gms
seguridad de
la información

HACKEAR PERSONAS

La técnica vigente para perjudicar empresas

Conozca el procedimiento criminal que pone en riesgo la seguridad de la información de su organización y los cuatro pasos que se deben seguir para mitigar los riesgos

www.gmsseguridad.com/is.html

David Chiriboga / Jefe de Proyecto
david.chiriboga@gmsseguridad.com
Oficina: +593 2 399-3000 Ext. 7572, 7592
Celular: +593 999 24 14 12
www.gmsseguridad.com

Fuente: Websites informativos y especializados en Seguridad de la Información.

gms seguridad de la información

HACKEAR PERSONAS:

La técnica vigente para perjudicar empresas

Se ha tornado cada vez más acelerada la evolución de las tecnologías que mitigan las vulnerabilidades informáticas. Sin embargo, con demasiada frecuencia, se deja de lado el elemento más importante que está presente en todas las Tecnologías de la Información y de la Comunicación: el ser humano.

Algo tan simple como un correo electrónico engañoso puede ser suficiente para manipular a los responsables de tesorería para que realicen transferencias a cuentas de ciberdelincuentes. Ataques de esta naturaleza no requieren de tecnología avanzada, infraestructura robusta, ni de mayor especialización en informática.

Basta con usar redes sociales para ubicar a los contactos correctos de la empresa víctima, crear una cuenta de correo gratuito, y utilizar las técnicas de ingeniería social al comunicarse con ellos para inducirlos a que realicen acciones que favorecen a los estafadores.

¿Qué es la ingeniería Social?

La Ingeniería Social es el conjunto de actividades o engaños que las personas o atacantes emplean para obtener información o bienes de las organizaciones a través de la manipulación de los usuarios legítimos. En otras palabras, la Ingeniería Social es la ciencia y el arte de hackear a los seres humanos

¿Cómo se utiliza la ingeniería social en los ataques a las empresas?

1. Motivadores psicológicos
2. Objetivo de Ataque
3. Contenido
4. Vector/Medio

www.gmsseguridad.com/is.html

Fuente: Websites informativos y especializados en Seguridad de la Información.

David Chiriboga / Jefe de Proyecto
david.chiriboga@gmsseguridad.com
Oficina: +593 2 399-3000 Ext. 7572, 7592
Celular: +593 999 24 14 12
www.gmsseguridad.com

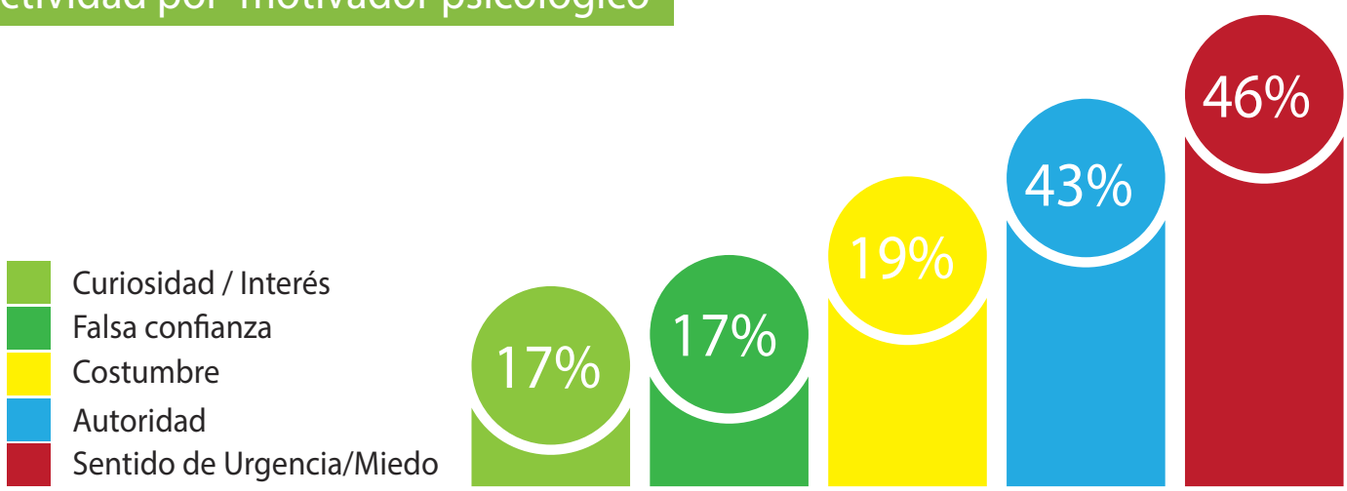
HACKEAR PERSONAS:

La técnica vigente para perjudicar empresas

1. Motivadores Psicológicos:

La clave está en los motivadores psicológicos. GMS, con su plataforma de Gestión de la Ingeniería Social, identificó en 2017 que el sentido de la urgencia y/o del miedo son las características que más efectividad tienen en los ataques (46%). Por ejemplo, cuándo nos notifican que nos van a cerrar la cuenta bancaria si no abrimos el enlace adjunto en el correo electrónico para confirmar el nombre de usuario y la contraseña de acceso, o que nos van a multar por supuestamente haber infringido alguna ley de tránsito, solemos sucumbir al miedo. Por eso estas tácticas son muy utilizadas para robarnos las credenciales de acceso o para descargar un virus en nuestros equipos.

Efectividad por motivador psicológico



El segundo motivador psicológico con alta efectividad es la autoridad (43%). Funciona muy bien cuando recibimos una orden de nuestros jefes; de hecho, así han sido afectadas varias empresas a nivel nacional e internacional. A través de mensajes falsos, en los cuales los cibercriminales se hacen pasar por jefes, se da la orden de realizar transferencias bancarias de manera inmediata a alguna cuenta. Así se han robado millones de dólares: http://www.bbc.com/mundo/noticias-39454968

También tenemos registrados los motivadores psicológicos de la costumbre, la curiosidad y la falsa confianza, que, así mismo, se emplean en algunos ataques.

www.gmsseguridad.com/is.html

Fuente: Websites informativos y especializados en Seguridad de la Información.

David Chiriboga / Jefe de Proyecto
david.chiriboga@gmsseguridad.com
Oficina: +593 2 399-3000 Ext. 7572, 7592
Celular: +593 999 24 14 12
www.gmsseguridad.com

gms seguridad de la información

HACKEAR PERSONAS:

La técnica vigente para perjudicar empresas

2. Objetivo del Ataque:

Los objetivos de ataques más comunes – y, de paso, los más peligrosos – son:

- Fraude: consiste en robar dinero, sin necesidad de utilizar la fuerza (ni verbal ni física). Solamente se requiere un mensaje falso para engañar a la persona responsable de tesorería de una empresa, e inducirla así a realizar una transferencia a la cuenta de un cibercriminal. Una empresa de producción nacional perdió cerca de $100.000 al ser víctima de esta estrategia.
- Infección: las víctimas son engañadas para que descarguen e instalen diferente software malicioso; entre ellos, uno conocido como ransomware, que secuestra la información para después solicitar un rescate económico. Este año, se hicieron notables dos eventos con impacto mundial, uno de ellos denominado WannaCry, que impactó a grandes corporaciones en Europa y Latinoamérica.
- Robo de credenciales: con el cual se desvía a las víctimas a un sitio falso donde se sustraen las claves de acceso de los sistemas personales y corporativos, como correo electrónico, sistemas de pago en línea, plataformas de facturación, entre otros.

En nuestra plataforma de Gestión de Ingeniería Social, tenemos registrado, hasta octubre de 2017 el siguiente comportamiento en la región:

39.5%

Abre el adjunto o sigue el link

N = 946

30.1% Sigue el link

10.4% Llena el formulario

N = 891

100%

Sigue instrucciones de pago a tercero

N = 7

www.gmsseguridad.com/is.html

Fuente: Websites informativos y especializados en Seguridad de la Información.

David Chiriboga / Jefe de Proyecto
david.chiriboga@gmsseguridad.com
Oficina: +593 2 399-3000 Ext. 7572, 7592
Celular: +593 999 24 14 12
www.gmsseguridad.com

HACKEAR PERSONAS:

La técnica vigente para perjudicar empresas

3. Contenido:

Lo cibercriminales pueden registrar varios tipos de contenido dependiendo de lo que más llame la atención de las personas, no olvidemos que pretenden engañar y pueden utilizar varios temas de interés permanentes, temas mediáticos, política, deportes, trabajo, etc. Incluso cuando desean algo específico de una empresa, llegan a conocer los gustos, intereses y hasta deseos de una persona en particular dentro de la empresa, ¿qué pasaría si conocen cómo engañar a la persona encargada de los sistemas o a la persona encargada de efectuar pagos de una empresa?

4. Vector o Medio:

Con una visión clara de los motivadores psicológicos, el objetivo de ataque y el contenido, los criminales determinan el/los vectores (canales o medios de despliegue) sobre los cuales desea realizar los ataques. Los vectores comunes son el correo electrónico, la navegación, las redes sociales, las redes inalámbricas, los dispositivos de almacenamiento, e – incluso – las visitas personales en el sitio de trabajo.

¿Cuál es el impacto de la Ingeniería Social en la Seguridad de la Información?

La Ingeniería Social es una técnica tan efectiva para los ciberdelincuentes que ha llegado a formar parte de la gran mayoría de los ataques dirigidos. Ha superado una incidencia de más del 90% de los casos, según los estudios de diversos líderes mundiales en Seguridad de la Información. En los últimos años, las empresas han perdido miles de millones de dólares con ataques de Ingeniería Social. La tendencia a que los incidentes de seguridad se incrementen son exponenciales, y las cifras pueden ascender a números exorbitantes, puesto que las empresas siguen descuidando el pilar más importante: sus recursos humanos.

www.gmsseguridad.com/is.html

David Chiriboga / Jefe de Proyecto
david.chiriboga@gmsseguridad.com
Oficina: +593 2 399-3000 Ext. 7572, 7592
Celular: +593 999 24 14 12
www.gmsseguridad.com

Fuente: Websites informativos y especializados en Seguridad de la Información.

HACKEAR PERSONAS:

La técnica vigente para perjudicar empresas

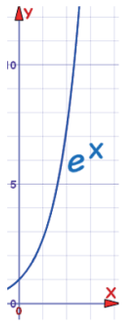
¿Por qué la Ingeniería Social debe preocuparnos?

Actualmente, estamos viendo que la Ingeniería Social es la punta de la lanza para desarrollar los ataques de grandes magnitudes, que siguen afectando a las empresas. Lastimosa y peligrosamente, no se le da la importancia que se merece y se sigue confiando y hasta enfocando la totalidad de la Seguridad de la Información en herramientas tecnológicas. Se adquieren buenos antivirus, firewalls, antispam, etc., pero es imprescindible complementar estos productos con la gestión orientada a los recursos humanos.

Basta que solamente un colaborador de la empresa sea víctima de la Ingeniería Social, para que toda la organización se vea impactada. Se pueden perder cantidades enormes de dinero, se puede infectar con un virus a toda la red, y se puede perder la información confidencial. ¿Qué precio tiene un listado con los datos de los clientes estratégicos o la documentación de los nuevos proyectos o las estrategias comerciales?

¡Es de vital importancia la revisión y la gestión de este tema!

Alerta I-050417-PSA del 04-may-2017 del FBI:



2370%

de incremento en incidentes de enero 2015 a diciembre 2016

$5,3 mil millones

en pérdidas entre enero 2015 y diciembre 2016

https://www.ic3.gov/media/2017/170504.aspx

www.gmsseguridad.com/is.html

David Chiriboga / Jefe de Proyecto
david.chiriboga@gmsseguridad.com
Oficina: +593 2 399-3000 Ext. 7572, 7592
Celular: +593 999 24 14 12
www.gmsseguridad.com

Fuente: Websites informativos y especializados en Seguridad de la Información.

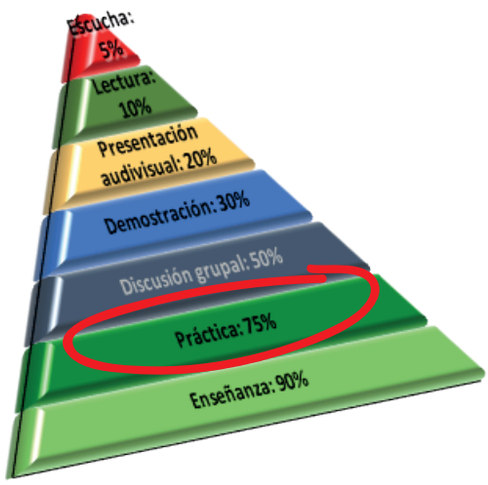
HACKEAR PERSONAS:

La técnica vigente para perjudicar empresas

¿Qué se debe hacer?

Las empresas deben tener en cuenta que, para gestionar su Seguridad de la Información, no basta con revisar y actualizar sus herramientas tecnológicas (erróneamente, se sigue pensando que es lo único en lo que se debe enfocar). Los recursos humanos son un pilar vital dentro de las empresas.

Para evitar que los empleados sean víctimas de la Ingeniería Social, las empresas deben prepararlos frecuentemente para que puedan detectar los ataques que podrían afectar negativamente a la organización. La mejor manera no es mediante actividades eventuales de capacitación. Más bien, se recomienda que la concienciación sea continua, para que, con la práctica, las personas puedan intuir los ciberataques y sepan identificarlos – todo esto en un ambiente controlado.



GMS aporta con esta efectiva concienciación: pone a disposición de las empresas un innovador servicio que incluye una plataforma de Gestión de la Ingeniería Social. Este servicio permite configurar ataques controlados (es decir, que carecen de una amenaza real) y desplegar inmediatamente los mensajes de alerta a los usuarios después de haber sido víctimas. Con el tiempo, no solamente detectarán estos ataques falsos, sino que, además, estarán en la capacidad de detectar los ataques reales. Sabrán qué acciones deben realizar para alertar al departamento encargado de la Seguridad de la Información, y sabrán bloquear las amenazas. El objetivo es transformar al equipo humano del eslabón más débil a verdaderos agentes de detección contra los ataques que ponen en riesgo la Seguridad de Información de las empresas.

www.gmsseguridad.com/is.html

David Chiriboga / Jefe de Proyecto
david.chiriboga@gmsseguridad.com
Oficina: +593 2 399-3000 Ext. 7572, 7592
Celular: +593 999 24 14 12
www.gmsseguridad.com

Fuente: Websites informativos y especializados en Seguridad de la Información.

HACKEAR PERSONAS:

La técnica vigente para perjudicar empresas

Los cuatro pasos para mitigar el riesgo:

1. Ataques controlados: Dado que la práctica por naturaleza genera más conocimiento en las personas, se debe preparar a las personas con simulaciones de ataques. Estos ataques deben imitar las estrategias cibercriminales, pero en un ambiente sin amenazas. Esto hará que los empleados y colaboradores conozcan y aprendan acerca de los ataques.

2. Retroalimentación instantánea: No solamente se debe conocer el número de víctimas de un ataque, sino que cada una de ellas debe hacérsele llegar inmediatamente la alerta que le comunica que ha sido víctima. Ese shock emocional provoca el almacenamiento efectivo del conocimiento en la persona y, por ende, aporta a la verdadera generación de la concienciación. Los métodos antiguos (charlas, capacitaciones esporádicas, entrega de material impreso) tienen baja efectividad.

3. Seguimiento y análisis: Es necesario saber qué factores inciden en que el equipo humano sea víctima, y conocer las dimensiones del motivador psicológico, del objetivo de ataque, del contenido, y del medio. También hay que mantener la visibilidad del perfil del usuario que fue víctima (con datos como función, departamento, edad, género, capacitaciones recibidas, etc.), y de las variaciones en la forma de un ataque (por ejemplo, horario, frecuencia y antecedentes).

4. Regresar al paso 1: Para evitar ser víctimas de virus, ¿solamente se compra la licencia del antivirus por un mes o un año? ¿Sigue teniendo el mismo firewall de hace 5 años? ¿Jamás realizó una inversión adicional para esta herramienta? En el contexto de la seguridad para las empresas, el equipo humano es un sistema al que debemos dar mantenimiento constantemente: ¡no se lo puede descuidar!

Conozca más acerca del impacto que está ocasionando la Ingeniería Social y la manera de gestionar la Seguridad de la Información enfocada al equipo humano de su organización:
https://gmsseguridad.com/ingsocial.html

www.gmsseguridad.com/is.html

David Chiriboga / Jefe de Proyecto
david.chiriboga@gmsseguridad.com
Oficina: +593 2 399-3000 Ext. 7572, 7592
Celular: +593 999 24 14 12
www.gmsseguridad.com

Fuente: Websites informativos y especializados en Seguridad de la Información.