

# Consejos para Proteger Su Privacidad en Línea y Seguridad Cibernética

División de Protección a la Comunidad  
Oficina del Fiscal del Distrito de Boulder



## Proteja su información de identificación personal (IIP)



- IIP esencialmente es cualquier información que pueda usarse para identificarlo.
- IIP incluye su nombre, dirección, fecha de nacimiento, número de seguro social, número de cuentas financieras, y dirección de correo electrónico.
- IIP también podría incluir información más indirecta, como su ubicación o preferencia de productos.
- **Ciberdelincuentes, así como muchos negocios, valoran su IIP como dinero, y por lo tanto, también usted debería hacerlo.**

## Actualice la configuración de privacidad y seguridad para sus cuentas en línea y dispositivos



Para enlaces directos a las instrucciones, visite el sitio para mantenerse seguro en línea con La Alianza Nacional de Seguridad Cibernética:

<https://staysafeonline.org/stay-safe-online/managing-your-privacy/manage-privacy-settings/>

## Use contraseñas complejas y únicas para todas las cuentas, más autenticación de dos factores (2FA)



- Una contraseña compleja es difícil de adivinar: al menos 12 caracteres, no una palabra común del diccionario, incluye letras mayúscula y minúscula, números, y caracteres especiales.
- Una contraseña única es aquella que no se usa para varias cuentas (por ejemplo, para el correo electrónico como para las cuentas bancarias en línea).
  - Esto ayuda prevenir que la violación de una cuenta conduce a la violación de otras.
- Para aún más protección, habilite 2FA. Después de introducir su contraseña, un código de acceso de un solo uso se envía al celular, y no puede acceder a su cuenta hasta que introduce el código de acceso también.
  - Con 2FA, aún si alguien tiene su contraseña no puede acceder a su cuenta a menos que también tenga su teléfono celular.
  - Para enlaces a instrucciones para habilitar 2FA, visite el sitio de Para Piensa Conéctate: <https://stopthinkconnect.org/campaigns/lock-down-your-login>



## Solo utilice sitios de web encriptados (codificados)



- Verifique la barra de dirección de la navegadora web: si ve un símbolo de candado cerrado o "https" al comienzo de la URL, el sitio es seguro
- Note: "http" no es seguro; la "s" al final de "https" significa "seguro."

Michael Dougherty, District Attorney

BOULDER OFFICE: JUSTICE CENTER · 1777 6TH STREET · BOULDER, COLORADO 80302 · 303.441.3700

LONGMONT OFFICE: 1035 KIMBARK · LONGMONT, COLORADO 80501 · 303.441.3700

WWW.BOULDERCOUNTYDA.ORG · EMAIL: BOULDER.DA@BOULDERCOUNTY.ORG · TDD/V: 303.441.4774



# Consejos para Proteger Su Privacidad en Línea y Seguridad Cibernética

División de Protección a la Comunidad  
Oficina del Fiscal del Distrito de Boulder



## Mantenga el software actualizado



- La mayoría del software (como para el sistema operativo, navegadores de web, aplicaciones, y seguridad cibernética) pueden configurarse para actualizar automáticamente.
- Instale las actualizaciones lo antes posible para minimizar el tiempo que ciberdelinquentes tengan para aprovechar debilidades en el software.

## Asegure la red wifi de su hogar

El router de wifi del hogar es la manera principal que ciberdelinquentes intenten acceder a los datos que pasan a través de la computadora de casa y otros dispositivos conectados al internet.



- Cambie la contraseña administrativa predeterminada (que es diferente a la contraseña de la red wifi), ya que a menudo las contraseñas predeterminadas son las en todas las marcas y son fácil de obtener.
- Cambie el nombre predeterminado de la red wifi (también se llama un SSID), ya que el nombre predeterminado podría indicar que router tiene.
  - No elija un nombre de la red que indique su nombre, dirección, u otra información sobre donde se encuentra la red.
- Habilite el cifrado del router. Al configurarlo, elija WPA3 si está disponible, pero si no, elija WPA2-AES.
- Apague cualquier función de “administración remota.”
- Deshabilite cualquier red de invitados que no tenga una contraseña.

## Evite redes wifi públicas

Use la red de datos del teléfono celular, o cree un punto de acceso wifi desde el teléfono para conectar una computadora portátil u otro dispositivo.



- Instrucciones para punto de acceso en Apple iOS: <https://support.apple.com/en-us/HT204023>
- Instrucciones para punto de acceso en Google Android: <https://support.google.com/android/answer/9059108?hl=en>

## Proteja sus videoconferencias

A medida que el uso de aplicaciones de videoconferencia ha aumentado, también lo han hecho las instancias de ciberdelinquentes no invitados que se unen para robar información, enviar enlaces o archivos maliciosos, o hostigar a participantes invitados.



- Cree y use un número de identificación de reunión único para cada reunión (no use uno que le haya designado la aplicación).
- Proteja la reunión con una contraseña.
- No comparta el número de identificación de la reunión o la contraseña públicamente (por ejemplo, en las redes sociales). En lugar, provéalas en privado por correo electrónico.
- Configure los ajustes para que nadie pueda unirse a la reunión hasta después del anfitrión.
- Habilite la función de “sala de espera,” le permite al anfitrión ver quien está intentando unirse y decidir si los deja entrar.
- Una vez que los participantes invitados se hayan unido, cierre la reunión para mantener a otros fuera.
- Restrinja el intercambio de archivos así que los invitados no deseados no puedan recibir o enviar archivos a través de la función de chat. En su lugar, envíe archivos al grupo por correo electrónico.