Publicado en el 09/02/2016

Consejos para mantener la seguridad y la intimidad en la Red

En OCU publican un comunicado con motivo del día de Internet Seguro, en el que cuentan todo lo que se necesita saber para atrapar conocimientos y escapar de los piratas.

10 enlaces para estar seguro:

Uno de cada tres ordenadores está infectado por un virus, pero tenemos Recetas para ser inmune.

Cuando sueltas la pasta es cuando te la roban: Pagar online sin pasar miedo.

Se presentan como la cura, pero son la infección: Antivirus Engañosos.

Figuran entre las webs más visitadas y generan muchas quejas: descubre cómo funcionan realmente las Páginas Web de Descuentos.

Por muy cibernética que sea, en la Red también tienes derechos: apréndetelos con este Test.

Compartimos nuestra intimidad en Facebook, Twitter y Tuenti, pero ¿sabemos protegernos?: Redes sociales y privacidad.

Ladrones que se hacen pasar por la autoridad: Virus con placa de policía.

Los más pequeños no siempre tienen claro de qué va la cosa: Protege a tus hijos en Internet.

Lo sepas o no, tu prestigio está en juego en la red. Descubre de qué va la Reputación Online.

Se dice que los españoles somos piratas por naturaleza, pero ¿cuánto pagarías tú por ver una peli online?

10 consejos para defenderte

1. No importa que tu software de seguridad sea excelente: no sirve de nada si no está actualizado. En tu configuración elige que las actualizaciones sean automáticas y ten en cuenta que también tu sistema operativo necesita estar al día.

2. Combina con destreza tu antivirus y tu cortafuegos. La mayoría de sistemas incluye un cortafuegos. Si instalas uno diferente, desinstala primero el otro para evitar un conflicto entre ambos. Si vas a instalar antivirus y cortafuegos por separado, empieza siempre por el antivirus.

3. Los productos de Microsoft son blanco habitual de los piratas informáticos. Elegir productos de otras marcas puede ayudar a reducir riesgos.

4. No abras ficheros que vengan de soportes externos sin someterlos primero a un programa de detección de malware.

5. Si recibes un e-mail sospechoso, bórralo. No respondas, no descargues los ficheros adjuntos y no pinches en sus enlaces.

6. Si necesitas dejar una dirección de correo en un foro o aplicación de la que no te fías, lo mejor es crear una para la ocasión.

7. Protege tus datos sensibles: nunca los envíes por correo. Para acceder a tu banco, teclea la dirección web en el navegador y desconfía de los enlaces que te lleguen por e-mail. Comprueba siempre que estás en una dirección segura (la dirección empieza por HTTPS).

8. Cuando uses un ordenador público (en un cibercafé, en la biblioteca...) extrema las precauciones y acuérdate de cerrar todas las sesiones que inicies.

9. Mejor prevenir que llorar: haz copias de seguridad de tus ficheros para no lamentarte si al final eres víctima de un ataque informático.

10. Si decides embarcarte por la Red solo con un antivirus y un cortafuegos, recuerda que muchos navegadores ofrecen sus propios servicios antispam y antiphishing.

Datos de contacto:

Nota de prensa publicada en:

Categorías: E-Commerce Ciberseguridad

NotasdePrensa
https://www.notasdeprensa.es