Diputació de València | Protecció de Dades i Seguretat de la Informació

Boletín DivalData

Boletín del Departamento de protección de datos y Seguridad de la Información de la Diputación Provincial de Valencia

Boletín N.º 37| Julio 2023

RECOMENDACIONES DE SEGURIDAD PARA EL PERIODO VACACIONAL

ÍNDICE

RECOMENDACIONES DE SEGURIDAD PARA EL PERIODO VACACIONAL

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

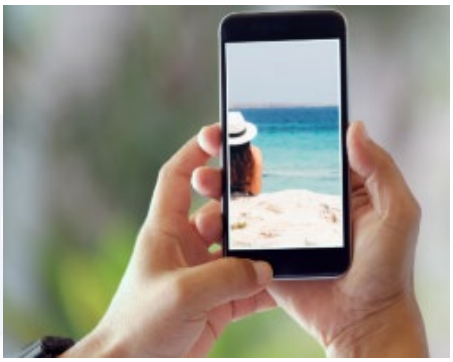
Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirse a nuestro Boletín informativo accede al siguiente enlace

INTRODUCCIÓN



Con la llegada del verano, comienza la época de vacaciones para muchos de nosotros. A pesar de ser días de desconexión del trabajo y de conexión con nuestra familia, amigos y nuestras aficiones, debemos seguir implementando rutinas seguras en el uso de nuestros dispositivos. Y es que, en esta época, se produce un aumento significativo de las ciberamenazas, que podrían poner en peligro nuestros datos personales o, incluso, aquellos de los que nuestra organización es responsable. Es por ello que, no podemos bajar la guardia y debemos seguir siendo activos en la protección de datos, afrontando las situaciones de riesgo que se presentan.

En el presente boletín os presentamos algunos consejos sobre cómo afrontar estas situaciones para la protección de los datos personales en época estival.

RECOMENDACIONES DE SEGURIDAD PARA EL PERIODO VACACIONAL

1. REDES WIFI PÚBLICAS

Las redes *WiFi* públicas son aquellas que no están protegidas por una contraseña y nos permiten conectarnos a internet de una forma cómoda y rápida. También son aquellas a las que, aun teniendo contraseña de acceso, se conectan muchos usuarios. Estas no cifran la información que se transmite a través de ellas, por lo que no son seguras. A pesar de sus ventajas, uno de sus principales inconvenientes es su naturaleza abierta y accesible, lo que puede comprometer la información de nuestra organización.

En caso de acceder de manera puntual a los servicios o aplicaciones de la Diputación de Valencia cuando estamos de vacaciones -lo que nos llevaría a conectarnos a este tipo de redes en hoteles, aeropuertos, cafeterías, etc.- sigue estas recomendaciones de seguridad:

- **No te conectes a redes inalámbricas abiertas.** Tanto el administrador como alguno de los usuarios conectados pueden utilizar técnicas para robarnos información.

- **Es preferible que te conectes a la red 3G/4G/5G del operador de telefonía.** Hoy en día cualquier operador ofrece una cantidad notable de GB para tráfico de datos.

- En caso de necesidad, si vas a conectarte a una red inalámbrica pública, es **preferible acceder a una red con seguridad WPA o WPA2.** Las redes abiertas y con seguridad WEP son totalmente inseguras. Consulta los detalles de la red *WiFi* para comprobar ante qué tipo de red estás.

- **Comprueba** que la **red** gratuita disponible es la **oficial** del lugar en el que estás.

- Siempre que estén disponibles, conéctate a páginas con **certificado de seguridad https://**

- **No inicies sesión en ningún servicio** mientras estés conectado a una red pública.

- **Evita realizar transacciones bancarias, compras en línea** o cualquier otra tarea que suponga el intercambio de datos desde redes *WiFi* públicas.

- **Deshabilita cualquier proceso de sincronización** de tu equipo si vas a usar una red pública.

- Mantén siempre el **equipo actualizado y el antivirus instalado** correctamente.

- Tras la conexión, **elimina los datos de la red memorizados** por tu equipo.

2. CONTRASEÑAS

Uno de los mecanismos de autenticación más utilizados para proteger el acceso a los dispositivos, aplicaciones y, en general, a la información, son las contraseñas. Estas son una forma de autenticación que utiliza información secreta para controlar el acceso a algún recurso, constituyendo la primera línea de contención para evitar ciberataques. Por ello, para no poner en riesgo la información contenida en nuestros sistemas o los sistemas de información de nuestra organización, durante nuestras vacaciones debemos asegurarnos de haber creado claves seguras y hacer un buen uso de estas.

A continuación, ofrecemos una serie de recomendaciones de seguridad:

- **No** utilices las contraseñas que se te proporcionen **por defecto**.
- Las contraseñas deben ser **robustas** (más de 8 caracteres y que contenga letras, números y símbolos).
- **No** tienen que ser **las mismas** las empleadas en el **ámbito personal** y las empleadas para el acceso los sistemas o aplicaciones en el **ámbito laboral.**
- **No compartas** tus contraseñas.
- **No** mantengas tus contraseñas **por escrito a la vista** o al alcance de terceros.
- **No** utilices las credenciales de **acceso de otros usuarios**, aunque dispongas de la autorización de su titular.
- **Evita** utilizar el **recordatorio de contraseñas**.
- Si recibes una **llamada telefónica o mensaje solicitando tu usuario y contraseña, nunca los facilites**.
- Utiliza un **gestor de contraseñas seguro**.

3. ATAQUES DE INGENIERÍA SOCIAL. *PHISHING*.

En época estival aumentan los ciberataques, en especial, de *phishing*. Esta es una de las técnicas de ingeniería social más utilizadas por los ciberdelincuentes para obtener información personal de los usuarios suplantando a una persona o entidad.

La técnica consiste en el envío de un mensaje o la realización de una llamada, por parte de un ciberdelincuente, a un usuario simulando ser una persona o una entidad de confianza con el objetivo engañarle y manipularle, a fin de que acabe realizando alguna acción, que puede en peligro sus datos personales o los de la organización a la que pertenece.

Debemos tener especial cautela, ya que, como indicábamos, esta es una época en la que recibimos muchos emails de empresas para confirmar la reserva de una habitación de hotel, el pago de un coche de alquiler o la compra de un billete de avión, que podrían llevar a confusión, por lo que tenemos que prestar especial atención. En cualquier caso, no debiéramos utilizar el correo electrónico corporativo para este tipo de menesteres.

A continuación, ofrecemos una serie de recomendaciones de seguridad para protegernos frente al *phishing:*

- Si el mensaje te pide hacer alguna **acción extraña, ignóralo**.
- Si el mensaje te obliga a **tomar una decisión en poco tiempo**, es **mala señal**.
- **Comprueba el dominio del correo remitente** y que su nombre coincida con su cuenta de correo.
- **Evita abrir archivos adjuntos si desconoces el remitente** o no esperas el documento.
- **Sospecha** de mensajes con **faltas de ortografía, errores gramaticales y saludos genéricos**.
- Ten cuidado con las **solicitudes de datos a través de webs a las que has llegado siguiendo el enlace.** Mejor accede directamente a la web de la organización.
- Mantén **actualizado el navegador, el sistema operativo y demás software**.
- **Evita** el uso de **medios extraíbles.**

4. CÓDIGOS QR

Las iniciales de QR se traducen del inglés *Quick Response,* literalmente, como 'respuesta rápida'. Estos sirven para almacenar información y hacerla más accesible a los usuarios. Hoy en día, a través de cualquier cámara de un *smartphone* o *tablet* se pueden escanear estos códigos para acceder directamente, por ejemplo, a una página web o descargar una aplicación. Muchos lugares de interés u hostelería utilizan este tipo de códigos para que las personas puedan acceder rápidamente a la información del lugar como, por ejemplo, la carta de un restaurante.

No obstante, hay que tener precaución a la hora de escanear estos códigos, ya que podrían llevarnos a enlaces o a la descarga de aplicaciones no deseadas, capaces de explotar fallos de seguridad del sistema operativo y obtener la información almacenada en el dispositivo.

Su uso debe realizarse de manera segura, por ejemplo, con una herramienta gratuita para analizar la URL, verificando que es la correcta y no está manipulada.

A continuación, te proporcionamos algunas recomendaciones que puedes aplicar:

- Si a primera vista la **URL** nos parece **sospechosa**, directamente **no debemos acceder a ella**.

- Asegurarnos de que la **web** a la que vamos a acceder siempre cumple con **estándares de protección y navegación segura**, como, por ejemplo, que tenga **HTTPS.**

- Hacer uso de **analizadores de enlaces**. El Instituto Nacional de Ciberseguridad recomienda algunos como VirusTotal y URLVoid. De esta manera, antes de abrir la web podremos comprobar que no se trata de ningún ataque de ingeniería social.

- También podemos recurrir a **aplicaciones**, como Kaspersky QR Scanner, disponible en Android e iOS, que realizan una serie de chequeos de seguridad antes de activar el código QR en el smartphone.

- **No proporcionar ningún dato privado ni ninguna contraseña, personal o profesional**, a páginas web que hayamos accedido a través de un código QR. Es conveniente que si accedemos a páginas de bancos o tiendas online donde introducimos datos de nuestra tarjeta bancaria, lo hagamos desde la URL completa o a través de su aplicación propia.

5. PROTECCIÓN DE DISPOSITIVOS

Cuando viajamos o realizamos actividades veraniegas como ir a la piscina, la playa o visitar lugares turísticos, aumentan los riesgos de perder o que nos sustraigan nuestros dispositivos portátiles (ordenadores, móviles, *tablets*). Estos dispositivos contienen multitud de información personal, nuestra o, en muchos casos, información que podría comprometer a nuestra organización -por ejemplo, en caso de que en alguna ocasión se haya utilizado el dispositivo personal para consultar información profesional o realizar alguna tarea profesional y se haya mantenido la misma en el dispositivo, o en caso de haber introducido en el mismo las credenciales de nuestra organización y no se hayan eliminado después-.

A continuación, ofrecemos una serie de recomendaciones de seguridad para proteger tus dispositivos:

- Utiliza un **sistema de clave o patrón para bloquear** los dispositivos.
- **Evita compartir los dispositivos** con familiares, amigos y extraños.
- **Bloquéalos** cuando no estén en uso.
- Guarda los **documentos sensibles y confidenciales en un lugar seguro.**
- **No** conectes dispositivos **USB desconocidos.**
- **No** dejes **dispositivos móviles desatendidos o visibles** en lugares públicos.
- **No** utilices **cargadores públicos.**
- **Actualiza el software** lo antes posible.

6. SHARENTING

En época de vacaciones se aumenta el uso de las redes sociales para compartir momentos entre las familias y amigos. Muchas personas han encontrado en estas plataformas el lugar idóneo para publicar fotos y vídeos de diferentes momentos de la vida de los menores, acompañados de comentarios (entre los que se puede encontrar el nombre o la edad), contribuyendo a alimentar su huella digital, sin contar con que sus hijos puede que no estén de acuerdo el día de mañana.

El *sharenting* creció de forma exponencial durante el confinamiento y su práctica es habitual en esta época, por lo que es importante reflexionar antes de publicar este tipo de contenidos en la red. Para ello, es conviene recordar algunas recomendaciones para su uso:

- Tenemos la obligación de cuidar su imagen e intimidad. Las personas menores de edad tienen derechos que deben ser protegidos de forma especial.

- Es posible que no seamos consciente de cómo se están difundiendo las imágenes. No siempre es fácil entender y gestionar la lógica y los cambios de gestión de privacidad de las redes sociales.

- Existen otras formas más seguras para compartir imágenes. Es necesario limitar con quién compartir la información y elegir la plataforma adecuada.

- Habitualmente, se comparte más información que la que se aprecia a simple vista. Una imagen inocente puede contener detalles de contexto importantes e incluso geolocalización.

- Al compartir las imágenes con otras personas, estas pueden asumir que eso significa que las pueden publicar y que las imágenes no son tan privadas. Sin mala intención, de forma directa o indirecta, pueden expandir el alcance e incluso hacerlas públicas.

- Compartir imágenes de otras personas sin su consentimiento puede ser una infracción de la normativa de protección de datos. No es un buen ejemplo para nadie, menos aún para los menores de edad.

7. TECNOLOGIAS EN MENORES

Si tienes hijos adolescentes, el verano puede ser la época donde más tiempo pasan con sus dispositivos, ordenadores, *tablets* y móviles. Además durante gran parte de ese tiempo hacen uso de sus redes sociales compartiendo fotos y contenidos que no siempre son los más adecuados.

Por eso, es recomendable tener una serie de medidas o pautas a la hora de permitir el uso de estos dispositivos en el hogar:

- El **control parental** es un mecanismo para controlar en diferentes sitios web, sistemas operativos o equipos el acceso y uso que los menores de edad le dan a internet. A través del control parental podemos monitorear la navegación, restringir contenidos no aptos para menores y bloquear páginas o usuarios que puedan ser una amenaza para los niños.

- Además, es posible establecer **límites de tiempo** en el que los menores pueden estar con el ordenador encendido, evitar que jueguen o accedan a ciertas aplicaciones y juegos o impedir que ejecuten ciertos programas.

- También, en **redes sociales** como Facebook, Twitter o Instagram **si alguna publicación no es apta** para que un menor de edad la vea, se puede **reportar** y el contenido desaparecerá de la línea de tiempo.

Hacer de internet un espacio seguro para nuestros niños está en nuestras manos. No los descuidemos mientras navegan en la red.

"En verano se produce un aumento significativo de las ciberamenazas, que podrían poner en peligro nuestros datos personales o, incluso, aquellos de los que nuestra organización es responsable. Para protegerlos, sigue estos consejos de seguridad: no te conectes a redes inalámbricas abiertas; antes de irte de vacaciones, asegúrate de haber creado claves seguras y haz un buen uso de estas; presta atención a los correos electrónicos, mensajes o llamadas recibidas, analizando su contenido antes de proporcionar información; ten precaución a la hora de escanear códigos QR, ya que podrían llevarnos a enlaces o a la descarga de aplicaciones no deseadas, capaces de obtener nuestra información; protege tus dispositivos con clave y no los dejes desatendidos en lugares públicos; vigila que tus hijos no hagan un uso inadecuado de los dispositivos".

MATERIAL COMPLEMENTARIO

- Protección de datos en vacaciones (AEPD). Puedes consultar la infografía en este enlace.
- Protección de datos en vacaciones (AEPD). Puedes consultar el artículo en este enlace.
- Consejos de ciberseguridad durante las vacaciones (APDCAT). Puedes consultar el artículo en este enlace.
- Consejos para unas vacaciones ciberseguras (INCIBE). Puedes consultar el artículo en este enlace.
- Prepárate para disfrutar de unas vacaciones ciberseguras en familia (INCIBE). Puedes consultar el artículo en este enlace.
- Escanea códigos QR de manera fiable y segura (INCIBE). Puedes consultar el artículo en este enlace.
- Diez recomendaciones de ciberseguridad para las vacaciones (GVA). Puedes consultas el artículo en este enlace.

NOTICIAS

- **La AEPD publica una Circular sobre el derecho de los usuarios a no recibir llamadas comerciales no solicitadas.** La circular fija los criterios conforme a los que va a actuar la Agencia en aplicación del artículo 66.1.b) de la Ley General de Telecomunicaciones, que implica cambios para poder realizar este tipo de llamadas y que se aplica desde el 29 de junio. Puedes consultar la Circular en este enlace.

- **La AEPD sanciona a la organizadora del Mobile World Congress en 2021 por utilizar datos biométricos de los asistentes sin haber realizado adecuadamente una Evaluación de Impacto en Protección de Datos.** La AEPD considera que la recogida de datos biométricos en el reconocimiento facial establecido para la identificación de los asistentes al Congreso debió contar con una Evaluación de Impacto de Protección de Datos. Puedes consultar la Resolución en este enlace.

- **El TJUE abre la puerta a revelar la identidad de los empleados que consultan datos personales.** El Tribunal de Justicia de la Unión Europea (TJUE) determina que cualquier persona tiene derecho a saber la fecha y las razones por las que una entidad ha consultado sus datos personales, y abre la puerta a revelar la identidad de los trabajadores que lo hicieron cuando sea indispensable para permitir al interesado ejercer efectivamente los derechos que le confiere la normativa y siempre bajo la condición de que se tengan en cuenta los derechos y libertades de los empleados. Puedes consultar la Sentencia en este enlace