Cuidado con el “deepfake”: 5 claves para no caer en esta estafa digital

La inteligencia artificial sigue avanzando y, con ella, también evolucionan las formas de estafa digital. Estas últimas semanas, se ha visto un incremento en las campañas fraudulentas que usan tecnología de ***“deepfake”*** para simular la voz o imagen de figuras públicas o líderes de empresas reconocidas, ofreciendo productos o promociones falsas. Este tipo de contenido digital manipulado, generado o editado mediante el uso de inteligencia artificial, puede mostrar personas reales o ficticias en situaciones o acciones que no ocurrieron realmente, o promocionando inversiones con tasas de rentabilidad extraordinarias con el fin de cometer un fraude o estafa. Frente a esta amenaza, **Luis Chávez, líder de Educación en Prevención de Fraudes del BCP,** comparte cinco recomendaciones clave para evitar caer en estas trampas.

Tómate un minuto para verificar bien la información y no caer en deepfake.

LEA TAMBIÉN: Empresas frente a los ciberataques: protocolos y respuestas frente a los hackers

1. No tomes decisiones impulsivas:

Los estafadores aprovechan momentos de alta expectativa para captar tu atención con supuestas promociones limitadas, regalos instantáneos o inversiones que multiplican tu dinero fácilmente. No te dejes llevar por la emoción: tómate un minuto para verificar la información.

2. Verifica siempre la fuente:

Revisa con atención el nombre del usuario y asegúrate de que se trate de la cuenta o página oficial de la fuente de información. Un simple error en el nombre o un enlace sospechoso puede marcar la diferencia entre estar seguro o ser víctima de un fraude.

3. Si suena demasiado bueno, probablemente no es real:

Desconfía de las promociones que prometen ganancias rápidas o premios increíbles sin sorteos. Las tasas de inversión extraordinarias y las recompensas inmediatas son señales de una posible estafa.

4. Cuidado con la presión por actuar rápido:

Los estafadores suelen crear un falso sentido de urgencia. Si una oferta aparece “solo por hoy” y te piden ingresar datos de tu tarjeta, clave, token o CVV de manera inmediata, desconfía. Esa presión es parte del engaño.

5. Presta atención a las señales:

Busca expresiones faciales que no coinciden con el tono de la voz, parpadeos raros o movimientos desincronizados entre los labios y el audio. Además, las voces generadas por AI suelen sonar planas, o con una entonación extraña, como si la persona tuviera un acento o errores de pronunciación. Estos pueden ser indicios que estás frente a un “*deepfake*”.

LEA MÁS:

Ciberseguridad para pymes: pasos clave para evitar ataques digitales

Ciberseguridad: recomendaciones para que los emprendedores eviten los hackeos o estafas