CIBERSEGURIDAD
Universidad Nacional del Comahue

Recomendaciones de Seguridad para el Uso de Mensajerías Instantáneas

Aplicando estas recomendaciones, puedes proteger tu privacidad y seguridad al usar aplicaciones de mensajería instantánea frente a riesgos como phishing, robo de datos o malware.

- Ignorar archivos sospechosos o no solicitados: No abras archivos enviados por contactos desconocidos o inesperados, ya que podrían contener malware o software malicioso.
- Transmite información sensible solo si la comunicación es cifrada de extremo a extremo: Asegúrate de utilizar aplicaciones que ofrezcan cifrado de extremo a extremo, como WhatsApp, Signal o Telegram en modo secreto, para proteger la privacidad de tus mensajes.
- Mantén actualizado el software de mensajería: Las actualizaciones incluyen parches de seguridad que corrigen vulnerabilidades. Usa siempre la última versión de la aplicación.
- Verifica solicitudes fuera de lo común por medio alternativo: Si alguien te pide información sensible o acciones inusuales, confirma su autenticidad a través de una llamada telefónica u otro canal confiable.
- Resguarda los códigos de validación de acceso: No compartas códigos de verificación con nadie, incluso si parece ser un contacto confiable. Estos códigos son personales y permiten proteger tus cuentas.
- Desconfía de llamadas sospechosas o intimidantes: Si recibes una llamada que genera sospecha o te exige información personal, corta la comunicación y verifica la autenticidad por otro medio.
- Ignora links sospechosos, incluso si provienen de contactos conocidos: Antes de hacer clic en un enlace, asegúrate de que sea legítimo. Los contactos pueden haber sido hackeados y los enlaces podrían dirigir a sitios maliciosos.
- Verifica las fuentes de información: Ciber-delincuentes a menudo se hacen pasar por instituciones oficiales, bancos o empleadores. No compartas información ni accedas a enlaces sin confirmar su legitimidad.
- Activa la autenticación en dos pasos (2FA): Habilita el 2FA en las aplicaciones de mensajería para añadir una capa extra de seguridad a tus cuentas.

- Evita compartir datos personales en grupos o chats generales: No publiques datos como números de cuenta, direcciones o identificaciones en chats grupales, ya que pueden ser vistos por personas no deseadas.
- Configura la privacidad de tu perfil: Ajusta las configuraciones de la app para que solo tus contactos puedan ver tu foto de perfil, estado o última conexión.
- No confíes en ofertas o premios enviados por mensajes:Los sorteos y premios falsos suelen ser trampas para robar información personal o bancaria.