Cápsulas de tecnologías de la información de la Coordinación de Sistemas de Cómputo · Por Cuauhtémoc Vélez Martínez

Seguridad en redes sociales

Sin duda alguna, en los últimos años las redes sociales se han convertido en un medio de comunicación masivo y en muchos casos, necesario. Como es sabido, su función básica es compartir información de diversa índole (comentarios, fotografías, ideas, imágenes, videos, entre otros), llegando casi de manera inmediata a los destinatarios estableciendo una interacción peculiar e innovadora.

De acuerdo a un estudio realizado por la Asociación Mexicana de Internet, durante abril del 2015, el 85% de los usuarios mexicanos (de una muestra de 1662 individuos), utilizó internet para acceder a las redes sociales poniendo por primera vez a este servicio como puntero en las estadísticas (comparado con el 2014 que fue del 77%). Este incremento ha provocado que los malhechores volteen a ver con lupa las vulnerabilidades existentes en las redes sociales, en particular las de uso más común en México como Facebook, Twitter, YouTube e Instagram.

Symantec, empresa dedicada a la seguridad informática, publica cada año un reporte de amenazas, señalando durante el 2015 algunas como:

- ***Manual sharing*** (compartir manualmente): desafortunadamente, los mismos usuarios consciente o inconscientemente, se encargan de expandir amenazas al compartir videos, fotos o comentarios de forma manual conteniendo ligas a sitios maliciosos o ejecución de *malware*. Durante 2014, el *manual sharing* llegó al 70% del total de amenazas en redes sociales, cifra alarmante pues denota poca importancia o conocimiento en temas relacionados con riesgos y amenazas en redes sociales.
- ***Fake offering*** (ofertas falsas): este tipo de engaños busca invitar a los usuarios de redes sociales unirse a ciertos grupos que ofrecen regalos a cambio de información personal (como correo electrónico). Esta amenaza alcanzó el 23% en el 2014; aunque es una cifra elevada, disminuyó 58 puntos porcentuales con respecto al año anterior.
- **Ingeniería social:** los hackers utilizan métodos de persuasión para obtener información sensible. Por lo general buscan ser amigables, comprensivos o serviciales logrando un nivel de confianza elevado sobre su víctima potencial haciendo que después de un tiempo, sea sencillo lograr su cometido.

- **Contraseñas débiles y duplicadas**: por desgracia, sigue existiendo la mala costumbre de crear contraseñas poco seguras haciéndolas muy evidentes y fáciles de adivinar, persistiendo el nombre de la mascota, el apellido del usuario, fecha de nacimiento o las placas del automóvil. Asimismo, es recurrente el uso de la misma contraseña en más de una plataforma siguiendo los mismos criterios básicos de asignación. Una contraseña débil, permitirá al delincuente acceder al perfil del usuario y obtener información delicada que más adelante utilizará para cometer fechorías.

Algunas de las recomendaciones que permitirán reducir el riesgo de ataques son:

- **Utilizar filtros de seguridad:** ofrecidos por las redes sociales para que únicamente las personas que el usuario haya elegido, sean las que accedan a los recursos autorizados por su propietario.
- **Aceptar contactos conocidos**: en ocasiones, los usuarios compiten por tener el mayor número de "amigos" o contactos, y aceptan a todos aquellos que realizan una solicitud de amistad. Es muy importante entender que no toda la gente tiene buenas intenciones y que muchos usuarios crean perfiles falsos para acceder y obtener fácilmente información que en ocasiones, es confidencial (hábitos de consumo, datos familiares, relaciones interpersonales o laborales, información financiera, entre otros).
- **No dar clic en enlaces sospechosos**: es muy común que entre usuarios se compartan ligas en sus muros para acceder a páginas web que muestran imágenes o videos. En ocasiones, estos links pueden redirigir al usuario hacia páginas sospechosas o de dudosa procedencia. Aquellas ligas, propaganda, u ofrecimiento de dinero a cambio de nada, deben ser evitados.
- **Utilizar contraseñas robustas:** para impedir que delincuentes cibernéticos intenten acceder a las cuentas de usuarios, es importante tener una contraseña adecuada. Normalmente se recomienda que sea de al menos ocho caracteres, incluyendo siempre una mayúscula y un dígito empleando palabras con poca o nula vinculación con el usuario.

Por último, es esencial comprender que antes de publicar cualquier foto, comentario o video, será visto por mucha gente y aunque sea eliminado, seguramente habrá alguien que lo haya replicado en algún otro sitio, descontextualizando su contenido con la posibilidad de ser mal interpretado o utilizado indebidamente en contra del mismo usuario.

Las recomendaciones anteriores, más el sentido común (además de contar con antivirus y sistema operativo actualizados) permitirán navegar a través de las redes sociales de forma más segura y confiable.