3.2 Datos y ejemplos

ALGUNOS DATOS Y EJEMPLOS QUE EVIDENCIAN FRAUDES Y VIRUS

La última encuesta sobre hábitos de uso y seguridad de Internet de menores y jóvenes en España revela algunos datos en relación a este tema que hemos de tener en cuenta:

- **Uso de antivirus** El 82% de los equipos informáticos están protegidos con software antivirus.
- ***Configuración de perfil en redes sociales.*** El 53,1% de los usuarios de redes sociales tienen costumbre de configurar sus cuentas para que sólo sus contactos puedan acceder a sus perfiles.
- ***Uso de contraseñas.*** El 58,2% de los usuarios hace uso de las contraseñas para proteger sus equipos.
- ***Existencia de virus.*** El 22 % manifiesta haber sido infectado por un virus.
- ***Spam.*** El spam sigue siendo la incidencia más común que sufren los internautas (85%)
- ***Malware.*** Se ha detectado que alrededor de un 60% de los ordenadores están infectados de malware.
- ***Información a desconocidos***. Un 14,3% de las principales incidencias relacionadas con los menores se basan en haber facilitado información personal a desconocidos.
- ***Fraude electrónico***. El 48% de los usuarios ha sufrido alguna vez un intento de fraude electrónico.
- ***Datos personales.*** Existe un alto porcentaje de usuarios (44%) que tiene poca o ninguna confianza a la hora de facilitar sus datos personales mediante un e-mail o un servicio de mensajería instantánea.

A continuación vamos a ver algunos **ejemplos reales de infecciones de virus y fraudes o estafas**:

- La linterna molona

Se trataba de una aplicación que oficialmente ofrecía a los clientes de Android una linterna led para el teléfono, pero que una vez descargada permitía al desarrollador meterse en el terminal ajeno y enviar mensajes a números de tarificación elevada. En concreto, al aceptar las condiciones de uso –que se presentaban en una ilegible letra gris sobre fondo negro–, el usuario autorizaba al fabricante a entrar en el dispositivo y enviar y borrar mensajes, tanto los que llegan como los que se mandan.

El programa publicaba automáticamente un post en la cuenta de Facebook de los usuarios que se lo descargaban. El post contaba las supuestas bondades de la app, un texto que todos los amigos del escritor inconsciente leían con gran entusiasmo creyendo que el autor había sido quien suscribía las líneas.

La aplicación fraudulenta se anunciaba como un programa que "hace brillar el led más que ninguna otra app de linternas y es totalmente gratuita", promesa que atrajo a miles de personas y que, por otro lado, en ningún caso se cumplía.

http://www.elconfidencial.com/espana/2015-03-05/medio-millon-de-estafados-por-una-app-linterna-que-se-suscribia-a-mensajes-premium-sin-autorizacion-del-usuario_722330/

- Vidas infinitas. Panda security descubre un estafa para el juego ‘Top Eleven Be a Football Manager’

PandaLabs han descubierto un malware en Windows que actúa disfrazado de aplicación. En teoría, si la descargamos podremos ganar tokens para el Football Manager con los que comprar jugadores.

Evidentemente, esto no sucede y, si lo que hacemos es seguir las instrucciones que nos dan, no solo no vamos a conseguir tokens gratis para Top Eleven sino que podremos perder el acceso a nuestra cuenta de correo electrónico o de Facebook.

La estafa para conseguir tokens gratis para el Top Eleven se hacía de la siguiente manera: 1º Te descargas esta app desde diferentes foros sobre juegos. 2º Para conseguir el número de tokens que selecciones tienes que insertar tu cuenta de correo electrónico o de Facebook, así como las contraseñas con las que accedes. Finalmente esos datos son enviados a los ciberdelincuentes que los utilizan para hacerse con el control de tu cuenta, impidiéndote el acceso a la misma.

http://www.pandasecurity.com/spain/mediacenter/noticias/estafa-para-top-eleven-football-manager/

- Estafas de falsos “amigos” en Facebook

Usted recibe una solicitud de amigo, pero no tiene tiempo de revisar esta nueva persona y pulsa ” aceptar ” de todos modos. O puede ser que la configuración de privacidad de su página está tan abierta y cualquiera puede verla. De cualquier manera, el estafador utiliza el acceso a su cuenta para ver las imágenes y otros datos de su perfil. Luego crea una nueva cuenta bajo su mismo nombre y la llena de sus fotos, intereses y actualizaciones de estado. Con 500 millones de personas en Facebook en todo el mundo, es poco probable de detectar al impostor.

Después de crear una cuenta duplicada, el estafador envía solicitudes de amistad a sus amigos de Facebook. La gente reconoce su nombre y pulsa ” aceptar “, sin darse cuenta de que la cuenta es una falsificación. No se dan cuenta que algo anda mal hasta que su impostura comienza el envío de solicitudes de dinero y enlaces que son spam.

Los mensajes y los enlaces pueden ser estafas obvias cuando provenga de una dirección de correo electrónico desconocido, pero son mucho más creíbles cuando se comparte por un “amigo” de Facebook. ¡Siempre tenga cuidado con lo que haga clic, sin importar quién la comparte!

http://www.lafamiliadebroward.com/cuidado-con-las-estafas-de-falsos-amigos-en-facebook/

- El virus de la Policía ataca de nuevo al sistema Android

El virus de la policía es uno de los ransomwares más extendidos en los últimos años. Este virus, que está activo desde 2011, “secuestra” todos los archivos del ordenador, argumentando que el usuario ha estado navegando por páginas web pornográficas con contenido infantil, y pide “como multa” 100 € para liberar la información.

Hace varios días apareció una nueva familia de malware para Android, Android/Koler.A. Los medios se hicieron eco del mismo ya que era un ataque del tipo del “Virus de la Policía” / ransomware, parecido a los que hemos visto en ordenadores Windows, aunque en esta ocasión estaba dirigido a teléfonos móviles.

En este caso, el malware no es capaz de cifrar los datos del teléfono, pero aún así es bastante molesto y difícil de eliminar (si no cuentas con antivirus para Android) ya que el mensaje que muestra en pantalla está encima de todo lo demás y el usuario sólo dispone de unos pocos segundos para intentar desinstalarlo.

http://www.pandasecurity.com/spain/mediacenter/noticias/virus-policia-android/

Revision #1
Created 1 February 2022 12:07:29 by Equipo CATEDU
Updated 1 February 2022 12:07:29 by Equipo CATEDU