



Dirección de Investigación Criminal e INTERPOL Centro Cibernético Policial



BALANCE **SEMANA**
20/2023

Cyber noticias

Notas de voz de WhatsApp pueden ser usadas para estafar a sus amigos o familiares. Los ciberdelincuentes se han especializado en diseñar una nueva modalidad de estafa que incorpora tácticas de ingeniería social junto a tecnologías que les permiten sintetizar la voz de una víctima para crear audios lo suficientemente convincentes para estafar a otra persona. McAfee estima que la mayoría de los reportes sobre víctimas de estas estafas son los padres o abuelos que denuncian que un cibercriminal clonó la voz de sus hijos o nietos. **Fuente: MSN**

WhatsApp ahora permite proteger chats con contraseña y con huella. La aplicación WhatsApp, una de las más populares a nivel mundial, implementó una nueva mejora para ofrecer una mejor experiencia a sus usuarios. Se trata de la opción para bloquear algunos chats con contraseña, reconocimiento facial o huella dactilar para evitar que alguien lea sus chats más íntimos. Ya se encuentra disponible en algunos dispositivos Android y iOS, así lo confirmó la red de mensajería en su [sitio web oficial](#). **Fuente: Caracol**

Nuevas tendencias de ransomware en 2023. En una búsqueda, los ciberdelincuentes se dirigen a todo tipo de organizaciones, desde instituciones educativas y de salud hasta proveedores de servicios y empresas industriales. En 2022, las soluciones de Kaspersky detectaron más de 74 millones de intentos de ataques de ransomware, un 20 % más que en 2021 (61 millones). Aunque a principios de 2023 se registró una pequeña disminución en la cantidad de ataques de ransomware, estos fueron más sofisticados y mejor dirigidos. **Fuente: Securelist.**

Discord informa a sus usuarios de que ha sufrido una brecha de datos. La plataforma de mensajería instantánea Discord ha notificado a sus usuarios que parte de su información se ha visto expuesta en un incidente de ciberseguridad que involucra a un proveedor de servicios externo. Desde Discord no han especificado cuál ha sido el proveedor que se ha visto comprometido, aunque algunos usuarios especulan con que pudo haber sido [Zendesk](#), el cual Discord utiliza para administrar los tickets de soporte. **Fuente: Escudodigital.**

Modalidad más reportada al CAI Virtual ; Phishing Davivienda!

A través del servicio de CAI Virtual, se identificó una campaña de phishing vía correo electrónico, la cual busca evadir los sistemas de seguridad de detección y análisis de seguridad, difundiendo una supuesta solicitud de cambio de número DaviPlata por parte de **Davivienda**, con el fin de capturar información confidencial, credenciales de acceso a los servicios financieros, afectar el patrimonio de las personas y posteriormente la transferencia no consentida de activos. Este correo esta asociado al asunto: **“SOLICITUD EN PROCESO”**.

1 El correo allegado, notifica el cambio de número en su cuenta de **DaviPlata**, indicando que si no lo realizó deben acceder a un enlace para cancelar el proceso.

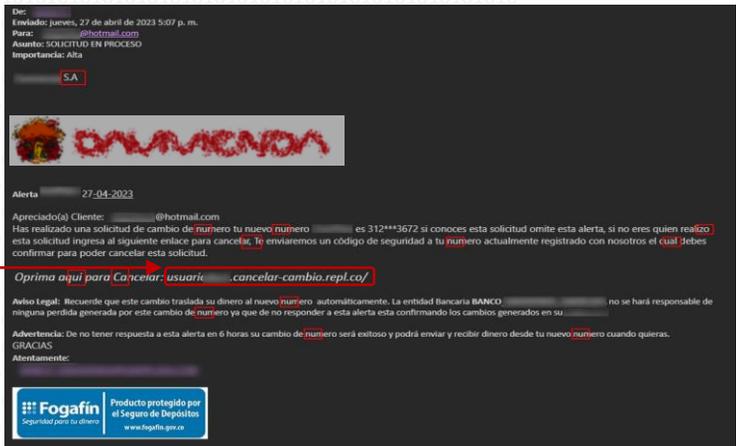
2 Solicita acceder al enlace: **“usuariodavi.cancelar-cambio.repl.col”**, que redireccionará a un sitio web simulando ser la banca móvil de la App DaviPlata.



3 Luego envían un presunto código de verificación, usando esto como señuelo para más credibilidad.



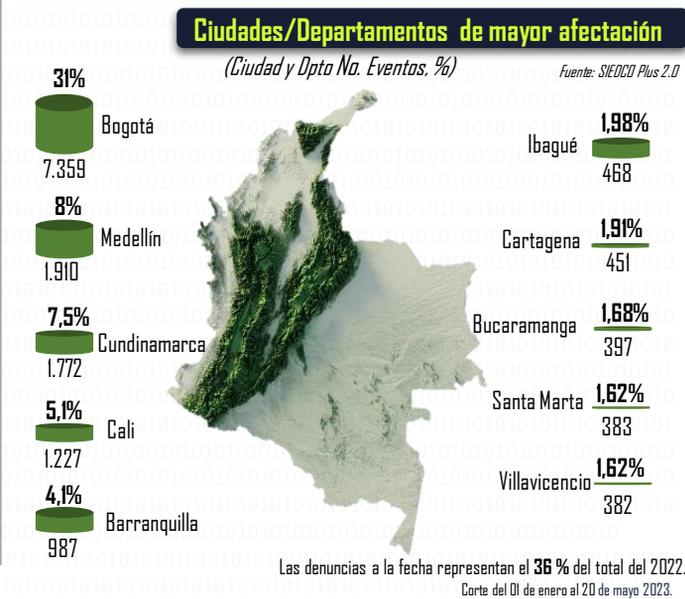
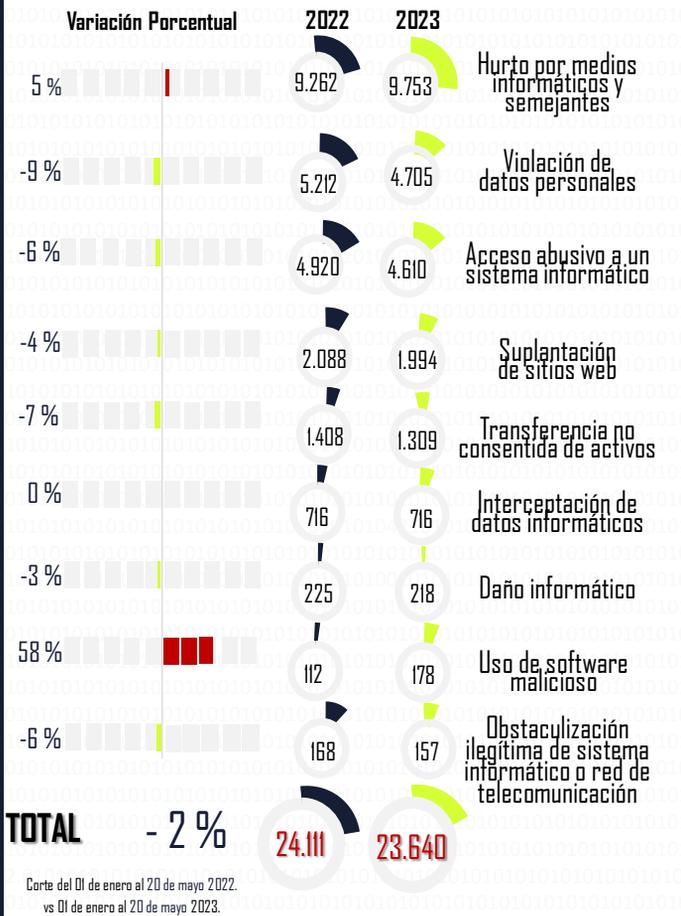
4 Posteriormente, los ciberdelincuentes proceden con la captura de los datos suministrados por la víctima.



5 RECOMENDACIONES

- EVITE** dar clic sobre links o abrir archivos adjuntos en correos electrónicos desconocidos.
- VERIFIQUE** ortografía y redacción, usualmente hay errores.
- VERIFIQUE** que el remitente del correo electrónico, corresponda a una entidad bancaria.
- No** ingrese ningún tipo de información en el formulario mostrado en este sitio web.
- VERIFIQUE** los enlaces o archivos antes de ejecutarlos en un entorno de prueba (sandbox), Ej: [Any.Run](#), [Csirt.Ponal](#).
- REPORTE** el correo electrónico allegado, a través de nuestro canal de atención del CAI Virtual <https://caivirtual.policia.gov.co>

Balance Cibercriminalidad - Ley 1273/09



Actividades de gestión en seguridad digital

Capturas

Delitos informáticos.
Explotación sexual infantil en Internet.

105
32

137

241

Alertas y contenidos preventivos
10 durante la semana

Incidentes gestionados
a través del CAI Virtual

5.620

81

Actividades de relacionamiento
estratégico, resaltando en la semana:



Charlas de ciberseguridad
Personas impactadas

6.818

54

11.163

Páginas bloqueadas
Material de abuso sexual infantil.
Juegos ilegales de azar.

10.607
556

Para sugerencias sobre este producto, por favor diligencie este formulario :<https://bit.ly/3mz5C8d>



Canales de atención y redes sociales



Página web



Twitter



Instagram



Facebook



WhatsApp