



Recomendaciones de seguridad para los usuarios .



A continuación te brindaremos algunas recomendaciones para que puedas acceder de forma segura a tus espacios de reunión programados en ZOOM y otras plataformas.



Escribe directamente en el navegador web la dirección de la página a la que necesitas acceder.

 Video Conferencing, Web Conferenc X

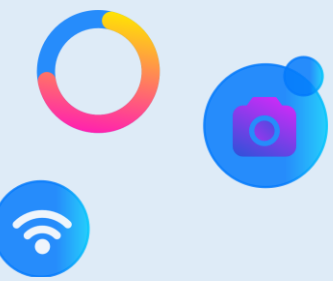
← → ↻  zoom.us

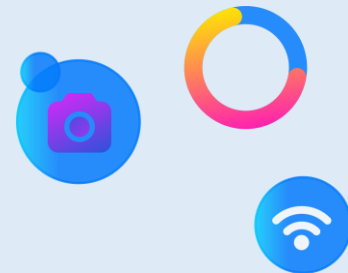
Valida que la página a la que accedes siempre tenga un candado que representa que la conexión es segura y la dirección empieza por **https://**



 Mi perfil - Zoom X

← → ↻  https://zoom.us/





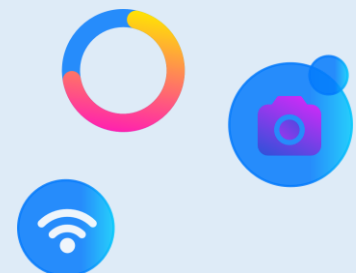
La invitación que recibes es **personal e intransferible**, por favor no la reenvíes a otros usuarios ni la publiques en tus redes sociales, estados de WhatsApp ni lugares públicos.

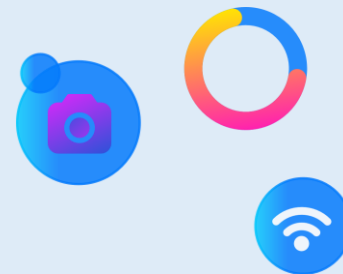


Evitar abrir mensajes que llegan por SMS o WhatsApp informándote que ganaste dinero, viajes, vehículos, descuentos u otros, con el fin de que el interesado se contacte con el autor del mensaje para que proporcione los datos personales.



Nunca entregues tus **datos personales o datos bancarios** como claves, usuarios o números de tarjetas por mail, vía telefónica o mensajes de texto o en nuestras salas de reunión.





Verifica la dirección de correo desde la cual recibes los correos promocionales antes de abrir cualquier enlace, estas deben provenir de un correo corporativo.



Los correos enviados por entidades reconocidas, por lo general en la parte inferior del correo electrónico mencionan tu nombre, leyes de protección de datos personales o se direcciona a la política de privacidad de la entidad.



Observa detenidamente la redacción e imágenes en los correos recibidos.

