2025 es un año en el que sí o sí debemos mejorar nuestra seguridad digital y cuidar la salud financiera personal, principalmente ante acontecimientos globales, conflictos geopolíticos y el propio contexto nacional de cambios e incertidumbres que, sin duda, tendrán un impacto en la economía del país y la propia. ¿Sabías que la zona occidente, donde se ubica Aguascalientes, es la segunda con mayor crecimiento de compradores digitales? y ¿adivina qué? México es uno de los países con mayor tasa de cibercriminalidad. Seguramente tienes algún amigo que ha sido engañado durante la compra de algún servicio u ofertas que promocionan a través de *Whatsapp*, quizá conoces a alguien que ha sido víctima de fraude a partir de *malware* recibido en el dispositivo móvil o que ha padecido del acceso no consentido a su espacio en alguna red social. En este sentido es fundamental asegurarnos de proteger nuestra información personal para evitar usos indebidos por terceras personas, instituciones o empresas. El sentido común, destaca el maestro Óscar Jesús Zúñiga Ruiz, profesor del Departamento de Comercio Electrónico, es el que debe primar cuando realizamos alguna compra o contratación de servicios en línea. **“Es importante cuidar la información que estamos dando y cuestionarnos para qué la quiere esa empresa, a veces no lo pensamos, y nos hemos acostumbrado a lo gratuito, que no alcanzamos a ver el costo que esto tiene detrás”.** Explicó que las aplicaciones o versiones *freemium* son un modelo del comercio electrónico que busca dar un valor con el propósito de generar confianza hasta llegar a la versión premium. Es ahí, donde “debemos preguntarnos cuál es el precio que estoy pagando a cambio de que sea gratis, muchas veces en ello está el tema de los datos, entre más datos pueda recopilar una aplicación móvil, una compañía o una tiene e-Commerce, más certera será la información o publicidad que nos envía. Eso es bueno, pero muchas veces se recopilan datos que van más allá de lo que nosotros queremos dar o permisos que deseamos otorgar, como la geolocalización, los archivos multimedia, contactos e incluso, el estado de la batería”. Por su parte, el ingeniero en sistemas computacionales Diego Perales Salas, administrador de tecnologías de la información del Departamento de Redes y Telecomunicaciones de la UAA, indicó que al vivir en un mundo totalmente digital debemos tomar mayor conciencia sobre los riesgos que tenemos como usuarios, pues el 80 por ciento de los servicios que anteriormente tramitábamos de manera personal ahora se hacen en plataformas de internet. Esto significa que al loguearnos o iniciar sesión, entregamos nuestro número de teléfono o correo electrónico personal, “y estamos dando pauta a que nuestros datos estén en plataformas de terceros o que se encuentren en algún punto de la nube de internet donde los ataques son constantes y más fuertes que antes, pues ya no se trata de un virus que nos despliega un gusanito o que nos mueve el mouse en nuestra computadora; ese tipo de ataques ya cambiaron, por lo que al momento de la transferencia de datos pueden cachar nuestra contraseña, usuario y número de teléfono”, aseguró Perales Salas. Por ello, agregó, es muy importante hacer conciencia sobre el riesgo que tenemos y que, aunque no tengamos el conocimiento informático, debemos conocer estos riesgos y prevenirlos. Puso como ejemplo que, para obtener un correo electrónico, ya sea el institucional o con cualquier otro proveedor, se requiere el nombre, fecha de nacimiento y un

teléfono personal, en caso de necesitar recuperar la cuenta o la contraseña. En el contexto de nuestra universidad, es indispensable atender las recomendaciones, así como las políticas de seguridad establecidas por el Departamento de Redes y Telecomunicaciones, pues no podemos olvidar que las cuentas de correo electrónico de todos los miembros de la comunidad pueden manejar información sensible, por ejemplo, las tesis, los protocolos de investigación, trámites de patentes, información administrativa importante, etcétera. **“Es fundamental que todo el personal administrativo, académico y la comunidad estudiantil tomen en cuenta las recomendaciones que ponemos a su disposición; hay personas que son muy renuentes a los cambios, porque ya están acostumbrados a tener su contraseña guardada en el navegador”**, dijo el ingeniero Diego Perales Salas quien también es responsable de la administración de la plataforma Office 365. En este sentido explicó que guardar nuestras contraseñas en el navegador es una pésima práctica, ya que el navegador puede sufrir vulnerabilidades en sus esquemas de seguridad, lo que puede afectar nuestro correo electrónico robando información o haciendo uso indebido del correo. **Comercio en línea, el más vulnerable ante la ciberdelincuencia** A partir de la pandemia por el Covid-19, el mercado del comercio electrónico no solo representa una oportunidad de crecimiento para todo tipo de empresas, sino también el de mayor valor; al menos en México, según datos de la Asociación Mexicana de Venta Online (AMVO), durante 2023 el comercio minorista a través de plataformas digitales alcanzó más de 658 mil millones de pesos. El mismo reporte de la AMVO, “Estudio de Venta Online. Panorama del comercio electrónico y el consumidor digital en México 2024”**,** hace referencia a la creciente inclusión financiera, debido a que hay más compradores del nivel socioeconómico bajo, y al uso de medios no bancarizados para la transacción. En 2023, casi 66 millones de personas compraron algún producto o servicio, siendo los teléfonos inteligentes los de mayor uso (con un 98%) para las transacciones digitales. No por nada, los fraudes en la compra de bienes de consumo o servicios a través de redes sociales o sitios electrónicos fraudulentos también están en aumento. La AMVO también dio a conocer que 4 de cada 10 compradores declaró dejar guardados sus datos personales y bancarios al momento de la compra en línea. Ante este contexto, el maestro Óscar Jesús Zúñiga Ruiz, profesor e investigador del Departamento de Comercio Electrónico de la UAA, mencionó que este año también es fundamental que las personas sean cuidadosas al momento de hacer compras en plataformas digitales, comenzando por asegurarse de que el sitio web de la empresa sea el auténtico, pues la falsificación de tiendas online también se da continuamente. Mencionó que esta situación también es muy común que se dé con instituciones financieras, pues es a través de la *Deep web* que se pueden obtener recursos idénticos para engañar a los usuarios mediante enlaces a sitios fraudulentos que son idénticos a los oficiales, con excepción del dominio; es decir es importante verificar que éste sea el correcto. Otra modalidad es el robo de datos o identidad a través de WhatsApp, mediante el buzón de voz o enlaces falsos que te envían directamente a la aplicación; engaños durante la entrega de productos a domicilio por paqueterías establecidas o servicios de reparto independientes, ya que

podrían robar el producto, cometer un daño o robo mayor en el domicilio; o que te envíen enlaces engañosos durante la confirmación de la compra o la entrega. El académico Zúñiga Ruiz destacó también **desde la pandemia el comportamiento de los usuarios también cambió, pues en independencia de la compra online, los compradores contrastan precios y productos en internet, además de buscar beneficios, "el comercio electrónico llegó para quedarse"**; las transacciones van en aumento y las opciones de compra también se han modificado con la tecnología, pues ya se pueden realizar pagos digitales mediante QR, proximidad de la tarjeta, entre otros.

UAA a la vanguardia en seguridad institucional Gracias a la infraestructura tecnológica y los protocolos de seguridad establecidos, la Universidad Autónoma de Aguascalientes no ha tenido ataques fuertes que trasciendan en perjuicios legales o institucionales, **"gracias a que estamos tomando las precauciones correspondientes para prevenir, pero no son suficientes ya que**

estamos expuestos a vulnerabilidades en la información que manejamos en internet”, puntualizó Diego Perales Salas, administrador de tecnologías de la información. Entre las acciones que impulsa la UAA, destaca la implementación del factor de doble autenticación para toda la comunidad universitaria; si bien no garantiza la protección al 100 por ciento, sí brinda mayor estabilidad en todas las cuentas institucionales. Las cuentas de correo electrónico de todos los estudiantes de nuevo ingreso, así como las de personal administrativo y académico de nuevo ingreso o reingresos, deberán aplicar esta política, descargando la aplicación Microsoft Authenticator en el cual se recibirá el código de seguridad para tener acceso a la cuenta. Otras de las medidas son el bloqueo de cuentas si se teclea la contraseña equivocada. Si se equivocan tres veces para ingresar al correo institucional la cuenta se bloquea por un periodo de cinco minutos, pero si el usuario se vuelve a equivocar la cuenta se bloquea de manera definitiva; en ese caso se tiene que acudir con el administrador de tecnologías. También se está trabajando para unificar el uso de las cuentas institucionales en las aplicaciones internas; así como la implementación de protocolos de seguridad rigurosos para detectar ataques maliciosos y garantizar la seguridad del dominio y la administración de las tecnologías institucionales. En la UAA existen cerca de 28 mil cuentas institucionales @edu.uaa.mx, por lo que para el área de tecnologías de la UAA es importante lograr la confianza de la comunidad universitaria para aplicar las medidas de seguridad y contribuyan a la protección de la información institucional. Diego Perales Salas recalcó que lograr que todos los usuarios lleguen a utilizar el doble factor de autenticación es el principal reto, pues eso significaría una garantía para mantener una información sana, sin amenazas dentro del buzón y sin que le lleguen más.

Referencias Estudio de Venta Online. Panorama del comercio electrónico y el consumidor digital en México 2024, Asociación Mexicana de Venta Online
https://www.amvo.org.mx/estudios/estudio-sobre-venta-online-en-mexico-2024-3/