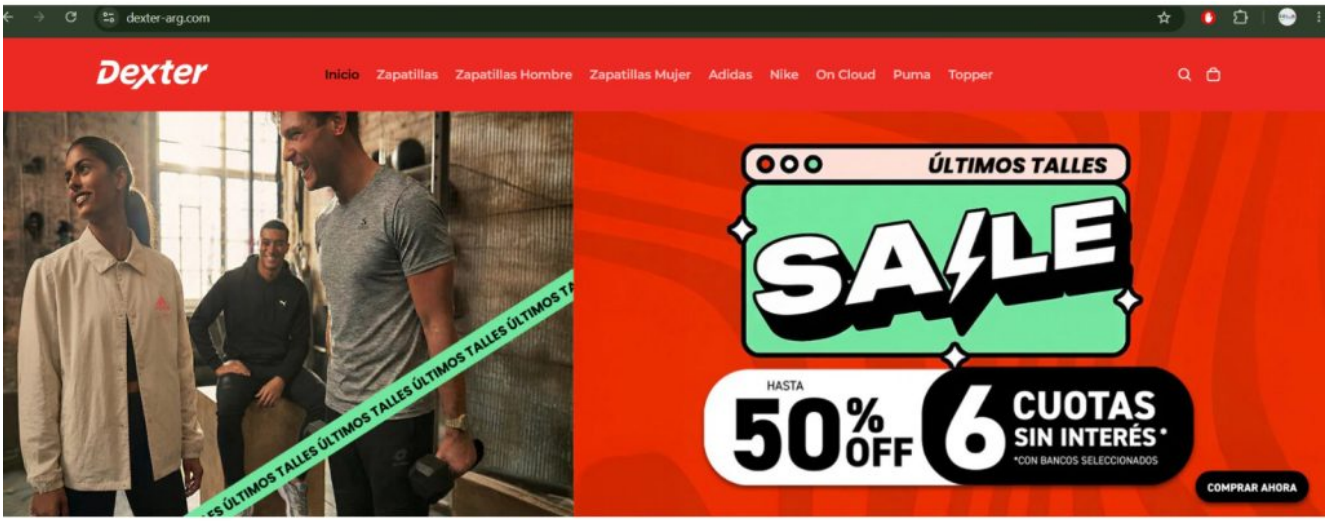
Siguen las estafas a través de páginas web clonadas: en qué consiste el engaño y cómo prevenirlo

27/05/2026



ÚLTIMOS TALLES

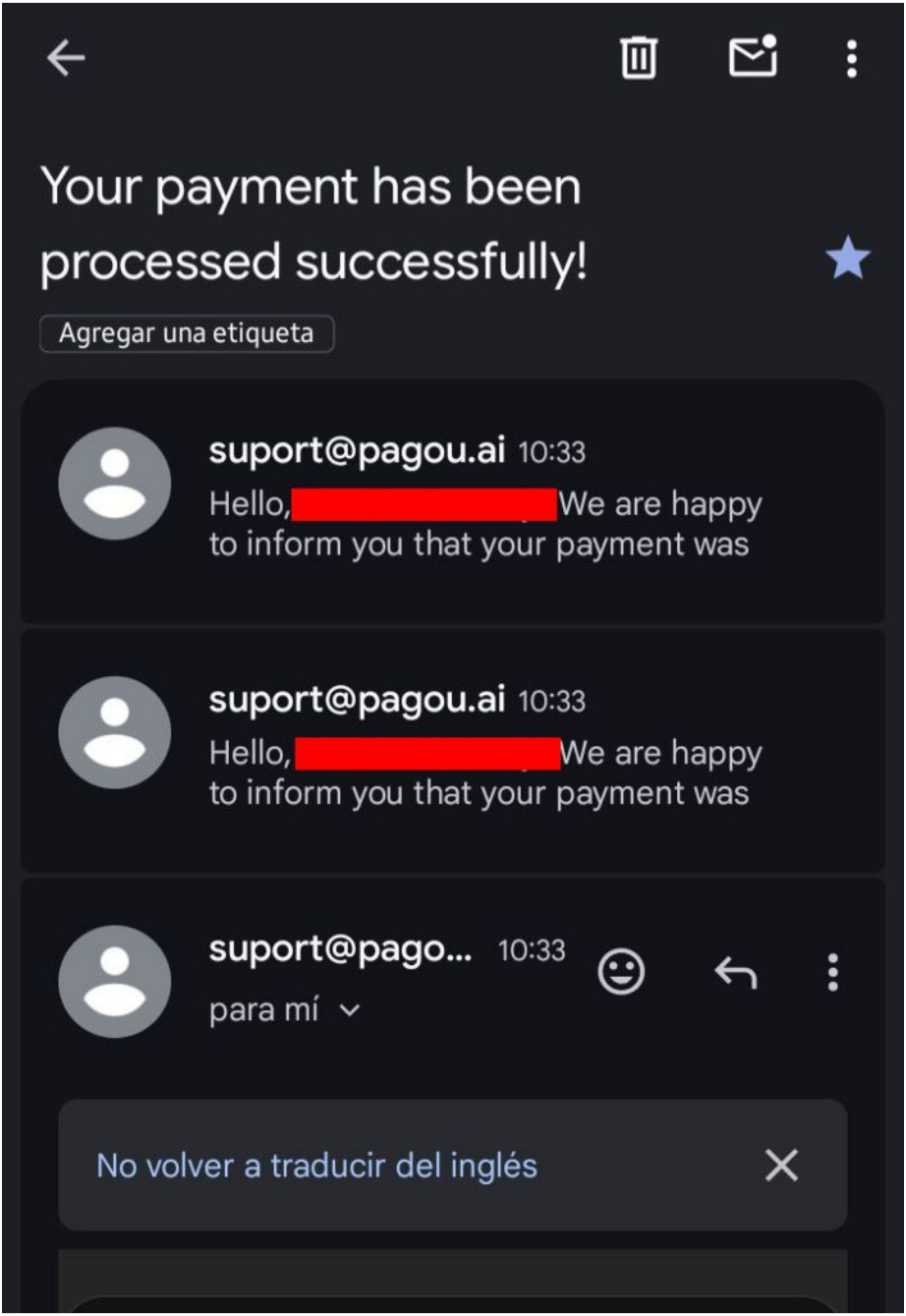
El accionar de delincuentes que aprovechan la tecnología para delinquir claramente no tiene límites, y así queda demostrado tras conocerse una serie de estafas virtuales que ha padecido más de un sanrafaelino.

Para contar bien a fondo en qué consiste este nuevo artilugio al que apelan sujetos de malvivir, nos ocuparemos del caso de Julio, un vecino de nuestro departamento que cayó en la trampa.

Según relató en diálogo con **Diario San Rafael**, se encontraba navegando en la sección **Marketplace de Facebook**, donde suele haber diferentes productos para la compra y venta. A Julio le llamó la atención una publicidad que – a simple vista – correspondía a **Dexter**, una reconocida tienda de calzado e indumentaria deportiva que también cuenta con página web para

adquirir múltiples productos de esos rubros de manera virtual. La imagen que acaparó el interés de la víctima era de unas zapatillas **marca Adidas que, en oferta y con descuento, quedaban en $30.000**.

Al hacer click en la imagen antes mencionada, Julio ingresó al sitio de Dexter, más precisamente al apartado donde figuraba el producto. **“Pude hacer todo como si estuviese en el sitio propio de la empresa, desde seleccionar el talle y luego el método de pago. Fui a pagar para terminar la operación y opté por realizar la compra con mi tarjeta de crédito, lo que ejecuté sin problemas. Tras llenar mis datos, el sitio indicó que la transacción había finalizado correctamente”**, detalló el damnificado.



Las sospechas de Julio surgieron cuando recibió un correo

electrónico en inglés, que si bien – traducido – informaba "que el pago había sido recibido con éxito", en ningún lado estaba vinculado a Dexter, la tienda donde – a priori – había efectuado la compra del calzado.

En virtud de lo anterior, Julio se comunicó con una operadora del Banco de la Nación Argentina, emisor de la tarjeta con la que realizó el pago, desde donde confirmaron que dicha operación no se había realizado con la tienda Dexter. A modo preventivo, y para evitar otras operaciones por parte de los delincuentes, desde la entidad bloquearon el plástico para dejarlo inutilizable.

"Es un sistema muy sofisticado, de hecho, me enviaron un correo para solicitar el seguimiento del producto que nunca iba a llegar, pero son maniobras complementarias para dotar de credibilidad a lo que montan", añadió Julio.

De acuerdo a las averiguaciones realizadas por este diario, no es el primer caso que se registra en San Rafael y mucho menos a nivel país, donde – según reportes de diferentes medios y

advertencias policiales – los hechos se han multiplicado, especialmente en períodos como el reciente “Hot Sale”, programa de ofertas y descuentos en tiendas virtuales.

Los delincuentes, con claros conocimientos tecnológicos, clonan páginas web auténticas, pagan publicidad en Google o en redes sociales, difunden importantes ofertas y así buscan captar la atención de internautas que acceden como si se tratara de los sitios verdaderos, entregan datos de tarjetas de crédito y/o débito y realizan pagos a cambio de productos que nunca recibirán. Y de no advertirlo de inmediato, quedan expuestos a que los maleantes realicen múltiples operaciones por las que las víctimas pierden más dinero.

¿Cómo evitar este tipo de estafas?

Hay un dato clave que tiene que ver con la dirección web que utilizan los delincuentes para ejecutar las estafas antes mencionadas. En el caso de Julio, el sitio al que accedió para adquirir las zapatillas continúa online y es **www.dexter-arg.com**, cuando el verdadero sitio de la empresa es **www.dexter.com.ar.** Es muy importante prestarle atención a este detalle, más allá de claras diferencias entre una y otra página, aunque muchas veces eso puede pasar inadvertido.

Además, especialistas en delitos informáticos sugieren evitar acceder a sitios cuyos enlaces llegan por correo electrónico o Whatsapp. Y otro detalle a tener en cuenta: este tipo de engaños viene acompañado de ofertas que suelen ser muy tentadoras, tanto que es importante revisar la dirección web de la empresa que realiza la promoción o ingresar a buscadores como Google para constatar el sitio de la parte vendedora.