SEGURIDAD DIGITAL

Buenas Practicas para Periodistas

PROTEGER SUS CONTRASEÑAS

- Las contraseñas deben tener al menos ocho (8) caracteres.
- No utilice palabras del diccionario e idealmente, elija una frase como contraseña (una frase corta)
- Agregue letras mayúsculas y minúsculas, números y símbolos para que su contraseña sea más segura.
- Cambie sus contraseñas con bastante regularidad. Se aconseja hacerlo cada tres meses.
- Utilice un administrador de contraseñas (por ejemplo: Keepass, 1Password o LastPass), que le permite generar contraseñas únicas y almacenarlas de forma segura con una sola frase de acceso que sirve como contraseña maestra para acceder a todas las demás contraseñas. Asegúrese de guardar la contraseña maestra en una ubicación segura

SEGURIDAD PARA EL TELÉFONO CELULAR

- Proteja siempre su teléfono celular con una contraseña. Una combinación de dígitos, letras y símbolos es la opción más segura. Active las contraseñas no sólo para acceder a su teléfono celular, sino también para entrar en las aplicaciones (correo electrónico, redes sociales, etc.)
- Para mayor seguridad, proteja su tarjeta SIM con un código PIN SIM, normalmente accesible en la configuración del teléfono.
- No comparta nunca información altamente confidencial en un chat. Por “altamente confidencial” entendemos su información bancaria o sus contraseñas, pero también cualquier otra cosa que no quiera que otros lean sin su autorización.
- Para comunicarse de forma segura con otras personas, utilice aplicaciones que integren cifrado de extremo a extremo, como Signal o Wire. Esto significa que sus mensajes están codificados y ningún intermediario puede leerlos.

SEGURIDAD DIGITAL

Buenas Practicas para Periodistas

PROTECCIÓN DE FUENTES

- Si comunica con fuentes que no están familiarizadas con la seguridad en Internet, siga estos pasos para comunicar por correo electrónico:
  1. Créase una cuenta de correo electrónico Protonmail aquí: https://protonmail.com.
  2. Pídale a su fuente que se cree una también, recomendándole que use una contraseña segura. Si la fuente decide utilizar Protonmail desde una computadora pública, recomendamos que utilice el navegador en modo Privado/Incógnito y guarde los archivos adjuntos, si los hubiera, en una memoria USB personal en lugar de usar el disco duro local.

- Si comunica con fuentes que están más familiarizadas con la seguridad en Internet, pídales que activen PGP (Pretty Good Privacy), que le permite configurar una contraseña pública y firmar electrónicamente documentos para autenticarlos. Comparta su contraseña de PGP con sus fuentes.
- Utilice una contraseña segura para poder acceder a la lista de contactos en su computadora y teléfono celular

PROTECCIÓN DE DATOS

- Evite descargar software pirateado o cuestionable para no poner sus datos en riesgo.