21 Seguridad en Internet: Smishing y Pharming

Otros peligros en la Web, ¡conócelos y protégete!

Nuestra meta

Esta interesante experiencia nos pondrá al tanto del funcionamiento de dos peligros inminentes que existen cuando navegamos en la red: smishing y pharming.

¿Cómo lo haremos?

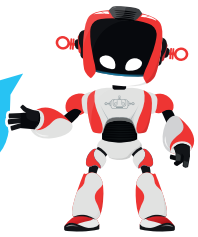
1. A partir de una lectura comentaremos sobre los cuidados que debemos tener al navegar en Internet desde cualquier dispositivo.
2. Mediante dos videos conoceremos el concepto de smishing y pharming como dos amenazas web.
3. Mediante una actividad virtual y un reto en el aula probaremos cuánto hemos aprendido con respecto a estas dos amenazas.

Planifiquemos

Momento	Actividad	Recurso	Tiempo
Inicio experiencia 21	Nuestra meta, ¿Cómo lo haremos?	Libro	10 min
Activando Presaberes	Lectura: "A un clic del peligro"	Libro	5 min
	Actividad en libro	Libro y lápiz	5 min
Aprendamos haciendo	Lectura: "Smishing y pharming"	Libro	10 min
	Video: "Smishing: estafa por mensajes de texto"	Virtualtek: Tutorial código 9-20-01	10 min
	Video: "Cuidado con el pharming"	Virtualtek: Tutorial código 9-20-02	10 min
Manos a la obra	Reto: "Creando protocolo de seguridad"	Computador	25 min
¿Qué aprendí?	Evaluación	Libro	10 min
¿Qué logré?	Autoevaluación	Libro	5 min
Soy creativo	Comparte	Computador	Flexible
Para reforzar	Visita virtual	Virtualtek	Flexible

Ten el valor de

Formarte para ser un ciudadano digitalmente responsable.



Activando Presaberes

A un clic del peligro

La llamada WWW, sigla de la frase World Wide Web, se forma de la interconexión de computadores a nivel mundial. El acceso, de manera ágil, desde cualquier equipo facilita la consulta de todo tipo de información. Esta característica la ha convertido en uno de los más valiosos instrumentos de investigación y desarrollo, porque abre nuevas y económicas posibilidades de comunicación global.

Por esta razón, el volumen de información que circula en la red también abre las puertas a un mundo sin leyes, generando un entorno en el que hay que saber moverse. Riesgos a las injurias y calumnias, riesgos en las comunicaciones, riesgos contra la privacidad y riesgos contra la propiedad intelectual son factores clave de los que hay que protegerse en el proceso de navegación.

En este sentido, el malware o código malicioso, aplicaciones y programas, robo de información personal, como nombres de usuarios y contraseñas, suplantación de la identidad del usuario, entre otros, hacen posible los riesgos mencionados.

Aprendamos haciendo

Smishing y pharming

El Código Penal de 1995 señala en el párrafo segundo el art. 248 del capítulo VI, que: «También se consideran reos de estafa los que con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero».

De acuerdo con este artículo, se consideran estafas dos técnicas usadas en la web con el propósito de obtener un beneficio económico: el pharming y el smishing.

Pharming: este ataque informático modifica o sustituye el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de la plataforma Web 2.0.

¿Sabías que?

Tabnabbing es una técnica utilizada para atacar la seguridad del sistema. Se basa en aprovechar el sistema de navegación por pestañas o tabs.

Normalmente, cuando navegamos en Internet acostumbramos a escribir una dirección en la barra del navegador como www.dagabot.com y entrar rápidamente a este sitio. Sin embargo este nombre que digitamos es producto del servicio DNS que fue creado para facilitar a los usuarios la memorización de una dirección web a través de un lenguaje natural en vez de números.

De esta manera, cuando un computador recibe un nombre de página, lo que realmente hace es interpretar la dirección IP correspondiente. Si un equipo está siendo atacado por la técnica de pharming, al escribir el nombre del sitio web en la barra de direcciones, el navegador redirige automáticamente al usuario a otra dirección IP, donde se aloja una web falsa.

Este tipo de ataque es bastante usado por los delincuentes para lograr la obtención de datos personales de los usuarios de Internet, así como datos de tarjetas de crédito, PIN de usuarios, etc.

Smishing: consiste en una variante fraudulenta del pishing. A través de técnicas de ingeniería social se envían selectivos de mensajes SMS a usuarios de telefonía móvil para que visiten una página web fraudulenta. Mediante reclamos atractivos con alertas urgentes, ofertas interesantes o suculentos premios tratan de engañar al usuario aprovechando las funcionalidades de navegación web que incorporan los dispositivos móviles actuales.

Para lograrlo, envían mensajes a través del teléfono móvil, pidiendo, por medio de textos engañosos, el número de tarjeta y la fecha de caducidad. Con esta información los delincuentes falsifican tarjetas de crédito (skimming) que usan para adquirir productos en el mercado, cargados a la cuenta asociada de la víctima.

Virtualtek

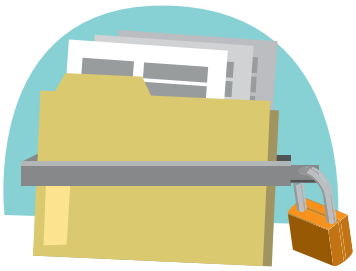
- Visita tu aula virtual y amplia tus conocimientos sobre las técnicas de ataque en la web a través del video " **Smishing: estafa por mensajes de texto** " con código: 9-21-01.
- Luego observa otro video "**Cuidado con el pharming**" con código: 9-21-02 que te instruirá sobre otro tipo de ciberataque.

Para no olvidar

El pharming es una modificación técnica de las direcciones DNS (domain name server)

Manos a la obra

Creando protocolo de seguridad



Ahora que ya conoces la definición y características de los dos ciberataques: smishing y pharming, deberás crear un manual de usuario en donde indiques, mediante un sencillo reglamento, los cuidados que debe tener una persona para evitar ser víctima de estas dos graves amenazas. Puedes usar el software que más te llame la atención.

¿Qué Aprendí?

- Indico los tipos de riesgos a los que se somete un usuario en la web:

  _____.
- Explico el concepto de DNS:

  _____.
- Describo de manera sencilla a qué se refiere el ataque llamado "smishing":

  _____.
- Describo de manera sencilla a qué se refiere el ataque llamado "pharming":_____.
- Planteo una diferencia entre los dos ciberataques smishing y pharming.
- Una posible forma de protegerse ante estos dos ataques es:

  _____

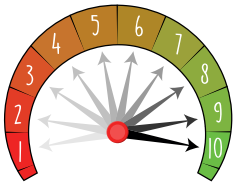
¿Sabías que?

Conviene no acceder a ninguna dirección web que llegue vía SMS, más aún si el remitente es desconocido?

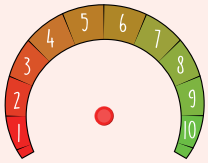
¿Qué logré?

Dibuja la aguja del medidor en el nivel que consideres fue tu desempeño en esta experiencia.

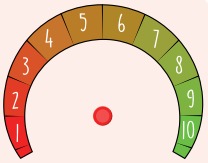
- 7-10: sé hacerlo fácilmente
- 4-6: hago pero se me dificulta
- 1-3: necesito ayuda para lograrlo



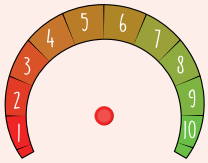
- Conozco los riesgos que existen al navegar en Internet



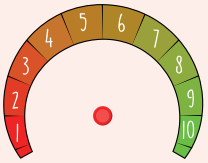
- Entiendo el concepto de smishing y las características de su ataque.



- Defino el concepto de pharming y las características de su ataque.



- Reconozco la importancia de estar atentos al navegar en la red para evitar ataques al sistema.



Soy creativo

Reúno a mi familia y me intereso por invitar a los parientes que usan a menudo el celular y se conectan asiduamente a Internet. Les explico lo aprendido sobre los dos ataques: pharming y smishing.

Para reforzar

Virtualtek

- Visita tu aula virtual y aprovecha los recursos que se encuentran en la sección **"Para reforzar"**.

MIS APUNTES