huridocs
human rights information and documentation systems

Información básica de seguridad digital para los defensores de derechos humanos (DDH)

Esta nota proporciona información general sobre prácticas básicas de seguridad digital que los defensores de los derechos humanos (DDH) pueden tener en cuenta en el contexto de su trabajo. No proporciona información exhaustiva sobre cómo manejar cada incidente de seguridad digital, por lo que se aconseja a los defensores de derechos humanos que también consulten fuentes confiables para mejorar su seguridad digital.

ASEGURE SU COMPUTADORA

- Asegúrese de que su computadora reciba actualizaciones regulares y evite usar software o programas sin licencia.
- Utilice una contraseña fuerte para la autorización del usuario.
- Active su firewall.
- Active el cifrado completo de su disco.
- Instale un antivirus confiable (por ejemplo, Malwarebytes).
- Asegúrese de que no se almacenen datos sensibles en su computadora y considere guardar los datos sensibles en una cuenta segura en la nube.
- Utilice siempre contraseñas fuertes para todas sus cuentas y no reutilice las mismas contraseñas para varias cuentas.
- Use un gestor de contraseñas para almacenar todas sus contraseñas seguras y únicas para cada cuenta.
- Proteja sus cuentas con autenticación de dos factores (2FA) mediante una aplicación (por ejemplo, Google Authenticator) y evite la autenticación por SMS. Siempre que sea posible, genere códigos de respaldo como opción secundaria de 2FA y guárdelos en un gestor de contraseñas o en otro lugar seguro.
- Limpie regularmente su computadora de datos innecesarios.
- Utilice siempre una red privada virtual (VPN) cuando trabaje en lugares públicos (cafés, bibliotecas, aeropuertos) y cuando se conecte a redes públicas.
- Verifique la configuración de su navegador y asegúrese de que su información de inicio de sesión (nombres de usuario y contraseñas) no esté guardada en el navegador.
- Considere borrar regularmente las cookies, la caché del navegador y el historial de navegación.

ASEGURE SU TELÉFONO MÓVIL

- Asegúrese de que su teléfono esté actualizado con el último sistema operativo y reciba actualizaciones de seguridad regulares.
- Descargue únicamente aplicaciones de sitios y recursos autorizados y seguros (Google Play Store, Apple Store).
- Use una contraseña fuerte para bloquear su teléfono.
- Desinstale las aplicaciones que no utilice o no necesite.
- Elimine archivos sensibles y archivos no utilizados, y considere borrar el historial de textos y llamadas.
- Desactive la visualización de contenido de mensajes en las notificaciones (por ejemplo, en Signal: Ajustes Notificaciones Mostrar elija «Solo nombre» o «Ni nombre ni mensaje»).

SEGURIDAD FÍSICA

- Sea discreto con los dispositivos digitales y manténgalos a la vista y cerca de usted en todo momento.
- Esté alerta y consciente de su entorno (sala de reuniones, espacio de coworking, desconocidos).
- Desconfíe de extraños que muestren una curiosidad general por su trabajo.
- Tenga cuidado con los dispositivos que se han dejado abandonados (USB, tabletas e incluso computadoras portátiles), especialmente cuando trabaje en un espacio público.
- Información específica de los dispositivos

Síguenos para obtener más consejos y actualizaciones para defensores de derechos humanos, o contáctanos para colaborar.

www.huridocs.org

hello@huridocs.org