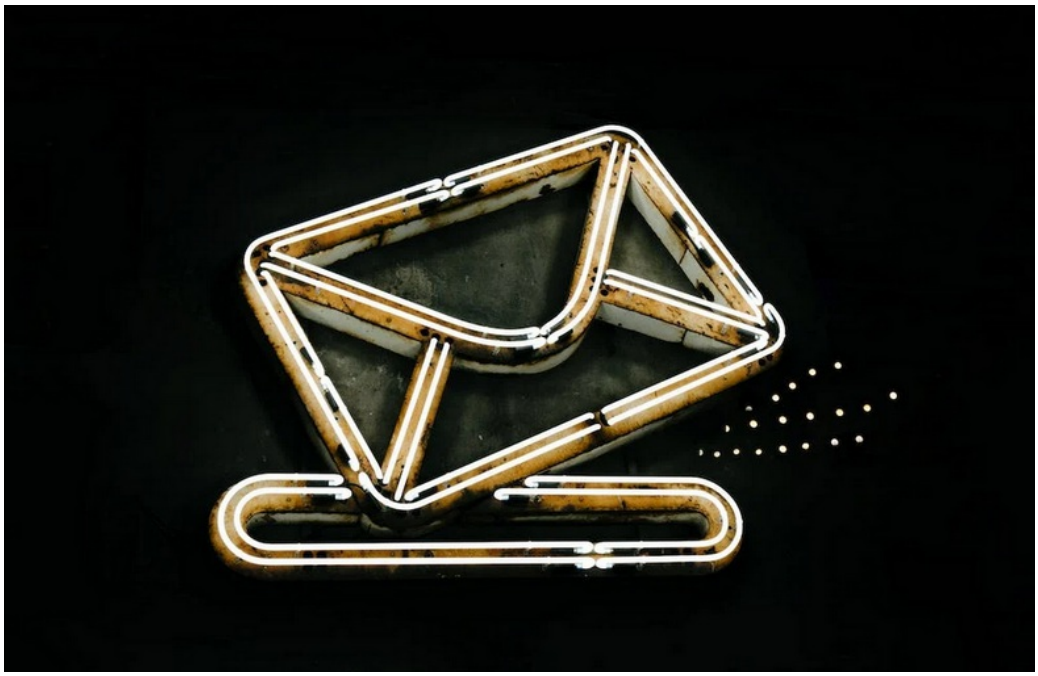
Consejos de seguridad a la hora de usar el correo, mensajería instantanea, y SMS

Publicado el El Informatico - 13 de septiembre de 2022 -



El correo electrónico y los SMS aún se utilizan de manera generalizada para comunicarse entre las personas. En el caso de los SMS se utilizan, sobre todo, para comunicaciones de empresa a clientes o incluso comunicaciones de entidades del gobierno (como la TGSS) a los ciudadanos.

Es por ello que muchos delincuentes se aprovechan de éstas plataformas para engañarnos e intentar atacarnos.

En éste artículo se enumeran algunos consejos para detectar éstos ataques antes de caer en su trampa.

Ojo al remitente de los SMS, podría no ser quien dice ser

Los teléfonos modernos tienen la manía de mostrarnos por defecto el nombre del remitente, pero no su número de teléfono. Los delincuentes pueden hacerse pasar por un falso remitente para intentar engañarte. Por ejemplo, pueden enviarte un SMS falso bajo el nombre de tu entidad bancaria, con un enlace malicioso.

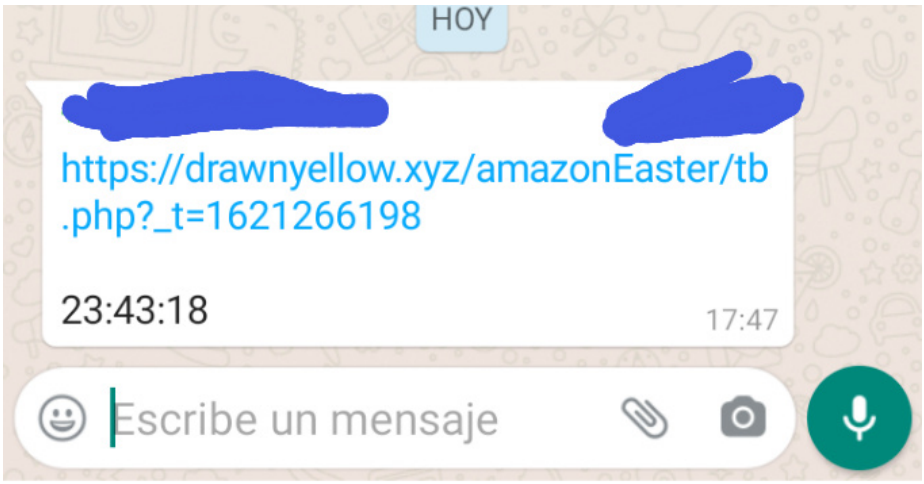
SMS falso con un enlace malicioso

Para identificar éste tipo de ataques conviene tener especial atención al enlace que aparece en el mensaje, así como a la redacción del SMS que, en muchas ocasiones, contiene faltas ortográficas o una mala redacción.

Conviene además saber que en caso de acceso no autorizado, puedes acceder a tu banco digital sin necesidad de hacer click en el enlace y comprobar los accesos a tu cuenta. En caso de tener cualquier duda, lo mejor es ponerse en contacto directamente con la entidad pertinente.

Ojo también a los Whatsapp con enlaces a ofertas, promociones, gangas, y similares

Está muy extendido el uso de la mensajería instantánea en móviles a través de plataformas como Whatsapp y similares (Line, Telegram, etc). Estas plataformas son también un vector masivo de ataques. Por ejemplo, existe malware capaz de hacerse con el control de un dispositivo móvil y mandar mensajes fraudulentos a todos sus contactos.



Enlace malicioso enviado por Whatsapp

Es mucho más fácil caer en éste tipo de trampas ya que al venir de uno de nuestros contactos podemos pensar que es de confianza. En ocasiones estos mensajes se acompañan con mensajes vistosos para animar a las victimas potenciales a que abran el enlace, con invitaciones a ofertas y promociones o incluso artículos gratis.

Es ideal verificar que el enlace tenga un dominio que sea de confianza, pero lo mejor en éstos casos es preguntar directamente al remitente sobre la procedencia del mensaje.

Si además sospechas que alguien pudiera estar suplantando la identidad de ese contacto, puedes probar a realizar alguna pregunta trampa que sólo ese contacto pueda responder correctamente. Si recibes una respuesta incorrecta o extraña, desconfía de ese contacto.

Recuerda: Evita dar información personal a nadie que no sea de confianza.

Confirmaciones de recibos de paquetería, cobros y pagos, denuncias de la policía, etc

Está muy de moda ahora entre los delincuentes mandar mensajes de phising suplantando la identidad de empresas de paquetería o entidades bancarias o incluso gubernamentales, con el fin de engañar a las víctimas y recibir dinero e información personal.

Por ejemplo, imagina que pides un paquete y recibes el siguiente mensaje:

Mensaje de phising con remitente falso

Es fácil caer en la trampa, ya que al haber pedido un paquete puedes pensar que está relacionado con tu pedido.

Pero es fácil detectarlo antes de caer si prestas un poco de atención al remitente. En el caso del ejemplo, la dirección de correo no se corresponde para nada con ningún correo de SEUR. Presta también atención al dominio, ya que aunque en ocasiones pueden contener palabras como «seur» en el nombre del dominio, puede no ser un dominio de seur (por ejemplo seur-españa.es no pertenecería a SEUR aunque pueda parecerlo).

También es fácil detectarlo si prestas atención a la redacción del mensaje, ya que normalmente suele contener fallos ortográficos, fallos en la redacción, o enlaces sospechosos. En éste caso, ninguna empresa de paquetería te va a pedir rellenar un formulario para recibir un paquete, ya que la información va con el pedido.

Es posible que recibas también correos de phising suplantando la identidad de la policía nacional, la TGSS, etc. Por ejemplo:

Ejemplo de suplantación de identidad con un falso mensaje de la policía (Fuente: OSI)

En éstos casos es conveniente saber que no puedes ser juzgado sin haber recibido previamente una denuncia, y que cualquier comunicación del juzgado suele hacerse o por correo ordinario, o directamente por los agentes de la policía. Es decir, que cualquier correo electrónico de ésta índole es **falso**.

Desactiva las imágenes en tu gestor de correo.

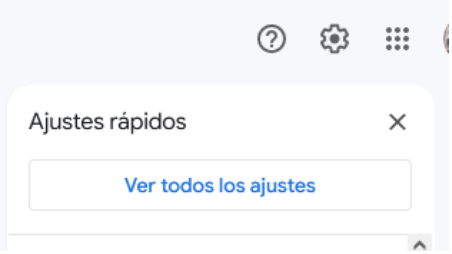
Los gestores de correo suelen mostrar por defecto imágenes incrustadas en los correos electrónicos y código HTML. Esto es un fallo de seguridad ya que permite, entre otras cosas, monitorizar la actividad del usuario en el correo.

Por ejemplo, una práctica muy extendida es la del uso del «píxel mágico». Consiste en insertar una imagen en el correo, normalmente de 1 pixel de tamaño, que al abrirse con el gestor de correo registra la fecha, la hora, la procedencia de la

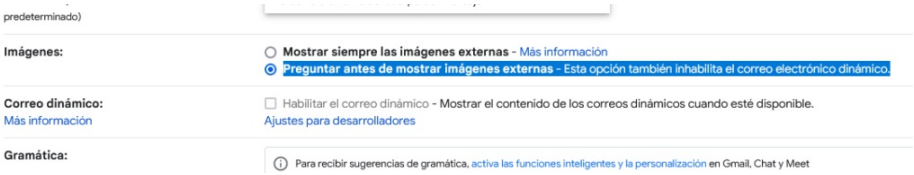
conexión, y la dirección IP de la máquina. Esto permite saber cuándo has abierto un mensaje, pero también permite saber la procedencia de la conexión. Los atacantes pueden usar esa información para realizar otros ataques más adelante.

En GMail

Inicia sesión en la interfaz web de gmail y pulsa el icono del engranaje que aparece en la esquina superior derecha de la interfaz web de gmail. Pulsa sobre «ver todos los ajustes»



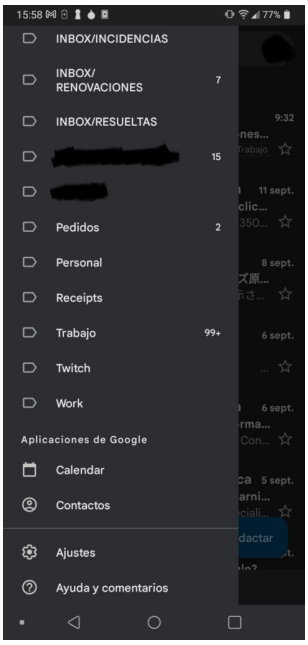
En la pantalla de «todos los ajustes», navega hasta la categoría Imágenes, y selecciona la opción «*Preguntar antes de mostrar imágenes externas*«



Navega hasta abajo y pulsa sobre el botón `Guardar cambios` para confirmar los cambios en tu cuenta.

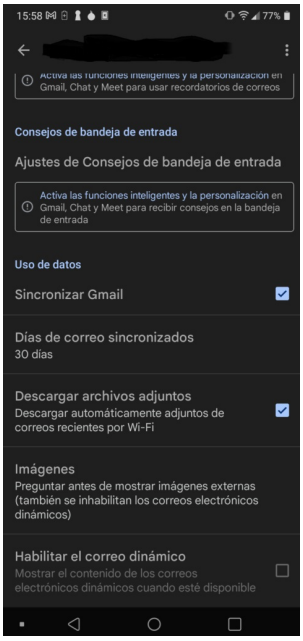
Cliente de GMail para movil (Android)

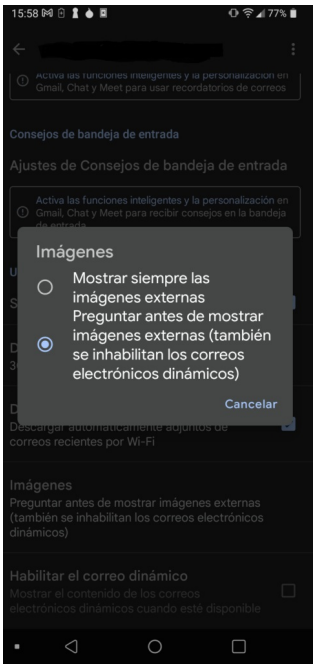
Pulsa sobre el icono de las tres líneas que aparece en la esquina superior izquierda de la pantalla. En el menú, selecciona la opción «Ajustes» que aparece por abajo.



Selecciona la cuenta para la que quieres desactivar las imágenes y el contenido

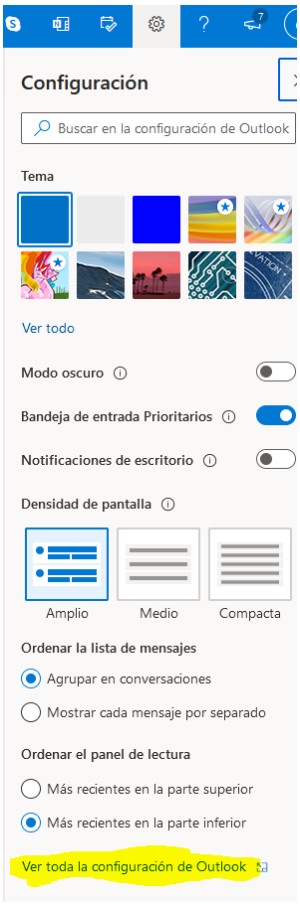
dinámico. Baja abajo del todo y selecciona la opción «Imágenes». Selecciona la opción «Preguntar antes de mostrar imágenes externas». Los cambios se guardarán automáticamente.



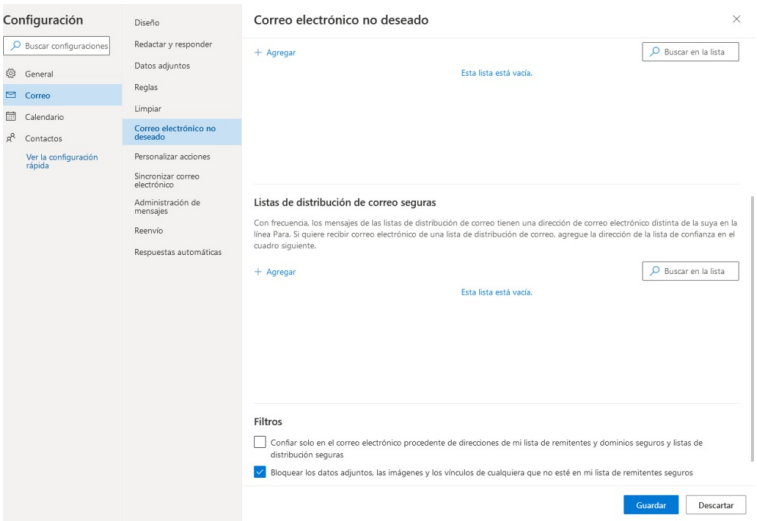


Outlook/Hotmail

Inicia sesión en la interfaz web de Outlook. Pulsa sobre el icono del engranaje en la esquina superior derecha de la pantalla, y pulsa sobre «Ver toda la configuración de outlook».



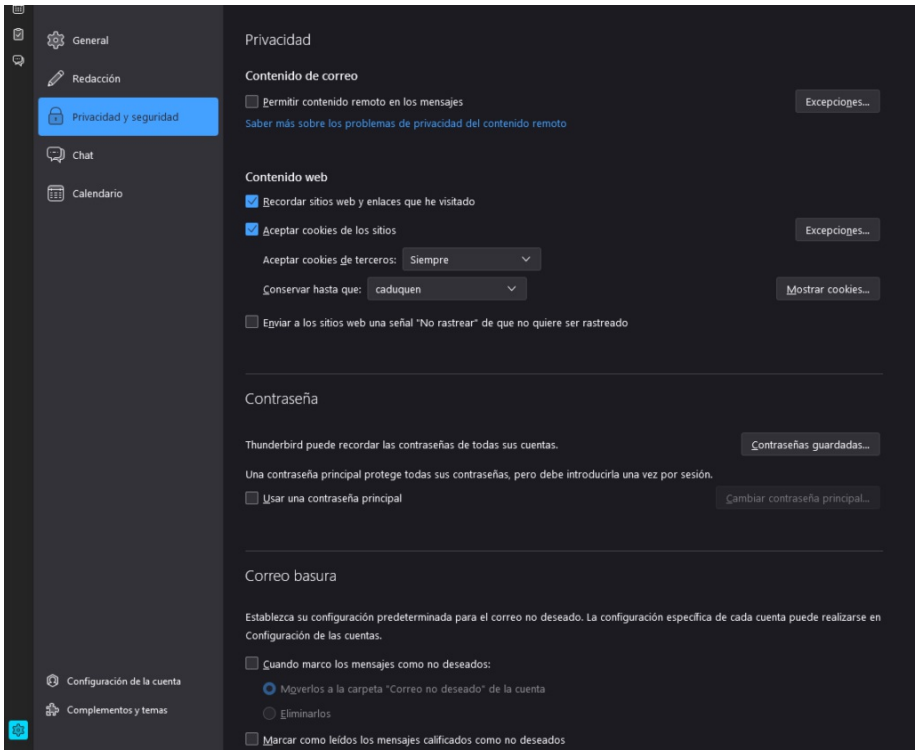
En la pestaña «Correo electrónico no deseado», marca la opción «Bloquear los adjuntos, las imágenes y los vínculos de cualquiera que no esté en mi lista de remitentes seguros».



Pulsa sobre **Guardar** para confirmar los cambios.

Mozilla Thunderbird

Pulsa sobre el icono del engranaje en la parte inferior izquierda de la ventana de Thunderbird. En la pestaña «privacidad y seguridad» desmarca la opción «Permitir contenido remoto en los mensajes».



Los cambios se guardarán automáticamente y se aplicarán para todas tus cuentas.

Usad PGP para cifrar y firmar vuestros mensajes

Con el fin de ocultar los mensajes a cualquier posible atacante, y de verificar la procedencia de los mensajes, es recomendable usar PGP con tu correo electrónico.

En éste blog tengo dos entradas al respecto:

Encriptación de correos electrónicos con GnuPG y OpenPGP
Encriptación de correos electrónicos en Android con K-9 Mail y OpenKeychain

ANTERIOR

Consejos, trucos y curiosidades de Python

SIGUIENTE

Acerca de ChatGPT...

Buscar ...

Entradas Recientes

- Estoy hasta las narices de la web moderna
- Ingenieria inversa básica con Ghidra
- Acerca de la nueva ley transgénero (Y sobre la disfória de género)
- Depresiones causadas por las redes sociales
- ¿Necesito saber matemáticas para aprender informática?
- ¿Es el fín de los discos duros tradicionales?

Categorías

Actualidad | Android | Básicos | Ciberseguridad | Clima | Criptografía | Electronica | Emulación / Virtualización | FOSS | Hacking | Hardware | Informática | Internet | Juegos | Opinion | Otros | Personal | Privacidad | Programación | Tecnología | Time Machine | Tutoriales

RSS

Subscribirse al feed RSS