DIARIO de IBIZA

Publicación	Diario de Ibiza Suplemento, 12	Fecha	11/02/2024
Soporte	Prensa Escrita	País	España
Circulación	4555	V. Comunicación	5 323 EUR (5,740 USD)
Difusión	3785	Tamaño	521,19 cm² (83,6%)
Audiencia	22 000	V.Publicitario	1767 EUR (1906 USD)

UNIÓN PROFESIONAL

CIBERSEGURIDAD

LOS DATOS PERSONALES, AMENAZADOS POR LA IA

FDV

LOS ATAQUES CONTRA LA PRIVACIDAD EN EL ÁMBITO CIBERNÉTICO SON CADA VEZ MÁS SOFISTICADOS Y DIFÍCILES DE ADVERTIR DEBIDO A LOS AVANCES EN INTELIGENCIA ARTIFICIAL GENERATIVA.

POR **ÁGATHA DE SANTOS**

En España,30 millones de personas –el 85% de entre 12 y 74 años– utilizan redes sociales y una cuarta parte de las compras totales se realizan ya través de Internet. Por eso,no es de estrañar que los delincuentes se hayan pasado al formato digital. De hecho, uno de cada cinco delitos en España se comete en la red. Los ciberdelincuentes no sólo acechan en busca de dinero; los datos personales también son un bien codiciado. Por ello, el Colegio Profesional de Ingeniería en Informática de Galicia (CPEIG), con motivo del Día Europeo de la Protección de Datos que se celebró el 28 de enero,pone de manifiesto la necesidad de que la sociedad esté informada y concienciada sobre los peligros a los que están expuestos los usuarios de internet.

Según el presidente del CPEIG, Fernando Suárez, los últimos ataques contra la privacidad en el ámbito de la ciberseguridad reflejan un panorama cada vez más complejo y sofisticado. Respecto a esto,el representante de los informáticos gallegos señala que los ciberdelincuentes estuvieron en los últimos meses capitalizando los avances en inteligencia artificial (IA), particularmente en IA generativa (la que hace posible aplicaciones como el ChatGPT), para crear ataques de *phishing* y suplantación de identidad más convincentes. Suárez explica que esta tendencia incluye la creación de mensajes de texto, vídeos y audios fraudulentos que son difíciles de distinguir de los legítimos. Además,se observó un uso creciente de la IA para automatizar la recopilación de datos en línea y utilizarlos en ataques dirigidos, como el *spear-phishing*, mejorando la eficacia de estos ataques al permitir la imitación de personas específicas. «Estas tendencias revelan la necesidad de una vigilancia constante y de estrategias de ciberseguridad más fuertes y adaptativas para proteger la privacidad de los datos y la integridad de los sistemas en un entorno digital cada vez más interconectada y dependiente de tecnologías avanzadas», explica el informático o,que también es el presidente del Consejo General de Colegios Profesionales de Ingeniería en Informática de España (CCII).

Suárez cree necesario avanzar en la concienciación y capacitación de toda la población,ya que no sólo los denominados colectivos vulnerables (niños y mayores) son víctimas de ataques contra la privacidad, sino que también afectan a la franja de edad entre 30 y 55 años, un foco cada vez mayor por su perfil de uso habitual de la tecnología en ámbitos como las redes sociales y el comercio electrónico. «En internet, todos somos vulnerables. Absolutamente todos», sostiene.

Lo que cambia es la tipología de los delitos. En este sentido detalla que en el caso de los jóvenes y adolesentes los más comunes son el ciberacoso,el *sexting* y el *glooming* (adulto que se hacen pasar por menores para ganarse su confianza para que compartan contenidos que luego pueden utilizar para chantajearlos). En el caso de los mayores,explica que el hecho de no haber tenido acceso a la tecnología hasta una edad más madura hace que les cueste más percibir los riesgos, lo que les convierten en el blanco de los ciberdelincuentes. Pero,insiste, en la red nadie está a salvo, ya que los adultos de 30 a 55 años, si bien ya han tenido un contacto con la tecnología y se les presupone una madurez en su uso, su posición socioeconómica y el elevado número de transacciones *online* que realizan también les convierten en el blanco de ataques de *phishing* bien por WhatsApp o SMS.

Pero el dinero no es el único bien que codician los ciberdelincuentes. Según Suárez, hay cierta tendencia a focalizar las noticias de los ciberataques de índole económica, cuando su origen suele estar en la filtración de datos personales. Por ello, considera «de vital importancia» que la sociedad tome conciencia de la necesidad de incorporarse a la cultura de la protección de datos, un derecho fundamental amparado en el artículo 18.4 de la Constitución Española,y proteger la identidad digital de las personas.

Asimismo, señala que es preciso avanzar en la visibilidad de la importancia de la higiene digital, un concepto que comprende una serie de recursos y recomendaciones orientadas a proteger la identidad digital de la persona y los datos ligados a ella, y que también tiene que ver con preservar su salud de los efectos nocivos de una sobreexposición a la tecnología. «Esto es algo que nos afecta a todos: a los jóvenes porque muchas veces hacen prácticas poco recomendables, como dormir con el móvil bajo la almohada, y a los adultos para quienes muchas veces el teletrabajo, la conexión permamente, también tiene efectos nocivos, ya que genera más estrés».

DECÁLOGO DE SEGURIDAD

- **No interaccionar** con archivos adjuntos procedentes de correos sospechosos.
- **Sistema operativo.** Mantener el sistema operativo actualizado y no descargar aplicaciones extrañas.
- **Redes públicas.** No conectarse redes públicas y, en su lugar, emplear una red privada virtual (VPN).
- **Privacidad.** Ajustar los perfiles en las redes sociales.
- **Dispositivos extraíbles.** Ser cautos a la hora de conectar dispositivos extraíbles (memorias USB, discos duros portátiles, tarjetas de memoria, CD...) a un equipo cuando provienen de terceros.
- **Incidentes de seguridad.** Avisar de los incidentes de seguridad.
- **Rastreo.** Hay que tener en cuenta que los móviles pueden ser rastreados incluso cuando están apagados.
- **'Plugins'.** Mantener todos los *plugins* y extensiones del navegador actualizados.
- **Contraseñas.** Usar contraseñas complejas y únicas. Las contraseñas largas son más seguras que una corta. No incluir datos personales en ellas.
- **Borrado seguro.** Eliminar documentación sensible de los dispositivos mediante herramientas de borrado seguro.