

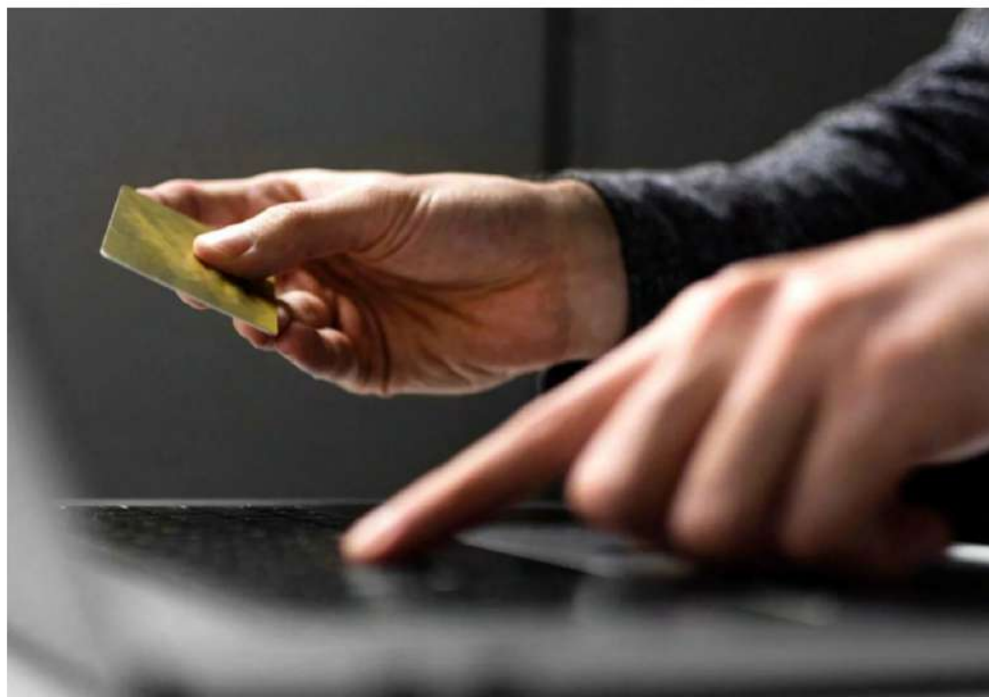
Proponen innovadoras estrategias para frenar el fraude digital

En un contexto de aumento sostenido de los fraudes en medios de pago digitales en Chile, la Facultad de Economía y Negocios de la Universidad de Chile y el Servicio Nacional del Consumidor (SERNAC) presentaron dos estudios que analizan el fenómeno y ofrecen recomendaciones para fortalecer la protección de los usuarios.

Los estudios, liderados por el académico de la FEN Uchile, Cristóbal Barra, junto al equipo del SERNAC, abordan tanto los determinantes de la autoprotección del consumidor como la eficacia de las campañas contra el phishing. Ambos documentos son parte de una alianza estratégica entre el SERNAC y la FEN, con foco en el diseño de políticas

En respuesta al creciente aumento del fraude en medios de pago digitales, la Facultad de Economía y Negocios de la Universidad de Chile y el SERNAC desarrollaron dos investigaciones que revelan el impacto del vishing en el país

Sigue en página siguiente



Viene de página anterior

públicas basadas en evidencia.

EL FACTOR HUMANO EN LA SEGURIDAD DIGITAL

Uno de los hallazgos clave es que la tecnología, por sí sola, no basta para frenar el fraude digital. Según el profesor Barra, el comportamiento de los usuarios es el principal factor de riesgo: “La eficacia de la tecnología en la prevención del fraude es limitada sin la promoción activa de conductas de autoprotección entre los consumidores”, explica.

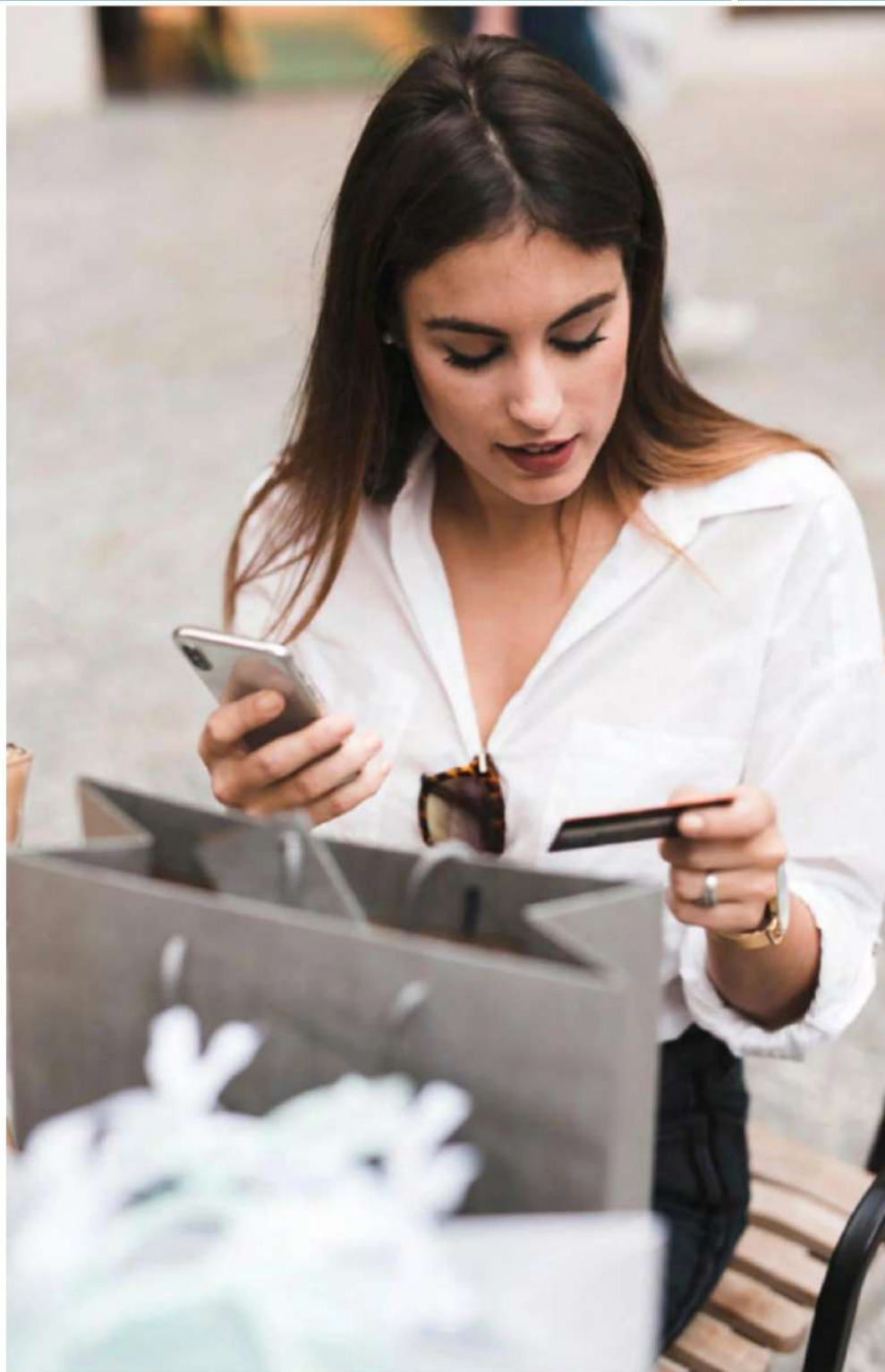
Por eso, los estudios proponen estrategias conductuales para aumentar la conciencia y cambiar hábitos, basándose en modelos como la Teoría de la Motivación de Protección y la Teoría del Comportamiento Planificado.

El análisis reveló que la autoeficacia, es decir, la creencia del consumidor en su capacidad para protegerse, es el factor más relevante para reducir los riesgos de fraude. Además, la percepción de la gravedad del fraude es otro motor de cambio: “Los consumidores que consideran graves las consecuencias del fraude están más motivados para adoptar medidas preventivas”, indicó Barra.

También se identificó un problema: los costos percibidos (tiempo, esfuerzo o complejidad) desincentivan la acción. Por eso, el estudio recomienda simplificar los procesos de protección y facilitar el acceso a la información.

EL VISHING: FRAUDE TELEFÓNICO EN ALZA

El trabajo también revela datos preocupantes sobre las formas de fraude más frecuen-



tes. Si bien el phishing (correo o mensaje fraudulento) sigue siendo relevante, el vishing (fraude telefónico) se ha convertido en la modalidad más extendida.

“Según los reclamos recibidos por el SERNAC, el vishing representa el 71 % de los fraudes vinculados al phishing en Chile. Dentro de estos casos, casi el 70 % de las víctimas son mujeres”,

advirtió Cristóbal Barra.

JUEGOS SERIOS Y CAMPAÑAS PERSONALIZADAS: UN NUEVO ENFOQUE

El segundo estudio evaluó, mediante un experimento con-

Sigue en página siguiente



Cristóbal Barra, académico de la FEN Uchile, lideró las investigaciones que proponen estrategias conductuales para prevenir el fraude digital.

Viene de página anterior

trolado aleatorizado (RCT), cómo mejorar las campañas de prevención. Los resultados mostraron que los mensajes tradicionales no son suficientes. La incorporación de juegos serios, dinámicas interactivas que simulan situaciones de fraude, resultó ser la estrategia más eficaz para cambiar actitudes y conductas preventivas.

“Los juegos permiten a las personas poner en práctica las recomendaciones de seguridad en un entorno controlado, reforzando la autoeficacia y mejorando su disposición a actuar”, explicó el académico de la FEN.

ADEMÁS, EL ESTUDIO PROPONE:

Explicar las técnicas de ingeniería social: es clave que los usuarios conozcan cómo operan los delincuentes para poder identificar fraudes.

Incorporar mensajes motivacionales bien diseñados, pero

siempre combinados con elementos prácticos.

Personalizar las campañas según el perfil del consumidor, usando medios adecuados para cada grupo etario. Los adultos mayores, por ejemplo, prefieren el correo electrónico, mientras que los jóvenes responden mejor a videos interactivos.

Evaluar y ajustar constantemente las campañas, con métricas claras y herramientas de retroalimentación.

HACIA UNA POLÍTICA PÚBLICA MÁS EFECTIVA

Ambos estudios entregan recomendaciones concretas para fortalecer la educación digital y la protección del consumidor, en línea con la nueva

Ley N° 20.009, que impone a los usuarios la responsabilidad de adoptar medidas de autoprotección y a las entidades financieras el deber de informar adecuadamente sobre los riesgos.

“Las campañas de ciberseguridad son esenciales, pero deben evolucionar. Necesitamos herramientas que realmente impacten la conducta del usuario, y ahí los juegos serios y las intervenciones conductuales tienen un rol clave”, concluye Cristóbal Barra.

