USA BASEBALL

moonshot

Staying Safe on Social Media

Checklists for USA Baseball athletes, parents and coaches

Why is this important?

Everyone deserves to feel safe on social media. For athletes, maintaining a public profile on social media can be critical to advancing your career.

Every action you take online leaves a trace: your very own digital footprint. This information can be used by people looking to exploit this information and cause harm.

It is possible to build a public profile and keep yourself safe online. The U.S. Olympic and Paralympic Committee has partnered with Moonshot to improve online safety for Team USA. For USA Baseball, Moonshot has pulled together a summary of key steps you can take to improve your safety online.

More resources will be launched in Summer 2025.

TASK 1 Check and reduce your digital footprint

Step 1
Make a list of the accounts you have. Focus on social media, online banking, and email accounts.

Step 2
Identify the ones you no longer need and close them down.

Step 3
The remaining accounts are your "need to have" list. The next task is to check that they're properly protected.

You may not remember all of your accounts. You can use https://checkuser.org/ (inputting your typical usernames). This will point you to the platforms where these "orphaned" accounts might exist.

Data breaches

Any website storing your personal information can be hacked. This may have already happened without you knowing. You can check for free to see if your data has been compromised.

Step 1
Check your email addresses at: www.haveibeenpwnd.com

Step 2
Change the password of - or delete entirely - any impacted accounts.

TASK 2 Strengthen your passwords

Strong passwords are the most important line of defense. There are several core principles to follow when creating and managing your passwords.

Don't recycle your passwords across multiple websites.

Refresh your passwords at least twice a year.

Create long, complex and unique passwords. See the **Diceware** method.

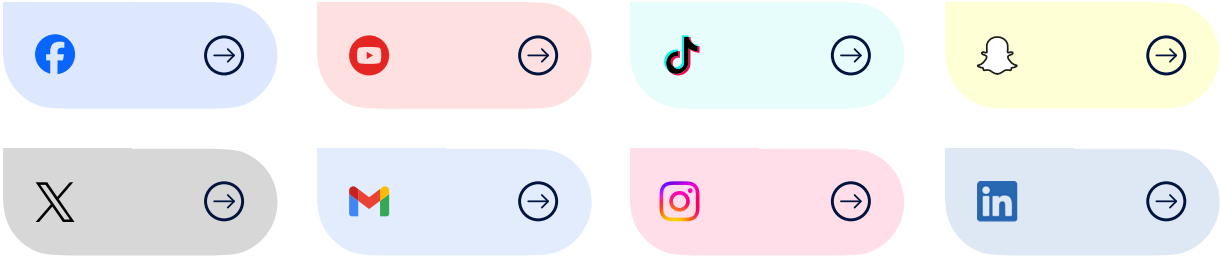
Use a password manager, like **LastPass**, **Dashlane**, **Google** or **Apple** (they offer password generation too).

TASK 3 Strengthen your social media protections

Your social media profiles are the most obvious target for anyone attempting to cause harm. Taking the following steps will reduce the risk that your profiles will be compromised.

Step 1: Implement two-factor authentication (2FA)

2FA is a powerful tool which makes your account much safer. You should use 2FA on any platforms that offer it, whether they're social media, email, Netflix, or anything else. Click the image to see a guide for setting up 2FA on each platform:



Extra tip: Block location tagging

Extra tip: Prevent unwanted tagging

Step 2: Protect – and maybe separate – your personas

We recommend you consider creating a public-facing profile and a separate private one (also known as a 'finsta' – fake Instagram account), to create a better work-life separation, and to better silo your personal data such as likes. Click the image to see how to turn your profile private.

Extra tip:
LinkedIn can be a valuable public presence to have, it can also be a source of information for those looking to dox you, check what your profile looks like to a member of the general public by following these steps.

Step 3: Check how visible your accounts are

If you're unsure, here's how to set your visibility settings:

Instagram Privacy Settings

Snapchat Privacy Settings
Control your visibility by setting your "contact me" settings to "friends" to prevent yourself from appearing in people's "find friends" suggestions.

TikTok Privacy Settings
Here's how to set your privacy settings on TikTok, and click here to hide your TikTok likes from your profile.

X Privacy Settings
For visibility settings on X, scroll down to "Control what others see about you. Here are some additional profile visibility settings on X.

Step 4: Take control over your comments and the people who leave them

Here's how to hide and report comments, and how to block users:

Hiding comments

Here's how to hide a comment on Instagram, and restrict a user on Instagram; filter all comments on TikTok (this will automatically hide comments until you approve them); adjust your conversation settings on X, to limit who can reply to your posts.

Reporting comments

Here's how to report a comment on Instagram, and delete a comment; report a comment on TikTok, and delete a comment. Snapchat only has public facing comments on spotlight stories, which you can manage – here's how to report and delete them. X does not let you delete other people's replies to your posts, but you can report a reply.

Blocking users

Here's how to block a user on Instagram; on Snapchat; on TikTok; on X.

Step 5: Control your conversations

Here's how to hide and report comments, and how to block users:

Instagram Message Settings

Extra tip: Consider turning your account into a professional account because this separates your inbox into "Primary" (for people you're close with), "General" (for everyone else), and "Requests" (for first time messagers or users you want to hide).

Snapchat Message Settings

Here's how to block, delete, report, and control who can contact you.

TikTok Message Settings

X Message Settings

How to manage direct messages on X, DM block someone, and generally block someone.

Step 6: Control what other people can do with your content

Here's how to manage:

- Who can tag you on Instagram, and who can remix your content
- Who can add your posts to their story on TikTok to manage who can remix your content including things like stitches and duets, and how to remove original sounds.
- Who can tag and mention you on X.

Here's how to control your location tracking settings on Instagram, TikTok, and on X. Where available, consider leaving the option to tag your location in your posts blank.

TASK 4 Understand what's out there about you

Now that the online presence you control is secured, it's time to check what other information is out there.

Step 1: Google yourself

Use incognito mode on your browser and conduct the following searches:

NB: Do not type in your actual address or password.

- "[your name]" email OR phone
- "[your email]" AND "password"
- "[your name]" AND "address"
- "[your name]" filetype:pdf

Step 2: If you see something you don't like, you can do something about it

The searches might highlight gaps in your social media privacy settings. Your address, email or phone number may come up in the top results, making you an easy target.

DeleteMe

Some results will feature data brokers, who collect and sell your data on a regular basis.
You can either directly request that the broker removes your data, or use a service like DeleteMe.

TASK 5 Identifying and responding to threats

Doxxing

Doxxing is the act of leaking personal information with malicious intent. It can lead to harassment, extortion and physical violence. Completing Task 3 will significantly reduce your risk of being doxxed. But if it does happen, these are the steps you should take:

Step 1: Review all of your social media accounts, change the passwords, check that no other accounts or apps have been given administrative access

If you receive harassing or threatening communications, screenshot and report them to police.

Step 2: Inform your immediate family about the doxxing, encourage them to secure their accounts

Phishing

Phishing is the fraudulent activity of trying to gain access to private information. It is one of the most common ways that your personal data will be targeted. It often takes the form of scam emails, texts or phone calls. These are the steps you can take to make sure you don't fall victim to Phishing:

Step 1: Be vigilant for phishing attempts, they often have telltale signs

- Urgent language
- Generic greetings
- Requests for sensitive information
- Unfamiliar or mismatched URLs
- Spelling and grammatical errors
- Sender email addresses are slightly wrong
- Requests to open an attachment/download an attachment

Step 2: Confirm your suspicions

If you suspect a phishing attempt but aren't sure, seek verbal confirmation (via another method) from your contact. This will prove whether or not the message is genuine.

Step 3: Record and report the attempt

It is important to stay on top of phishing attempts. To reduce the amount you receive, you can do this in a few ways:

Take a screenshot

Mark/report the message as spam or junk

- ⊗ Never click links or download attachments
- ⊗ Never provide any personal information
- ⊗ Never reply to the message

Hacking

2FA makes it much less likely that your social media profiles will be compromised. However, if you do find yourself dealing with a breach there are steps you can take:

Step 1: Change your password immediately

Step 2: Make sure that the hacker hasn't updated the associated email or phone number

Step 3: Enable 2FA: The first step to preventing future breaches

Step 4: Revoke access to other apps: Your profile may have been linked to third-party apps that you don't recognize

Step 5: Update the passwords of <u>all</u> of your other accounts

TASK 6 Strengthen your device protections

Step 1: Check that your computer has up to date malware protection

Most of these software packages come at a price, but there are high quality free alternatives, including Avast and Malwarebytes.

Avast

Malwarebytes

Step 2: Review and bolster your phone security settings

Guidance for iPhone

Guidance for Android

These are the key steps to keeping yourself safe as you build your online profile!

Stay tuned for more resources to be launched in Summer 2025.

About Moonshot

VISIT MOONSHOT

Moonshot works to end online abuse and violence. We design technology to keep athletes safe as they compete on the global stage, whether at the Paris Olympics or in college sports. We support the United States Olympic and Paralympic Committee to protect Team USA from online threats. We collaborate with leagues, clubs, and schools to make sports safer for thousands across the globe.