Básicos para mejorar la seguridad de tus redes sociales

La Libre

Este manual presenta algunas buenas prácticas para la seguridad digital en redes sociales.

En los últimos años, el aumento de ataques contra cuentas en redes sociales de activistas y organizaciones ha sido alarmante.

Aunque estas plataformas han permitido conectarnos con personas y organizaciones de todo el mundo y han mejorado las comunicaciones, también han creado nuevos riesgos en línea.

Para las organizaciones sociales, las redes sociales son herramientas vitales para visibilizar sus luchas, informar a sus comunidades y crear una comunidad más sólida. Sin embargo, estas herramientas también pueden ser problemáticas si no se toman medidas para protegerse.

Para ayudar a evitar estos problemas, este manual proporciona prácticas y recomendaciones sobre aspectos de seguridad digital básica para la gestión segura de las redes sociales.

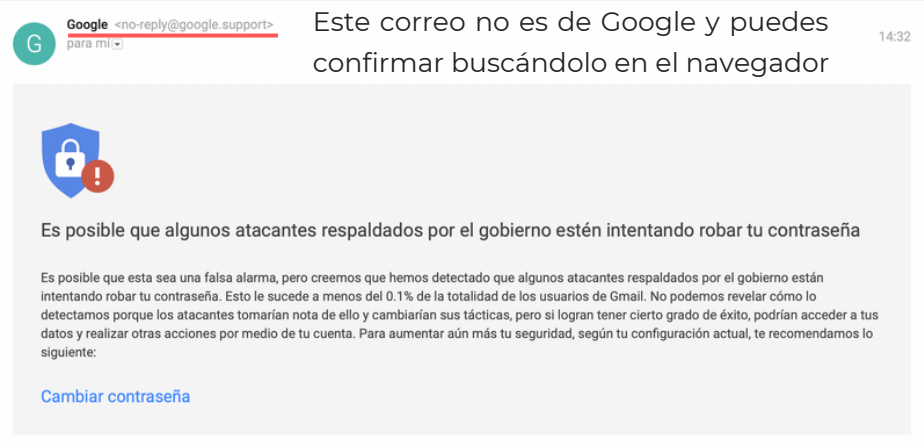
Prácticas para lograr mayor seguridad digital

- Crea contraseñas seguras. ¿Cómo? Piensa en tu plato favorito, o tu canción favorita. Una frase larga es más difícil de adivinar. Si quieres saber qué tan segura es tu contraseña, verifícalo en este link: https://howsecureismypassword.net
- No compartas información personal, como números de teléfono, direcciones o información financiera en las redes sociales. Y asegúrate que quien lo solicita no use una cuenta falsa.
- Desactiva la geolocalización de tus publicaciones para evitar que otros sepan tu ubicación exacta y evitar futuros rastreos.
- Antes de abrir una URL, verifica que esta sea real y tenga siempre un protocolo SSL (https).
- Usa una VPN para acceder a las redes sociales, especialmente si estás en una red pública.
- Activa la autenticación de dos factores (2FA) para todas las cuentas Esto proporcionará una capa adicional de seguridad al requerir un código de acceso adicional al iniciar sesión.
- Limita el acceso a la información confidencial solo a los miembros que necesiten tenerlo. Así, evitar que caiga en malos manos y desarrollar una Política de Seguridad Interna es una buena práctica.
- Instala un antivirus en todos tus dispositivos y mantenlos siempre actualizados para que cumplan con su labor.
- Nunca uses dispositivos desconocidos para acceder a tus redes sociales. Si es una emergencia, usa un navegador en modo incógnito, y asegúrate de cerrar la sesión después de eso.

Identificar estafas o malware

Son muy fáciles de identificar, si prestas atención a los detalles.

Por ejemplo, si recibes un correo electrónico o mensaje que solicita información personal, como tu nombre de usuario y contraseña o tu número de tarjeta de crédito, debes tener cuidado. Las empresas legítimas nunca solicitan información personal a través de correos electrónicos no solicitados o mensajes de texto. Es importante revisar el correo electrónico que envía este mensaje, como se ve en el siguiente ejemplo:



Por otra parte, algo muy común ahora es recibir un enlace por correo, WhatsApp o en publicaciones en redes sociales. NO HAGAS CLIC EN ÉL. Si el enlace parece sospechoso o no conoces la URL que se muestra, no lo abras porque puede ser un intento de phishing.

Estos sitios duplicados son más difíciles de identificar, pero puedes verificar que el dominio utilice cifrado para transmitir los datos (protocolo HTTPS). Esto último, aunque no es garantía de la legitimidad de un sitio, sí es requisito indispensable y, por lo general, el navegador te advertirá si no lo tiene.

Aprende más aquí: https://phishingquiz.withgoogle.com

Otros consejitos más...

Cuando no uses tu webcam, tápala, ponle un sticker o un post-it. Así evitarás que alguien pueda espiarte. Por extraño que suene, esas cosas pasan.

Complica el acceso a tu computadora o a tu celular usando claves fuertes y evitando reconocimientos faciales o huellas digitales.

Revisa el registro de accesos y actividad de tu correo o red social, para saber que dispositivos han iniciado sesión. Te recomendamos cerrar las sesiones que no conozcas.

Evita que alguien esté escuchando tus conversaciones sin tu permiso. Si tienes un par de audífonos que no te funcione, corta el conector y colócalo en el puerto de tu computadora cuando no lo estés usando.

Realiza copias de seguridad periódicas de toda tu información en un lugar seguro. Así, si algo se pierde, tienes un respaldo al que acudir.

Entérate si tu información, contraseña y otros datos han sido filtros en:

https://haveibeenpwned.com