SECURITY GUIDE

The McAfee Safety Series

Back to School Protection Guide

Table of Contents

Is it back-to-school time already?

It has a way of sneaking up on you.

Before you know it, summer break has blown right by, and there you are in the checkout line with a cartload of notebooks, paper, and pens. Yet, busy as this time can be, it can conjure up some good feelings. After all, you're preparing your children for a strong start, and maybe it stirs some fond back-to-school memories of your own.

Yet that's the thing. Back-to-school time looks different for many parents today. Now, they need to take one more step to get everyone ready for the new school year—making sure the family's devices are safe, secure, and ready to go.

Increasingly, devices have woven their way our children's learning, whether that takes the form of a school-issued device, one of their own, one shared by the family, or even a mix of all three. Consequently, your child may find themselves spending a fair amount of time online for school and homework, in addition to the six to nine hours they may already spend online where they play games, watch shows, and connect with friends.

All that calls for some extra protection.

In this guide, we'll look at ways you can protect your family's smartphones, computers, and laptops in advance of the new school year. We'll also cover with something far more important—ways you can protect your children from harm online.

We'll break it down into three sections:

- Protecting Their Smartphones
- Protecting Their Computers and Laptops
- Protecting Them Online

Yes, this will call for a little more work on your part during an already busy time of year. Yet given the sheer volume of time that our children spend online, taking these steps is just as important as stocking them up with notebooks, pens, and paper—if not more important.

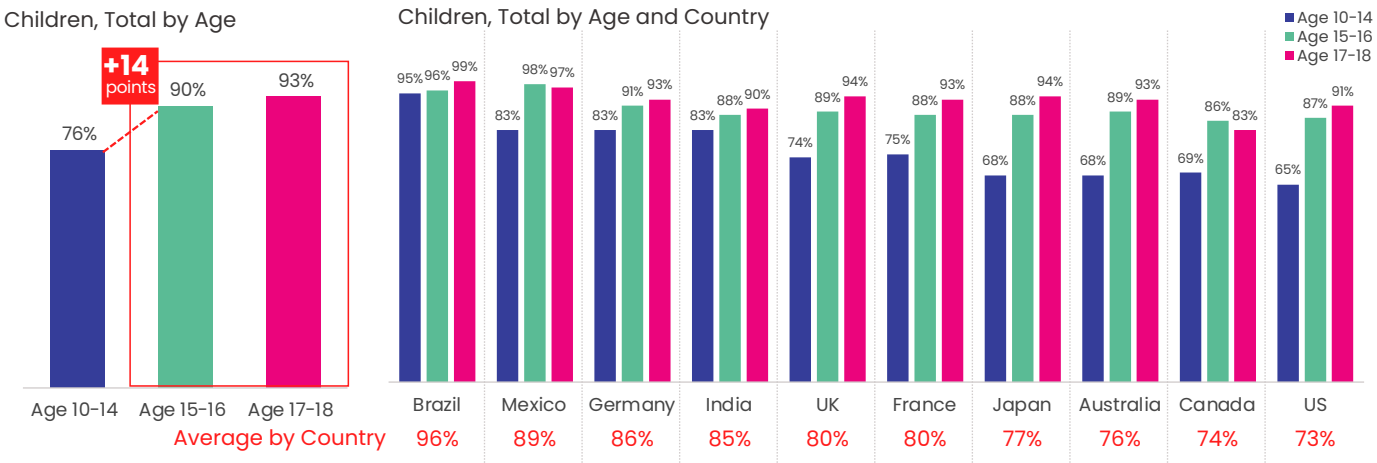
Parents need to take one more step to get everyone ready for the new school year—making sure the family's devices are safe, secure, and ready to go.

Protecting their smartphones

If you're the parent of a tween or teen, chances are they're not the only ones going back to school. Their smartphones are going back too.

Our recent global research showed just how many tweens and teens use a smartphone. Plenty. Depending on the age band, that figure ranges anywhere from 76% to 93%, with some noteworthy variations between countries.

Mobile/Smartphone Device Usage



C1. Which of the following devices do you use? (Base: Children, n=12,057)

One of the top reasons parents give their child a phone is to stay in touch, so it likely follows that those phones will likely make their way into the classroom. Whether or not that's the case for your child, back-to-school time is still a great time to help your child stay safer on their phone—and keep their phones safer too in the event of loss or theft.

Seven steps for keeping your child's phone safer

1. Install protection on their phone.

Comprehensive online protection software can protect your phone in the same ways that it protects your laptops and computers. Unfortunately, while many people use it on their laptops and computers, far fewer people use it on their phones—only about 42% of tweens and teens worldwide use it on their smartphones, again, according to our research.

Installing it can protect your child's privacy, keep them safe from attacks on public Wi-Fi, and automatically block unsafe websites and links, just to name a few things it can do. You can find our smartphone apps in both Google Play and the Apple App Store.

2. Set their apps to automatically update.

Updates do all kinds of great things for gaming, streaming, and chatting apps, like adding more features and functionality over time. Updates do something else—they make those apps more secure. Hackers will hammer away at apps to find or create vulnerabilities, which can steal personal info or compromise the device itself. Updates will often include security improvements, in addition to performance improvements.

iPhones update apps automatically by default, yet you can learn how to turn them back on here if they've been set to manual updates. For Android phones, this article can help you set apps to auto-update if they aren't set that way already.

Much the same goes for the operating system on smartphones too. Updates can bring more features and more security. iOS users can learn how to update their phones automatically in this article. Likewise, Android users can refer to this article about automatic updates for their phones.

3. Use a lock screen with a passcode, PIN, facial recognition, or pattern key.

Another finding from our latest global research is just how few people use a lock screen on their phone. Only 56% of parents said that they protect their smartphone with a password or passcode, only 42% said they do the same for their child's smartphone—a further 14% drop between parents and kids.

The issue here is clear. If an unlocked phone gets lost or stolen, all the information on it is an open book to a potential hacker, scammer, or thief. Enabling a lock screen if you haven't already. It's a simple feature found in both iOS and Android devices.

4. Learn how to remotely lock or wipe a smartphone.

Preventing the actual theft of your phone is important too, as some hacks happen simply because a phone falls into the wrong hands. This is a good case for password or PIN protecting your phone, as well as turning on device tracking so that you can locate your phone or even wipe it remotely if you need to. Apple provides iOS users with a step-by-step guide for remotely wiping devices, and Google offers up a guide for Android users as well.

5. Use a password manager.

Strong, unique passwords offer another primary line of defense. Yet with all the accounts we have floating around, juggling dozens of strong and unique passwords can feel like a task—thus the temptation to use (and re-use) simpler passwords. Hackers love this because one password can be the key to several accounts. Instead, try a password manager that can create those passwords for you and safely store them as well. Comprehensive security software will include one, and we also offer a free service with True Key.

6. Have your kids steer clear of third-party app stores.

Google Play and Apple's App Store have measures in place to review and vet apps to help ensure that they are safe and secure. Third-party sites may not have that process in place. In fact, some third-party sites may intentionally host malicious apps as part of a broader scam. Granted, cybercriminals have found ways to work around Google and Apple's review process, yet the chances of downloading a safe app from them are far greater than anywhere else. Furthermore, both Google and Apple are quick to remove malicious apps once discovered, making their stores that much safer.

7. Take advantage of platform tools on their phones.

Device manufacturers have responded to the concerns of parents and families with tools for basic safety and wellbeing. Apple has a thorough site dedicated to its family sharing and monitoring features. Likewise, Android has a similarly thorough site that outlines its features for families. Some time spent on those sites will outline several ways you can set limits, keep tabs on activity, and do more as a family, such as sharing photos and subscriptions to streaming and news services.

A word about their social media apps

Our recent research confirms what you likely have seen with your own eyes. The top social media apps children use include the familiar names of Instagram, Facebook, and TikTok.

Just like the device manufacturers, they have put together resources and features designed for parents and their children to help keep them safer and happier on their social media platforms.

- Instagram has a site that outlines how teens can safely enjoy the app, along with ways you can set time limits, see who your teen follows and who follows them, and be notified when your teen shares that they've reported something.
- As part of their overall Safety Center, Facebook provides parents with a site dedicated to child safety, with tools, resources, and guidance designed for families.
- TikTok has its own Safety Center as well, which covers safety and privacy controls, a wellbeing guide, and further guidance for parents and guardians.

Given all the hours our children spend on these social media apps—along with the concerns parents have about screen time, cyberbullying, and exposure to inappropriate content—carving out some time to take advantage of the family-oriented features offered by these platforms makes good sense. Once in place, they may help you have more control and more peace of mind when your children are using these apps.

Protecting their computers and laptops

Plenty of the same advice for safer smartphone usage applies to desktops and laptops as well—strong online protection software, password management, lock screens, and so on. What's good for a smartphone is good for them too. You can take those same steps on your computers and laptops.

Note that on school-issued laptops, your school district will likely have technology teams who manage them. As part of that, they typically have established apps, policies, and restrictions in place to help keep them running safe and sound. If you have any questions about what kind of protections are in place on these school-issued devices, contact your school district.

In the case of your computers and laptops, there are several extra protections you can put in place to make those devices, along with the people who're using them, much safer than before.

Extra steps for computers and laptops

Track your laptops

Just like a smartphone, you can track these devices as well. The process differs from smartphones, yet it's still quite straightforward. Windows and Mac users can enable the following settings—and you can click the links below for complete instructions from the source:

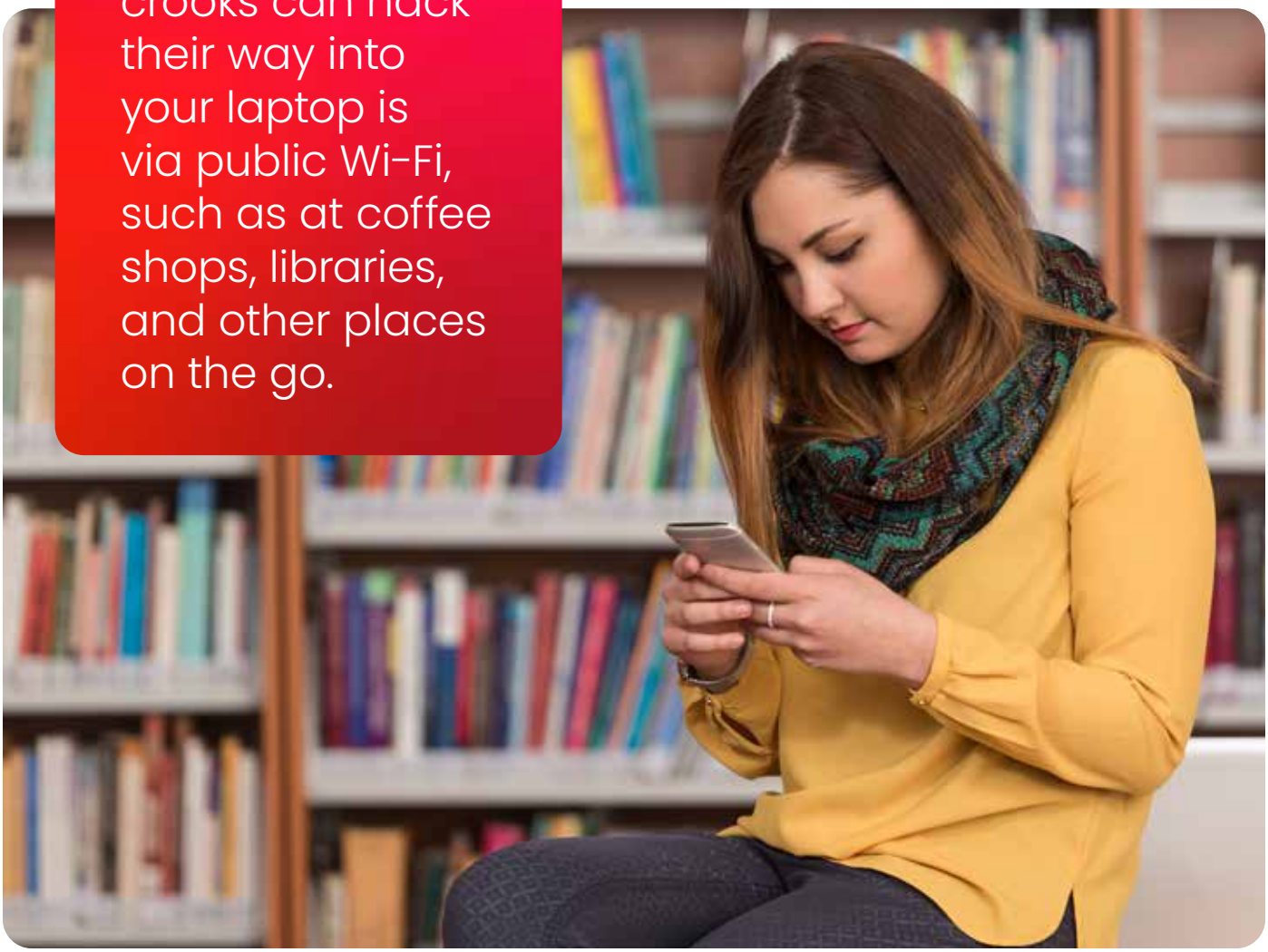
- Windows: Enable in Settings > Update & Security > Find my device
- macOS: Enable via Settings > Your Name > iCloud > Find My Mac

Teach your kids how to use a VPN on public Wi-Fi

One way that crooks can hack their way into your laptop is via public Wi-Fi, such as at coffee shops, libraries, and other places on the go. These networks are public, meaning that your activities are exposed to others on the network—your banking, your password usage, all of it. One way to make a public network private is with a VPN, which can keep you and all you do protected from others on that Wi-Fi hotspot. Note that our VPN can turn on automatically for public Wi-Fi, protecting account credentials, search habits, and other activities online.

At home, whether that's on a laptop or a desktop computer, a VPN offers additional benefits. It can help protect your privacy by making your browsing more anonymous, keeping it safer from advertisers who'd track your activity online, in addition to protecting you from hackers and attackers.

One way that crooks can hack their way into your laptop is via public Wi-Fi, such as at coffee shops, libraries, and other places on the go.



Can my Mac get a virus?

It's a long-standing question. Can Macs get viruses?

While Apple goes to great lengths to keep all its devices safe, this doesn't mean your Mac is immune to computer viruses. Any connected device is subject to attack from viruses, in addition to other attacks such as phishing attempts, invasions of privacy, and attempts at identity theft.

So do Macs need extra protection? To answer that question, it helps to know what kind of built-in protections Apple offers. Macs contain several built-in features that help protect them from viruses:

- **XProtect and Automatic Quarantine:** XProtect is Apple's proprietary antivirus software that's been included on all Macs since 2009. Functionally, it works the same as any other antivirus, where it scans files and apps for malware by referencing a database of known threats that Apple maintains and updates regularly. From there, suspicious files are quarantined by limiting their access to the Mac's operating system and other key functions. However, XProtect relies upon up-to-date information to spot malicious files. In some instances, this information can lag behind the current threat landscape—meaning that XProtect may not always protect Mac users from the latest threats.
- **Malware Removal Tool:** To further keep Apple users protected, the Malware Removal Tool (MRT) scans Macs to spot and catch any malware that may have slipped past XProtect. Similar to XProtect, it relies on a set of constantly updated definitions that help identify potential malware. According to Apple, MRT removes malware upon receiving updated information, and it continues to check for infections on restart and login.

- **Notarization, Gatekeeper, and the App Review Process:** Another way Apple keeps its users safe across MacOS and iOS devices is its *Notarization* Apps built to run on Apple devices go through an initial review before they can be distributed and sold outside of Apple's App Store. When this review turns up no instances of malware, Apple issues a Notarization ticket. That ticket is recognized in another part of the MacOS, Gatekeeper, which verifies the ticket and allows the app to launch. Additionally, if a previously approved app is later found to be malicious, Apple can revoke its Notarization and prevent it from running.

  Similarly, all apps that wish to be sold on the Apple App Store must go through Apple's App Review. While not strictly a review for malware, security matters are considered in the process. Per Apple, "We review all apps and app updates submitted to the App Store in an effort to determine whether they are reliable, perform as expected, respect user privacy, and are free of objectionable content."

- **Further features:** In addition to the above, Apple includes technologies that prevent malware from doing more harm, such as preventing damage to critical system files.

Does my Mac need extra online protection?

There are a couple reasons why Mac users may want to consider additional protection in addition to the antivirus protection that Mac provides out of the box:

- **Apple's antivirus may not recognize the latest threats.** A component of strong antivirus protection is a current and comprehensive database of virus definitions. As noted above, Apple's virus definitions can lag behind the latest threats, leaving Mac owners who solely rely on XProtect and other features susceptible to attack.
- **Apple's built-in security measures for Macs largely focus on viruses and malware alone.** While protecting yourself from viruses and malware is of utmost importance (and always will be), the reality is that antivirus is not enough. Enjoying life online today means knowing your privacy and identity are protected as well.

In all, Macs are like any other connected device. They're susceptible to threats and vulnerabilities as well.

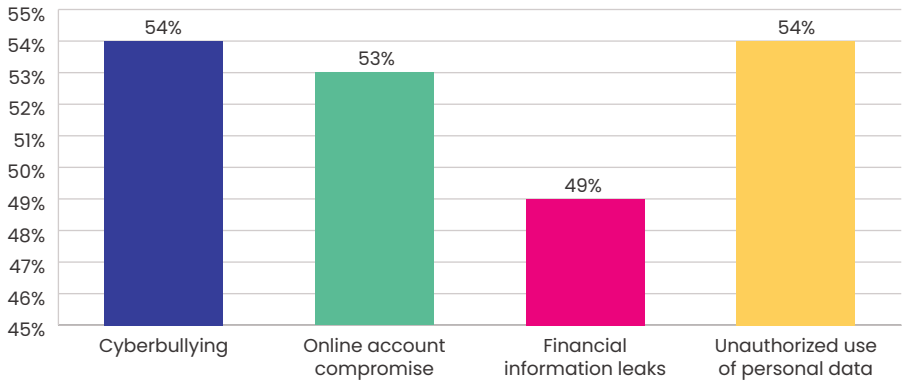
In all, Macs are like any other connected device. They're susceptible to threats and vulnerabilities as well. Looking more broadly, there's the wider world of threats on the internet, such as phishing attacks, malicious links and downloads, prying eyes on public Wi-Fi, data breaches, identity theft, and so on. It's for this reason Mac users may think about bolstering their defenses further with online protection software.

Protecting them online

While we've largely focused on protecting devices, there's also the importance of protecting the person using them. In this case, your child—what they see, do, and experience on the internet. Device security is only part of the equation when it comes to protections like these.

Protecting your child online opens a range of topics, several of which are very much on the mind of parents. In our recent global research, nearly half if not more than half of parents worldwide were either "concerned" or "very concerned" about the following for their children:

Topics of concern for parents, worldwide



Nearly half if not more than half of parents worldwide were either "concerned" or "very concerned" about these topics.

While cyberbullying is a point of concern that understandably garners plenty of attention, it's noteworthy that concerns about cyberbullying rank right alongside identity theft and invasions of privacy. Perhaps that's unsurprising, given that parents worldwide experienced identity theft or misuse of personal data themselves at a rate of 25% to 33%. It only makes sense that they'd worry that their children could become victims too.

What makes a child's identity so compelling to scammers and thieves? Being young, they often have a clean sheet of credit—one waiting to be written. Or, in this case, written without their knowledge. It's arguably uncommon for families to run credit checks on their children. This way, if a child's identity has been stolen it may not get uncovered years later until that child is an adult and has their credit report pulled for to rent an apartment or purchase a car. An ugly surprise for sure!

Moreover, children already have things of value such as their online game accounts and cash apps, not to mention teens who may have their first debit cards. Put plainly, each of these have a dollar value attached to them, thus making them a target.

It's for this reason that protecting your child's identity today can help avert big headaches both now and in the long term.

While we've largely focused on protecting devices, there's also the importance of protecting the person using them.

Protecting their identity

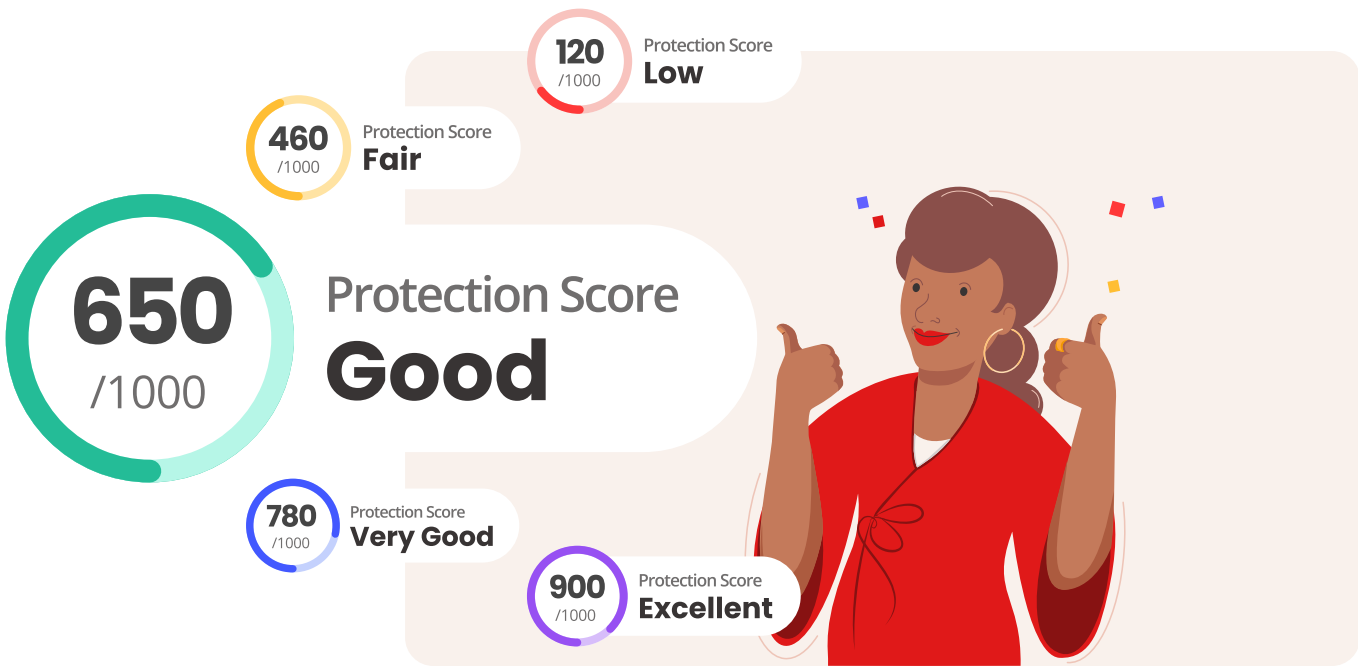
The good news is that you have several tools that can help protect your child's identity online, and yours as well. Where this was once a highly manual and time-consuming proposition, it's now far more automatic and streamlined thanks to what comprehensive online protection software offers today.

With it, you can:

Get their protection score

One of the trickiest parts of staying safe online is knowing exactly how safe you are. *Do I have the right protection in place? Is there more I could be doing?* Those are good questions to ask, and now you can get the answers to them with your Protection Score. As part of your McAfee subscription, the Protection Score gives you a clear and easy-to-read overview of your online protection and how healthy it is. Next, it identifies and helps you fix security weak spots with simple instructions and then offers personalized feedback that helps you maintain healthy online protection.

For example, one way a Protection Score can help keep your child's identity secure is in the case of data breach. If your information is found in a data breach, the Protection Score goes down and the app sends an alert. It then assists you in resolving the breach, the Protection Score goes back up, and monitoring continues, maintaining a lookout for future breaches and issues.



Clean up their personal info

Personal information shares something in common with the pieces of a jigsaw puzzle. With enough pieces in place, a thief can attempt to steal your identity. However, they don't always need to go to a dark marketplace online to get useful pieces. Another place they can get it is from websites that gather personal information from public records, social media, and other online sources. Known as data broker sites, they build profiles of individuals that identity thieves, hackers, and spammers can use to wage their attacks.

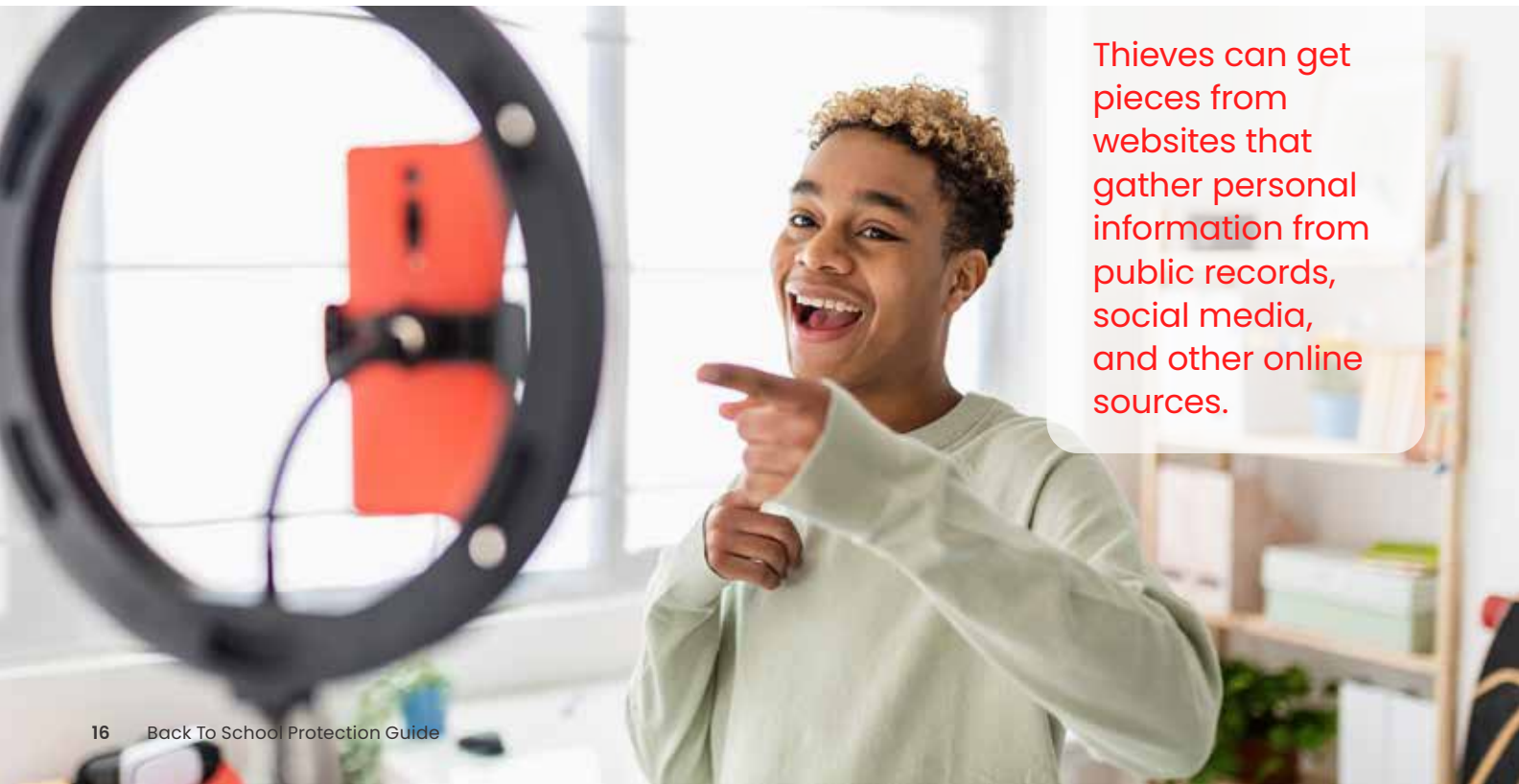
While getting personal info removed from these sites this can seem like a daunting task (where to start, and just how many of these sites are out there), we're rolling out our **Personal Data Cleanup**[1] to help. It regularly scans these high-risk data broker sites for info like your home address, date of birth, and names of relatives. It identifies which sites are selling your data, and depending on your plan, removes it for you.

Monitor their credit

A credit monitoring service keeps daily tabs on their credit report. While you can do this manually, there are limitations. First, it involves logging into each bureau and doing some digging of your own. Second, there are limitations as to how many free credit reports you can pull each year. A service does that for you and without impacting your credit score.

Depending on your location and plan, McAfee's credit monitoring looks after their credit score and accounts to see fluctuations and identify unusual activity, all in one place, checking daily for signs of identity theft.

1. Personal Data Cleanup is not available in all plans or locations.



Monitor their identity

When we mentioned Personal Data Cleanup earlier, we brought up the dark web where PII is bought and sold, stored, and exchanged. The problem is that it's particularly difficult for you to determine what, if any, of your PII is on the dark web where hackers and thieves can get their hands on it. Identity monitoring can help.

McAfee's identity monitoring helps you keep your child's personal info safe by alerting you if their data is found on the dark web, an average of 10 months before our competitors. Monitored info can range anywhere from bank account and credit card numbers to email addresses and government ID number, depending on your location. If their information gets spotted, you'll get an alert, along with steps you can take to minimize or even prevent the damage if the information hasn't already been put to illegal use.

Take advantage of identity protection

Identity protection through McAfee takes identity monitoring a step further by offering financial coverage for losses and expenses due to identity theft, in addition to hands-on help from a recovery professional to help restore you or your child's identity—all in addition to the identity monitoring called out above, again depending on your location and plan.

Protecting them from harm

Back to the important topic of cyberbullying.

First off, a definition helps. According to StopBullying.gov, cyberbullying is:

... bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behavior.

Our global research found that 17% of children aged 10 to 18 said that they'd been cyberbullied at some time, alongside 17% of their parents—more than 1/3 of people worldwide. These numbers trended highest in the U.S., with 28% of children and 26% of parents saying they'd experienced it at some point—a stark contrast to nations like Japan where those numbers were 6% and 7% respectively.

This speaks to a higher rate of cyberbullying compared to the findings from the Pew Research Center, which indicated that 4 in 10 of Americans (of all ages surveyed) say they have been subjected to some form of harassment online over the course of 2020. In the Pew findings, all forms of cyberbullying saw a rise, including less severe forms like name-calling and purposeful embarrassment, along with more severe forms like physical threats, stalking, and sexual harassment.

With figures such as these, there's a good chance you or someone you know will get harassed online if it hasn't happened already.

Most importantly, **if you ever feel you or your child are in imminent danger from any kind of harassment online, contact your local emergency number**. If you believe that a threat made online can turn into a threat against you, your family, or your property, follow through just as you would if that threat were made any other way. If it's happening to someone else you know, warn them, and advise them to do the same if they feel they're in danger.

Of course, not all harassment goes that far. Yet that doesn't mean it still isn't dangerous or harmful. Also, according to StopBullying.gov, it can lead to depression, anxiety, and other health complaints—along with decreased achievement at school or work.

Cyberbullying separates itself from throwaway and offhanded remarks that we may occasionally come across online, which can certainly sting, yet don't form a pattern. In fact, a telltale sign of serious cyberbullying is that it persists over time and the victim feels consistently targeted. Another sign is that the harassment is permanent, meaning that it's posted online for others to see, time and time again.

According to WebMD, further signs of cyberbullying include if your child:

- Becomes noticeably upset after being online or on their phone.
- Doesn't engage with family or friends.
- Doesn't want to participate in activities they normally enjoy.
- Their school grades have unexpectedly declined.
- They don't want to go to school or the playground.
- Increasingly saying they're too sick to do anything else.
- Shows signs of depression or sadness.

In all, trust your intuition. If that post, text, or message looks like cyberbullying, it probably is cyberbullying. Particularly if your child shows any signs of its effects.

Six Steps you can take if your child is being harassed online

Whatever form it takes, the best way to deal with cyberbullying is to deal with it immediately.

1. Don't respond to it. While you might want to strike back with a message or post of your own, don't. This may only escalate the situation or, worse yet, make you look like the instigator. In all, responding will only do more harm than good.

2. Document everything. Grab screenshots of the messages, posts, texts, photos, or whatever was involved in the harassment. Include the screenname of the person behind it, along with a time and date. This will help you document a timeline of the harassment.

3. Report it. Depending on the context and situation, you have options here. For example, this may be a matter that you want to report to your child's school. Likewise, harassment will nearly always violate the terms of service on websites, services, and apps. You may be able to flag a negative post to get it removed and other sites, services, and apps may have other avenues to report harassment. Use them. And get that content taken down if it is posted publicly.

4. Determine if it breaks the law where you live. Of course, laws will vary based on your nation, state, or province, yet anti-harassment laws are on the books—not to mention defamation, slander, and libel laws. A search for governmental resources on cyberbullying and online harassment can offer a good start, and you can consult with licensed counsel in your area if you think that the harassment you've encountered may have crossed a legal line.

5. Monitor. As said, harassment is often persistent. Keep an eye out for more of it and follow the same steps here as needed.

6. Contact your local emergency number if you're in immediate danger. Simply repeating what we said above. If you fear for the wellbeing of your family or home, make the call.

Harassment and threats in their more extreme expressions can leave emotional scars. Victims may need support in the wake of them, possibly from a professional. You and your judgment will know what's best here, yet given the harm it can cause, keep an eye for signs of lasting effects such as the ones mentioned above.

Where can you start if you're worried about effects like these? In the U.S., the Department of Health & Human Services has a list of resources available for victims and their families. Likewise, the Canadian government website hosts a list of similar mental health resources, and in the UK the NHS hosts a list of resources as well.

Protecting our children, protecting their devices

The two go hand-in-hand today.

Our philosophy for staying safe online focuses on protecting the person, which by extension means protecting their devices. In this guide, we've looked at several ways you can do both for your children.

Another powerful tool you have at your disposal is conversation. As your child dives into their world of apps, social media, messaging, gaming, and schoolwork too, take an interest. Look for opportunities to ask about their day and what it was like online.

By asking if they grabbed any cool pictures, what their favorite games are, and how their friends are when your child is texting them, questions like these can open a look into a world that would otherwise remain closed. This way, talking about their life online becomes part of normal, everyday conversation.

Further, find out what apps they're using and give them a try yourself. See how they work and what they're all about. Become friends with them on their social media accounts. Actions like these can get the conversation rolling too.

Conversations today can reap benefits down the road when your child encounters the inevitable bumps along the way, whether they're dealing with a technical issue or something as difficult as cyberbullying or harassment. Talking about their life online on a regular basis may make them more apt to come forward when there's a problem than they otherwise might.

For more about staying safe and getting the most out of life online, our blog offers you and your family a terrific resource across a wide range of topics from online banking, gaming, and shopping to tough yet important topics like cyberbullying and which apps are safe for kids.

Our aim is to help you think about what's best for your family and the steps you can take to see it through so that you can make everyone's time online safer and more enjoyable.

Visit us any time!

https://www.mcafee.com/blogs

About McAfee

McAfee is a worldwide leader in online protection. We're focused on protecting people, not devices. Our solutions adapt to our customers' needs and empower them to confidently experience life online through integrated, easy-to-use solutions.

www.mcafee.com

For more information about online protection, visit us at mcafee.com/blogs

McAfee™

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com