LA CIFRA **125 mil** **muestras de malware** son detectadas cada día en el mundo, de acuerdo con Kaspersky Lab.

EL DATO **Brasil y México** son dos de los países que registran la mayor cantidad de ataques en Latinoamérica.

LA CIFRA **31%** **de las víctimas** de ataques cibernéticos reutilizaron sus contraseñas en diferentes sitios, según McAfee.

CELEBRIDADES MUNDIALES MÁS PELIGROSAS EN EL CIBERESPACIO

1. Emma Watson
2. Jessica Biel
3. Eva Mendes
4. Selena Gómez
5. Halle Berry
6. Megan Fox
7. Shakira
8. Cameron Díaz
9. Salma Hayek
10. Sofía Vergara

PERSONAJES PERUANOS USADOS PARA COMETER DELITOS

1. Tilsa Lozano
2. Maju Mantilla
3. Tula Rodríguez
4. Ciro Castillo
5. Rosario Ponce
6. Vanessa Tello

FUENTE: McAfee

USUARIOS LATINOAMERICANOS ATACADOS VÍA WEB

	%
Chile	39
Colombia	39
Panamá	38
Brasil	37
Honduras	37
Paraguay	37
Perú	37
Guatemala	36
México	35
Argentina	35
Uruguay	35
Costa Rica	34
Bolivia	34
Ecuador	34
Nicaragua	34
El Salvador	33
Venezuela	32
Rep. Dominicana	30

FUENTE: Kaspersky Lab

CÓMO CREAR CONSTRASEÑAS SEGURAS

1. Use contraseñas diferentes en todas las cuentas.
2. Asegúrese de que nadie esté mirando cuando escribe su clave secreta.
3. Cierre la sesión cuando deje el dispositivo y haya alguien cerca.
4. Use software de seguridad completo y manténgalo actualizado.
5. Evite escribir contraseñas en equipos que no controla.
6. No escriba contraseñas cuando use una conexión Wi-Fi que no está protegida (como en el aeropuerto o una cafetería).
7. No divulgue su contraseña.
8. Cambie de contraseña periódicamente y evite la reutilización de una de ellas durante, al menos, un año.
9. Use, al menos, ocho caracteres de letras minúsculas y mayúsculas, números y símbolos.
10. Use el teclado como una paleta para crear formas.
11. Diviértase con códigos, oraciones o frases cortas conocidas.
12. Puede guardar las contraseñas por escrito, pero lejos de la computadora y mezcladas con otros números y letras.

FUENTE: McAfee

¿CÓMO ROBAN LOS DATOS DE SU TARJETA DE CRÉDITO?

- Cuando la víctima ingresa datos en un sitio web falso.
- Al hacer click en el enlace de un e-mail de phishing.
- Al escribir erróneamente la dirección web de un banco.
- Al dirigirse a una conexión no segura a través de un Wi-Fi gratuito.
- Por usar una PC infectada.
- El código malicioso puede redireccionar a un sitio web de phishing.
- También roba contraseñas y números de tarjetas de crédito almacenadas en el disco duro.
- Además, puede interceptar la información bancaria en tiempo real.

¿CÓMO ACCEDEN A LOS DATOS DE SU CUENTA DE HOME BANKING?

- Cuando la víctima visita un sitio web legítimo pero comprometido.
- Los sitios web también puede ser infectados.
- Al interceptar lo escrito a través del teclado.

FUENTE: Kaspersky Lab

PRINCIPALES PELIGROS EN INTERNET PARA LOS NIÑOS

	%
Pornografía y material erótico	53.63
Redes sociales	15.67
Software ilegal	14.31
Juegos	3.63
Violencia	3.10
Armas	2.68
Servidores anónimos	2.43
Lenguaje explícito	1.73
Tiendas en línea	1.24
Drogas	0.47
Juegos ocasionales	0.42
Foros y chat	0.37
Correos electrónicos	0.25
Sistemas de pago	0.08

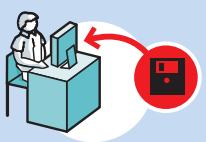
FUENTE: Kaspersky Lab

ATAQUES POR INTERNET MÁS COMUNES

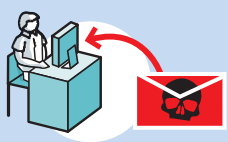
Phishing
El delincuente crea una réplica casi perfecta de la página web de una institución financiera y luego intenta engañar al usuario para robar sus datos personales a través de un formulario.

Virus
Programa que se expande desde un archivo a otro y de PC a PC. Adicionalmente, puede ser programado para borrar o dañar datos.

Keylogger
Programas que registran las pulsaciones de teclas (es decir, lo que un usuario escribe en el teclado), lo que puede ser utilizado por un hacker para obtener datos confidenciales.



Malware
Cualquier software creado deliberadamente para llevar a cabo una acción no autorizada y, a menudo, perjudicial.



Spam
Correo electrónico anónimo y no solicitado que se envía en cantidades masivas por los spammers para ganar dinero. El spam también se utiliza para el phishing y para propagar códigos maliciosos.

FUENTE: Divindat-Kaspersky Lab