

**MODERNIST[®]
FINANCIAL**

CYBERSECURITY TOOLKIT

*Resources for keeping yourself
and your loved ones secure*









Cybersecurity 24-Hour Checklist

Below are practical steps anyone can implement in less than 24 hours to reduce the chances of being a victim of cybercrime or identity theft.

- ✓ **Emails, texts or phone calls telling you to take immediate action are a red flag.** Stop, take a breath and trust your gut instincts – if it doesn't make sense, it isn't true.
- ✓ **Don't click on links from unknown senders.** Instead open a separate browser and go to the site at the web address you know is legitimate.
- ✓ **Keep your devices, including your phone, updated.** Those updates are often to fix security holes, so the longer you wait to update, the longer you are vulnerable.
- ✓ **Use a password manager or system that allows you to follow best password practices and go through a monthly review.**
- ✓ **Create a "Family Password" for you and your family members that can be used to verbally confirm they are who they say they are or are claiming to be or acting on behalf of a family member.**
- ✓ **Set up two-factor authentication on financial and social media sites.** Two-factor authentication will send a code to your phone if sign-in occurs from a new device.
- ✓ **Perform a credit freeze – including for your kids.** A credit freeze is the best way to prevent someone from opening credit in your name.

Cybersecurity “Never Ever” List

-  **Never ever will the IRS email, text or call you to initiate a tax bill or refund.** The IRS will always contact you via U.S. Postal Service mail. If you are contacted by an alternate method, look up the number for your local IRS office and report it.
-  **Never ever will someone know your computer has a virus.** Someone calling and telling you that and offering to fix it is attempting to gain unauthorized access. Popups on your PC with a number to call are also fake. If you think your computer has an issue, physically take it to a business you know to be legitimate.
-  **Never ever write down or re-use the same passwords.** Passwords should never be written down – they can easily be lost or stolen. Using the same password multiple times increases the risk of a data breach involving one password leading to other accounts being breached. Consider using a password manager.
-  **Never ever take online quizzes about yourself.** These quizzes are mostly designed to gather data about you that could be used to correctly guess your answers to security questions. Never ever share vacation plans on social media. Doing so alerts others to when you may not be home for an extended time. Also, avoid posting photos of your trip while still on vacation and instead wait until you get back home.
-  **Never ever skip past two-factor authentication when setting up your account for a web site or app.** Two-factor authentication is a great way to add an extra level of security and protects you if your password for that account is ever stolen.
-  **Never ever respond to pressure or threats from an email, phone call or text.** These are almost always a method of social engineering designed to get you to give someone money or sensitive data. Instead, call the company that the person is claiming to be from at a phone number you know to be legitimate to let them how you were contacted and to confirm it was fraudulent.

Requesting a Credit Freeze for a Child

The process for freezing credit for kids is more involved and requires more steps than doing a credit freeze as an adult; however, it is the best method to protect children from having credit opened in their name if someone acquires their Social Security number.

No credit file should exist for a child – when fraudsters steal a child’s identity and use it to apply for credit, they in effect open that credit file for the first time. Credit bureaus don’t knowingly create files for minors. The issue is today it is impossible for the credit bureaus to verify the identity and age of the person opening it – they can only verify that the Social Security number being used is a valid number.

Therefore, when applying to have your child’s credit frozen, each credit bureau will create a credit file in their name and then immediately freeze it.

A child’s credit should be frozen with all three major credit bureaus – Equifax, Experian and TransUnion. Each has variance on the process and what is required, so we tried to simplify in the instructions below.

How to Freeze a Child’s Credit

To simplify the process, we recommend sending the same set of documents to all three credit bureaus – any documents a bureau does not need, they will simply disregard. Make three copies of the following documents and create three stacks – you will send one of each to the three major credit bureaus.

- A government-issued ID for yourself (a driver’s license is the easiest)
- Your birth certificate
- The birth certificate of the child whose credit you are freezing
- Your Social Security card
- The Social Security card of the child whose credit you are freezing
- A bank statement, insurance statement or utility bill with your name on it

Download and print the following forms:

[Equifax](#)

[Experian](#)

[TransUnion](#)

Mail each form and the supporting documents you have printed out to the following addresses:

TransUnion
P.O. Box 380
Woodlyn, PA 19094

Experian
P.O. Box 9554
Allen, TX 75013

Equifax Information Services LLC
P.O. Box 105788
Atlanta, GA 30348

Because you are sending sensitive information via postal mail, you may want to send each of these packets via certified mail. At a minimum, mail them by dropping them off at your local post office.

- Once each credit bureau processes the credit freeze, you will receive confirmation by postal mail that will include a PIN number that can be used (if need be) to unfreeze a child's credit. Store this PIN in a secure place, such as a fireproof safe or safety deposit box. If you use a password manager app, that is a good place to store it electronically.
- The credit freezes that have been applied will stay in place, which should give you peace of mind that nobody can open credit in their name.

The freeze will remain in place until you or your child unfreezes it later when they are older and need to apply for a credit, a student loan, etc.