Military families online safety guide

Blue Star Families, USAA and Facebook connect you with information military families need to stay safe online.

Social media has dramatically changed how servicemen and servicewomen stay in touch with their families and friends. Today, we use social media to share, connect and be a part of events in real time – from daily updates about "what's for dinner" to milestones like birthdays and graduations.

Over the last four years, military families have significantly increased their use of social media. In fact, 93% of military families currently use Facebook to stay connected.

As with any new technology, it is important to know how to use it safely and wisely. This is especially true for our military families, who face unique and specific safety risks.

That's why Blue Star Families and USAA teamed up with Facebook to provide a guide specifically for service members and their families. This guide provides information on the safety policies and tools that allow you to connect and share online, while maintaining your personal safety and the safety of your loved ones.

93% of military families currently use Facebook to stay connected

How do I take care of myself and my family online?

The following sections will provide an overview of the importance of security, privacy and safety in protecting yourself and your family online.

1 ## Security
Take advantage of technical tools and best practices that protect your data.

2 ## Privacy
Take advantage of tools and best practices to control what you share and with whom.

3 ## Safety
Identify and address safety issues such as unwanted contact, inappropriate content, bullying and harassment, and evidence of depression or suicidal thoughts in a friend or loved one.

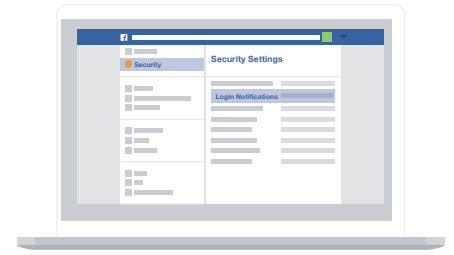## What does online safety mean for me and my family?

Online safety includes everything from protecting sensitive or personal information on your home network to protecting your children and family from risks related to over-sharing, poor judgment, or bad digital citizenship.

Military service members and their families face additional specific challenges:

- United States' enemies sometimes target military personnel and their families via social media;

- Sharing seemingly innocuous personal information can inadvertently conflict with good operations security procedures;

- Insecure networks or websites can leak sensitive documents or orders stored on home computers;

- Online scammers frequently target military members and their families; and

- Service members returning from deployment and family members dealing with their absence experience higher rates of depression, anxiety and suicidal thoughts.

🔒 Security

Good Internet security practices—from your WiFi network to your web passwords—are key to keeping your information safe.

Keeping your mobile device secure

What you need to know

Even the smartest smartphone is susceptible to attack. Securing your mobile devices reduces the likelihood that someone will gain unauthorized access to your device and/or the accounts and content associated with it.

What you need to do

• Lock your mobile device screen by enabling a passcode feature with time-out option.

• Enable remote wipe and location features to help protect your personal information if your device is lost or stolen.

• Utilize stronger authentication. Use options such as face or voice biometric technology, if available.

• Avoid links from unknown sources. Don't use a link from sources you don't trust, including emails and social media posts. Malicious links could direct you to websites or applications that compromise your device.

• Consider using anti-virus software.

• Use trusted networks. Connecting your device to unknown wireless networks can expose your data. Crooks operate look-alike hot spots with the sole purpose of eavesdropping.

• Turn off unnecessary services. Wi-Fi, Bluetooth, location apps, near field communication apps and other connection abilities can be disabled to protect your device when you're not using them.

• If you've lost your phone, to prevent someone else from accessing your Facebook account with it: log into Facebook on a computer, go to your mobile settings and click "Lost your phone?" and then click "Log Out on Phone."

Keeping your personal information secure

What you need to know

For military personnel and families, taking care of finances online is not simply a convenience, it's often a necessity. To help protect yourself from fraud, monitor your financial account activity on a regular basis and take advantage of all the tools offered by your financial institution to mitigate risks when checking your account on your desktop, smartphone or tablet.

What you need to do

• Create a strong password. Use a combination of at least 6 letters, numbers and punctuation marks. Avoid including your name or common words. Your password should be difficult to guess. Don't use your Facebook password anywhere else online and never share your password.

• Never share your login information (ex: email address and password). Sometimes people or Pages will promise you something (ex: free poker chips) if you share your login info with them. These types of promises violate Facebook's Terms of Service. If you're ever asked to re-enter your password on Facebook (ex: you're making changes to your account settings), check to make sure facebook.com is still in the URL (web address).

Key Takeaways

• Secure your home WiFi network and all your online accounts with strong, unique passwords.

• Secure your mobile device.

• Make sure websites employ https to secure your information.

• Enable additional security features such as two-factor authentication.

• Log out of Facebook when you use a computer you share with other people. If you forget, you can log out remotely.

• Only accept friend requests from people you know.

• Watch out for fake Pages and apps/games. Be suspicious of Pages promoting offers that are too good to be true. Be mindful when you install new apps or games. Sometimes scammers use bad apps and games to gain access to your Facebook account.

• Update your browser. The newest versions of internet browsers have built-in security protection. For example, they might be able to warn you if you're about to go to a suspected phishing website. Facebook supports Mozilla Firefox, Safari, Google Chrome and Internet Explorer.

Security Checkup

Use Security Checkup to review and add more security to your account. Security Checkup will help you:

• Log out of Facebook from unused browsers and apps.
• Set up login alerts that notify you if someone tries logging into your account from a unknown computer or phone.
• Learn how to protect your password.

fb.me/SecurityCheckup

• Use our extra security features.

– Manage log in locations. The "Where You're Logged In" section of your security settings page shows you a list of browsers and devices that have been used to log in to your account recently. Each entry includes the date, time and approximate location when signing in, as well as the type of device used to access your account. You'll also see the option to "End Activity" and log yourself out on that computer, phone or tablet.

– Activate login alerts. When you turn on login alerts, you will receive a notification if someone tries logging into your account from a new place. To turn on login alerts, go to your security settings, click the "Login Alerts" section and choose the type of alert (ex: email alerts) you'd like to receive and click "Save Changes."

– Enable login approvals. If you turn on login approvals, you'll be asked to enter a special security code each time you try to access your Facebook account from a new computer, phone or browser. To turn on login approvals, go to your security settings, click the "Login Approvals" section and check the box and click "Save Changes." After you turn on login approvals, if you haven't saved the device (ex: computer) or browser you're using, you'll be asked to do so when you turn on login approvals. This way you won't have to enter a code when you log in from any of your recognized devices or browsers. Don't click "Save this Browser" if you're using a public computer (ex: a library computer).

👓 Privacy

If 'Security' covers the tools you need to keep bad guys out of your account, 'Privacy' covers the tools you need to control what you share online and with whom. These choices are critical to your safety and well-being online.

Key Takeaways

- Always consider what you're sharing and with whom when posting something online—don't forget to consider your intended and unintended audience.

- Find the privacy settings on the websites and services you use and be sure you understand how they work.

- Maintain good personal security and OPSEC by looking at your accounts through the eyes of a potential adversary.

Navigating your privacy settings on Facebook

What you need to know

When you share something online, ask yourself "What am I sharing" and "With whom am I sharing?" For military families, we should take this a step further.

- Think about whether you are comfortable with other people seeing what you are sharing and whether that content could be used against you or your family by someone hostile to the military.

- Remember when you share with your friends or followers, they may reshare with a larger audience. Also, ask yourself whether your public accounts have followers you don't know.

What you need to do

- The first place to start on Facebook is your "About" section, where you might have shared your hometown, where you currently live, where you went to school, current or past employers and more. Many military service members and their families have decided to remove much of this information, which is perfectly reasonable. But did you know that you can also set the audience on each piece of information you share?

- You have the opportunity to review and adjust your privacy settings at anytime. To view your privacy settings, click the downward arrow at the top right of your Facebook profile and select "See More Settings" in the dropdown menu. Privacy settings help you manage what others see about you, how others interact with you and what you see.

Privacy Checkup

Take a moment and use the Privacy Checkup to review and adjust your privacy settings to help make sure that you're sharing with who you want. The Privacy Checkup will help you review who sees your posts, your settings for apps you've logged into with Facebook and who can see info from your profile like your phone number and email address.

fb.me/PrivacyCheckup

Navigating your privacy settings on Facebook step-by-step guide

Friend people you know and trust

Facebook is a place for connecting with people you know personally, like your friends, family, classmates and colleagues. If you'd like to make new friends, try connecting with Pages and groups that interest you. Facebook is based on authentic identities, where people represent who they are in the real world. Unfortunately, some individuals use tactics such as impersonating a friend to gain access to personal information. If you receive a friend request from someone you thought you were already friends with, ask them if they created a new profile and report the impersonating profile to Facebook.

Select your audience

You'll find an audience selector tool when you share status updates, photos and other things you post. Remember, when you post to another person's Timeline, that person controls what audience can view the post. Additionally, anyone who gets tagged in a post may see it, along with their friends. If you accidentally share a post with the wrong audience, you can use the audience selector next to the timestamp on your post to change who can see stuff you share on your Timeline after you share it. Keep in mind that when you share something on someone else's Timeline, they control the audience for the post.

Review tags

Timeline review lets you approve or dismiss posts that people tag you in before they go on your Timeline. When people you're not friends with tag you in a post, they automatically go to Timeline review. If you'd also like to review tags by friends, you can turn on Timeline review for tags from anyone. Tag review is an option that lets you approve or dismiss tags that people add to your posts. When you turn it on, any time someone tags something you posted, that tag won't appear until you approve it.

Control links to search engines

If you don't want search engines to link to your profile, you can adjust this under your privacy settings. Under the ' "Who can look me up?" ' section, click ' "Do you want other search engines to link to your timeline?" ' and make your selection using the check box. Note: Information from your profile and some things you share can still appear in search engine results even if you select "No." Public information may still appear in search results. To learn more, visit **fb.me/SearchEngines**

Review what people can see

The Department of Defense (DoD) notes that OPSEC "challenges us to look at ourselves through the eyes of an adversary." You can see what your profile looks like to other people by using the View As tool. By looking to see what people might see when they visit your Facebook Profile, you may be able to identify information, photos or updates that you need to restrict the audience on. To learn more visit **fb.me/ViewAs**

Manage your timeline

You get to decide whether friends are allowed to post things on your Timeline or not. To manage who can post on your Timeline, go to your settings and select Timeline and Tagging. Under the section "Who can post on your Timeline?" there's a menu that gives you control over whether "only you" can post on your Timeline or whether friends can post there, too.
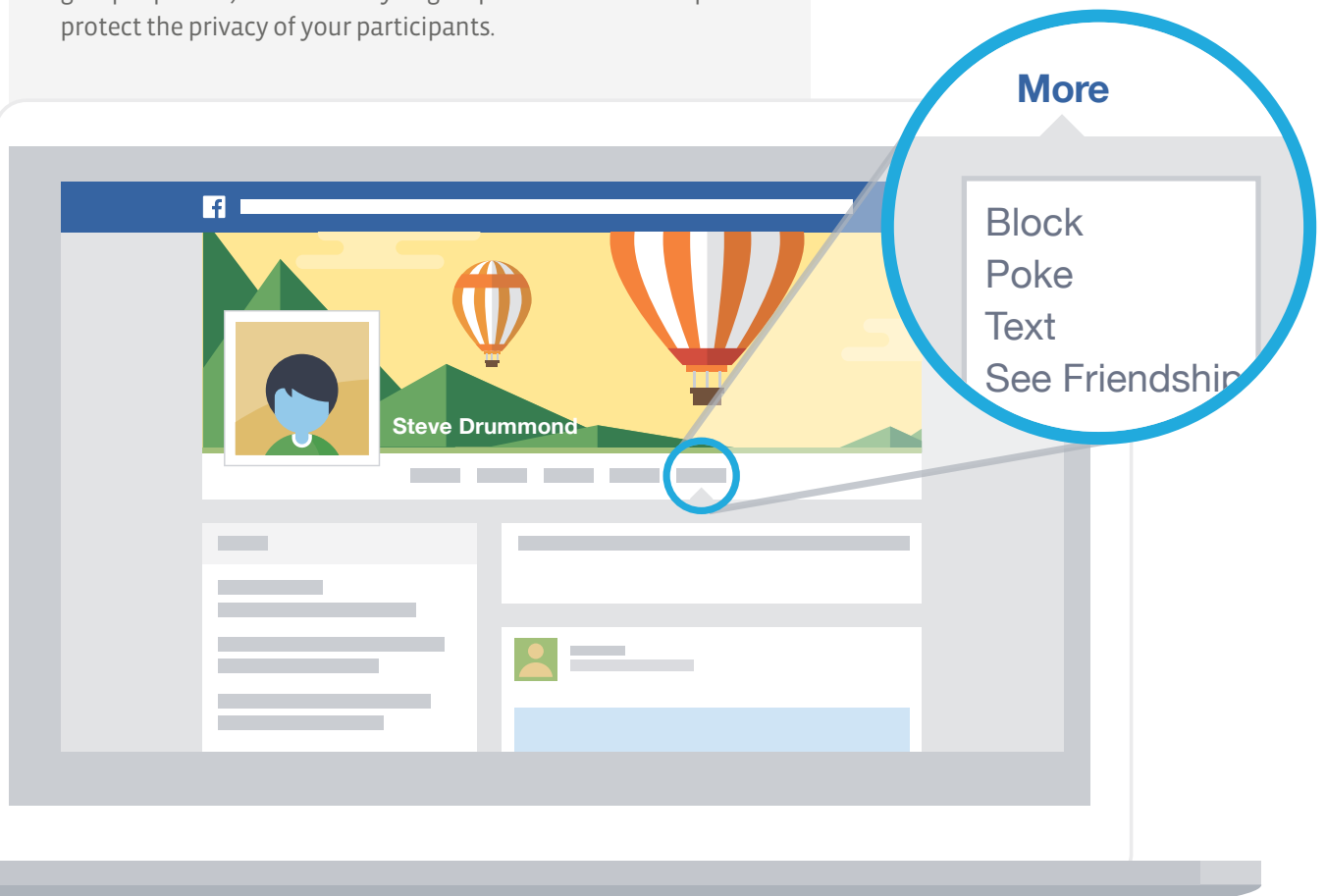
Unfriending and blocking

To stop someone from bothering you, you can either unfriend or block them. Anyone you unfriend or block will not be notified. Blocking someone means you won't be friends anymore and they won't be able to add you as a friend, see things you post on your profile (as long as it isn't shared publicly), tag you, invite you to events or groups, or start a conversation with you. Someone you block might still see things such as if you like or comment on someone else's post or share something in a group you're both in.

More social media privacy tips

Geo-tagging sometimes occurs when a person uses a location-based device, such as a smartphone, to post a status update or upload a photo or video. The U.S. Army recommends that soldiers' location based services be turned off in order to ensure their safety and the safety of other soldiers.

Use messaging services like Facebook Messenger or direct messages on Twitter for private communications.

Use Facebook Groups to communicate privately among a larger group such as your extended family, support groups, or other affinity groups. In a military readiness setting, we suggest you create groups that are "closed," not "open." This means that while the list of group members is public, the content of the group is private, available only to group members. This helps protect the privacy of your participants.

More

Block
Poke
Text
See Friendship

Steve Drummond

You're in charge!

To learn more about ways to protect your privacy on Facebook visit
web.facebook.com/about/basics

⚠ Safety

Safety is all about how you respond to situations that could be dangerous.

Key Takeaways

- Don't accept friend requests from strangers even if you may have friends in common.

- Use reporting features that almost all social media and sharing sites have to flag inappropriate content, bullying, and harassment.

- Contact the authorities in situations where someone is threatening to harm himself/herself or someone else.

Community Standards

What you need to know

Facebook's mission is to give people the power to share and make the world more open and connected. Every day, people come to Facebook to share their stories, see the world through the eyes of others and connect with friends and causes. The conversations that happen on Facebook reflect the diversity of a community of more than one billion people.

Facebook wants people to feel safe when using Facebook. For that reason, they have developed a set of Community Standards, outlined below. These policies will help you understand what type of sharing is allowed on Facebook, and what type of content may be reported to us and removed. Because of the diversity of our global community, please keep in mind that something that may be disagreeable or disturbing to you may not violate our Community Standards.

To read more of our Community Standards, visit: facebook.com/communitystandards.

Reporting

What you need to do

Report any content that violates the Facebook Terms. The most efficient way to report abuse is to do it right where it occurs on Facebook, using the "Report" link near the post, timeline or Page.

If you receive a harassing message from one of your Facebook friends, you can click the "Report" link next to the sender's name on the message, and remove the person as a friend. You can also use the "Report/Block" option that appears under the gear icon on the top right of every person's timeline.

Reports are confidential. People you report won't know that they've been reported. After you submit a report, we'll investigate the issue and determine whether or not the content should be removed based on the Facebook Terms. We research each report to decide the appropriate course of action.

Remember to...

Visit the **Facebook Family Safety Center** for more information, tools and resources about staying safe online.

facebook.com/help/safety

Social Reporting

What you need to do

Social Reporting is a feature of the reporting tool that helps you resolve issues with posts, timelines or other content on the site. If you are reporting content you don't like, but that doesn't violate the Facebook Terms, we make it easy for you to communicate with the person who posted it. For example, if you are reporting a photo of yourself, you can easily send the person who posted it a message letting them know you don't like it. In most cases, they will take the photo down if you ask.

In cases of bullying or harassment, where you don't feel comfortable reaching out to the person directly, you can use social reporting to get help from a parent, teacher or trusted friend. You can share that piece of content and a message about the situation with someone you trust. You also have the option to block the person who posted the content and report it to Facebook so we can take action, if appropriate.
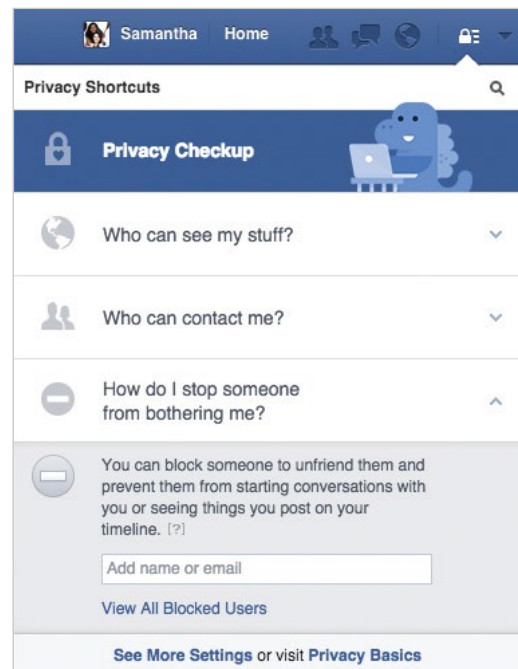
Social Reporting can also be used to help a friend in need.

Blocking

What you need to do

If you are being harassed by someone or if you just don't want be visible to them on Facebook, you can block them from your timeline. When you block someone, it breaks all ties you have with them (friendship connections, friend details, etc.). The two of you will no longer be able to see each other's timelines or find each other's timelines in search results.

The easiest way is by going to their Profile and selecting "Block" from the menu on their cover photo. You can also select the lock icon at the top right of any Facebook Page, select "How do I stop someone from bothering me?," enter their name or email address and click "Block." If you entered a name, a list will appear for you to select the right Profile.

Help a friend in need

Facebook is proud to work with the Jed Foundation and the Clinton Foundation, nonprofits that work to promote emotional well being, to share potential warning signs that a friend might be in emotional distress and need your help.

What you need to know

Trust your instincts

If you see someone posting messages, photos, videos or links that suggest the person is in emotional distress, you should reach out and get them the help they may need.

Be aware

Look out for statuses/posts, messages, photos or videos that include the following themes:

- Talking about feeling alone, hopeless, isolated, useless or a burden to others: "I feel like I'm in a black hole"; "I don't want to get out of bed...ever;" "Leave me alone;" "I can't do anything right."
- Showing irritability and hostility that is out of character: "I hate everyone; F*@K the world."
- Showing impulsive behaviors: Like driving recklessly, taking risks and especially a significant change in substance abuse.
- Insomnia posts: "3am again and no sleep"
- Use of Negative Emoticons: Repeatedly using emoticons that describe feeling angry or irritated.

For more information on how to help a friend in need, visit: fb.me/helpafriend

What you need to do

If you have a friend who seems to be struggling with an issue that may be more serious than they can handle, there is a lot that you can do to support them.

- **Reach out** and let them know they are not alone in feeling this way and that its ok to ask for help.
- **Be clear and direct** and do not use hints such as using the "Like" button or replying with an emoticon, as the person you're trying to help could misinterpret these symbols.

Understanding that it can be tough to start this conversation, here are some suggestions:

- "I'm worried about you because you seem..." (e.g. sad, withdrawn, etc.)
  - Have examples ready such as, "It concerned me when you said..." Be specific about what you noticed.
- "Do you want to talk about it?" "What can I do to help?"

If they say no, then you might say:
  - "It's okay if you don't want to talk to me, but it is important that you talk to someone."
- Offer to help them connect with the campus counseling service or health center, chaplain or dean of students or other mental health services.

Think before you share

Your own stuff

Remember that anything you share could end up being seen by people you don't want to send it to.

Be aware that if something prompts you to share something you're not comfortable with; you have the right to say no.

For more information on Think Before You Share, visit fb.me/thinkbeforeyoushare.

Fixing things if they go wrong

If you're unhappy about something being shared, ask the people you sent it to not to pass it on or ask the person who posted it to take it down.

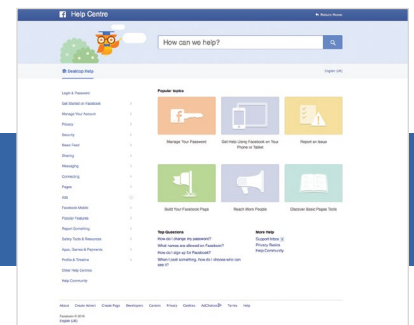Facebook also provides you with other safety resources to help you fix things when they go wrong.

By partnering with suicide prevention organizations globally and featuring report links throughout the site, Facebook connects people in need and their friends with the resources and people who can best help them.

For even more information on suicide prevention, go to: **facebook.com/help/suicideprevention**

HELP CENTER

At every point in the service, we offer help and resources people might need to ensure their safety. To access our Help Center, visit **facebook.com/help**

🍎 Resources

Networking and employment resources available on Facebook

Army Spouse Employment Partnership:
facebook.com/ArmySpouseEmploymentPartnership

Hiring Our Heroes:
facebook.com/HiringOurHeroes

Military Spouse Corporate Career Network:
facebook.com/MSCCN

Military Spouse Employment Partnership:
facebook.com/MSEPOnline

Military Veterans Employment Network:
facebook.com/MVENetwork

Military Spouse JD Network:
facebook.com/groups/160135920719440/

National Military Spouse Network:
facebook.com/NSMNetwork

VA Careers:
facebook.com/vacareers

Resources available at BlueStarFam.org

Become a member:
bluestarfam.org/connect/join-us

Find a chapter:
bluestarfam.org/connect/chapters

Volunteer:
bluestarfam.org/connect/volunteer

Military Family Lifestyle Survey:
**bluestarfam.org/resources/
military-family-lifestyle-survey**

Caregivers Empowering Caregivers:
**bluestarfam.org/resources/
caregivers-empowering-caregivers**

Blue Star Careers:
bluestarfam.org/resources/blue-star-careers

Blue Star Networks:
bluestarfam.org/resources/blue-star-networks

Blue Star Spouse Employment Toolkit:
**bluestarfam.org/resources/blue-star-spouse-
employment-toolkit**

Resources available at USAA.com

Advice Center:
usaa.com/advice

> "I like to keep in touch with my former sailors and former co-workers on Facebook. I have a 'professional' friends list set up to make it easier to network when I need to. In an instant, I can see what everyone is up to and it makes it much easier to stay connected."
>
> – *Trey, Navy Veteran*

Other resources: Service social media directories

U.S. Army:
army.mil/media/socialmedia/

U.S. Navy:
navy.mil/media/smd.asp

U.S. Air Force:
af.mil/AFSites/SocialMediaSites.aspx

U.S. Marines:
marines.mil/News/SocialMedia.aspx

U.S. Coast Guard:
dhs.gov/xabout/gc_1238684422624.shtm

Local/regional/specialized group

Alabama Blue Star Families
Alaska Blue Star Families
Arizona Blue Star Families
Blue Star Caregivers
Blue Star Caregivers – CEC Forum
Blue Star Educators
Blue Star Entrepreneurs
Blue Star Health Care Professionals
California Blue Star Families
Colorado Blue Star Families
D.C. Blue Star Families
Florida Blue Star Families
Georgia Blue Star Families
Germany Blue Star Families
Guam Blue Star Families
Guard & Reserves Blue Star Families
Hawaii Blue Star Families
Illinois Blue Star Families
Italy Blue Star Families
Japan Blue Star Families
Kentucky/Indiana Blue Star Families

Korea Blue Star Families
Louisiana Blue Star Families
Maryland Blue Star Families
Massachusetts Blue Star Families
Michigan Blue Star Families
Mississippi Blue Star Families
Missouri Blue Star Families
Nebraska Blue Star Families
Nevada Blue Star Families
New Jersey Blue Star Families
New Mexico Blue Star Families
New York Blue Star Families
North Carolina Blue Star Families
Ohio Blue Star Families
Pennsylvania Blue Star Families
South Carolina Blue Star Families
Texas Blue Star Families
United Kingdom Blue Star Families
Virginia Blue Star Families
Washington Blue Star Families

Find Blue Star Families and USAA on Facebook
facebook.com/BlueStarFamilies
facebook.com/USAA