AURA

Military Kids Online Safety

A Guide to Digital Protection for Military Kids and Families

December 2022

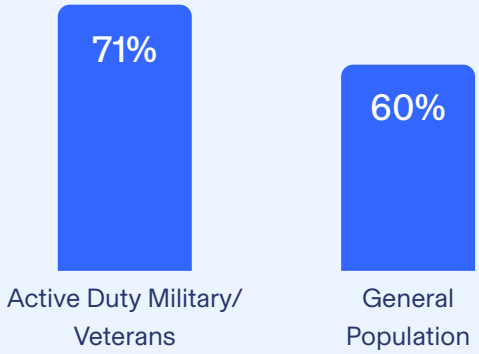
Americans lost nearly $7 billion dollars to cybercrime in 2021, indicating that scammers and criminals continue to become more sophisticated in the tactics they use to commit fraud[1].

With their clean and often unmonitored credit histories, many cybercriminals consider children to be an easy target. And unfortunately, the data supports that belief, given child identity fraud cost families $688 million last year.[2]

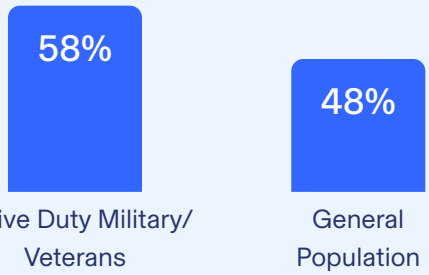
Veterans, active-duty service members and their families are already at higher-than-average risk of identity theft, fraud and other digital crimes[3], making it especially critical that you discuss online safety with your children early and often.

In this guide, consumer cybersecurity company Aura offers suggestions for military families as they navigate children's use of technology, the internet and social media. To help you navigate digital safety, technology empowerment and healthy boundaries for children of all ages, visit The Digital Talk, Aura's education hub for American civilian and military families alike. For more suggestions on digital parenting, check out guidance from the Family Online Safety Institute.

7 out of 10 active-duty service members and veterans have experienced some form of digital crime — more than the general population.[4]



Active-duty service members and veterans are more likely to have been victims of data breaches than the general population.[4]

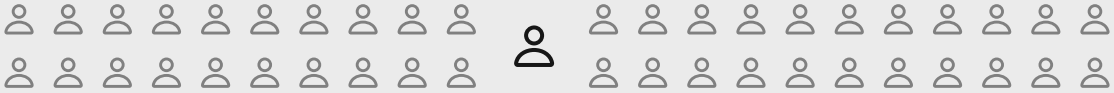


Online Safety Tips for Military Families

Protect your child's information

We understand that as proud parents, you're eager to share photos or videos of your children. It's a great way to stay connected and keep your loved ones updated on what's happening in your lives. But be thoughtful of how you do so. Cybercriminals scour social media for information they'll collect to commit fraud; and, often, your child's name and birthday is enough information for them to be successful. Even if your profiles are set to private, your online friends could still share or sell this information.

Fact

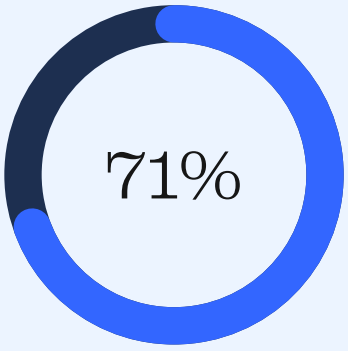


One in 43 minors had personal information exposed in a breach, affecting 1.74 million kids.[5]

As military families, it's highly possible that your information was already compromised in a past government data breach. And your children may have been affected, as well. In fact, last year, one in 43 minors had personal information exposed in a breach, affecting 1.74 million children[5]. Cybercriminals can purchase that data on the dark web for as little as $2 and pair that with information found on social media to commit identity theft, fraud or another type of digital attack.

Finally, a staggering 71% of parents don't see the importance of monitoring a child's presence on social media. But this can be a great way to prevent identity theft and fraud before it happens, or at least to detect it sooner.

71% of parents don't see the importance of monitoring a child's presence on social media.[5]



Build trust with your children

It's never too late to begin fostering an open dialogue with your children about digital safety. Military kids are likely to attend multiple schools over the course of their childhood, which can translate to spending more time online — whether they're connecting with friends or family they miss, or are building new, online friendships as they navigate creating new, in-person ones.

Whether you've recently relocated, just bought your child a new device or your kids have been online for years, it's never too late to create an open, honest and safe space to have judgment-free conversations that build trust. Address the power of technology to create independence, in uncovering new passions and in building new relationships. Follow them on social media, praise safe online behaviors, compliment their latest post or another aspect of their social presence. Regularly ask them about how social media makes them feel and if it empowers them rather than hurts them. Most importantly, remind them that you're on their team, that they can trust you and that you're there to support them — no matter what the situation might be.

Inform them of the risks they face online

Let your children know that as a military family, you're already at higher risk of digital attacks. Discuss that criminals are trying to get as much information about your family as possible, so they can steal what you worked very hard to create. Explain that information as innocent as your birthday, school or address is private and should never be shared on social media, in gaming forums, in online chats or other forums. Discuss what to do if someone online tells your child they know his or her parents or claims to be famous. Address that even if your settings are set to private, hackers can often find a way to breach that line of defense. Explain what's at stake and that they have a part in keeping your family safe.

Set house rules

Boundaries are good. Setting them as a family? Even better. As part of the conversation you have with your children about safe online behavior, discuss what these rules should be. Listen to your child's needs, consider your own perspective and as much as possible, meet in the middle. This will show your child that you trust them, and in return, they can trust you. They may even be more inclined to willfully follow the rules, given they had a say in creating them.

This can be an especially effective strategy for military families, given the amount of time you'd need to effectively manage all aspects of your child's online presence when your spouse is deployed and you're running the household on your own.

Agree on screen time limits, privacy settings, who they're allowed to talk to (friends, family and classmates, but not strangers), what's off limits and what happens when rules are broken (e.g. remove tech privileges). Make sure your child feels heard, understands why you're setting these boundaries and is on board with them. Agree with them on what's private information and what's not. Consider using this checklist:

Not Allowed

- ⊘ Your full name (use a screen name instead)
- ⊘ Mom or Dad's full name, birthday or SSN
- ⊘ Mom and Dad's email addresses
- ⊘ Your school's name or location
- ⊘ Your home address
- ⊘ Your phone number
- ⊘ Your birthday
- ⊘ If you're home alone
- ⊘ Where you were born
- ⊘ Your passwords
- ⊘ If mom or dad are deployed
- ⊘ Where mom or dad is deployed
- ⊘ Inappropriate photos
- ⊘ Photos of your house or school
- ⊘ Photos of you in a school/sports team uniform
- ⊘ Your location — current or future
- ⊘ Valuable things you or your family own
- ⊘ Photos of mom and dad's car or license plate
- ⊘ Mom's, dad's or your medical history

Allowed

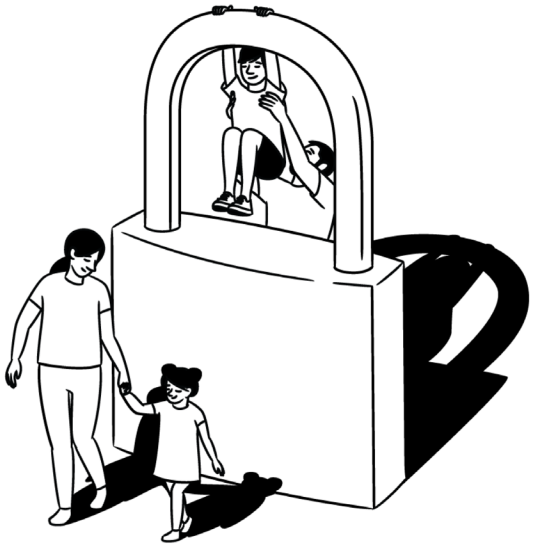
- ✓ Your hobbies
- ✓ Your favorite bands, movies, sports or TV shows
- ✓ Your favorite games
- ✓ Pictures of your pets or places you've visited
- ✓ Your favorite foods or recipes
- ✓ Family photos, with Mom or Dad's permission
- ✓ Your favorite toy or product
- ✓ Experiences or advice

Encourage them to be part of your family's strong defense

Explain that they have a very important role to play in creating a strong defense against a different kind of enemy — one that is invisible, anonymous and capable of a kind of harm that's difficult to trace and almost impossible to prosecute.

Update privacy and location settings

In a recent survey of military families and cybercrime, Aura found that Veterans and active-duty service members who have public social media accounts and share their location data with third-parties are significantly more likely to have experienced digital crime than those who don't. Consider setting a rule that social media profiles be set to private and that location data cannot be shared with third-party apps unless absolutely necessary, like when using a map or navigation service.



Don't shy away from the scary stuff

Depending on your child's age and what platforms they're using, consider explaining what a predator is. Explain that social media profiles, usernames and more can be faked — that a digital friend who says he or she is a kid in a nearby town or in the same grade, could be someone else entirely. Address that they should never meet anyone they've met online, in-person, without discussing with you first.

Explain what cyberbullying is, encourage them to use technology in a positive and safe way and to be kind, polite and respectful of others online. Emphasize the benefits of technology and how it enables learning and education, communication and connection, exposes them to new ideas and perspectives that foster creativity. Encourage them to celebrate others' sharing ideas or perspectives that are new to them, and that if they disagree with someone or get a bad feeling about a conversation, to come talk to you about it. Explain that talking digitally can lead to misunderstandings and misinterpretations, and that they can come to you should they ever be confused or uncomfortable. Finally, encourage them to understand that they should expect the same courtesy from others online, and that if they feel — even the slightest bit — that they're being mistreated, that you can help them decide how to address the situation.

Get Help

Managing your child's online safety can be overwhelming and time-consuming. But you don't have to do it alone. Tools like Aura can help you strike the right balance between independence and safety by keeping you in the loop without giving your child the impression that you're invading their privacy. Aura helps parents block malicious sites, filter out inappropriate content, monitors screen time and flags signs of identity theft. Kidas, another innovator in kids online safety, integrates into popular games and Discord, using machine learning-powered software to send parents weekly reports on their child's activity, as well as alerts in case of a potentially unsafe situation.

As always, no technology can replace important conversations with your children about practicing online safety. For more information about creating an open, honest dialogue with your children about their digital experiences, check out Aura's The Digital Talk and FOSI's Good Digital Parenting ToolKit.

Visit aura.com/military for up to 50% off all protection plans for active-duty service members, Veterans and their families, and for more resources designed for military families.

Citations

[1] FBI: Nearly $7 Billion Lost to Cybercrime in 2021 | AARP

[2] Child Identity Fraud | Javelin 2022

[3] Aura for the Veterans, Active-Duty Service Members and their Families

[4] Aura/Ipsos: The Impact of Digital Crime on U.S. Military and Veterans (November 2022)

[5] Child Identity Fraud | Javelin 2022

No one can prevent all identity theft or monitor all transactions effectively.