☑ **E.P.E.T. N° 7**

☑ **Docentes**: Olivieri, Leonardo-Zarate, Daniel

☑ **Año**: 2° **Div**: **1º, 2º y 3º**

☑ **Ciclo**: Básico

☑ **Turno**: Mañana y Tarde

☑ **Espacio Curricular**: Informática

☑ **Título de la propuesta**:

"Ciberataque y Seguridad Informática"

GUÍA PEDAGÓGICA PARA LA FORMACIÓN GENERAL

Queridos estudiantes ¡esperamos que se encuentren muy bien! Les enviamos una serie de actividades, a través de la guía N°7. Les pedimos el mayor compromiso posible ya que la mismas serán evaluadas cuando reanudemos las clases presenciales.

Objetivos:

- Aprender los conceptos básicos relacionados con el mundo de la seguridad informática.
- Describir cuáles son los principios básicos de la seguridad.

Capacidad General: Aprender a Aprender

Capacidad Especifica: Reflexión sobre los propios procesos.

Contenidos a trabajar:

Eje 2-Delitos Informáticos. Fraude Informático.

Bibliografía:

Santillán, J.V. (2016). Informática I, Serie Integral por competencias.D.F.

DESARROLLO DE LA PROPUESTA

Caso práctico:

- Lee el siguiente artículo y responde a las preguntas que se hacen a continuación del mismo.

La compañía de seguridad para Internet BitDefender ha localizado un nuevo fraude en la red social Facebook que utiliza para propagarse el etiquetado en las fotos que permite dicha red social.

El método utilizado es el siguiente: un usuario es etiquetado en una foto de una chica joven y vestida de manera provocativa. Junto a esa foto, se incluye un mensaje que dice: "Descubre quiénes son tus principales seguidores", junto con un *link* para utilizar una aplicación que permitiría conocer esa información.

Si el usuario pincha en el *link*, será redirigido a una aplicación que, por un lado, le pedirá su nombre de usuario y contraseña y, por otro, le pedirá permisos para publicar mensajes en su muro y para acceder a su lista de contactos en Facebook. Una vez haya introducido los datos y dado permiso a la aplicación, esta mostrará un mensaje de error, señalando que no está disponible en ese momento.

Sin embargo, inmediatamente, comenzarán a publicarse nuevas fotos en la galería del usuario en la que serán etiquetados todos sus amigos. Además, en el muro de estos aparecerá que alguien les ha etiquetado en esa foto, junto con el comentario inicial ("Descubre quiénes son tus principales seguidores") más el *link* que conduce a la aplicación falsa.

En el momento en que uno de esos amigos pinche en el *link* e instale la aplicación creyendo que su amigo ya la ha aprobado y que se la está recomendando, el proceso volverá a comenzar. De esta manera, la aplicación consigue un efecto viral, propagándose por la red social.

Fuente: Europa Press. Madrid. 13/04/11

a) ¿De qué tipo de ataque se trata?

b) ¿Qué recomendaciones darías para evitar esta situación?

c) ¿Cuáles son las fases que se observan en un ataque informático?

Ataques

Un ataque es una acción que trata de aprovechar una vulnerabilidad de un sistema informático para provocar un impacto sobre él e incluso tomar el control del mismo. Se trata de acciones tanto intencionadas como fortuitas que pueden llegar a poner en riesgo un sistema. De hecho, en alguna metodología como MAGERIT ***(MAGERIT es la metodología de análisis y gestión de riesgos desarrollada por el Consejo Superior de Administración Electrónica. Es un método formal adoptado por las Administraciones Públicas para investigar los riesgos que soportan los sistemas de información y recomendar las medidas adecuadas que deberán adoptarse para poder controlar dichos riesgos)***, se distingue entre ataques (acciones intencionadas) y errores (acciones fortuitas).

Como ejemplos de ataques, podemos citar la utilización de programas para conseguir acceso al servidor de forma ilegítima o la realización de ataques de denegación de servicio para colapsar el servidor.

Normalmente un ataque informático pasa por las siguientes fases:

– Reconocimiento. Consiste en obtener toda la información necesaria de la víctima, que puede ser una persona o una organización.

– Exploración. Se trata de conseguir información sobre el sistema a atacar, como, por ejemplo, direcciones IP, nombres de host, datos de autenticación, etc.

– Obtención de acceso. A partir de la información descubierta en la fase anterior, se intenta explotar alguna vulnerabilidad detectada en la víctima para llevar a cabo el ataque.

– Mantener el acceso. Después de acceder al sistema, se buscará la forma de implantar herramientas que permitan el acceso de nuevo al sistema en futuras ocasiones.

– Borrar las huellas. Finalmente, se intentarán borrar las huellas que se hayan podido dejar durante la intrusión para evitar ser detectado.

En el mercado existen una gran variedad de herramientas de seguridad que permiten conseguir un nivel óptimo de seguridad, pero hay estrategias de ataque que hacen ineficaces a estas herramientas, como las orientadas a explotar las debilidades del factor humano.

Publicidad y correo no deseado

Llamamos correo no deseado a todo correo no esperado por el usuario que lo recibe. Este correo puede resultar muy molesto porque se trata de correo no solicitado que en algunos casos se envía de forma masiva, llegando a saturar la bandeja de entrada de nuestra cuenta de correo de información no deseada.

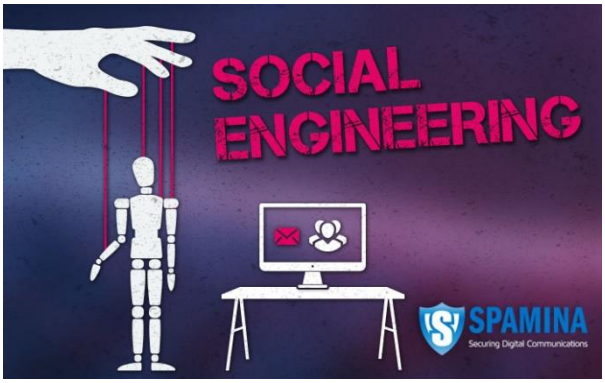
El ***correo electrónico*** es una forma de comunicación rápida, gratuita y fácil de utilizar, por lo que muchas empresas lo utilizan masivamente para darse a conocer al público o presentar algún producto, constituyendo una nueva variedad de correo no deseado, el correo basura o spam.

Con frecuencia, se confunden los términos *correo no deseado y spam*, llegando a utilizarse indistintamente, pero es conveniente distinguirlos correctamente. Ambos están integrados por mensajes enviados al destinatario sin su consentimiento, pero aplicamos el término spam para el correo no deseado que *tiene fines publicitarios o económicos*.

Las intenciones que hay detrás de estos correos son muy variadas. En algunas ocasiones, usuarios malintencionados envían correo no deseado a una gran cantidad de víctimas para propagar software malicioso que puede llegar a darle el control de la máquina al atacante. En otras ocasiones, contienen bromas o mentiras que los autores envían a un conjunto de usuarios con la intención de conseguir repercusión o notoriedad. No obstante, es muy frecuente la utilización de correo electrónico con intenciones comerciales o publicitarias.

- **Explica las diferencias que hay entre correo no deseado y spam. ¿Para qué se utiliza el spam?.....**
- **¿Cómo pueden las empresas obtener beneficios a través del envío de correos electrónicos no deseados?.....**

Ingeniería social.



La mayor parte de las veces, los piratas informáticos no necesitan desarrollar complejos programas para conseguir las contraseñas o los datos bancarios de los usuarios, ya que son estos los que facilitan esta información a los atacantes. **La ingeniería social** es una forma de fraude informático muy utilizado por piratas informáticos y consiste en manipular el comportamiento natural de los usuarios mediante engaños y mentiras, es decir, se vale de métodos que son propios de la condición humana, para obtener alguna información de relevancia, haciéndose pasar por el administrador del sistema de su organización.

Aunque el *correo electrónico* es el método más empleado, también se suelen utilizar mensajes de texto, redes sociales o llamadas de teléfono.

A veces es difícil imaginar hasta dónde puede llegar el contenido que publicamos en Internet. Por suerte, las redes sociales poseen configuraciones de privacidad que nos permiten decidir quiénes pueden ver nuestra información y quiénes no.

Privacidad en redes sociales.

En general, las redes sociales nos ofrecen la posibilidad de decidir con quién queremos compartir la información que publicamos en ellas, mediante lo que se conoce habitualmente como configuración de privacidad.

Sin embargo, de forma predeterminada estas configuraciones no tienen los niveles más restrictivos, lo cual puede causar que parte de nuestra información sea accesible para más personas de las que nos gustaría. Por lo tanto, es recomendable dedicar un tiempo prudencial a ajustarlas y revisar de forma periódica cada una de las aplicaciones que usamos para verificar que solo sea visible aquello que queramos que sea visible.

- **Contestá las siguientes preguntas, pensando en cada una de las redes sociales y aplicaciones que usás a diario. ¿Conocés la respuesta para todas ellas? Responde las siguientes preguntas:**
  - ☑ ¿Quiénes pueden acceder a la información disponible en tu cuenta?
  - ☑ ¿A quiénes aceptás como contactos, amigos, seguidores, etc.?
  - ☑ ¿Resultás fácil de encontrar y reconocer? ¿Tu nombre y/o foto de perfil es visible para todos?
  - ☑ ¿Quiénes pueden escribirte por chat?
  - ☑ ¿Podés bloquear cuentas de desconocidos que intenten contactarte o compartan contenido que te resulta agresivo o desagradable?
  - ☑ ¿Cuánta información pueden ver otras personas sobre vos? ¿Todos pueden ver lo mismo?
  - ☑ ¿Alguna de las redes sociales que usás se vincula con otras cuentas que uses? ¿Publica automáticamente lo que subís en algún otro sitio? ¿Te pregunta cada vez?
  - ☑ ¿Podés ser etiquetado en publicaciones ajenas? ¿Quiénes pueden compartir tus publicaciones?
- **Ingresá a las redes sociales con una cuenta que no forme parte de tus contactos y, una vez adentro, buscá tu nombre y apellido:**

  ¿Con qué te encontraste? ¿Sabías que lo que ves está disponible para cualquier persona?.....

- **Completá la siguiente tabla con tus hallazgos sobre la privacidad de tus datos en las tres redes sociales que utilices con más frecuencia.**

RED SOCIAL	¿QUÉ ENCONTRASTE?	¿SABÍAS QUE ESA INFORMACIÓN ERA ACCESIBLE PARA CUALQUIERA?	¿QUERÉS QUE ESA INFORMACIÓN SEA ACCESIBLE PARA DESCONOCIDOS?

CIERRE

Después de haber realizado las actividades de la presente guía, hacemos una reflexión:

Remarcamos la importancia de la privacidad en línea. Enfatizamos especialmente la importancia de ser conscientes de qué información estamos compartiendo y con quién. En particular, a cuál pueden acceder desconocidos, de forma tal que siempre que compartamos contenido lo hagamos de acuerdo con nuestra voluntad. Reflexionamos, también, acerca de los peligros de no manejar correctamente la privacidad y confiar en las opciones que vienen predeterminadas en las redes.

Evaluación: Puesta en común con los compañeros cuando se retomen las actividades normalmente. Pasar guías al cuaderno de forma escrita (preguntas y respuestas). Si dispones de algún dispositivo electrónico con Microsoft Word, realízalo allí. Enviar fotos o archivo de la guía a los profesores una vez terminada. **Fecha límite de presentación: 01/08/2020**

Recomendaciones:

- Se recomienda que el trabajo escolar se realice en un lugar cómodo y luminoso.
- Realizar pausas cada 40 minutos como si fuesen recreos ya que luego de este tiempo la atención decae. Los recreos deben ser no mayores a 10 o 15 minutos para luego volver a trabajar en el tema solicitado.
- Si utiliza computadora, celular u otro elemento electrónico desvíe la vista cada cierto tiempo para descansar la misma.

- **Prof. Olivieri Leonardo-Teléfono: 2644698669**
  - **Correo: leonardoolivieri843@gmail.com**
- **Prof. Zárate Daniel-Teléfono: 2644523275**
  - **Correo: danusfacu@gmail.com**

Director: Lic. Daniel Ramé