DOCENTE: RICARDO SANCHEZ **AREA: TECNOLOGIA E INFORMATICA**
GRADO: OCTAVO
FECHA DE INICIO: Agosto 18 **FECHA DE FINALIZACIÓN: Septiembre 25**

MATERIALES COMPLEMENTARIOS:
Grupo de Facebook SOMOS ACADEMICO 8

RECEPCION: Entrega de trabajos on line (programados una guía por semana)
A los correos electrónicos: ricardosanchez@ieacademico.edu.co o somosacademico@gmail.com

- **En el asunto del correo colocar nombre completo y grado al que pertenece.**
- **CELULAR: 3228499405 (Atención de 7 am a 1:00 pm- lunes a viernes)**

GUIA 01
TIK TOK PROGRAMA ESPIA

Anonymous asegura que Tik Tok fue creado como programa espía por el Gobierno de China
Según asegura el grupo de hackers, la aplicación recopila y retransmite información al país asiático sin el consentimiento de los usuarios.
La red de usuarios de Tik Tok abarca a más de 800 millones de personas y ya se contabilizan más de 2 mil millones de descargas en todo el mundo. La app de medios de ios y Android permite crear y compartir videos cortos, pero el fin principal -según Anonymous- apunta a recopilar información y retransmitirla a una entidad externa, sin el consentimiento de los usuarios.
Para algunos especialistas, Tik Tok -conocida en China como Douyin- "no es spyware. La gente que la instala acepta compartir sus datos. El tema es que la aplicación tiene al Gobierno chino entre sus inversores y se supone que el Partido Comunista del país asiático recibe los datos de los usuarios"

En cambio, Anonymous considera que la supuesta plataforma de espionaje permite, por ejemplo, revelar hábitos de navegación e información personal, mostrar anuncios e instalar marcadores de teléfonos. El colectivo surgido en 2008 del foro Hackers y del sitio 4chan logró comprobar en 2019 que las máximas autoridades de China habían colocado aplicaciones spyware en móviles de turistas, para controlar sus movimientos durante sus estadías.

Anonymous ha creado su teoría a partir de un tuit de un usuario de Reddit que hizo ingeniería inversa de la aplicación. A partir de ese proceso afirma haber descubierto que Tik Tok, aplicación de moda durante el confinamiento, recopila datos que van desde información sobre el teléfono, sobre otras aplicaciones, uso de la memoria o espacio del disco...

ACTIVIDAD

Basados en la lectura.
¿Cree Ud en esta información y en que existen mas aplicaciones que te roban la información?
Argumente su respuesta.

GUIA 02
ROBO DE INFORMACION EN LA INTERNET

A la hora de navegar por la red podemos ser víctimas de **múltiples tipos de ataques** que comprometan nuestra privacidad y seguridad. Esto es algo que afecta tanto a usuarios particulares como a empresas. Sin embargo, estas amenazas pueden estar dirigidas de formas muy diversas. En ocasiones buscarán dañar nuestros equipos, otras puede que introducir malware capaz de obtener beneficio (ransomware, mineros de criptomonedas…), mientras que en otras ocasiones el objetivo principal es nuestra **información**. Precisamente esto último es lo que ha aumentado considerablemente en los últimos tiempos.

La información personal, objetivo de los piratas informáticos

En los últimos tiempos la **información y datos de los usuarios** han ganado valor de cara a los piratas informáticos. Cada vez utilizan más métodos para lograr el robo de datos a la hora de navegar por la red. De hecho un informe de Positive ha alertado del aumento de un 61% en el robo de datos.

Hay que mencionar que no solo afecta a la información personal, a los datos de los usuarios particulares; también está muy presente en las empresas. Los ciberdelincuentes buscan la manera de **obtener información privilegiada** de los negocios, así como recopilar todos sus movimientos.

Tener información es tener valor. Esa es una realidad, ya que hoy en día los **datos de los usuarios** son muy cotizados en Internet. Uno de los motivos principales es para llevar a cabo campañas de marketing. Nos incluyen en listas para poder ofrecernos productos en función de una serie de factores como pueden ser nuestros gustos, edad, dónde vivimos, por dónde nos movemos…

Ahora bien, los métodos para obtener toda esta información en ocasiones sobrepasan la línea de lo ético y legal. Ha habido casos en los que plataformas importantes han comercializado con los datos de sus clientes o usuarios. Por ello también corresponde a los propios usuarios tomar medidas para evitarlo.

Cómo evitar que roben nuestra información en la red

Por suerte podemos tener en cuenta una serie de consejos interesantes para evitar que roben nuestros datos e información en la red. Vamos a dar una lista de lo que consideramos imprescindible si queremos protegernos al navegar por Internet.

Proteger nuestras cuentas

Sin duda un paso principal es **proteger nuestras cuentas** correctamente. Con esto nos referimos a utilizar contraseñas que sean fuertes y complejas. Una manera de evitar posibles intrusos que recopilen información o que puedan hacer uso de nuestra cuenta.

Es necesario que la clave tenga letras (mayúsculas y minúsculas), números y otros símbolos especiales. De la misma manera es vital que esa contraseña sea única y que la cambiemos de manera periódica para ampliar aún más la seguridad.

Cuidado con el Spam

El **Spam** es uno de los métodos que utilizan los piratas informáticos para poder obtener información de los usuarios. Un correo Spam puede ocultar un ataque Phishing a través del cual puedan robar datos importantes. Es importante que nunca contestemos a un correo de este tipo. Tampoco debemos descargar ningún archivo que tenga adjunto o acceder a links que puedan ser una estafa.

Utilizar una configuración correcta de la privacidad.

Los piratas informáticos pueden recopilar información personal de los usuarios a través de keyloggers o troyanos. Es importante que evitemos la entrada de este tipo de malware.

ACTIVIDAD

Basados en la lectura.

¿Que Otros métodos de prevención para el robo de información conoce?

GUIA 03
ESPIONAJE POR EL CELULAR

La tentación está ahí: un familiar se olvida el móvil sobre la mesa y surge la curiosidad de husmear en el WhatsApp, las llamadas recibidas o qué páginas web ha visitado esta persona, sobre todo si surgen dudas sobre la fidelidad en pareja. Esta tentación no es nueva pero más allá de hacerse con el móvil de la víctima y navegar por su contenido, ahora hay herramientas que hacen ese trabajo sucio sin el conocimiento (ni consentimiento) de la misma. Este fenómeno tiene nombre y ha sido bautizado como *stalkerware* (algo así como "virus del acosador"), y la mala noticia es que cualquiera puede ser espiado sin tener conciencia de ello. **¿Cómo detectar si el móvil está afectado por este software?**

Aparición de pop-ups inesperados en el navegador
El popular programa de radio en Estados Unidos, Kim Komando, alerta de que una manera de descubrir un móvil víctima de este espionaje es mediante la súbita aparición de ventanas emergentes (*pop-up*) en el navegador. Se trata de comportamientos fuera de lo habitual que no deberían ser minimizados por la víctima. Del mismo modo, un súbito incremento del *spam* en el correo electrónico y la recepción de mensajes de texto de desconocidos con excesiva frecuencia deberían ser motivos para disparar las alarmas.

¿Desapareció temporalmente el móvil?
Si el comportamiento extraño de un dispositivo ha sido precedido de una pérdida temporal del mismo (por ejemplo, se deja en una habitación y tras buscarlo, aparece tras unas horas en otra), este terminal es susceptible de haber sido sustraído temporalmente para instalar estos programas. Los expertos nos recuerdan que hacen falta unos minutos con el móvil en la mano para instalar estas apps.

La batería de pronto dura mucho menos
Un móvil con *stalkerware* trabaja mucho más que uno limpio, y esta actividad tiene su lógico impacto en la duración de la batería. Si se detecta un súbito descenso del rendimiento de la misma, acompañado de alguno de las otras situaciones mencionadas anteriormente, hay que sospechar y tomar las medidas necesarias.

El móvil se recalienta constantemente
Como continuación del consumo de la batería, un móvil afectado por este mal tiene que desempeñar muchas más tareas que otro *limpio* y esto deriva asimismo en un incremento de la temperatura del mismo.

Instalar apps fuera de las tiendas de aplicaciones
No se trata de un síntoma en sí, pero si se detecta alguno de estos comportamientos atípicos tras haber instalado una aplicación fuera de las tiendas oficiales (App Store o Google Play), la posibilidad de que el terminal haya sido infectado se dispara. Tanto Apple como Google se toman muy en serio la seguridad de sus plataformas, y por ello es extremadamente recomendable instalar apps de sus tiendas oficiales. La buena noticia para los dueños del iPhone es que este dispositivo es difícilmente vulnerable a este ataque puesto que Apple obliga a instalar todas sus apps a través de la tienda; Android es más susceptible de ser atacado porque es factible instalar aplicaciones fuera de control de Google.

ACTIVIDAD

Basados en la lectura.

¿Según Ud., cuál cree que son los métodos más eficaces para evitar el espionaje de su celular?

GUIA 04
FAKE NEWS

Las 'fake news' están por todas partes: son noticias falsas, bulos o rumores que no se han confirmado pero que recorren internet a la velocidad de la luz.
El último gran fichaje (falso) de un equipo de fútbol, un león que se comió a un turista de safari, cotilleos sobre estrellas de cine y televisión, imágenes de unos disturbios que en realidad sucedieron hace años…
Las *fake news* nos llaman la atención porque están protagonizadas por instituciones o personajes públicos que han hecho o dicho algo controvertido, o bien relatan hechos sorprendentes.
Suelen ser noticias polémicas, que provocan la indignación de la sociedad en general.
Existen diferentes tipos de *fake news*, pero todas tienen un elemento común: en seguida se convierten en noticias virales a pesar de ser falsas.
Difundir noticias falsas puede tener consecuencias muy graves, desde difamar a una persona y destruir su reputación (con todos les efectos que ello conlleva a largo plazo), hasta influir en la opinión pública o provocar alarma social.
La información es un arma muy poderosa en política, por ejemplo. Los rumores y noticias falsas se elaboran para perjudicar al resto de partidos o movimientos ideológicos.

En otros casos, algunas personas se inventan rumores sobre actos violentos o disturbios simplemente para divertirse mientras provocan el pánico. Aunque no tengan credibilidad, estas noticias se comparten rápidamente por las redes.

A menudo, las autoridades públicas y gobiernos tienen que desmentir estas informaciones… aunque, para entonces, ya hayan llegado a mucha gente.

Evitarlas: Combatir las *fake news* es sencillo: solo hay que utilizar el sentido común. Hay una serie de comprobaciones que puedes realizar fácilmente y que te permitirán confirmar la veracidad de una información: la fecha en que se publicó, si hay faltas de ortografía o errores en el texto, si las imágenes están pixeladas o parecen retocadas…

Otro aspecto a tener en cuenta es la fuente de información: ¿es un diario reconocido, un portal web oficial o un blog con pocos seguidores? Si no estás seguro, es mejor contrastar la información con otros medios más fiables.

Las noticias falsas no solo afectan a los ciudadanos: hay muchos medios de comunicación y periodistas que se han creído los bulos que corrían por internet.

Lo más importante es leer la información con una mirada crítica, sabiendo que no todo lo que se publica en internet es real. Antes de publicar o compartir una información, asegúrate de que sea verdad y reflexiona sobre las consecuencias que podría tener.

ACTIVIDAD

Basados en la lectura.

¿Que otras formas para evitar las Fake News conoce o cree se debe implementar?

GUIA 05
STARTLINK INTERNET MUNDIAL

La constelación de satélites de Elon Musk, Starlink, está a punto de comenzar a proveer de servicio de internet en Estados Unidos.
Aunque Elon Musk es más conocido como dueño de Tesla y por querer enviar humanos a Marte, tiene en su haber más proyectos en plena fase de desarrollo y despliegue. Uno de ellos es la creación de Starlink, una **constelación de satélites** capaces de proveer de conexión e internet en cualquier parte del mundo.
Algo similar a lo que ya se oferta a través de la conexión satelital en algunos teléfonos muy específicos a la vez que caros, pero con la ventaja de un menor coste para el usuario. Además, el internet satelital actual no tiene unas especificaciones muy avanzadas en lo relativo al ancho de banda y Musk quiere terminar con esto a golpe de lanzamientos espaciales. El último ha sido un **paquete de 60 satélites** y planea tener más de 40.000.

Los planes de Musk: El proyecto que desarrolló el bueno de Elon en un primer momento nada tiene que ver con lo que es hoy en día. Las primeras informaciones de **Starlink** datan del 2015 y consistía en lanzar 4.000 satélites en una órbita baja cercana a la superficie de la Tierra. Pero pronto comenzó a pedir ampliaciones del número de satélites a la autoridad competente hasta llegar los casi 42.000.

Satélites de Starlink SpaceX
Según el propio Elon Musk, se necesitan alrededor de 400 satélites orbitando para proveer de una conexión a internet de calidad menor y 800 para ofrecer una cobertura confiable de calidad media. Actualmente y a falta de datos oficiales, Starlink tiene 240 satélites en servicio y **espera comenzar a ofrecer un servicio comercial este mismo año** en Estados Unidos y Canadá.
Cómo funciona
El sistema de Starlink se basa en la propagación de las ondas electromagnéticas por el vacío, donde consiguen una **velocidad muy superior a cualquier conexión terrestre** por fibra óptica de hoy en día. Concretamente un **47% más rápido**, de acuerdo a un estudio de la Universidad de Florida, que será aprovechado para eliminar una de sus desventajas: el enorme recorrido que tiene que viajar nuestra información.
Aunque el secreto del éxito de la constelación de Musk está en la altura a la que orbitarán sus satélites. Los sistemas de internet satelital actuales se encuentran emplazados en **órbitas situadas a 35.000 kilómetros** y el retardo es tan grande que la solo sirve para algunas **conexiones no muy exigentes**, según recoge *Space*.

ACTIVIDAD

Basados en la lectura.

¿Qué ventajas y desventajas según UD ofrece este proyecto de conectividad?