La Asociación de Bancos orienta a los usuarios financieros en materia de ciberseguridad ante las compras de temporada

*La ABA citó el ‘smishing’ y el ‘quishing’, entre las nuevas modalidades de estafas, e invitó a visitar su portal yonavegoseguro.com.do, donde ofrece informaciones de ciberseguridad.*

**Santo Domingo, Rep. Dom.-** La Asociación de Bancos Múltiples de la República Dominicana (ABA) orientó a los usuarios sobre las nuevas tendencias en las modalidades de ciberdelitos y ofreció algunas recomendaciones, en aras de salvaguardar la integridad de sus transacciones durante la temporada de compras del Viernes Negro, CiberMonday y Navidad.

La ABA destacó que los ataques más frecuentes se realizan mediante ingeniería social, como el *phishing*, que emplea correos electrónicos o sitios web falsos para engañar a los usuarios y obtener información confidencial que luego puede ser usada en otros tipos de fraudes.

Expuso que la suplantación de identidad, donde se simula ser una fuente confiable o reconocida por el usuario, y el *malware*, un software malicioso diseñado para dañar la computadora o celular con el fin de robar datos o causar daños mayores, son otras formas de ciberataque.

“La información personal es sumamente valiosa y se debe evitar compartirla en sitios web o aplicaciones que no sean de confianza. Los bancos nunca solicitarán información confidencial por redes sociales, correo electrónico u otro tipo de mensajería digital”, recomendación que el Comité de Ciberseguridad asegura debe tomarse en cuenta no sólo en la época, sino de manera permanente.

**Nuevas modalidades de ciberdelitos**

La ABA detalló que, acorde avanzan las tecnologías, aparecen nuevas maneras en que los ciberdelincuentes intentan conseguir sus propósitos malsanos.

“Si bien, de fondo, se mantiene la misma tendencia de poder obtener las credenciales de clientes, lo que ha cambiado es la forma de conseguirlas. Con el uso de recursos de la inteligencia artificial para clonar la voz o para generar videos de personas a partir de imágenes, los defraudadores han sofisticado la forma de engañar”, advirtió el Comité de Ciberseguridad del gremio bancario.

Puso como ejemplo un video con la imagen (falsa) de alguien famoso recomendando invertir en un negocio muy rentable, para lo que requiere una pequeña inversión y suministrar sus datos confidenciales con el fin de hacer realizar la supuesta transacción.

En tanto, el *smishing*, término que combina “SMS” y “phishing”, es otra forma de ataque cibernético que utiliza mensajes de texto (SMS) para engañar a las personas y obtener información sensible como contraseñas, números de tarjetas de crédito o datos bancarios, agregó la ABA.

**“**En un ataque de *este tipo*, los delincuentes envían mensajes que parecen provenir de fuentes confiables, como bancos o empresas conocidas. Suelen crear un sentido de urgencia, pidiendo al destinatario que haga clic en un enlace o proporcione información personal para evitar consecuencias negativas”, detalló.

Indicó que otra nueva modalidad, como es el *quishing,* no utiliza enlaces sino que procura llevar a las personas a sitios web apócrifos solo con el escaneo de un código QR.

**Recomendaciones para navegar seguro en internet**

La Asociación de Bancos compartió algunas recomendaciones de utilidad para los usuarios financieros, como para el público en general que utiliza el ciberespacio, entre las que figuran:

* **No compartir información personal o financiera** a través de correos electrónicos o mensajes no solicitados.
* **Desconfiar de las ofertas extremadamente buenas,** pues tienen una alta probabilidad de ser una estafa.
* **Estar atento si se pide pagar con tarjetas de regalo**, transferencias bancarias o criptomonedas.
* **Verificar que los sitios web tengan una dirección física** y un número de teléfono de contacto.
* **Tomarse un momento,** pues los estafadores a menudo buscan que se actúe rápidamente y sin pensar.
* **Observar los errores** gramaticales y ortográficos que, con frecuencia, contienen los sitios falsos.
* **Mirar si no hay reseñas o abundan las negativas**, lo que puede ser indicativo de un sitio no confiable.
* **Velocidad de carga lenta** o comportamiento inusual del sitio, como redirigir a múltiples páginas, podría significar que está comprometido o es peligroso​.
* **Constatar que, en la barra de direcciones, el sitio comience con "https"** (la "s" indica una conexión segura).
* **Revisar regularmente los estados de cuenta** y de tarjetas de crédito para detectar cualquier actividad sospechosa y reportarla a la entidad bancaria.
* **Actualizar el software antivirus y de seguridad** para protegerse contra malware y otras amenazas.

Finalmente, la ABA invitó a ampliar estas y otras recomendaciones en el portal [www.yonavegoseguro.com.do](http://www.yonavegoseguro.com.do), iniciativa de la entidad que ofrece orientación en materia de ciberseguridad, tanto para uso personal como empresarial o institucional.

**Dirección de Comunicación y Marketing**

07 de noviembre 2024