HERALDO
DE ARAGON

EDITA: HERALDO DE ARAGÓN EDITORA, S. L. U. | **Zaragoza:** Paseo de Independencia 29. 50001 Zaragoza. Centralita: 976 765 000. Suscripciones: 976 763 211. Clasificados: 976 765 011. Publicidad: 976 765 010. Fax Redacción: 976 765 094. Fax Publicidad: 976 765 002. Apdo. Correos 175. E-mail: zaragoza@heraldo.es | **Huesca:** Alcalde Carderera, 1. 22002 Huesca. T: 974 239 000. Fax: 974 239 005. E-mail: huesca@heraldo.es | **Teruel:** José Torán, 6. 44002 Teruel. T: 978 608 260. Fax: 978 608 280. E-mail: teruel@heraldo.es | **Madrid:** Condesa de Venadito, 1. 28027 Madrid. T: 917 015 600. | **Depósito legal: Z-58-1958**

En la última

«Que algo llegue por Whatsapp no significa que sea verdad»

ALBERTO HERNÁNDEZ
Director general de Incibe

Hernández cerró el ciclo de cine del Colegio de Economistas. OLIVER DUCH

En una época en la que todos llevamos un móvil en el bolsillo que puede saber dónde estamos y nuestros datos, ¿es el momento de mayor riesgo en internet?

Sí. Ahora mismo es el momento de mayor probabilidad de sufrir un ciberataque o problemas en internet y probablemente, según pase el tiempo, ese riesgo se irá incrementando. Fundamentalmente porque cada día hay más dispositivos conectados a internet. Y porque gran parte de estos dispositivos no han sido diseñados teniendo en cuenta la ciberseguridad desde el principio.

¿Se puede prevenir un ciberataque?

Lo más importante es la prevención. Hay recomendaciones muy básicas. La primera de ellas es desconfiar de todo aquello que no conocemos como solicitudes de amistad o mensajes de personas que no conocemos.

O los correos que llegan anunciando una devolución de Hacienda inesperada.

Sí. Debemos desconfiar de cualquier correo electrónico si viene de una fuente que desconocemos. La segunda recomendación es que debemos tener el mismo nivel de desconfianza que en el mundo físico. Si por la calle alguien nos pregunta algo nos ponemos en alerta y damos un paso atrás, pero en internet, normalmente desde la falsa sensación de seguridad que tenemos en casa o en el trabajo, aceptamos todo lo que nos viene. La tercera es actualizar los dispositivos. Muchos ciudadanos no saben que los teléfonos pueden tener antivirus. Y, por último, utilizar contraseñas robustas.

Nada de fechas de nacimiento ni el DNI, supongo.

Sí. Hay reglas nemotécnicas sencillas. Por ejemplo, coger un refrán o una frase cotidiana y con las iniciales de las palabras, haciendo una combinación de mayúsculas y minúsculas, añadiéndole un número y un símbolo, así las contraseñas son prácticamente imposibles de adivinar.

¡Uf! Y de recordar. Con la lista de contraseñas que tenemos, ¿no se puede utilizar algo que unifique todas?

Uno de los grandes retos tecnológicos que hay en internet es la identidad digital, es decir, cómo puedo identificarte con el menor riesgo posible. Se han producido muchos avances en el ámbito biométrico, aplicaciones, por ejemplo, a través de la cara, pero hay un debate en torno a mantener el anonimato, a no ser identificado en internet.

Sin embargo, muchas personas exponen diariamente sus vidas. ¿Corren más peligro los menores que han nacido viendo normal esta situación?

Los menores tienen una percepción del riesgo de un menor. Cuando a un niño o niña se le dice que no hable en la calle con desconocidos es lo mismo que decir no hables con desconocidos en internet. Pero tienen un nivel de exposición mayor. No podemos desmotivar el uso de la tecnología, sino que se utilice con unas pautas de comportamiento.

¿No aconseja prohibir?

No. Pero que los menores no utilicen la tecnología para matar el tiempo sino con un propósito y que los padres les acompañen. En el centro del menor de Incibe (IS4K) hay un manual para proteger dependiendo de la edad.

¿Es difícil encontrar a quien está detrás de una cuenta falsa en una red social?

Es muy difícil, en muchos casos, prácticamente imposible llegar al origen. Existen dos problemas al identificar el origen de los ciberataques. El ciberespacio de internet tiene una característica que lo hace especialmente atractivo para hacer estas cosas, que es el anonimato. Y es global, llega a todos los rincones del mundo, todos estamos conectados en milisegundos. Eso no ha ocurrido nunca.

¿Tiene culpa el usuario por caer en ataques que se repiten?

La tecnología es vulnerable. Siempre habrá alguien que consiga encontrar una vulnerabilidad. Eso se une a que tenemos un nivel de concienciación bastante bajo. En el ámbito de las 'fake news' lo que hay que hacer es comprobar la validez de la información. Porque algo llegue por Whatsapp o se haya publicado en internet no significa que sea verdad.

B. ALQUÉZAR

EL PERSONAJE

Nacido en Madrid en 1973 es Ingeniero Superior de Telecomunicaciones y está al frente del Instituto Nacional para la Ciberseguridad (Incibe)