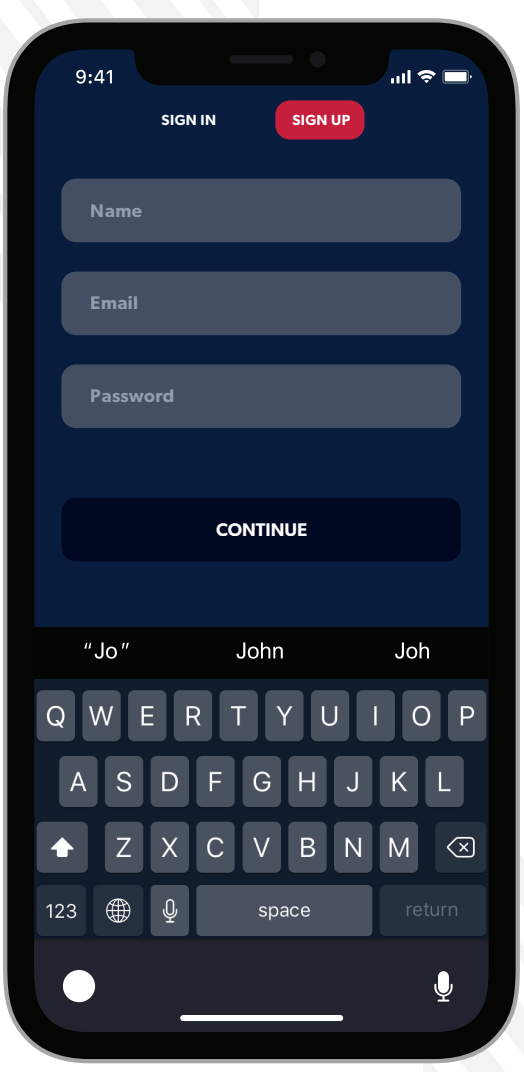
CYBERSECURITY & SOCIAL MEDIA

PROTECT YOURSELF & YOUR FAMILY



NEVER USE THE SAME PASSWORD FOR MULTIPLE ACCOUNTS

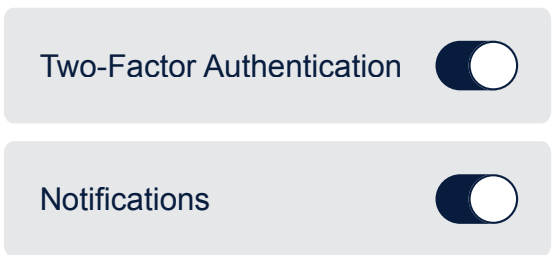
While it may be convenient, using one password for everything is actually quite dangerous. If a malicious actor gains access to just one of your username and password combinations, there is an excellent chance they will use this information to access multiple other websites and services in your name.

CREATE STRONG PASSWORDS

- USE a password manager such as 1Password to keep track of your various login combinations.
- When creating passwords, do not use predictable personal information such as your birthday, name, or pets name. Consider using a "passphrase" instead, utilizing multiple words, numbers and characters.
- A weak password containing 6 lowercase letters can take a hacker as few as 10 minutes to guess correctly. Choose something random, complex and creative.
- The stronger your passwords are, the harder they may be to remember; a password management application can help you stay secure and organized by keeping all your logins in one place. All you have to do is remember one master password.

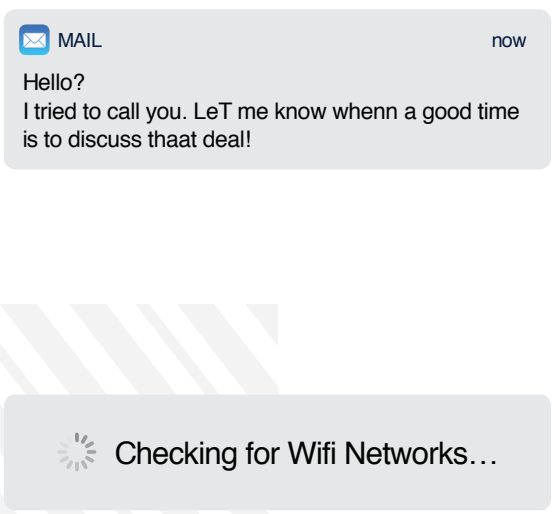
NEVER SHARE YOUR PASSWORDS WITH OTHERS

This includes technical support, significant others, friends, coaches, teammates, etc. Your accounts and devices are your responsibility. At the end of the day, you will always be held accountable for whatever content is on there.



ENABLE SECURITY FEATURES FOR THE APPLICATIONS YOU USE

Turn on two-factor authentication when possible; it will send a code to your phone each time you log in on a new device. Similarly, enable notifications for all transactions, logins from new locations, failed logins and purchases made on credit or debit cards, etc. This will allow you to deny logins and purchases from locations or devices that you do not recognize.



BEWARE OF PHISHING EMAILS AND SCAMS

Look out for the signs of a phish: misspelled words, incorrect addresses, fake email addresses, demands or altered logos. If you notice any of these, do not click links within the messages. Instead, forward it all to cybersecurity@mlb.com. Be careful of calls or text messages asking for information such as passwords, social security number, date of birth, address, etc.

DO NOT USE UNKNOWN WI-FI NETWORKS

Use your iPhone or iPad cellular connection for important transactions. Always ask the hotel, facility or stadium for official SSID (Wi-Fi) information to be safe.

REDUCE YOUR ONLINE FOOTPRINT

Limit the data that you post online – it can be often used against you. Do not publicly post your date of birth, hometown or address. Delete old social media and email accounts to prevent your personal information from being too openly exposed. Advise your friends and family to do the same because, unfortunately, cybercriminals may use them to get to you.

TREAT DIGITAL SECURITY LIKE PHYSICAL SECURITY

Lock it as you would the front door of your home. Turn your phone off, then on, to reset the biometric sign-in (Face ID or Touch ID) at times when others may have access to it (i.e. while you are sleeping). Always lock your devices before you walk away.

Have any questions? Need assistance? Reach out to cybersecurity@mlb.com.