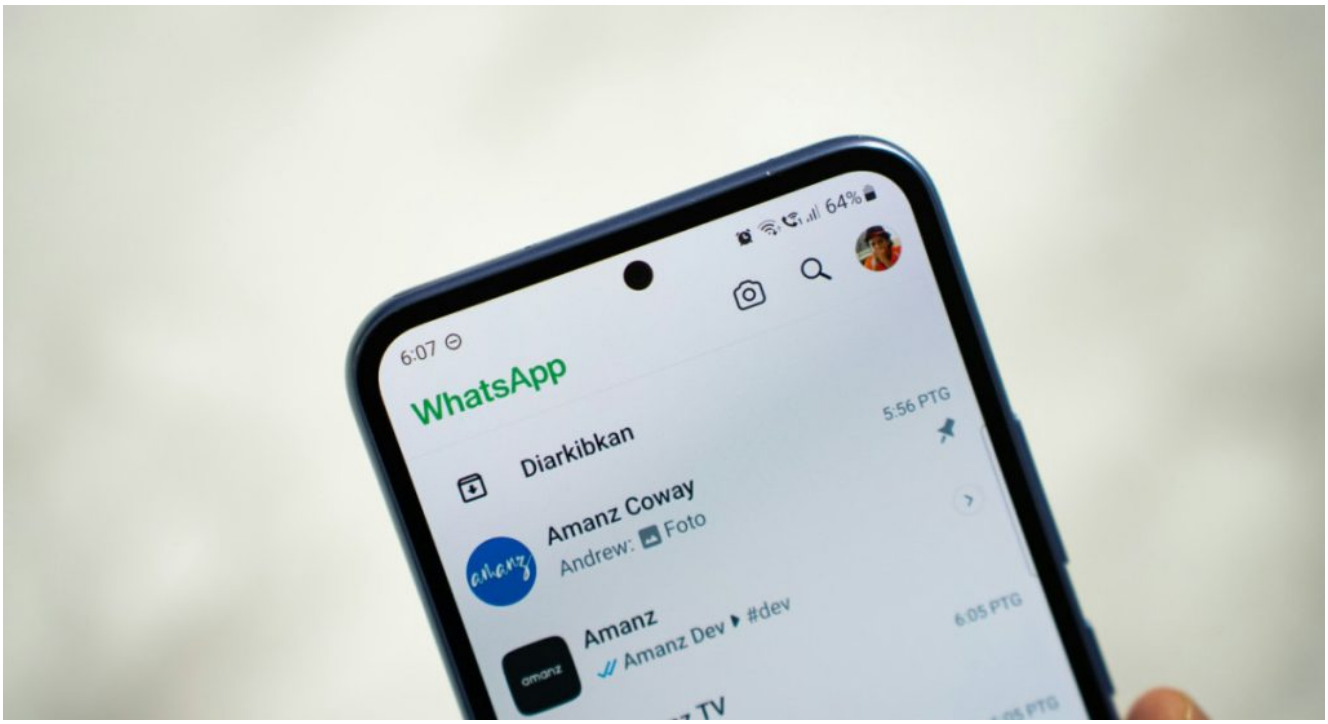
¡Cuidado! Nunca toques este botón en WhatsApp o podrán ingresar a tu homebanking

08/07/2024



En un contexto donde las estafas en redes sociales son moneda corriente, de manera diaria nos encontramos con consejos de especialistas para cuidarnos.

Sucede que los **ladrones virtuales** buscan nuevas tácticas y ahora, a través de una videollamada, pueden lograr su encomienda: acceder a los dispositivos en un instante.

El engaño es simple: hacerse pasar por un amigo o familiar, dado que es el «anzuelo» para atrapar a los internautas e ingresar a su homebanking.

WhatsApp. Foto: Unsplash

El botón que no debés presionar jamás

Los **ciberdelincuentes permite convencer** a las víctimas de aceptar una videollamada. Primero se hacen pasar por un amigo o familiar, rápidamente dan aviso de una falla técnica. Al comenzar la conversación, le solicitan apretar un botón que aparecerá en la pantalla de su celular.

«WhatsApp **tendrá acceso a toda la información que sea visible** en la pantalla o que reproduzcas en tu dispositivo durante una grabación o transmisión. Se incluyen las contraseñas, los detalles de pago, las fotos, los mensajes y el audio que reproduzcas», dice el alerta que envía la aplicación.

En caso de presionar la opción «**comenzar ahora»,** los delincuentes tendrán acceso a todas las aplicaciones del dispositivo. Eso es posible cuando el usuario comparte pantalla y, a partir de allí, tu homebanking está en riesgo.

La herramienta para proteger el celular

Para evitar **cualquier tipo de ingreso** al celular mediante imágenes, videos y otros enlaces, es importante desactivar el Bluetooth del celular. Los hackers lo utilizan para conectarse **a través de esta red inalámbrica** para hacer un escaneo de las vulnerabilidades del smartphone.

Al no tener **conectado el bluetooth**, no se pueden compartir archivos ni dar acceso al teléfono a ningún dispositivo y de esta forma, la información que se encuentra almacenada está protegida.

Ciberseguridad. Foto: Unsplash

Por otro lado, **cabe destacar que los usuarios no deben aceptar peticiones** de conexión si no lo están requiriendo y a la hora de usar el bluetooth, verificar muy bien el dispositivo con el que se emparejará el teléfono.

Además, **el software del celular** debe mantenerse siempre actualizado, las contraseñas deben ser seguras o difíciles de adivinar y sin datos demasiados personales.

Fuente: Canal 26