El 90% de los internautas españoles ignora cómo crear una contraseña segura

El estudio de Acierto.com revela que este desconocimiento va más allá, pues solo el 20% de los usuarios cambia su clave con la regularidad necesaria

Con motivo del Día Mundial de Internet y tras **la oleada de hackeos y filtraciones masivas de los últimos meses** –Twitter ha sido de las últimas en verse afectada a principios de este mismo mayo–, el comparador de seguros Acierto.com (www.acierto.com) ha realizado un informe que revela algunos comportamientos de riesgo entre los internautas españoles. ¿El objetivo? Concienciar a los usuarios de la importancia de llevar a cabo una actitud responsable y segura en la red.

Y es que España es el país europeo donde más se navega por Internet; una nación

que ya supera los 33 millones de navegantes y que cuenta con una tasa de penetración de smartphones de más del 80%. Sin embargo, muchos usuarios no actúan de forma responsable. Los españoles no solo no mantienen actualizados sus equipos, sino que ignoran cómo debería ser una contraseña segura. En concreto, 2 de cada 5 hacen caso omiso a las notificaciones de actualización automática de su equipo, y hasta el 89% desconoce cómo crear una clave segura que proteja sus datos. Pero **solo el 8% es consciente de su propia ignorancia**. El resto cree que basta con que no contenga el usuario o con alternar mayúsculas y números.

Una buena contraseña, no obstante, debería no solo combinar mayúsculas y números, sino también minúsculas y símbolos o signos de puntuación; y contar con más de ocho caracteres de longitud (cuanto más larga, más segura). Además, debería prescindir del nombre del propio servicio, así como de datos obvios como el nombre, año de nacimiento, palabras malsonantes y similares. Otro fallo recurrente es **emplear la misma para todos los servicios**. Una buena alternativa es usar un gestor de contraseñas.

El 80% de los españoles no cambia casi nunca su contraseña

El análisis de Acierto.com, por otra parte, evidencia que **los internautas españoles tampoco son conscientes de la importancia de cambiar esta clave** regularmente, al menos cada seis meses. Por desgracia, solo el 20% de los usuarios respeta este margen. Aquí tienen cabida aquellos que lo hacen todas las semanas (un escaso 7%) y los que dejan pasar medio año (el 13%). El resto de los encuestados reconoció no hacerlo nunca (16,7%), casi nunca (30,7%) o muy de vez en cuando (32,4%).

¿Las consecuencias? Según los datos del comparador de seguros, **más de la mitad de los españoles se han visto afectados por algún virus informático**. El gran protagonista fue el malware, responsable de la infección en 1 de cada 5 ocasiones. El phishing, curiosamente, ocupa la última posición en este ranking, pues fue el causante de solo el 2% de los casos referidos.

Consejos básicos de seguridad online

Más allá de las contraseñas, existen una serie de premisas clave para protegernos online. Para empezar, deberíamos optar por conexiones seguras, es decir, evitar Wifis públicas y similares. Revisar las **políticas de privacidad** y configurar las opciones en apps y plataformas sociales, no descargar archivos ni apps de remitentes y proveedores desconocidos, deshabilitar los complementos innecesarios del navegador y realizar copias de seguridad son otras recomendaciones.

Por otra parte y con motivo de **la Semana de Internet**, han sido muchos los comercios y tiendas que han decidido premiar las compras a través de sus páginas web con descuentos online; una iniciativa que lleva fraguándose años y que dispara las ventas en la red. Sin embargo, para realizar este tipo de transacciones con seguridad existen una serie de reglas básicas.

Para empezar, conviene **desconfiar de todos aquellos mensajes en cadena a través de WhatsApp que ofrecen suculentas y dudosas ofertas**. Este tipo de links pueden no solo redirigir al usuario a portales fraudulentos, falsas páginas de Facebook y similares; sino también descargar un archivo que infecte su dispositivo. Para evitarlo y en los casos comentados, revisar el nombre de la url, verificar que el site se conecta a Internet por el protocolo https y comprobar que cuenta con el sello de confianza de Facebook será clave. En cuanto a las promociones, nada como acudir al navegador para buscar la oferta antes de pinchar en ella y de –por supuesto– difundirla.

Asimismo, conviene aumentar las precauciones con los portales desconocidos -acudiendo a foros especializados o a registros de empresa, por ejemplo- y **recelar de los vendedores desconocidos en plataformas conocidas** -tipo Amazon- que cuenten con escasas reseñas. Lo mismo ocurre con las apps de compras, cuyas reviews en la Play Store y homólogas no deberíamos dejar de leer. Las descripciones con faltas de ortografía y las solicitudes de permisos sospechosos también son reveladores. Comparar online –ya son 9 de cada 10 españoles los que lo hacen antes de comprar– también será útil. Y si ya es tarde y hemos sido víctimas de este tipo de fraude, informar al banco y denunciar a través de la Oficina de Delitos Telemáticos de la Guardia Civil resultará imprescindible para evitar su propagación.

Un seguro contra hackers

“Todo este asunto resulta especialmente importante en el caso de las empresas”, comenta Carlos Brüggemann, cofundador de Acierto.com. Y es que estos comportamientos de riesgo individuales también se llevan a cabo en las empresas, algo especialmente importante si tenemos en cuenta el incremento de hackeos, ataques con ransomware y problemas similares que hemos experimentado durante los últimos años. De hecho, **el 70% de los ciberdelitos están dirigidos a PYMES**, y en solo un año los ataques informáticos a empresas han aumentado un 130%.

Por fortuna, existen seguros específicos que permiten a las compañías protegerse ante estos problemas. “Se trata de productos que pueden cubrir desde el asesoramiento legal y la investigación de la filtración, hasta los **gastos de responsabilidad civil**, la restauración de los equipos, la recuperación del software, las multas que puedan tener lugar por la Agencia Estatal de Protección de Datos, etcétera”, explica Brüggemann.