Buenas prácticas de seguridad digital

Se dedique o no al activismo por los derechos humanos, la seguridad digital le concierne: una buena higiene digital reduce su exposición a los ataques. Estos consejos sencillos le ayudarán a navegar con mayor seguridad.

Haga copias de seguridad de sus datos

Es la mejor manera de evitar la pérdida de sus datos si un dispositivo se pierde, se lo roban o deja de funcionar.

Cifre sus dispositivos

Si pierde el control físico de su dispositivo, sus datos estarán mejor protegidos con el cifrado completo del disco. Si el cifrado es ilegal en su país, siga estas alternativas.

Active la autenticación de dos factores en sus cuentas

La autenticación de dos factores (2FA, por su sigla en inglés) protege su cuenta incluso si alguien vulnera su contraseña. Elija siempre la 2FA mediante aplicación en lugar de la 2FA por SMS: así podrá acceder a sus cuentas aunque no tenga cobertura móvil. Consulte una lista de gestores de contraseñas y herramientas de 2FA recomendados.

Utilice una VPN

Cuando se conecta a una VPN, todos los datos que envía (por ejemplo, las solicitudes a los servidores al navegar por la web) parecen proceder de la VPN, lo que oculta su dirección IP y ayuda a proteger su privacidad (ya que la dirección IP indica su ubicación aproximada). Descubra cómo elegir el servicio de VPN que mejor le conviene.

Navegue de forma segura

Un navegador seguro, como Tor, le ayuda a proteger su tráfico de red en redes poco fiables, como las de aeropuertos u hoteles. Evite las redes wifi públicas siempre que pueda. Mantenga actualizados su navegador y sus complementos. Bloquee las ventanas emergentes y utilice un bloqueador de anuncios. Navegue en modo de «navegación privada» o active la opción «no rastrear» de su navegador.

Mantenga sus dispositivos actualizados

Un sistema con todas las actualizaciones de seguridad instaladas resulta más difícil de vulnerar y presenta menos vulnerabilidades conocidas.

Interactúe con ILGA Mundo en redes sociales de forma segura

Estas son las cuentas oficiales de ILGA Mundo: Facebook – X – Instagram – LinkedIn – YouTube – TikTok (inactiva) – Bluesky (inactiva).

Utilice una contraseña robusta y ÚNICA para cada uno de sus perfiles en redes sociales. Compruebe que conserva el acceso al correo electrónico o al número de teléfono con el que se registró. Si le preocupa que se revele su OSIEGCS sin su consentimiento, configure su perfil como privado. Rechace las solicitudes de amistad de personas que no conoce: en las redes sociales, las personas no siempre son quienes dicen ser.

En caso de ciberataque anti-LGBTI en redes sociales: no interactúe con los trolls; en su lugar, haga capturas de pantalla de sus mensajes, regístrelos y denúncielos. No haga clic en enlaces

sospechosos que reciba en comentarios o mensajes directos, sobre todo si proceden de personas que no conoce. Mantenga actualizadas sus protecciones de antivirus y cortafuegos. Si el hostigamiento se intensifica, configure su perfil como privado o desactive los comentarios. **¡ILGA Mundo nunca le pedirá sus contraseñas!**

Fuentes de esta guía: AccessNow; GlobalPride2020; Security in a Box, de Frontline Defenders y Tactical Tech; Surveillance Self-Defense, de la Electronic Frontier Foundation