LITORALPRESS

Fecha: 13-04-2026
Medio: Las Últimas Noticias
Supl. : Las Últimas Noticias
Tipo: Noticia general
Título: **A notera de TVN le robaron su celular desbloqueado: perdió $7.000.000**

Pág. : 19
Cm2: 612,6

Tiraje: 91.144
Lectoría: 224.906
Favorabilidad: No Definida

"No sabía que podían entrar al banco", admite Viktorya Ozbicakci

A notera de TVN le robaron su celular desbloqueado: perdió $7.000.000

Mejor prevenir: funciones nativas de los iPhone ayudan a contener la cadena de desastres que puede generar un lanzazo.

WILHEM KRAUSE

A la periodista Viktorya Ozbicakci, del "Buenos días a todos" y "El medio día", le ha tocado duro el inicio del año laboral. El lunes pasado, ella y su equipo fueron agredidos en vivo en medio de un retiro de autos abandonados en Peñalolén.

Pero el mes pasado a Viktorya le había tocado algo quizás peor. En lunes 2 de marzo partió a Américo Vespucio con la Rotonda Grecia para informar sobre el flujo vehicular. Mientras coordinaba su móvil, segundos antes de salir al aire, un motochorro le arrebató su iPhone desbloqueado de las manos y salió manejando veloz por Av. Grecia.

"Me desesperé, corrí detrás de él, pero obviamente fue imposible alcanzarlo y cancelé el despacho. Fue exactamente en un segundo, me lo quitó por la espalda y no alcancé a reaccionar ni a entender lo que había sucedido. Lo único que me importaba en ese momento era recuperar mi teléfono, nunca imaginé que me robarían dinero", recuerda la notera de TVN.

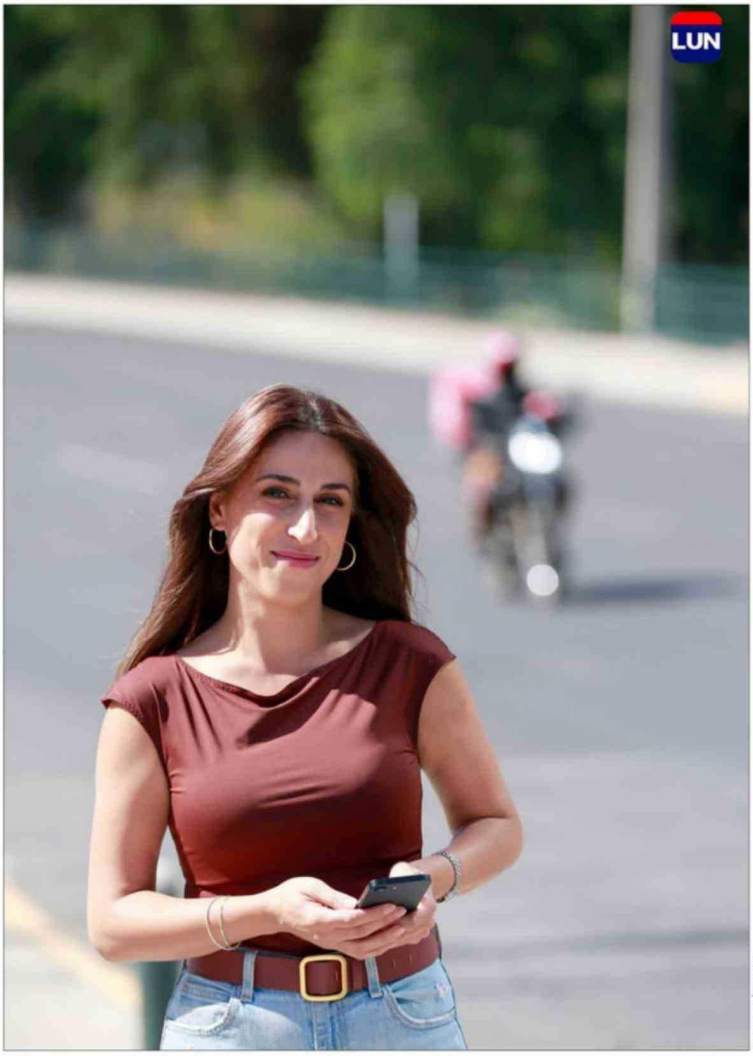
De inmediato fue a la PDI a presentar su denuncia: en eso demoró unos 40 minutos. "Cuando volví a la oficina intenté abrir mi correo y me di cuenta de que estaba hackeado: me habían cambiado el acceso y el número de recuperación. Al mismo tiempo recibía correos: vi las cuentas del banco y se habían realizado múltiples transferencias".

En paralelo, los ladrones también abrieron líneas de crédito a su nombre y pidieron avances en línea. ¿En total? Le quitaron cerca de $7.000.000 sumando diversos conejeos entre las cuentas.

Viktorya mandó fotos del motochorro y la PDI de Peñalolén incautó la moto con la que se concretó el delito, pero no encontraron su teléfono. "Ahora el caso está siendo investigado por la Fiscalía Oriente y la PDI. Yo quisiera dar a conocer un tema importante: los bancos digitales no tienen oficina ni canales eficientes de respuesta al cliente, eso ha sido y es angustiante", lamenta. De hecho, aún no recupera todo el dinero defraudado.

¿Sabía el riesgo de que le roben el celular desbloqueado?

"Sí, pero pensaba que iba a más por el lado de que le hicieran algún fraude a través del WhatsApp a mis contactos ahí registrados. Pero no sabía que podían entrar a las cuentas del banco, porque todas las aplicaciones del banco las tenía con clave. No me lo esperaba".



DAVID VELÁSQUEZ

En menos de una hora, Viktorya Ozbicakci fue víctima de un set de fraudes con su celular desbloqueado.

Después del robo

Camila Cubillos Valencia, socia de Cubillos Abogados, recomienda actuar de inmediato apenas ocurrió el robo: bloquear el smartphone o la línea, contactar de inmediato a los bancos y entidades financieras para cerrar cuentas, tarjetas, accesos y medios de autenticación asociados, y luego cambiar las claves del correo, de las apps bancarias y de otras plataformas sensibles.

Su advertencia es urgente: un teléfono desbloqueado deja de ser sólo un objeto robado y pasa a ser una vía de acceso directo a cuentas, correos y sistemas de verificación. "Lo primero que hay que hacer es bloquear el equipo o la línea lo antes posible", insiste.

Cubillos también subraya la importancia de dejar constancia formal del robo lo antes posible y guardar respaldos de cada gestión. La denuncia, explica, puede hacerse directamente en la página del Ministerio Público a través de su sistema en línea, sin necesidad de ir presencialmente, y conviene acompañarla con un registro de bloqueos, llamados, correos y reclamos al banco.

"Las primeras horas son decisivas: bloquear accesos, dar aviso inmediato al banco, cambiar claves y dejar constancia formal puede marcar la diferencia entre recuperar el dinero o perderlo", recalca Cubillos.

Doble bloqueo

Antes de que pase cualquier cosa conviene dejar el celular preparado para el peor escenario: que alguien lo robe desbloqueado. En los iPhone, ahí entra la **Protección del Dispositivo Robado**, función disponible desde iOS 17.3.

En simple, si el equipo está lejos de lugares conocidos -como la casa o el trabajo- Apple impone una espera de una hora para concretar los cambios más críticos: modificar la contraseña de Apple ID, cambiar el código del celular, agregar o eliminar Face ID. Luego, obliga a autenticarse de nuevo con biometría. La lógica es ganar tiempo para que el dueño denunice su iPhone como perdido antes de que los intrusos lo bloqueen de su propia cuenta.

Otra medida es proteger las apps más delicadas. En iPhone se pueden dejar bloqueadas para que pidan Face ID al abrirse; en el caso de aplicaciones descargadas, puede incluso ocultarlas. La lógica es bastante obvia pero no todos la siguen: apps bancarias, correo, billeteras y servicios de mensajería no tienen por qué quedar abiertas y expuestas apenas alguien desbloquea el smartphone.

"La idea es que, incluso con el código comprometido, el atacante ya no pueda ejecutar cambios críticos de forma inmediata. Eso rompe el modelo de ataque rápido que utilizan los delincuentes", destaca Camilo Garrido, investigador del Centro de Investigación en Ciberseguridad de la Universidad Mayor.

En Android la función más cercana es **Identity Check**, que exige biometría para cambios críticos fuera de lugares de confianza. En Samsung Galaxy con One UI 7, además, puede sumar una espera de una hora si alguien intenta restablecer los datos biométricos. Para aislar y ocultar apps sensibles, Android ofrece Private Space en equipos compatibles.

Camilo, si a alguien le roban el celular abierto, algunas medidas de seguridad son mandar códigos al celular o al mail, al que muchas veces tiene acceso inmediato el ladrón.

"Sí, hoy muchas medidas de seguridad son ilusorias en este contexto, porque el segundo factor llega al mismo dispositivo que ya está comprometido. Si el atacante tiene el teléfono desbloqueado, tiene también la llave para validar casi cualquier operación. Diría que hay que tratar de dejar de depender del SMS y el correo como segundo factor de autenticación y migrar a factores de autenticación fuera, además de llaves físicas en cuentas críticas".