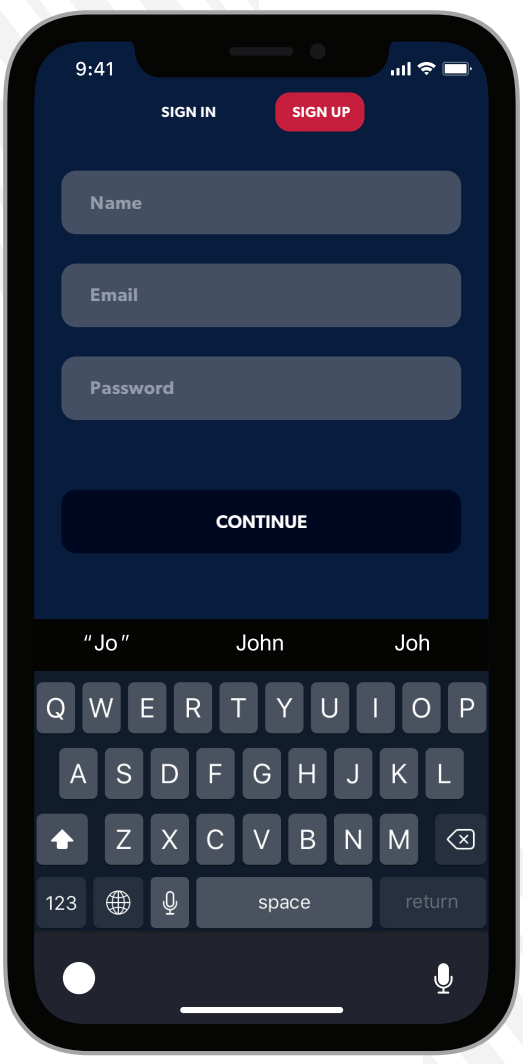
# MLB

# REDES SOCIALES Y CIBERSEGURIDAD

CÓMO PROTEGERSE Y PROTEGER A SU FAMILIA




## NUNCA UTILICE LA MISMA CONTRASEÑA PARA VARIAS CUENTAS.

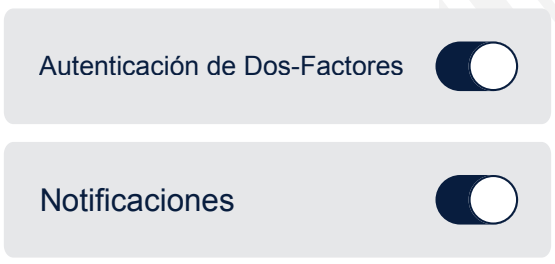
Si bien puede ser conveniente, usar una contraseña para todo es bastante peligroso. Si un actor malicioso obtiene acceso a solo una de sus combinaciones de nombre de usuario y contraseña, existe una gran posibilidad de que use esta información para obtener acceso a otros sitios web y servicios en su nombre.

## CREE CONTRASEÑAS SEGURAS

- Utilice un administrador de contraseñas como 1Password para almacenar las contraseñas de sus distintas cuentas.
- Al crear contraseñas, no use información personal predecible como su fecha de nacimiento, nombre o nombre de sus mascotas. Considere usar una "frase de contraseña" en su lugar, incorporando múltiples palabras, números y caracteres.
- Una contraseña débil que contenga 6 letras minúsculas puede llevar a un pirata informático tan solo 10 minutos para adivinar. Por lo tanto, elija algo al azar, complejo y creativo.
- Cuanto más fuertes sean sus contraseñas, más difíciles serán de recordar; una aplicación de administración de contraseñas lo ayudará a mantenerse seguro y organizado al mantener las contraseñas de sus distintas cuentas en un lugar seguro. Todo lo que tiene que hacer es recordar una contraseña maestra.

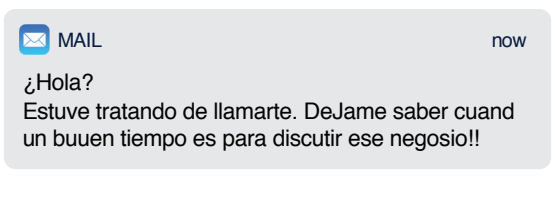
## NUNCA COMPARTA SUS CONTRASEÑAS CON OTRAS PERSONAS

Esto incluye personas de soporte técnico, parejas, amigos, entrenadores, compañeros de equipo, etc. Sus cuentas y dispositivos son su responsabilidad. Al final del día, siempre será responsable de cualquier contenido que esté allí.



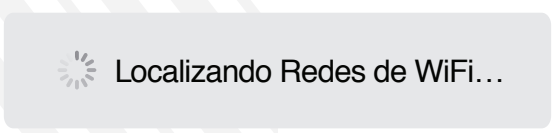

## ACTIVE TODAS LAS FUNCIONES DE SEGURIDAD QUE SEA POSIBLE PARA CADA UNA DE LAS APLICACIONES QUE UTILIZA.

Active la Autenticación de Dos-Factores siempre que sea posible. Esto enviará un código a su teléfono cada vez que inicie sesión en un nuevo dispositivo. Del mismo modo, debe habilitar las notificaciones para todas las transacciones, inicios de sesión desde nuevas ubicaciones, inicios de sesión fallidos y compras realizadas con tarjetas de crédito o débito, etc. Esto le permite negar el acceso a inicios de sesión y compras desde ubicaciones o dispositivos que no reconoce.




## CUIDADO CON LOS CORREOS ELECTRÓNICOS DE PHISHING Y ESTAFAS.

Esté atento a los signos de un Phish: palabras mal escritas, direcciones incorrectas, direcciones de correo electrónico falsas, demandas amenazantes, logotipos alterados. Si ve signos de phishing, no haga clic en ningún enlace dentro del mensaje. En cambio, reenvíelo a cybersecurity@mlb.com. Del mismo modo, siempre tenga cuidado con las llamadas telefónicas o los mensajes de texto que le soliciten información personal, como contraseñas, número de identificación/ seguridad social, fecha de nacimiento, dirección, etc.




## NO UTILICE REDES DE WIFI DESCONOCIDAS.

Considere utilizar su conexión celular de iPhone o iPad para transacciones importantes. Siempre debe preguntar al hotel, academia, estadio, etc. cuál es su SSID oficial (nombre de WiFi) para estar seguro.

## REDUZCA SU HUELLA EN LÍNEA.

Limite la información que publica en línea: esta se puede usar en su contra. No publique su fecha de nacimiento, ciudad natal, dirección, etc. Elimine las cuentas antiguas de redes sociales y correo electrónico que ya no usa, ya que pueden contener información personal que puede estar potencialmente expuesta o utilizada en su contra. Hable con sus amigos y familiares acerca de hacer lo mismo porque desafortunadamente, los delincuentes cibernéticos intentarán conectarse con ellos para llegar a usted.


## TRATE SU SEGURIDAD DIGITAL DE LA MISMA MANERA QUE SU SEGURIDAD FÍSICA

Bloquéela como lo haría con la puerta de su casa. Apague su teléfono y vuelva a encenderlo para restablecer el inicio de sesión biométrico (FaceID, huella digital) en momentos en que otros puedan tener acces a él (es decir, mientras duerme). Y SIEMPRE bloquee sus dispositivos antes de dejarlos sin supervisión.

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