9. Te encuentras en un lugar público, como en un aeropuerto o una cafetería, que ofrece Wi-Fi gratuitamente. ¿Estará protegida tu información cuando inicias sesión en tu correo electrónico escolar o en tus cuentas de redes sociales?

A. Sí.
B. No.
C. ¿Por qué no? El Wi-Fi público está protegido.
D. Si tus amistades lo hacen, tú también puedes hacerlo.

Respuesta: B
Al usar una conexión pública de Wi-Fi, tienes que suponer automáticamente que la conexión no está protegida. Al encontrarte en una red no protegida, es posible que las personas vean los sitios que visitas, y esto puede ponerte en riesgo.

10. Acabas de descargar una aplicación de bienestar o una aplicación de seguimiento de salud personal, y quieres enlazar tu información con tus amistades a fin de darles acceso a tus patrones de sueño, horas y ubicaciones de ejercicio, y otra información de salud. Antes de permitir dicho acceso, ¿qué deberías hacer?

A. Leer las Normas de Privacidad de la aplicación.
B. Revisar tus configuraciones de seguridad.
C. Preguntar a tus amistades sobre sus configuraciones de seguridad.
D. Investigar al desarrollador de la aplicación antes de descargarla.
E. Todas las opciones anteriores.

Respuesta: E
Más de una cuarta parte de los perfiles en aplicaciones de bienestar son públicos, y muestran las horas, ubicaciones, así como los puntos de inicio y fin, y otra información personal sobre el usuario. Otros ejemplos de la información que puede identificarse e interceptarse usando software y hardware bastante básicos son el género, estatura, edad, peso y condición física del usuario, así como la información de localización geográfica.

¿Qué tan buen resultado obtuviste?

Si respondiste correctamente a 9 preguntas y más, ¡eres un experto digital! ¡Bien hecho! Te has ganado el derecho a considerarte a tí mismo/a un/a experto/a. No solamente estás al tanto de la forma en que el comportamiento por Internet puede afectar la vida de las personas, sino que también comprendes cómo manejar situaciones cibernéticas difíciles. ¡Estamos impresionados! Llegó la hora de compartir tu destreza con tus amistades y tus parientes.

Si respondiste de 5 a 8 preguntas correctamente, puede que estés estés a riesgo ser una víctima cibernética. Esto quiere decir que, a pesar de que tú creas comprender debidamente la manera en que tu comportamiento por Internet puede afectarte a tí y a otros, puede que no sepas cómo protegerte a tí mismo/a y otros por Internet.

Si respondiste 5 preguntas correctamente o menos, ¡ten cuidado! Tus decisiones te habrían expuesto, a tí y a tus amistades y parientes, a riesgos innecesarios, incluyendo a programas espías y a robo de identidad. Por el simple hecho de que el Internet es digital, no quiere decir que las reglas del mundo real no aplican. Si algo parece incorrecto o peligroso, no te arriesgues.

Obtén más información sobre la seguridad cibernética visitando:

NJConsumerAffairs.gov/CyberSafe

Sensatez cibernética

Recursos adicionales

www.nj.gov/lps/dcj/idtheft.htm
www.njsp.org/tech/identity.html
www.cyber.nj.gov/citizens
www.consumer.ftc.gov/
www.identitytheft.gov/

Puntos de Contacto

Si deseas reportar un incidente sospechoso de fraude cibernético, puedes poner una denuncia ante la División de Asuntos del Consumidor, a través del sitio web de la División, o al llamar al 800-242-5846 (llamada gratuita en Nueva Jersey), o al 973-504-6200.

Prueba de –sensatez– cibernética

Contesta esta prueba para ver si estás realmente protegido/a cuando ingresas al Internet.

Comprueba que tán Ciberinteligente eres en realidad.

División de Asuntos del Consumidor New Jersey
800-242-5846 ■ www.NJConsumerAffairs.gov

1. ¿Qué es la información personal?

A. Tu nombre.
B. Tu dirección residencial.
C. Los nombres y apellidos de tus padres o tutor.
D. Tu número de identificación estudiantil.
E. Tu número de seguro social.
F. Ninguna de las opciones anteriores.
G. Todas las opciones anteriores.

Respuesta: G
Protege en todo momento tu información personal.

2. Al desbloquear tu teléfono inteligente, te das cuenta que 7 de tus aplicaciones cuentan con actualizaciones disponibles. ¿Qué haces en este caso?

A. Ignoro los avisos de actualización.
B. Actualizo las aplicaciones.

Respuesta: B
La actualización de aplicaciones y de sistemas operativos ayudará a protegerte contra vulnerabilidades conocidas que pueden poner en riesgo tu información..

3. ¿Cuál es la mejor manera de utilizar los sitios de redes sociales?

A. Limita la cantidad de información que compartes sobre tí mismo/a.
B. Habla únicamente con personas a quienes conozcas.
C. Configura tu página para que sea privada a todos, excepto a las personas que conoces.
D. Todas las opciones anteriores.

Respuesta: D
Toma las riendas de tu presencia digital. Cuando esté disponible, configura la privacidad en tu cuenta para que un intercambio de información sea bajo el nivel más estricto posible. Es una buena idea limitar la manera y las personas con quienes compartes información.

4. Te encuentras en las redes sociales, cuando de repente recibes una solicitud de amistad de parte de alguien que no conoces. ¿Qué deberías hacer?

A. Aceptar la solicitud de amistad, puesto que ignorar la solicitud es un gesto grosero.
B. Rechazar la solicitud de amistad, pues ¿quién es él/ella?
C. Enviar un mensaje y preguntarle a él/ella sobre cómo te conoce.
D. No tienes cuentas en las redes sociales.

Respuesta: B
El riesgo de robo de identidad y filtración de información aumenta al aceptar las solicitudes de amistad por parte de una persona extraña. Incluso la información que parecer ser inocente, tal como los nombres de tus amistades, nombres de mascotas, planes para días festivos, así como tus gustos y aversiones, puede agregarse y ayudar a que un estafador robe tu identidad.

Sensatez cibernética

5. Publicaste por Internet una fotografía, pero más tarde decidiste quitarla. Te preocupa que tu amigo/a pueda verla, pero como tu amigo/a no tiene una computadora, jamás verá la foto. ¿No es así?

A. Cierto. B. Falso.

Respuesta: B
Nunca sabes quién va a ver las imágenes que publicas en linea. Es posible que se distribuyan copias, y puede que alguien haya guardado una imágen antes de que la borraras. Sé responsable, reflexiona sobre lo que publicarás y si tú y/o tus amistades estarían de acuerdo con ello. Publica solamente las cosas de otras personas que te gustaría que ellos publiquen sobre tí.

6. Otras personas no pueden ver todo lo que uno envía por correo electrónico privado, o por mensaje instantáneo (IM) o por salas de charla (chats) ¿verdad?

A. Cierto. B. Falso.

Respuesta: B
Existen programas que pueden "observar" tu correspondencia privada en línea, y nunca se sabe si alguien la compartirá o no en el futuro. Así que, JAMÁS envíes información personal, a menos de que estés muy seguro/a de que se trata de un sitio o conexión segura.

7. Los metadatos son detalltes incorporados en las fotografías. Les dicen a la gente...

A. El lugar y la fecha en que tomaste la foto.
B. Dónde publicaste la foto.
C. Lo hermoso que se ve tu peinado.
D. Tu color favorito.
E. Ninguna de las opciones anteriores.

Respuesta: A
Antes de publicar cualquier fotografía, te convendría quitar de las imágenes los metadatos, de tal manera que no divulgues las coordenadas de GPS relacionadas con tus fotografías.

8. Luego de un disgusto en la escuela, un grupo de compañeros de clases te envían mensajes insultantes por redes sociales o a tu teléfono celular. ¿Qué deberías hacer?

A. Bloquearlos.
B. Guardar los correos electrónicos, los mensajes y los comentarios que recibiste.
C. Cuéntale a tus padres/tu tutor.
D. Todas las opciones anteriores.

Respuesta: D
Si piensas que alguien te está intimidando o acosando por Internet, deberías contarle a tus padres o a un adulto de confianza. Bloquea a la persona y guarda todos sus mensajes. Muchos sitios web cuentan con formas de reportar el abuso y/o ayudarte a responder a mensajes que te hacen sentir incómodo/a.