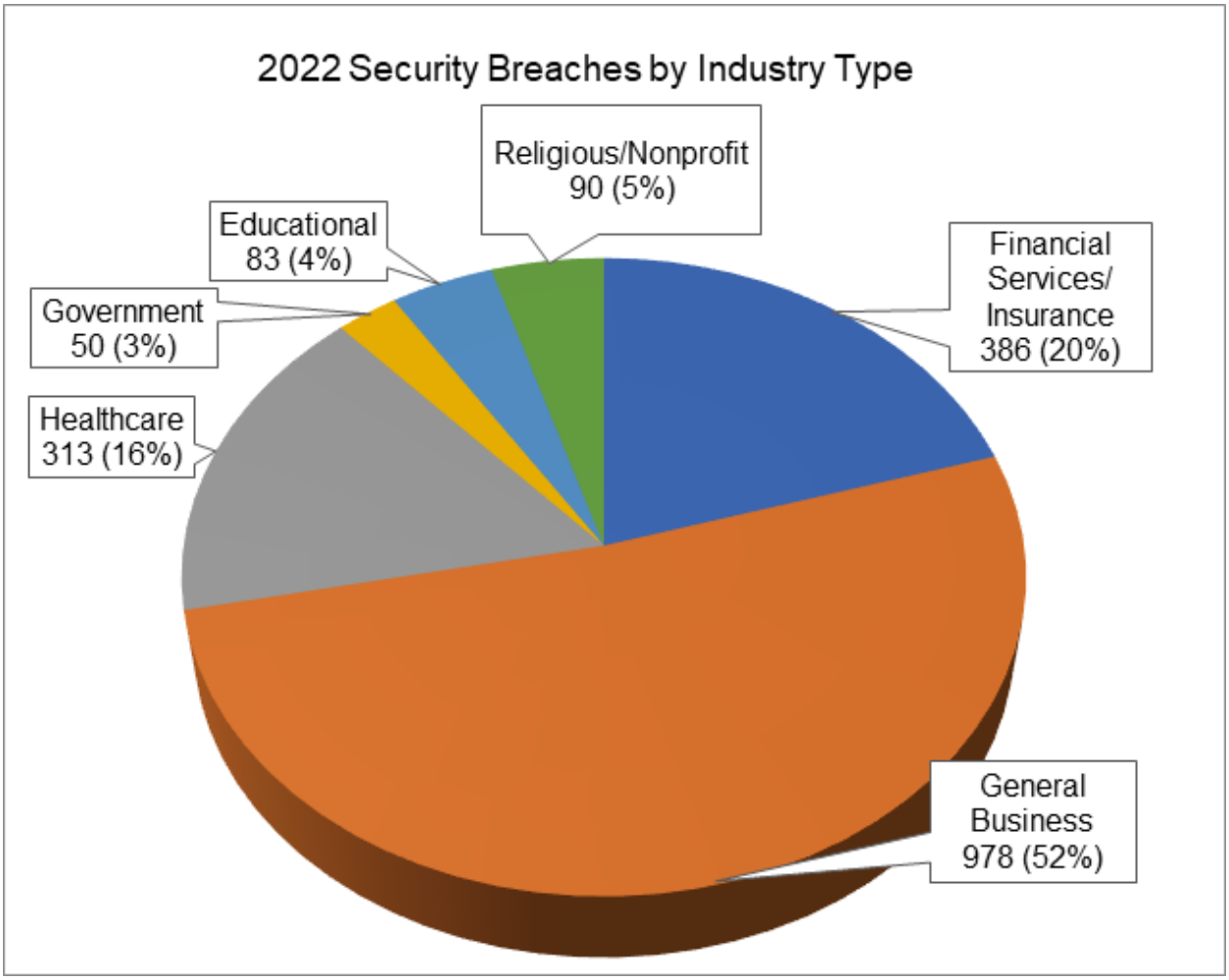
OVERVIEW OF 2022 BREACHES

In 2022, organizations submitted 1,900 data breach notices to DOJ, a decrease from the year before. But the breaches impacted 3,095,656 North Carolinians – the second highest number of people ever affected in a single year in the state. Since 2005, businesses have reported a total 12,820 breaches that impacted 24,290,392 people.





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.

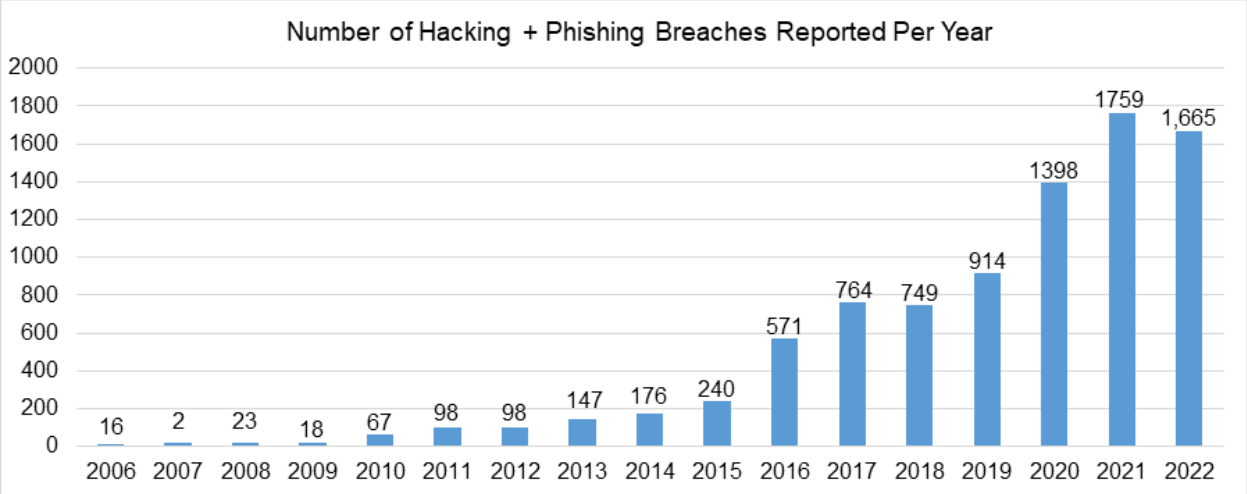


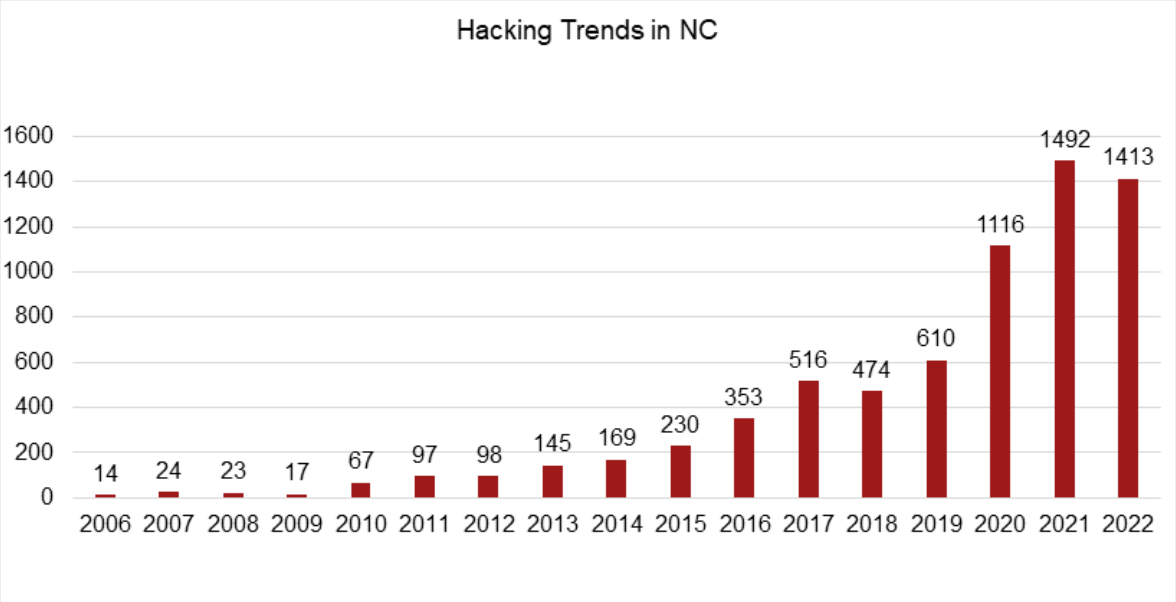
Similar to last year, data breaches were most often reported by general businesses, financial services institutions, insurance companies, and health care entities. Since we're often most likely to share sensitive financial data with financial institutions or with businesses we make purchases with, that data can often be a target for hackers. We're continuing to encourage organizations to revisit and revise their security policies so they are responsibly securing consumer and patient data. Companies that have access to sensitive information must also take reasonable precautions to keep that information safe.

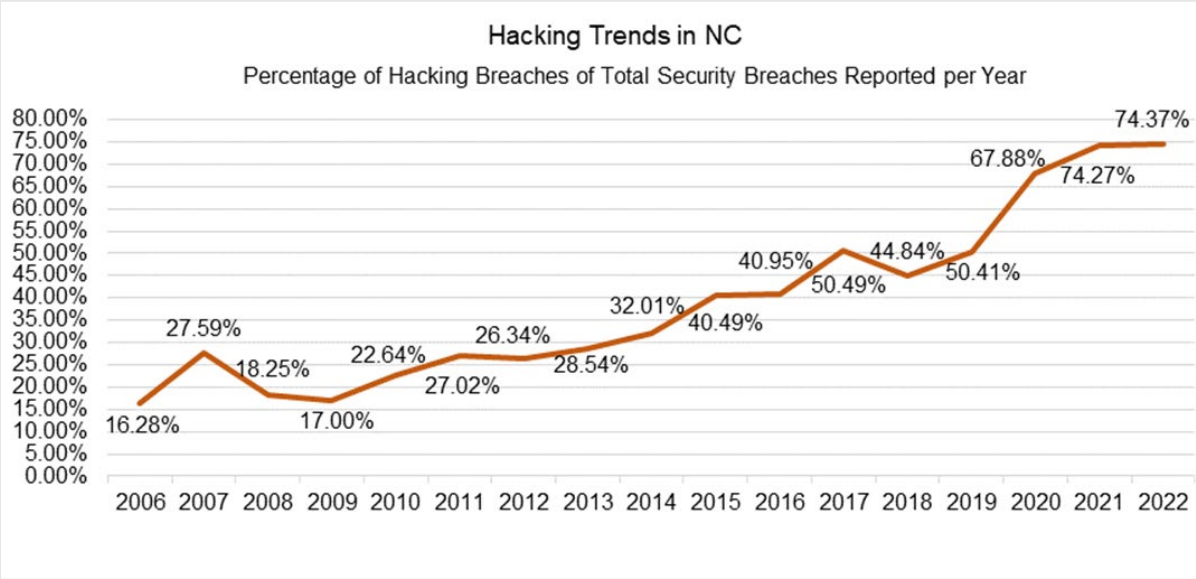
HACKING AND PHISHING

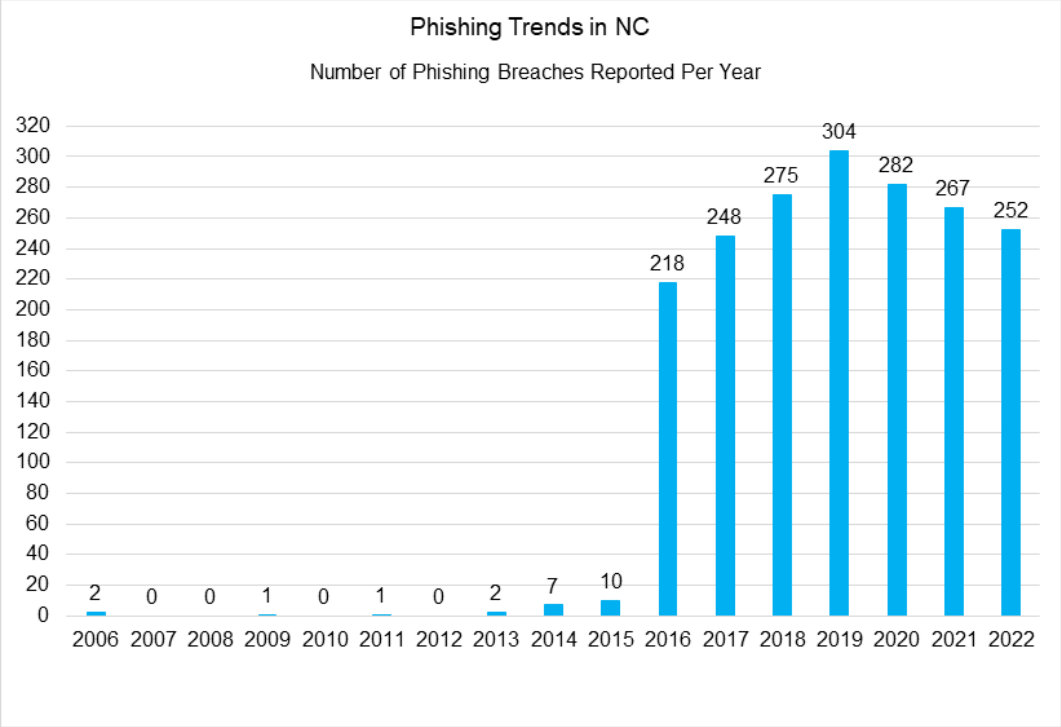
Hacking attacks are overwhelmingly the most common gateway that criminals use to access a network and the data stored there. Hackers get into your system in different ways – they can send you a link or attachment through a phishing email, employ a ransomware attack on your device or network, or simply steal your password and security information to log in as you. You should take precautions to always protect your data and passwords:

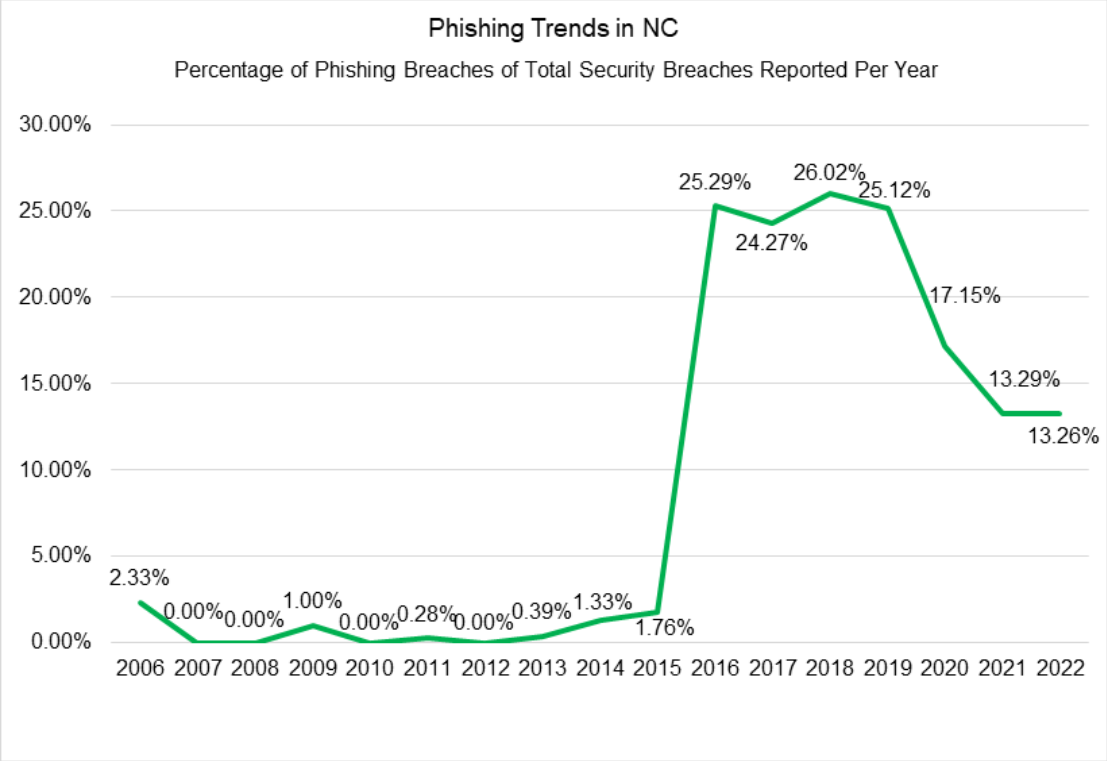
- Don't open emails, click links, or download attachments from unverified senders. Examine an email closely before you take action – do the email address, the subject and content, and the attachments or links seem authentic? Are they coming from people you know and email addresses you recognize? If you're not absolutely sure, contact the company or person directly to ask.
- Update software on your phone and computer regularly. These updates often include critical security patches to protect your devices from hackers. Don't forget updates on your smart watches, tablets, or any other electronic devices.
- 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 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.




Hacking Trends in NC
1600
1400
1200
1000
800
600
400
200
0
14
24
23
17
67
97
98
145
169
230
353
516
474
610
1116
1492
1413
2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022


Hacking Trends in NC
Percentage of Hacking Breaches of Total Security Breaches Reported per Year
80.00%
75.00%
70.00%
65.00%
60.00%
55.00%
50.00%
45.00%
40.00%
35.00%
30.00%
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
16.28%
27.59%
18.25%
17.00%
22.64%
27.02%
26.34%
28.54%
32.01%
40.49%
40.95%
50.49%
44.84%
50.41%
67.88%
74.27%
74.37%
2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022

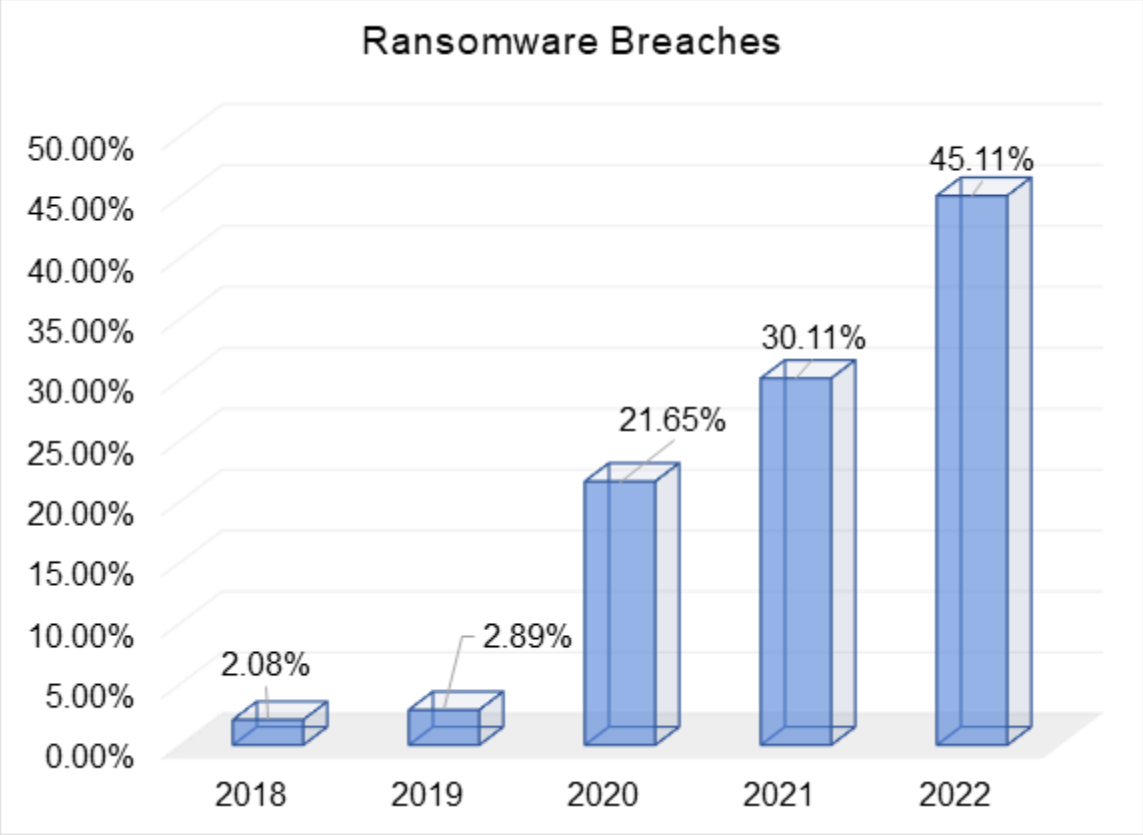

Phishing Trends in NC
Number of Phishing Breaches Reported Per Year
320
300
280
260
240
220
200
180
160
140
120
100
80
60
40
20
0
2 0 0 1 0 1 0 2 7 10 218 248 275 304 282 267 252
2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022


Phishing Trends in NC
Percentage of Phishing Breaches of Total Security Breaches Reported Per Year
30.00%
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
2.33% 0.00% 0.00% 1.00% 0.00% 0.28% 0.00% 0.39% 1.33% 1.76% 25.29% 24.27% 26.02% 25.12% 17.15% 13.29% 13.26%
2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022

RANSOMWARE

Ransomware attacks continue to increase in North Carolina. Last year, our office received a record 857 data breaches caused by ransomware, making up about 45 percent of all reported data breaches.

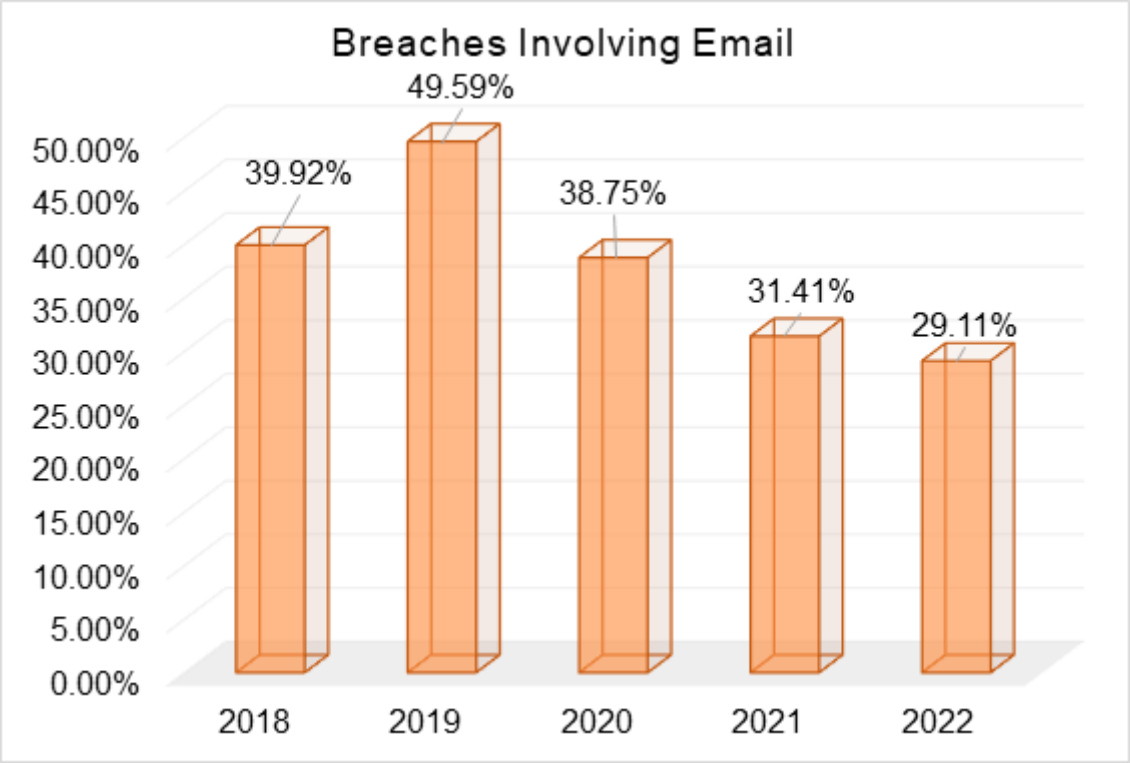
- Have a plan in place for you or your organization on how you'll respond to ransomware attacks. Make sure you update this plan regularly and train your employees to be ready to implement it.
- Back up your data regularly so you aren't at the mercy of hackers to access it.
- Regularly participate in and conduct trainings to help identify the signs of a ransomware attack.
- Keep all security and ransomware prevention software up to date on all of your devices.
- Have a plan in place to notify customers or people whose data you store if you become the victim of a ransomware attack.



EMAIL

Email breaches, which include misdirected emails that contain personal information, phishing access into email accounts, and any other unauthorized access, accounted for a significant number of breaches reported in 2022 – more than 29 percent. Protecting email accounts is important because emails contain personal information, and often, if a hacker can get access to an email account, they can get access to a company's network.

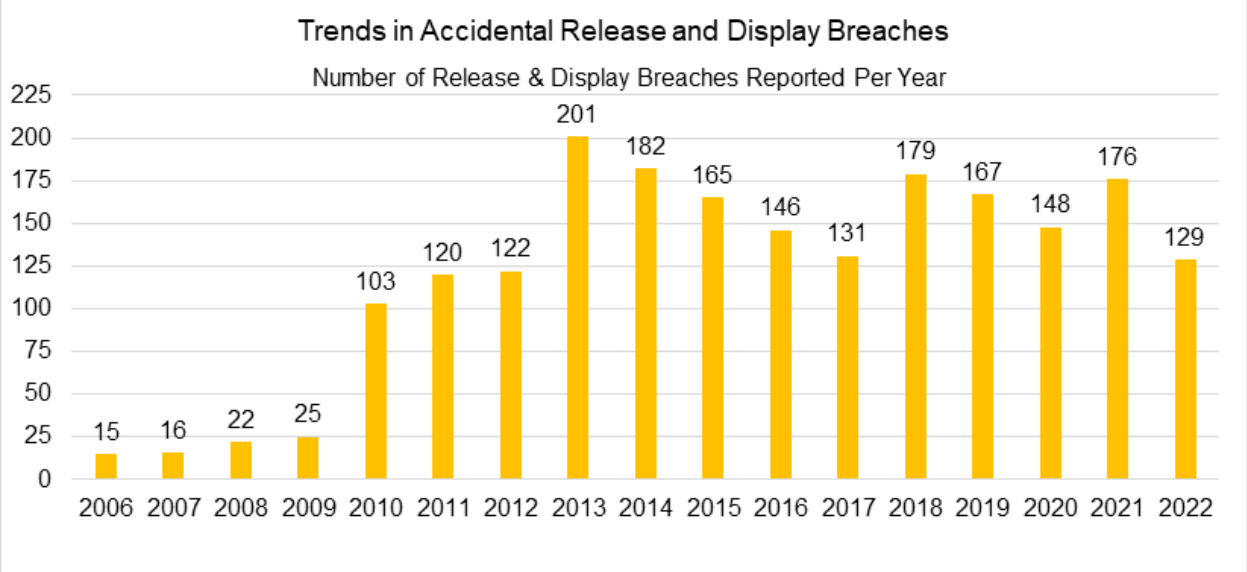
- Limit or eliminate the exchange of personal information through email. This will minimize the amount of personal information available if an email account is compromised.
- Create strong passwords and use multifactor authentication to make it hard to get into email accounts.
- Avoid using the same password for multiple accounts.
- Be wary of links and attachments in emails, and make sure the sender is a legitimate source or someone you know before clicking.

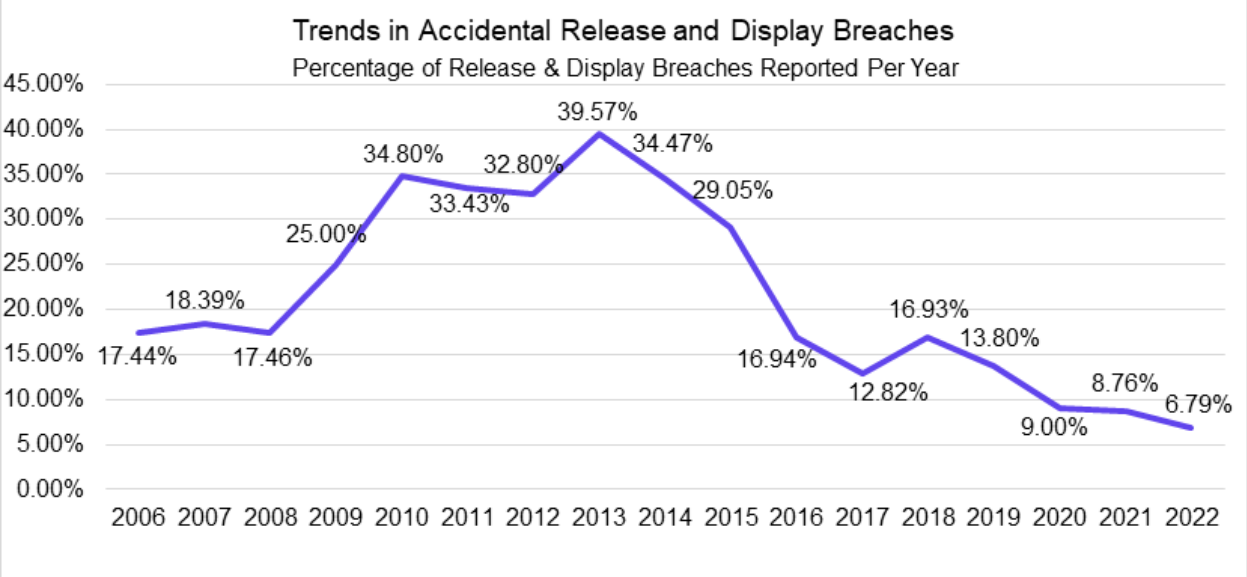


ACCIDENTAL RELEASE AND DISPLAY

Accidental release and display breaches occur when a person or business shares information without meaning to. At its simplest, this might mean leaving your laptop screen open to viewing in a high traffic area or maintaining your data outside of a secure area of your network. You can and should take steps to make sure you secure your hardware and double-check your data sharing practices.

- Log out of accounts on shared devices.
- Don't share passwords with other people.
- Be diligent and cautious about sharing information.

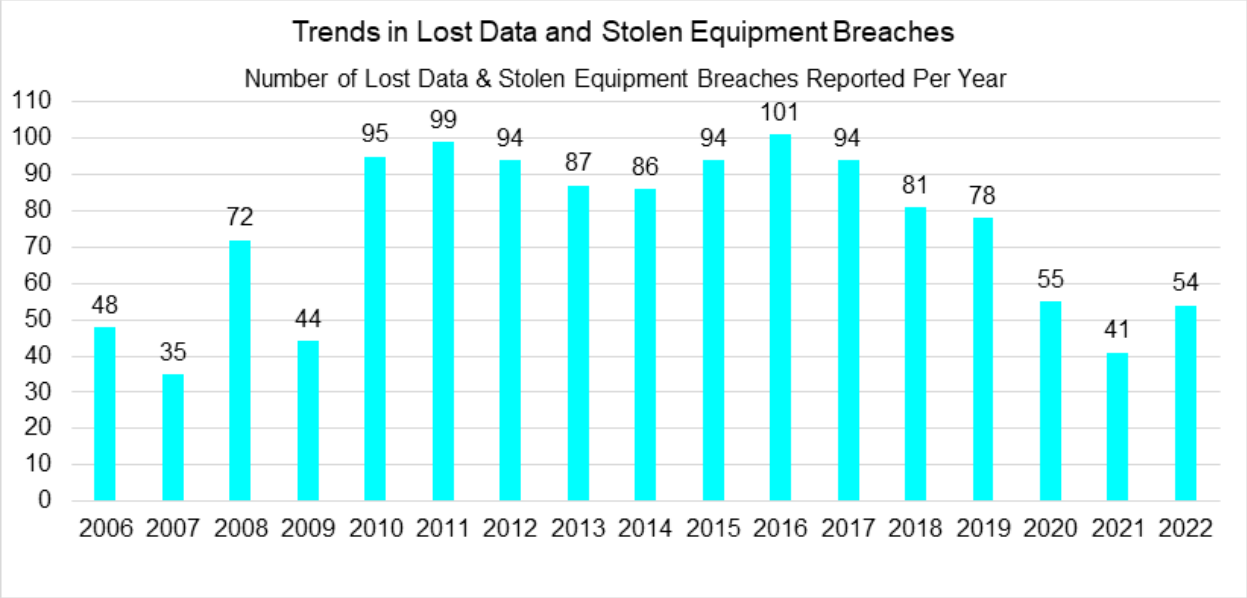


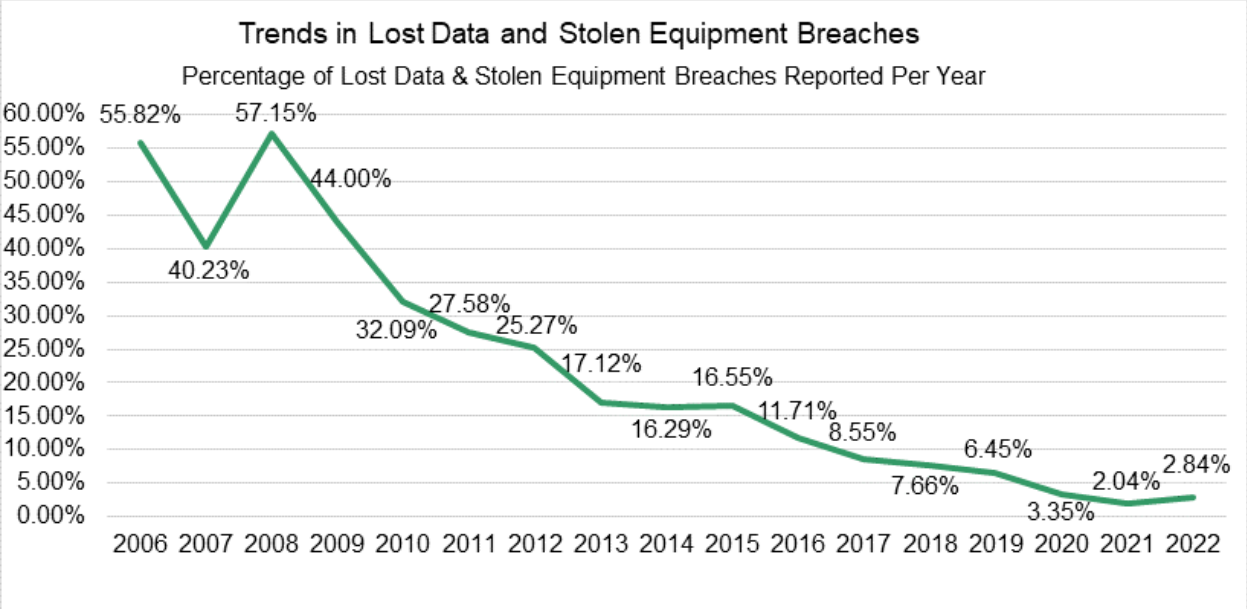


LOST AND STOLEN EQUIPMENT

Having your equipment get lost or stolen is always a headache – but it's much worse when your devices have other people's sensitive information. Lost and stolen equipment breaches increased slightly in 2022.

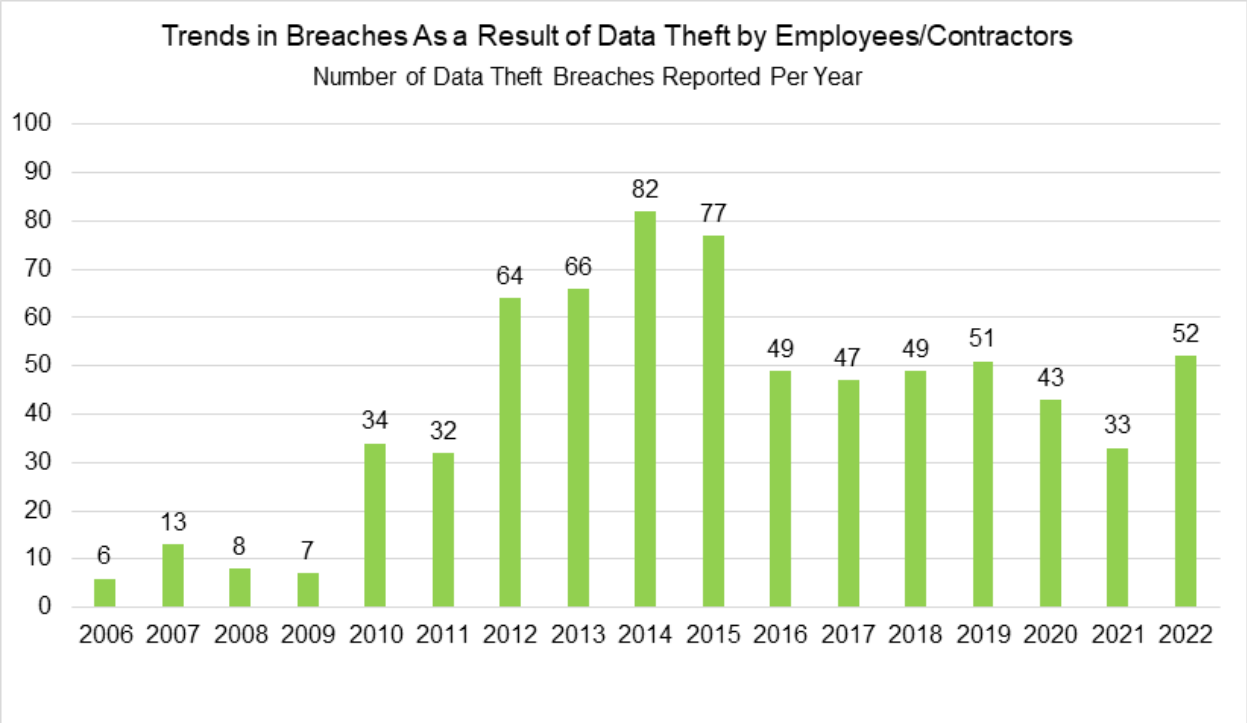
- Lock and store your laptop and other electronic devices when you're not using them.
- Make sure your organization is tracking device inventory and that employees know to report stolen equipment so you can take precautionary steps to prevent breaches.





DATA THEFT

Data theft increased slightly in 2022. This type of theft occurs when employees or contractors steal information they have access to. Business and agencies have a responsibility to safeguard the information and data they have – they should vet potential hires carefully and restrict access to data to only the people who need it.



SETTLEMENTS

When companies fail to properly secure customers' data or notify people of a breach, our office may investigate and hold companies accountable through litigation. Attorney General Stein resolved three privacy cases in 2022, including the largest in our nation's history.

In June, Attorney General Stein reached a $1.25 million multistate settlement with Florida-based Carnival Cruise Line over a 2019 data breach that compromised the information of 180,000 people, including 3,139 North Carolinians.

He also secured a $1 million multistate settlement with Experian Data Corporation for failing to warn consumers after an identity thief posed as a private investigator and stole personal information from an Experian database.

Additionally, in November, Attorney General Stein was on the executive committee of states that negotiated a $391.5 million multistate settlement with Google over its location tracking practices. This is the largest privacy settlement attorneys general have negotiated in U.S. history.