Ciberseguridad en México: aún falta conciencia, educación y talento especializado, advierte experto

BOLETÍN 209

- La ciberseguridad debe ser vista como un acto ético. No se trata de atacar, se trata de proteger.
- Las buenas prácticas del consumidor también son esenciales para evitar fraudes.

José de Jesús Jiménez Cruz, egresado de la Universidad Autónoma de Aguascalientes y especialista en seguridad informática, ofreció el taller “Ciberseguridad en el E-commerce” como parte de las actividades de la Ecommerce Week de la Licenciatura en Comercio Electrónico de esta casa de estudios.

Jiménez Cruz señaló que, en un entorno digital cada vez más vulnerable, la ciberseguridad se

convierte en una necesidad urgente para quienes desarrollan y gestionan tiendas en línea. No obstante, a pesar de los nuevos avances, México aún está rezagado en la materia: “Muchas pymes todavía no ven la ciberseguridad como una inversión. Falta educación digital, estandarización obligatoria y más talento especializado” advirtió.

Durante su charla en la UAA, abordó las principales amenazas que enfrentan actualmente los negocios digitales en México: *phishing, malware,* ataques de denegación de servicios (DDoS) y robo de datos bancarios, muchas veces provocados por configuraciones incorrectas o errores humanos. “Uno de los errores más comunes es la falta de actualizaciones y el uso de contraseñas débiles. Aunque suene básico, sigue siendo una de las principales puertas de entrada para los atacantes”, apuntó.

El *phishing*, explicó, suele manifestarse mediante correos electrónicos que aparentan ser legítimos, pero que redirigen a sitios falsos diseñados para robar información sensible. Asimismo, mencionó que el *malware* puede ocultarse en *plugins* o plantillas vulnerables, mientras que los ataques de denegación de servicio (DDoS) saturan las páginas con tráfico automatizado, impidiendo su funcionamiento normal.

Con respecto a la protección del usuario, recomendó estar atentos a señales básicas de seguridad como el uso del protocolo HTTPS, el ícono del candado en la barra de direcciones y la reputación general del sitio web.

Entre las tendencias emergentes en ciberseguridad, Jiménez Cruz destacó el uso malicioso de la inteligencia artificial, como los *deepfakes*, *bots* que simulan tráfico legítimo, y la adopción creciente del modelo Zero Trust, que exige validaciones continuas para cada acceso, tanto interno como externo.

A los futuros profesionistas, el analista junior en ciberseguridad, les aconsejó documentarse y mantenerse actualizados, sin importar el rol que desempeñen en el comercio electrónico. “Ya sea que diseñen, programen o gestionen plataformas, deben considerar la seguridad digital como parte esencial de su trabajo. En Internet, la información o la proteges tú, o alguien más la va a aprovechar”, declaró.

Finalmente, destacó que la ciberseguridad debe ser vista como un acto ético: “No se trata de atacar, se trata de proteger. Es una forma de servir a los demás. Ya sea profesional o digitalmente, la seguridad también es una responsabilidad”, concluyó.

Universidad Autónoma de Aguascalientes

Departamento de Comunicación y Relaciones Públicas

---000---

Ciudad Universitaria

25 de mayo del 2025