



FILTRO ANTIVIRUS Y ANTISPAM

Guía de Autoprotección y Buenas Prácticas en el Uso de Correo Electrónico y Navegación

1. INTRODUCCIÓN A LA SEGURIDAD DEL USUARIO

El ecosistema digital e Internet ofrecen múltiples herramientas de comunicación, trabajo y entretenimiento que son de acceso público. No obstante, para garantizar una experiencia óptima y segura, es fundamental contar con mecanismos que protejan y mitiguen los riesgos y amenazas informáticas a los que estamos expuestos de manera diaria.

MEGANET TELECOMUNICACIONES S.A.S., comprometida con la excelencia en el servicio y la protección de sus usuarios, pone a su disposición esta guía práctica de configuración y uso de herramientas de seguridad digital para prevenir infecciones por virus o la recepción masiva de correo electrónico no deseado (Spam).

2. ¿QUÉ ES UN ANTIVIRUS Y CÓMO FUNCIONA?

Un antivirus es una aplicación de software diseñada como medida de protección para resguardar los datos y el correcto funcionamiento de sistemas informáticos (móviles, ordenadores personales y empresariales) frente a amenazas lógicas conocidas comúnmente como malware o virus. Su propósito fundamental es detectar, contener y eliminar estos archivos maliciosos antes o después de que ingresen al sistema.

Las principales amenazas que combate un antivirus son:

- **Virus:** Códigos que se adjuntan a programas legítimos para replicarse y alterar el sistema.
- **Gusanos (Worms):** Programas que se propagan a través de la red explotando vulnerabilidades sin intervención del usuario.
- **Troyanos:** Archivos aparentemente inofensivos que abren compuertas traseras para el control remoto del equipo.
- **Spyware:** Programas espía diseñados para recopilar contraseñas, hábitos de navegación y datos bancarios.

Mecanismo de Detección: Los antivirus tradicionales escanean los archivos comparando sus firmas digitales contra una base de datos actualizada de virus conocidos. Los antivirus modernos complementan

este método mediante el análisis heurístico, el cual evalúa el comportamiento de los programas sospechosos en tiempo real para bloquear virus nuevos o mutaciones no catalogadas.

Recomendación de Actualización Continua:

Debido a que diariamente surgen nuevas variantes de malware, es de vital importancia mantener el motor de base de firmas del antivirus actualizado de forma automática. Un antivirus desactualizado pierde más del 80% de su efectividad frente a nuevas amenazas.



3. ¿QUÉ ES EL SPAM Y LAS HERRAMIENTAS ANTISPAM?

El **Spam** o correo electrónico no deseado corresponde a aquellos mensajes de carácter publicitario, engañoso o fraudulento enviados de forma masiva a miles de cuentas de correo sin el consentimiento previo del destinatario.

Una herramienta o filtro **Antispam** es una aplicación informática encargada de analizar el tráfico de correo electrónico entrante para identificar, clasificar y aislar estos mensajes no deseados, evitando que inunden la bandeja de entrada principal.

Las herramientas antispam emplean múltiples técnicas de detección:

- **Técnicas Locales (Filtros de Contenido):** Analizan el texto del mensaje buscando palabras clave o patrones comunes de fraude y publicidad engañosa (por ejemplo, ofertas financieras sospechosas, links extraños). Estos filtros aprenden continuamente con base en las indicaciones manuales del propio usuario (cuando marca un correo como spam).
- **Listas de Control (Blancas y Negras):** Permiten definir direcciones de remitentes o dominios de total confianza (Lista Blanca) de los cuales nunca se bloqueará un correo, o remitentes bloqueados expresamente (Lista Negra).
- **Consultas a Servidores Remotos (RBL / DNSBL):** Verifican en tiempo real si la dirección IP del servidor remitente está catalogada globalmente como emisora de correo basura o si carece de configuraciones de seguridad esenciales (SPF, DKIM, DMARC).

El Riesgo de los Falsos Positivos:

El principal desafío de un sistema antispam es evitar los "falsos positivos", es decir, catalogar erróneamente un correo legítimo e importante como correo no deseado. Por ello, se recomienda revisar periódicamente la carpeta de "Correo no deseado" o "Spam" para verificar que no se hayan filtrado mensajes válidos de clientes o proveedores.

4. RIESGOS ASOCIADOS AL CORREO NO DESEADO

El spam no es solo una molestia publicitaria; a menudo sirve como vector para ataques graves de ciberseguridad:

- **Phishing:** Correos que imitan la imagen gráfica de su banco o proveedor de servicios para robar credenciales.

- **Distribución de Malware:** Archivos adjuntos infectados (documentos PDF, Word o ejecutables comprimidos) que instalan virus al abrirse.
- **Ingeniería Social:** Engaños dirigidos a manipular al usuario con falsos premios, multas de tránsito o alertas de seguridad bancaria.



5. CONSEJOS PRÁCTICOS PARA PREVENIR EL SPAM Y MALWARE

Para mantener a salvo sus cuentas y dispositivos, le recomendamos implementar las siguientes medidas de seguridad diaria:

1. **Habilite el Filtro del Proveedor:** Utilice servicios de correo (como Gmail, Outlook, Yahoo) que cuenten con herramientas nativas de inteligencia artificial y filtrado de spam robusto. Ajuste el nivel de sensibilidad según sus requerimientos.
2. **Use Copia Oculta (CCO / BCC):** Al enviar un correo electrónico a múltiples destinatarios, utilice el campo CCO. Esto evita que las direcciones de correo de sus contactos queden expuestas públicamente y sean recolectadas por robots rastreadores de spammers.
3. **No Exponga su Correo en la Red:** Evite registrar su dirección de correo personal en foros, blogs, secciones de comentarios o sorteos de dudosa procedencia. De ser necesario, utilice cuentas de correo secundarias destinadas únicamente a registros y boletines comerciales.
4. **Sea Precavido al Instalar Programas:** Muchos instaladores gratuitos (freeware) intentan instalar de manera oculta barras de herramientas, adwares o programas espías. Lea siempre los términos y desactive las casillas de software adicional durante el proceso de instalación.
5. **No Responda Correos No Deseados:** Al responder a un mensaje de spam, le está confirmando al atacante que su cuenta de correo está activa y es leída por una persona real, lo que incrementará significativamente el volumen de spam recibido en el futuro.
6. **Verifique los Enlaces antes de dar Clic:** Coloque el cursor del mouse sobre cualquier link del correo para previsualizar la dirección URL real del enlace. Si esta no coincide con la página web de la empresa legítima, no ingrese ni ingrese datos sensibles.

6. COMPROMISO DE MEGANET TELECOMUNICACIONES S.A.S.

MEGANET TELECOMUNICACIONES S.A.S. cuenta con sistemas de monitoreo y seguridad perimetral para proteger la conectividad de nuestros clientes. Aconsejamos a nuestros usuarios complementar nuestras medidas de red implementando un software de seguridad (Antivirus y Firewall local) actualizado en sus terminales y dispositivos del hogar.

Canales de Atención y Reportes en Colombia:

Si sospecha de un fraude o delito informático, repórtelo en:

- **Portal de Denuncias CAI Virtual:** caivirtual.policia.gov.co

- **Línea de Atención de Emergencias:** 123 (Policía Nacional)
- **MEGANET TELECOMUNICACIONES S.A.S. Soporte:** info@meganet.com