

# Estafa por WhastApp: el falso mensaje viral que ofrece productos gratis por el aniversario de Mercado Libre

15/06/2021

**“El sorteo que está circulando por WhatsApp por el aniversario de nuestra compañía es falso. Se trata de un caso de publicidad engañosa y nuestro equipo especializado ya avanzó con la denuncia”.** El mensaje fue emitido por la cuenta oficial de Mercado Libre en Twitter.

Así, la empresa más valiosa de la Argentina, con un *market cap* según el precio de sus acciones en Wall Street de USD 70.000 millones, busca desbaratar otra estafa virtual. Esta vez llega por WhatsApp, promete 2000 productos gratis por el 20 aniversario de la empresa que fundó **Marcos Galperin** (que, en rigor, ya tiene 21).

“Para reconocer cuándo se trata de un caso engañoso, te recomendamos que corroboremos siempre que la dirección desde donde te llega la comunicación sea oficial y que tengas en cuenta que las empresas nunca te piden que ingreses datos fuera de sus sitios o apps”, siguió explicando la compañía en la red social.

“Recordá que los únicos canales oficiales de Mercado Libre son los identificados con el tilde azul en Facebook, Twitter e Instagram, y el sitio oficial”, asegura la empresa.

El intento de estafa y la interacción de los usuarios en Twitter hizo que el nombre de la empresa sea *trendig topic* en el país.

 Marcos Galperin, fundador de Mercado Libre

“Nadie regala nada, lo primero que tenés que pensar al recibir un mensaje de que te bloquean la cuenta (miedo) o que te regalan algo (tentación) es: ¿Es real esto? Mercado Libre no regala nada, no den datos”, destacaron desde la cuenta Derecho en Zapatillas, que sigue temas legales y de derechos de los consumidores.

## **Phishing**

Según información del ministerio de justicia, “la palabra **phishing** quiere decir suplantación de identidad”. “Es una técnica de ingeniería social que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esa persona. Los ciberdelincuentes envían correos electrónicos falsos como anzuelo para “pescar” contraseñas y datos personales valiosos”, destacan desde una publicación web oficial.

En estos intentos, los ciberdelincuentes buscan datos de contraseñas, números de tarjetas de crédito, DNI, Cuit o Cuil, nombres de usuario y códigos PIN. “Cuando obtienen estos datos realizan compras, reservas o extracciones de dinero en tu nombre. Una forma de verificar si fuiste víctima de una ataque de Phishing es revisar en forma periódica tus resúmenes bancarios buscando transferencias que no autorizaste”, se detalla.

☒ Los ciberdelincuentes buscan obtener datos de los por medio de técnicas como el phishing (EFE/SASCHA STEINBACH/Archivo)  
Entre las claves para prevenir el phishing, Justicia destaca:

– **Chequeá el remitente:** antes de abrir cualquier correo electrónico es importante chequear que no sea falso. Observa cuál es la dirección completa del remitente

– **Compará el remitente con los mensajes anteriores** de tu banco o servicio.

- **Comprabá si la dirección de internet (url)** que se muestra en la parte inferior izquierda en la ventana del navegador es igual a la de la empresa que te escribe. Podés hacer una búsqueda en internet de la empresa y comparar urls.
- **Verificá el certificado de seguridad de la página de internet:** es importante verificar que tenga el candado gris o verde y que sea una dirección https.
- **Si tenés dudas comunicate con los servicios de atención al cliente** antes de contestar cualquier comunicación por correo electrónico.
- **No contestes formularios en línea** enviados por destinatarios desconocidos.
- **No respondas a ningún correo electrónico, teléfono o fax, que te solicite divulgar información personal.**
- **No envíes ni compartas ningún código de seguridad** como el código PIN por teléfono o por correo electrónico.
- **Desconfiá de los archivos adjuntos:** pueden causar la descarga de la clave de registro o software “spyware” en su computadora.
- **Utilizá un antivirus** actualizado.
- **Actualizá tu sistema operativo.**

Las denuncias pueden realizarse en la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), (5411) 5071-0040; la Fiscalía de CABA. Equipo Especializado en Delitos Informáticos, 0800-333-47225; y la Dirección Nacional de Protección de Datos Personales, (54-11) 2821-0047.

Fuente: Infobae