GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR

POLICÍA NACIONAL

#movilseguro

USA TU SMARTPHONE CON INTELIGENCIA

@policia

En colaboración con red.es

#movilseguro

Nota de prensa

En España ya hay 20 millones de teléfonos inteligentes

"Usa tu *smartphone* con inteligencia": la Policía Nacional lanza una campaña por el uso seguro de los móviles y todas sus posibilidades

- **Los especialistas alertarán a través de las redes sociales de los riesgos para la seguridad y privacidad en el uso de los móviles inteligentes con el *hashtag* #movilseguro**
- **La prudencia y prevención, bases de los 15 consejos y puntos de riesgo para 20 millones de españoles que ya poseen un *smartphone***
- **La supervisión y concienciación de los padres, claves para la seguridad y buen uso del móvil por los menores**

11-mayo-2012.- La Policía Nacional lanza una campaña de información y concienciación a través de las redes sociales para el uso seguro y privado de los teléfonos móviles de altas prestaciones, con el lema "Usa tu *smartphone* con inteligencia". Los especialistas en la seguridad de las tecnologías han elaborado un breve informe con los principales riesgos y consejos para un buen uso de estos teléfonos y la infinidad de utilidades que permiten.

En España, como en el resto del mundo, se ha multiplicado el número de usuarios de este tipo de terminales, que facilitan utilizar infinidad de aplicaciones y una conexión permanente a Internet, mensajería instantánea, perfiles en redes sociales, mails… Analistas del sector tecnológico apuntan que se ha superado la cifra de 20 millones de usuarios de estos teléfonos, el

doble que hace un año. “Como es lógico, ese incremento ha supuesto un aumento exponencial de los riesgos, intentos de fraude y prácticas peligrosas o inadecuadas para la privacidad del dueño del móvil y sus interlocutores” explican los agentes de la Brigada de Investigación Tecnológica, la unidad especializada de la Policía Nacional.

Los agentes, en base a su experiencia más reciente y el conocimiento técnico y los hábitos de uso y consultas que atienden de los ciudadanos, han reunido en un documento los agujeros de seguridad, riesgos de privacidad y consejos para un uso “inteligente” de los *smartphones*:

Consejos para un uso inteligente y seguro de los *smartphones*

1. Los nuevos móviles tienen un gran valor económico y suponen una tentación para los “amigos de lo ajeno”. No lo pierdas de vista, como haces con tu bolso o cartera. Apunta el IMEI, la “matrícula” del terminal, para darlo de baja si lo necesitas. Si te lo roban avisa a tu operadora. También puedes instalar un software que te permita su localización y el borrado de tus datos privados en caso de robo.

2. Si compras un teléfono fuera de los circuitos oficiales de venta pide al vendedor la factura de compra para poder reclamar. Sé precavido porque detrás de estas ventas pueden esconderse fraudes (teléfonos sustraídos bloqueados por IMEI, averiados, inexistentes…).

3. Los terminales modernos permiten la protección de su contenido, teclado y aplicaciones y el desbloqueo del mismo, mediante una contraseña, numérica o táctil. Activa esa protección y no permitas a nadie utilizar tu móvil. Tampoco compartas la contraseña para proteger tu intimidad y la de tus comunicaciones. Evitarás *hackeos* o intrusiones de consecuencias desagradables. Si pierdes o te roban el *smartphone* cambia desde el PC las contraseñas de acceso al correo electrónico, redes sociales, aplicaciones de comercio electrónico,… que tuvieras instalados en el teléfono.

4. Sé consciente de las posibilidades que dan estos teléfonos a sus poseedores y a los interlocutores. Y no conviertas en normales acciones que pueden suponer un control excesivo de tu intimidad o acarrearte un bombardeo comercial: usa con prudencia la geolocalización que permite la mensajería instantánea y las distintas redes sociales.

5. Atención a hacerte, almacenar o enviar imágenes tuyas comprometedoras o, peor aún, de otros, así como redistribuir imágenes

ajenas pueden dañar la imagen de los protagonistas. Antes de enviarla o compartirla de forma instantánea en redes sociales asegúrate de que no va a suponer un problema para nadie, ni ahora ni en el futuro. Querer borrarla luego o pretender que otros lo hagan no es la solución.

6. El *sexting* -hacerse fotos de carácter erótico y/o compartirlas- es un error garrafal. En el caso de los menores puede originar situaciones de chantaje o ciberacoso sexual o acoso en el entorno escolar (*grooming y bullying)* Conocemos muchos casos de gente que se ha arrepentido cuando ya era tarde. Redistribuir esas imágenes de otras personas con el fin de perjudicarles es **delito**.

7. Los *smartphones* y *tablets* sufren, como el resto de ordenadores y equipos que se conectan a Internet, ataques a través de lo que se conoce como técnicas de "ingeniería social": correos electrónicos o mensajes colgados en perfiles en las distintas redes sociales, distribuidos de forma masiva a través de cuentas "secuestradas", incorporan links con un contenido supuestamente muy atractivo… y que esconde, bajo un link acortado, *spam* o *malware*. No accedas a enlaces facilitados a través de SMS no solicitados: ignora esos mensajes y, en caso de posible intento de fraude, hazlo llegar a la Policía Nacional.

8. Los nuevos móviles incluyen un sistema operativo y permite instalar infinidad de aplicaciones. Éstas tienen el riesgo de ser vehículos muy eficaces de transmisión, tanto para el envío de *spam* publicitario como para infectar con troyanos *smartphones* y *tablets*.

9. Los internautas están muy concienciados con la prevención y protección contra los virus en los ordenadores personales, pero sólo un 32% de los españoles poseedores de *smartphones* cuenta con un programa antivirus. Usa siempre plataformas, páginas, *firmware* y *software* oficiales y actualizados.

10. Haz periódicamente copias de seguridad del contenido de tu móvil o *tablet*. Si es relevante, duplica ese contenido en distintos soportes informáticos (USB, ordenadores domésticos o profesionales…).

11. No te conectes a redes WiFi de las que desconozcas su propiedad y sé prudente con las operaciones que realizas conectado a redes *wireless* públicas. Y, por supuesto, no *crackees* la clave de seguridad de redes protegidas ajenas.

12. Si utilizas el *smartphone* para comprar por Internet sigue las mismas pautas de seguridad y prevención que con el ordenador, pero extrema la

precaución en cuanto a las aplicaciones que utilizas y a la autenticidad y fiabilidad de la web vendedora (que la dirección web empiece por "https" que indica que es una conexión segura), así como a las condiciones de privacidad del vendedor o intermediario.

13. Desconfía de correos o SMS pidiéndote que envíes un mensaje o llames a un número de tarificación especial. De igual forma, asume que al enviar un SMS puntual te puedes estar suscribiendo de forma automática a un servicio de pago constante. Lee siempre las condiciones de uso de los servicios que aceptas para saber lo que contratas en la letra pequeña.

14. Evita ser utilizado para propagar el *spam* a través de mensajería instantánea en el móvil. Mensajes que advierten del fin de ese servicio gratuito si no se reenvía dicho mensaje son falsos y no buscan más que la distribución masiva del mismo.

15. Atención al *phishing* (páginas o links que se hacen pasar por banco, empresa o entidad oficial para que facilites tus datos y robarte dinero… o secuestrar tu cuenta). Además de este riesgo, también existente en los ordenadores, está el *smishing* (lo mismo, pero a través de un enlace que se envía vía SMS).

16. Cuando instalas determinadas aplicaciones en tu teléfono inteligente en muchas ocasiones autorizas el acceso a tus datos privados, su uso para terceros o, incluso, la promoción de esa aplicación entre tus contactos. Cuando pulsas "aceptar" asegúrate de los permisos que concedes al instalar los programas.

La supervisión y la concienciación al menor: consejos para los padres

Como en resto de las tecnologías, los niños y adolescentes tienen una gran facilidad para el uso de *smartphones*, al tiempo que sienten una fuerte atracción por los mismos y su infinidad de utilidades. El problema está en que ellos no perciben ni le dan importancia alguna a los riesgos que encierra su uso incontrolado para su seguridad.

Como en otros muchos aspectos de su educación (como, por ejemplo, la propia navegación online desde el ordenador de casa), la orientación, apoyo y supervisión de adultos y su familia serán fundamentales para un mejor uso de estos aparatos.

Los especialistas de la BIT recuerdan que es fundamental poner normas al uso del móvil por parte de los menores y, una vez que se hayan establecido

las pautas entre adulto y menores, conocer cómo lo utiliza, con quién habla o se conecta, qué aplicaciones utiliza, dónde y con quien navega… Es importante "acompañarles" y saber qué hacen con el móvil, tanto en su aprendizaje como en su uso cotidiano. Será importante alertarles de los riesgos, aconsejarles cómo afrontarlos y evitarlos, normas de seguridad, trucos… Con las premisas de sentido común y prudencia.

Los adultos deben mantener una constante vigilancia y concienciación hacia los menores, sabiendo distinguir el uso, los riesgos y pautas de seguridad en relación a la edad de los chavales, con normas y condiciones de utilización pactada entre todos.

Además:

- Establecer pautas o normas de utilización con los menores. Supervisión de lo que hacen con el móvil, cómo y con quién, desde la elección del terminal que realmente necesiten.

- Explicar las medidas de seguridad y prevención generales para el uso de *smartphones* por los adultos y pedir a los menores que las respeten al máximo para evitar problemas como el *ciberbullying o* el *grooming.* Formarles y concienciarles de la importancia de la privacidad y los riesgos de seguridad, así como pedirles responsabilidad.

- Recordar a los menores y adolescentes que sean especialmente cuidadosos con las fotos, vídeos y contenidos de todo tipo –como conversaciones de chat- que comparten.

- Que sólo den el móvil y agreguen a sus perfiles en las redes sociales a conocidos reales y de confianza.

- Que no usen el móvil para insultos, acoso, *sexting*… y que acudan a un adulto ante posible ciberacoso o *grooming* (acoso sexual).

- Antes de descargar aplicaciones o contratar servicios Premium con el móvil, consultarlo y obtener la autorización de los padres.

- Instalar en sus terminales herramientas de seguridad y protección o control parental.

España, tercer país del mundo en uso de *smartphones*

España, con 20 millones de *smartphones*, es el tercer país del mundo en número de usuarios de estos teléfonos, con una tasa de penetración del

35%, tras Singapur y Canadá, según desvelan los estudios realizados por prestigiosas consultoras internacionales. Los menores de 35 años son los principales usuarios de estos aparatos y de las muchas posibilidades que permiten sus aplicaciones y conexión permanente a Internet, mensajería instantánea y redes sociales.

El 89% de los poseedores de un móvil de este tipo hacen uso diario de sus prestaciones más avanzadas. La cuarta parte de los usuarios de redes sociales se conectan y comparten contenidos desde sus teléfonos móviles. 10 millones de españoles utilizan el servicio de mensajería instantánea para *smartphones.*

NOTA: Los medios de comunicación que lo deseen podrán obtener imágenes en el siguiente enlace:

http://www.policianacionalcomunicacion.es/movilseguro.rar

C) RAFAEL CALVO, 33
28010 - MADRID
TEL: 91 322 33 19
FAX: 91 322 33 11