Identificando timos y otros riesgos en servicios de mensajería instantánea

"He recibido un mensaje por WhatsApp el cual dice que puedo ganar un cupón de 50€ para gastar en una famosa tienda. Supuestamente solo tengo que rellenar una pequeña encuesta para obtenerlo y reenviar la promoción a 10 de mis contactos, ¿debo creérmelo?"

WhatsApp y el resto de aplicaciones de mensajería instantánea incorporan muchas funcionalidades: enviar/recibir mensajes de texto, vídeos, fotos… y como tal, están expuestos a los mismos riesgos asociados a otros servicios de Internet como el correo electrónico y las redes sociales: spam, bulos, timos, estafas, malware, etc.

Cómo identificar elementos sospechosos que deben ponerte en alerta

Conocer las estrategias de engaño que utilizan los ciberdelincuentes te puede ayudar a evitar caer en sus trampas. Presta atención si recibes:

- ***Mensajes de contactos desconocidos***
  - *Si no le conoces, mejor no le agregues.*
- ***Enlaces a páginas web***
  - *No hagas clic si no sabes a que página te redirige, mucho menos si se trata de un enlace acortado.*
- ***Bulos y mensajes en cadena***
  - *No los reenvíes. Contrasta la información y asegúrate que la información que te está llegando es veraz. Pon especial atención si el mensaje:*
    - ***Es alarmista***
      Si no haces lo que te piden, pasará algo.
    - ***Solicita información privada***
      Datos personales, bancarios, etc.
    - ***Contiene premios/cupones/sorteos***
      Te prometen algo simplemente por rellenar una encuesta, descargar una aplicación, facilitar tu número de teléfono, etc.

Consejos y recomendaciones

¿A qué otros riesgos te expones cuando utilizas aplicaciones de mensajería instantánea?

Riesgos de privacidad

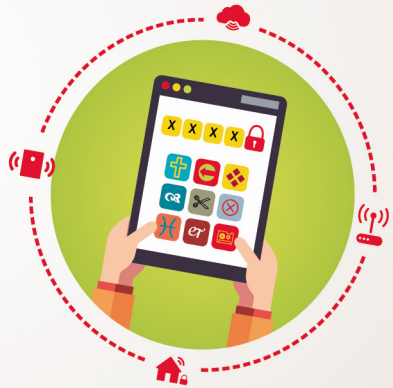
- *Si no quieres que una información sobre ti se haga pública, mejor no la difundas a través de un chat, no sabes lo que tus contactos podrían hacer con ella. Algunos consejos:*
  - ***Foto de perfil***
    Busca una que no sea muy comprometida.
  - ***Bloqueo de usuarios***
    Decide con quién quieres mantener comunicación y con quién no.
  - ***Información de estado***
    No utilices tu estado para facilitar información privada sobre ti.

Foto de perfil | *Bloqueo de usuarios* | *Información de estado*

- *Asegúrate de que el intercambio de mensajes esté cifrado, así, aunque alguien los intercepte, no podrá comprenderlos.*
- *Haz uso de la opción de chat privado y/o secreto y evita que personas ajenas a la conversación puedan espiarla.*
- *Realiza copias de seguridad sino quieres perder los mensajes de chat.*

Suplantación de identidad

Las apps de mensajería instantánea en smartphones no suelen pedir usuario y contraseña cada vez que las utilizamos. Esto significa que, en caso de pérdida o robo, la persona que se haga con el dispositivo podría enviar mensajes a todos los contactos de la víctima haciéndose pasar por ella.



- *Establece una contraseña de bloqueo en el smartphone, así impedirás que lo utilicen sin tu consentimiento.*