Bogotá, diciembre 2025

Sugerencias de ciberseguridad para temporada decembrina

Todos sabemos que diciembre es una época lucrativa para el comercio, pero también es la "temporada pico" para los ciberdelincuentes. Aprovechando que las personas están distraídas con las fiestas, las compras y los viajes, los ciberatacantes han perfeccionado nuevas modalidades y reactivado otras clásicas.

Este documento resume las amenazas críticas detectadas recientemente y sugiere cómo protegerse de forma simple y efectiva.

1. NUEVAS MODALIDADES DETECTADAS (Alta Peligrosidad)

Se han identificado, en especial, dos modalidades de estafa que están afectando masivamente a usuarios de equipos celulares. Preste especial atención:

A. La Trampa de la "**Solicitud de Dinero**" en Billeteras Digitales
Los delincuentes se aprovechan de la familiaridad con apps **como Nequi** para vaciar cuentas en segundos.

Cómo le tienden la trampa? Usted recibe una notificación en su celular que parece un envío de dinero. Simultáneamente, alguien (fingiendo ser un amigo, cliente o conocido) le avisa que "ya le giró la plata".

La notificación no es de dinero entrante, es una **SOLICITUD DE COBRO**. Al ver el aviso, el usuario instintivamente presiona "Aceptar", creyendo que está aceptando recibir el dinero.

La Realidad es que al hacer clic en "Aceptar", usted está autorizando que saquen dinero de su cuenta hacia la del estafador.

TIP DEL EXPERTO: Regla de Oro: Para recibir dinero **NUNCA** necesita presionar el botón "Aceptar" ni poner su clave. El dinero entra automáticamente.

Si ve una notificación que le pide "Aceptar" o "Confirmar" una transacción que supuestamente es a su favor, rechácela inmediatamente.

B. La "**Llamada Fantasma**" y el **Espionaje Silencioso**.

Una modalidad técnica preocupante que busca robar datos bancarios y contraseñas mediante el monitoreo del entorno del usuario.

Se da cuando usted recibe llamadas insistentes de números desconocidos. Al contestar, nadie habla, suena un tono o le cuelgan de inmediato.

El riesgo radica en que, en algunos casos sofisticados, esta interacción busca mantener activa una conexión en segundo plano para **activar el micrófono o la cámara** sin que usted lo note, permitiendo a los delincuentes escuchar conversaciones o ver datos sensibles.

Es posible que usted puede detectarlo observando la parte superior de la pantalla de su celular (punto verde o naranja indioca la activación de cámara o micrófono), dependiendo del modelo del equipo o el sistema operativo. En equipos antiguos, el riesgo es mayor porque el usuario no tiene forma de saberlo.

TIP DEL EXPERTO: Si sospecha, o como rutina, proceda de la siguiente forma:

- Active inmediatamente el "Modo Avión" por al menos 30 segundos (es más rápido que apagar el teléfono y corta la transmisión de datos al instante). Luego, con calma, apague o reinicie el dispositivo para cerrar los procesos maliciosos. Esto corta cualquier transmisión de datos.
- Luego, reinicie el dispositivo.
- Bloquee el número sospechoso de inmediato.

2. AMENAZAS CLÁSICAS REACTIVADAS PARA DICIEMBRE

Los viejos trucos vuelven porque siguen funcionando. Esté alerta a lo siguiente:

A. El **Falso Paquete Retenido** (Smishing)
Llega a su teléfono móvil un SMS o WhatsApp diciendo: "Su entrega de (Servientrega/Amazon/4-72) está retenida por falta de dirección. Ingrese aquí para actualizar datos".

¿Cuál es el Riesgo y el Peligro Real? El riesgo se materializa en el momento en que usted hace clic en ese enlace. El objetivo no es enviarle el paquete, sino:

1. Robar sus Datos Bancarios (Phishing): Lo redirigen a una página falsa idéntica a la de la transportadora o a un falso formulario de pago, donde le solicitan ingresar los datos completos de su tarjeta de

crédito/débito para cobrarle una tarifa mínima de reenvío (a menudo menos de $5.000). Con esa información, roban muchas veces más.
2. Instalar un Virus (Malware): El enlace puede descargar silenciosamente un *software* malicioso (*malware*) en su celular, que luego espía sus claves o toma control remoto de su dispositivo.

TIP DEL EXPERTO: Nunca abra enlaces de SMS. Vaya directamente a la página oficial de la transportadora con su número de guía.

B. La Oferta "**Demasiado Buena para ser Verdad**"
Usted recibe publicidad en Instagram o Facebook u otras redes sobre marcas reconocidas (Ray-Ban, Nike, Adidas) con descuentos del 80% o 90% debido, supuestamente, a promociones por la época.

Tenga cuidado ya que suelen ser páginas clonadas. Usted paga, el producto nunca llega y además se quedan con los datos de su tarjeta para hacer compras millonarias.

TIP DEL EXPERTO: Si el precio es irreal o le genera sospecha, la tienda es falsa. Verifique siempre la URL (dirección web) antes de comprar.

3. DECÁLOGO DE PROTECCIÓN PRÁCTICA

Para navegar seguro este fin de año, siga estos 5 pasos sencillos:

Cero Confianza: Si lo llaman del "Banco" por un supuesto fraude, para actualizar su equipo (de 4G a 5G) y le piden códigos que llegaron por SMS, **CUELGUE.** El banco nunca pide esos códigos; los estafadores los necesitan para robarle su cuenta.

No recicle contraseñas: Si usa la misma clave para su correo y para su banco, y una página de compras falsa le roba la clave, perderá todo.

Haga un monitoreo visual: Acostúmbrese a mirar los puntos de privacidad (verde/naranja) en su celular periódicamente.

Lea antes de tocar: En las Billeteras Digitales, tómese 5 segundos para leer si la notificación dice "Envío" o "Solicitud/Cobro".

Desconfíe de la urgencia: Cualquier mensaje que diga "Su cuenta será bloqueada en 24 horas" o "Última oportunidad" busca bloquear su juicio lógico mediante el miedo. Respire y verifique por canales oficiales.

"La seguridad no es solo tecnología, es desconfianza inteligente. Créale a su instinto" Por favor, comparta esta información con su círculo familiar y laboral.

My (RP) **Héctor Castro Corredor**
Administrador Policial.
Consultor SVSP.