

# Data Breach Guidance for Parents

*Data breaches have become so commonplace that many experts agree it's not a question of IF your data will be breached, but WHEN. NYSED's Data Privacy Office wants to make sure you have the information you need to protect your family.*

## Steps you can take to help prevent your child's data from being breached:

1. **Talk to your child about cybersecurity and data privacy** – You have already had the conversation about not talking to strangers. Continue that conversation by making sure they understand it includes strangers on the internet. Make sure they know people aren't always who they say they are and internet strangers might try to trick them into sharing information they shouldn't. **Here are some more tips for children and parents:**
  - a. **NEVER use unsecured Wifi!**
  - b. Keep your webcam covered when it's not being used.
  - c. Do not keep school/work apps on personal devices and vice versa.
  - d. Do not click on a link in an email or text. Manually navigate to the entity's website instead.
  - e. Don't loan out your devices – even to your friends.
  - f. Keep your devices locked when not in use.
  - g. Even if they're locked, don't leave your devices unattended.
  - h. Turn off location sharing for all apps on your kids' devices! If they need to use location sharing, only allow it while the app is in use.
  - i. Review the privacy settings for all of their apps and only allow apps to collect the minimum information they need to operate.
  - j. Updated their device settings to automatically update apps, software, and operating systems.
  - k. Set up their devices to automatically create backups frequently.
2. **Freeze your child's credit** – While it will require a little bit of leg work, and it won't prevent bad actors from acquiring your child's information, **if your child is under 16 you can freeze their credit.** This will prevent bad actors from opening accounts in your child's name without your knowledge or consent.
3. **Frequently check your child's information**
  - a. Via credit bureaus
  - b. Check what they are sharing on social media and consider privacy settings
  - c. Sign up for services that alert you when information has been shared illegally
4. **Protect your child's data**
  - a. Don't give out your child's sensitive information if you can avoid it.
  - b. Beware of scam calls and unusual emails.
  - c. Banks and other institutions always welcome a call back. So if you are unsure, hang up the phone, find a number you are sure is your bank or other institution and return the call.
5. **If someone asks for your child's Social Security Number (SSN), ask questions:**
  - a. Who are you?
  - b. What company/entity do you represent?
  - c. Why do you need it?



- d. How did you obtain my contact information?
- e. What is the phone number that I can use to call you? (No phone number, no data!)
- f. Can you use a different identifier?
- g. Can you use just the last four digits of my child's SSN?
- h. How will it be shared? Never email an SSN and only submit on a platform you are sure is secure.<sup>1</sup>

## 6. Protect your child's digital information

- a. Stop and consider how much identifiable information you are posting about your child. If a bad actor targets your child, public and breached information can be combined and might make your child more susceptible to identity theft or other crimes.
- b. Use strong passwords: the longer a password is, the harder it is to guess. Consider a third-party password generator that creates passwords for you. Search for "password generator" in your internet browser to find options that are free and easy-to-use.
- c. Use multi-factor authentication when possible.
- d. Be vigilant: be on the lookout for phishing and social engineering, including scams that use your child's voice, image or other information that appears personal and is intended to gain your trust.
- e. Update software and apps you use, and delete the ones you don't.
- f. Avoid saving important information in notes, texts, or images.

## 7. Protect paperwork with sensitive information

- a. Store important information in a lockable cabinet
- b. Shred sensitive information you no longer need
- c. Save digital information securely avoiding cloud based folders with no password or computers that can be accessed by multiple people.



<sup>1</sup> A site is secure if its address starts with "https://." It should also require you to create an account.

# Steps you can take if your child's data is breached:

Contact all three credit bureaus. Most minors will not have credit reports, so the bureaus will be able to identify abnormal activity.

|            |                                |                |
|------------|--------------------------------|----------------|
| Equifax    | alerts.equifax.com             | 1-800-525-6285 |
| Experian   | experian.com/fraud/center.html | 1-888-397-3742 |
| Transunion | transunion.com/fraud           | 1-800-680-7289 |



1. If you find unusual activity, report it as soon as possible! Report fraudulent activity to the credit bureaus (above) and to the business where the fraudulent account was opened.
2. Immediately close any new unauthorized accounts.
3. Consider placing a free, one-year fraud alert by contacting one of the three credit bureaus (that company must tell the other two; see [FTC Consumer Advice](#) for more information).
4. Report identity theft to the [Federal Trade Commission](#) (1-877-438-4338).
5. Make a report with your local police. Make sure you bring:
  - a. A copy of your FTC Identity Theft Report
  - b. A government-issued photo ID
  - c. Proof of your address
  - d. Any proof you have of the fraudulent activity
  - e. Make sure you get a copy of the police report
6. Report the fraudulent activity to any other relevant entities, such as your child's school, the Social Security Administration, your health insurance provider, etc.
7. Consider freezing your child's credit to prevent new accounts from being opened (see FTC [Consumer Advice](#) for additional information).
8. Change any compromised passwords.
9. Stay vigilant! Although there may be no immediate after-effects of a data breach, identity theft is a possibility and could have long-term financial consequences for your child.

For more information, visit:


Federal Trade Commission [https://www.bulkorder.ftc.gov/system/files/publications/pdf-0217-idt\\_data-breaches-what\\_to\\_know\\_what\\_to\\_do.pdf](https://www.bulkorder.ftc.gov/system/files/publications/pdf-0217-idt_data-breaches-what_to_know_what_to_do.pdf)



U.S. DOE Parent's Guide for Understanding Breaches [https://studentprivacy.ed.gov/sites/default/files/resource\\_document/file/Parent%20Guide%20to%20Data%20Breach.pdf](https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Parent%20Guide%20to%20Data%20Breach.pdf)

FTC Recovery Steps <https://www.identitytheft.gov/#/Steps>

ConnectSafely's Parent's Guide to Student Data Privacy <https://connectsafely.org/student-data-privacy/>

 NYS Data Privacy Office Website:  
<https://www.nysed.gov/data-privacy-security>

 Contact:  
518-474-0937

 Email:  
[privacy@nysed.gov](mailto:privacy@nysed.gov)

# Top 10 Tips to Stay Safe Online from NYSED's Chief Information Security Officer

## 1. KEEP A CLEAN MACHINE

Keep all software on internet connected devices – including personal computers, smartphones, and tablets – current to reduce risk of infection from ransomware and malware. If you want to “set it and forget it,” configure your devices to automatically update or to notify you when an update is available.

## 2. CREATE LONG, UNIQUE PASSWORDS

Length trumps complexity. Strong passwords are at least 12 characters long and include letters, numbers, and symbols. Ideally, your password is not recognizable as a word or phrase. And, yes, you should have a unique password for each online account. Sound hard to remember? Using a password manager has never been easier (we'll say more in a second) – many smartphones and web browsers include password managers and even suggest strong passwords. Otherwise, we recommend coming up with a password that is actually a “passphrase,” that is, a sentence that is at least 12 characters long. Focus on positive sentences or phrases that you like to think about and are easy to remember, such as ILoV3StayingSafeOnl1ne! (but don't use that one).

## 3. USE A PASSWORD MANAGER

It's time to ditch the notebook if that's where you keep your passwords – use it for doodles. Ditto for that Notes app or word processing doc – save the hard drive space. Instead, the simplest, most secure way to manage unique passwords is through a password manager application. A password manager is software created to manage all your online credentials like usernames and passwords. Many are free. Often, browsers and device operating systems include password management programs. Password managers store your passwords in an encrypted database (think of it as your personal data vault). These programs also generate new passwords when you need them. Really, it has never been easier to safely generate, store and access your passwords.

## 4. ENABLE MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA), sometimes called 2-factor authentication, adds a whole other level of security to your key accounts. MFA includes biometrics (think face ID scans or fingerprint access), security keys or apps that send you unique, one-time codes when you want to log on to a sensitive account. We recommend you use MFA whenever offered. Read more about the different types of MFA.

## 5. THINK BEFORE YOU CLICK

What's the most common way for cybercriminals to get your sensitive information? It's when you click on something you shouldn't have. Malicious links in email, tweets, texts, posts, social media messages and malicious online advertising (known as malvertising) are a direct way for hackers to get your sensitive information. Don't make it easy for them. Be wary of clicking on links or downloading anything that comes from a stranger or that you were not expecting. Whenever you get an email or message, count to five – usually that's all the time you need to determine if the message seems authentic or not.

## 6. REPORT PHISHING

One of the best ways to take down cybercriminals is by reporting phishing attempts, and nowadays it's easier than ever. If the email came to your work email address, report it to your IT manager or security team as quickly as possible. If you're at home and the email came to your personal email address, do not click on any links (even the unsubscribe link), or reply back to the email. Most email programs and social media platforms allow you to report phishing attempts. But don't keep that phishing message



around – delete it ASAP. You can further protect yourself by blocking the sender from your email program, social media platform or phone.

7. USE SECURE WI-FI

Public wireless networks and hotspots are unsecured, which means that anyone could potentially see what you are doing on your laptop or smartphone while you are connected to them. Limit what you do on public Wi-Fi. Especially avoid logging in to key accounts like email and financial services. Consider using a virtual private network (VPN) or a personal/mobile hotspot if you need a more secure connection.

8. BACK IT UP

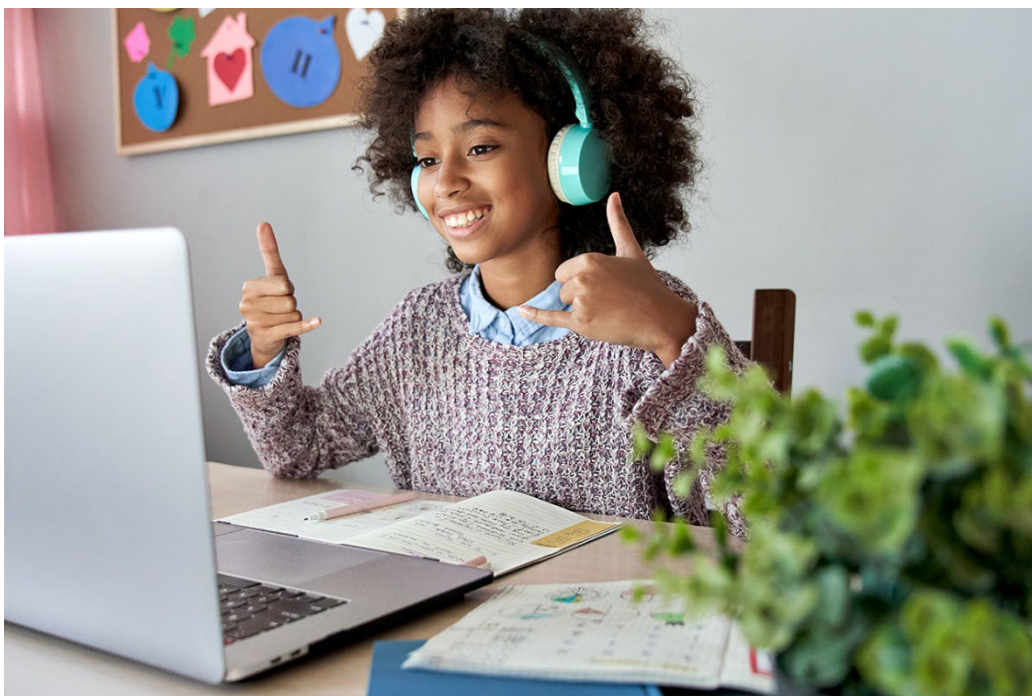
The best way to protect your valuable work, music, photos, data, and other digital information is to make copies and store them safely. If you have a copy of your data and your device falls victim to ransomware or other cyber threats, you will be able to restore the data from a backup. If you break your computer or it crashes, you won't lose the data along with the device. Use the 3-2-1 rule as a guide to backing up your data. The rule is: keep at least three (3) copies of your data, and store two (2) backup copies on different storage media, with one (1) of them located offsite. One of these storage possibilities can be backing up to the cloud, which are secure computer servers you can access through an account.

9. CHECK YOUR SETTINGS

Every time you sign up for a new account, download a new app or get a new device, immediately configure the privacy and security settings to your comfort level for information sharing. Regularly check these settings to make sure they are still configured to your comfort. Audit your apps, platforms, and games every few months and delete ones you no longer use – then you don't need to check their settings!

10. SHARE WITH CARE

Think before posting about yourself and others online. Consider what a post reveals, who might see it and how it might affect you or others.



# Resources for Families<sup>2</sup>

## Password Managers

It is best practice to use a unique password for each online account, but how are you supposed to remember them all? Use a password manager. Below data is current as of 8/7/2023.

### Password Managers Comparison

| Recommended by Wired      | Recommended by Experian | Individual Cost (annual) | Family Cost (annual) |
|---------------------------|-------------------------|--------------------------|----------------------|
| <a href="#">1Password</a> | 1Password               | \$36                     | \$60                 |
| <a href="#">Bitwarden</a> | BitWarden               | \$0                      | \$40                 |
| <a href="#">Dashlane</a>  | Dashlane                | \$42                     | \$90                 |
| <a href="#">NordPass</a>  | LastPass                | \$0                      | \$36                 |

\*[Keepass](#) Password Safe is another free, open-source option, primarily for Windows.

## Cloud Storage Options

### CNET - Cloud Storage Comparison

| Google Drive  | Google Drive2   | Microsoft One Drive   | Apple iCloud  | Dropbox   | Amazon Drive   |
|---------------|---|---|---|---|--|
| Free storage? | 15GB  | 5GB   | 5GB   | 2GB   | 5GB  |
| Paid plans    | 100GB of storage for \$2 a month (\$20 annually); 200GB of storage for \$3 a month (\$30 annually); 2TB of storage for \$10 a month (\$100 annually). | Microsoft 365 Family offers 6TB of storage and costs \$10 a month (\$100 annually); Microsoft 365 Personal offers 1TB of storage and costs \$7 a month (\$70 annually); OneDrive Standalone offers 50GB of storage for \$1 a month (\$10 annually). | iCloud Plus offers 50GB for \$1/month, 200GB (\$3/month) or 2TB (\$10/month). | Dropbox Plus offers 2TB of storage for \$10 a month; Dropbox Family offers 2TB for \$17 a month; Dropbox Professional offers 3TB of storage for \$17 a month. | 100GB of storage for \$2 a month; 1TB of storage for \$7 a month; 2TB of storage for \$12/month; plans go up to 30TB of storage. |
| Supported OS  | Android, iOS, MacOS, Linux and Windows  | PC, Mac, Android and iOS  | iOS and MacOS   | PC, Android and iOS   | Desktop, iOS and Android   |

<sup>2</sup> NYSED does not recommend any specific product or service for password management or cloud storage but is sharing this information for consideration by parents and families to help illustrate available services.

## TechRadar - Cloud Storage Comparison

| Cloud Storage Services | Free plan  | Best plan   | Storage Capacity  | Online editing and collaboration  | Offline access | Device backup | File versioning | Platforms available                        |
|------------------------|--|---|---|-----------------------------------|----------------|---------------|-----------------|--|
| Idrive                 | 10GB   | \$3.98 for one year of 10TB storage                               | Up to 50TB  | NO                                | YES            | YES           | YES             | Web, Windows, Linux, iOS, Android          |
| Internxt               | 10GB   | 2TB (sale - 90% off for personal and business plans)              | 20GB - 20TB   | YES                               | YES            | YES           | YES             | Web, Windows, Mac, Linux, Android          |
| pCloud                 | 10GB   | \$399 for 2TB for life  | 500GB - 10TB  | YES                               | YES            | YES           | YES             | Web, Windows                               |
| Sync.com               | 5 - 27GB   | Teams Unlimited (\$15/user/month), Solo Basic (\$8/user/month)    | 2TB - 6TB for individuals, potentially unlimited for businesses | YES                               | YES            | YES           | YES             | Web, Windows (64 and 32 bit), iOS, Android |
| Backblaze              | 10GB   | Free unlimited storage for a year with ExpressVPN                 | Potentially unlimited   | YES                               | YES            | YES           | YES             | Web, Windows, Mac, iOS, Android            |
| Icedrive               | 10GB   | \$15/month for 5TB, or \$999 for 10TB lifetime                    | 150GB - 10TB  | YES - LOCAL CHANGES ARE SYNCED    | NO             | YES           | YES             | Web, Windows, Mac, Linux                   |
| Nordlocker             | 3GB (personal plan, 2 week free trials for business plans) | \$19.99 for 2TB (personal), \$18.99/month for 2TB (business plus) | 500GB - 2TB, custom plans also available                        | NO                                | NO             | YES           | YES             | Web, Windows, Mac, Linux                   |
| Microsoft Onedrive     | 5GB  | Microsoft 365 personal subscription, 1TB for \$70/year            | 100GB - 6TB   | YES - WITH MICROSOFT OFFICE FILES | YES            | YES           | YES             | Windows, Mac, iOS, and Android             |
| Google Drive           | 15GB   | 100GB for individuals and teams up to 5                           | 200GB - 2TB, unlimited business plans available                 | YES                               | YES            | YES           | YES             | Web, Windows, Mac, iOS, Android            |