México D.F. a 27 de julio de 2015

ALERTA PREVENTIVA CONTRA LA CIBERDELINCUENCIA No. 030

"DISTRIBUCIÓN DE VIRUS POR REDES SOCIALES MEDIANTE ENLACES DE NAVEGACIÓN"

La Secretaría de Seguridad Pública del Distrito Federal, de conformidad con las atribuciones que tiene conferidas en los artículos 3°, fracciones I, IV y V de su Ley Orgánica, 1, fracción II, y 15, fracciones I y II de la Ley que Regula el Uso de Tecnología para la Seguridad Pública del Distrito Federal, así como en los artículos 3 y 14, fracción IV de su Reglamento Interior de la Secretaría, relativas a realizar en el ámbito territorial y material del Distrito Federal las acciones dirigidas a salvaguardar la integridad y patrimonio de las personas, prevenir la comisión de delitos e infracciones a las disposiciones gubernativas y de policía, así como preservar las libertades, el orden y la paz públicos.

Situación:

Ante el creciente uso de las Tecnologías de Información y la Comunicación (TIC), derivado del monitoreo y reportes recibido en la Policía de Ciberdelincuencia Preventiva de la Secretaría de Seguridad Pública del Distrito Federal, se realizó la siguiente "Alerta de Ciberdelincuencia" a fin de informar las medidas preventivas, ligado a **"DISTRIBUCIÓN DE VIRUS POR REDES SOCIALES MEDIANTE ENLACES DE NAVEGACIÓN".**

Modo de Operación:

- El virus llega por medio de un mensaje de un amigo o conocido en forma de video. Si alguien lo abre, aparecen imágenes de carácter sexual.
- El malware no solo infecta el equipo con troyanos para el robo de información, sino que además solicita instalar una extensión en el navegador para publicar en Facebook de forma automática y seguir propagando el contenido.
- El video solicita descargar la última actualización del plug-in de Flash Player que es falsa. Si el usuario accede a descargar la falsa actualización de Flash Player, bajará un archivo, que contiene cuatro ficheros troyanos, probablemente con la iconografía de Google Chrome.
- El programa malicioso instala una extensión en el navegador para publicar en Facebook de forma automática y seguir propagando el contenido, incluso es probable que después de la instalación de los troyanos, estos podrían permitir que alguien que no sea el dueño del equipo controle la PC de forma remota, de igual manera también robe las credenciales de Gmail mediante pantallas de autenticación falsas.

Recomendaciones:

- Revisar la configuración de la cuenta, entrar en "Biografía y etiquetado" y allí elegir la opción para que cada vez que se nos etiquete en cualquier contenido, se nos pida autorización antes de que el contenido aparezca en nuestro muro.
- Revisar quienes pueden agregar contenido a la biografía
- Es importante confirmar la autenticidad de los enlaces y solicitudes antes de responder o realizar clic sobre cualquier enlace. (Existen extensiones para navegador que pueden mejorar al interactuar en sitios web)
- Mantener las claves de manera confidencial y diferente para cada sitio web. Utilizando claves alfanuméricas
- Es recomendable no abrir archivos adjuntos en correos de desconocidos.
- Evitar responder mensajes en la bandeja de no deseados o promociones no solicitadas.
- Verificar personalmente la situación, siempre Preguntarse, ¿el porqué del mensaje? Evite ser curioso.
- Evite publicar información personal a través de internet.
- Activar los filtro de privacidad en sus cuentas dentro de las diversas plataformas, verificando las extensiones y los privilegios con los que cuenta cada una de las mismas.
- Cualquier duda, contacte a la Policía de Ciberdelincuencia Preventiva a través de sus cuentas en redes sociales.

"Nunca permita la instalación de software complementario si el instalador se encuentra en una página distinta a la del fabricante."

Secretaría de Seguridad Pública
Policía de Ciberdelincuencia Preventiva

Facebook: Cibernética SSPDF
Twitter: #CiberneticaCDMX
Correo: policia.cibernetica@ssp.df.gob.mx
Teléfono 5242 5100 ext. 5086
Centro de Atención del Secretario CAS: 5208 9898