Uso seguro de correo electrónico

El correo electrónico es uno de los elementos más vitales y utilizados en la actualidad en el ámbito laboral, educativo, financiero, investigativo, etc.

Se ha podido determinar que el correo electrónico es el mecanismo de entrega más utilizado por los(as) ciberdelincuentes del mundo, para engañar a sus víctimas. Existen muchos tipos de engaño, desde hacer creer que el correo viene de entidades judiciales o gubernamentales, hasta terminar con antiguos(as) compañeros(as) de clase o personas interesadas en su bienestar, porque supuestamente su pareja le engaña y envían las fotos o evidencia del engaño (claramente falsas).

Algunos ejemplos de engaños son los siguientes:

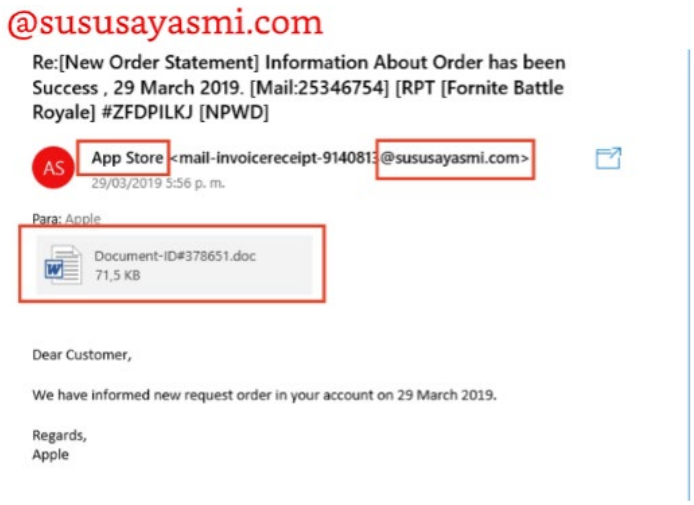
Supuesta entidad o persona que envía el mensaje	Asunto o motivo del mensaje	Supuesto archivo adjunto o contenido engañoso
Policía Nacional	Citación a un juzgado, multa de alguna clase, denuncia o demanda en su contra.	Documentos maliciosos tipo *Word* o archivos comprimidos que resultan ejecutables al final, o enlaces a sitios maliciosos.
Fiscalía	Citación a un juzgado o proceso por demanda.	Documentos maliciosos tipo *Word* o archivos comprimidos que resultan ejecutables al final, o enlaces a sitios maliciosos.
Policía de Tránsito	Multa o foto de multa por alguna infracción cometida.	Documentos maliciosos tipo *Word* o archivos comprimidos que resultan ejecutables al final, o enlaces a sitios maliciosos.
Hacienda	Multa por evasión de impuestos	Documentos maliciosos tipo *Word* o archivos comprimidos que resultan ejecutables al final, o enlaces a sitios maliciosos.
Bancos o entidades financieras	Supuesta actualización de datos o alertas de seguridad por intento de fraude.	Enlaces a sitios maliciosos
Loterías o sorteos	Supuesto premio obtenido	Documentos maliciosos tipo *Word* o archivos comprimidos

Supuesta entidad o persona que envía el mensaje	Asunto o motivo del mensaje	Supuesto archivo adjunto o contenido engañoso
		que resultan ejecutables al final, o enlaces a sitios maliciosos.
Personas preocupadas por usted	Supuesta evidencia de que alguien le engaña o le quiere hacer daño. Casi siempre comienzan con: *"usted no me conoce, pero me he enterado de…"*, y viene sumada la mentira de que su pareja le engaña o algún asunto similar y adjunto encontrará la supuesta evidencia.	Fotos, documentos maliciosos tipo *Word* o archivos comprimidos que resultan ejecutables al final, o enlaces a sitios maliciosos.
Herencias	Supuesto moribundo(a) multimillonario(a) en algún país lejano, que quiere dejarle millones de dólares o euros.	Solicitan enviar datos personales como pasaporte, números de teléfono, dirección, cuentas bancarias, para luego continuar con la estafa.
Cadenas	Supuesta imagen o mensaje religioso	Fotos, documentos maliciosos tipo *Word* o archivos comprimidos que resultan ejecutables al final, para infectarle.

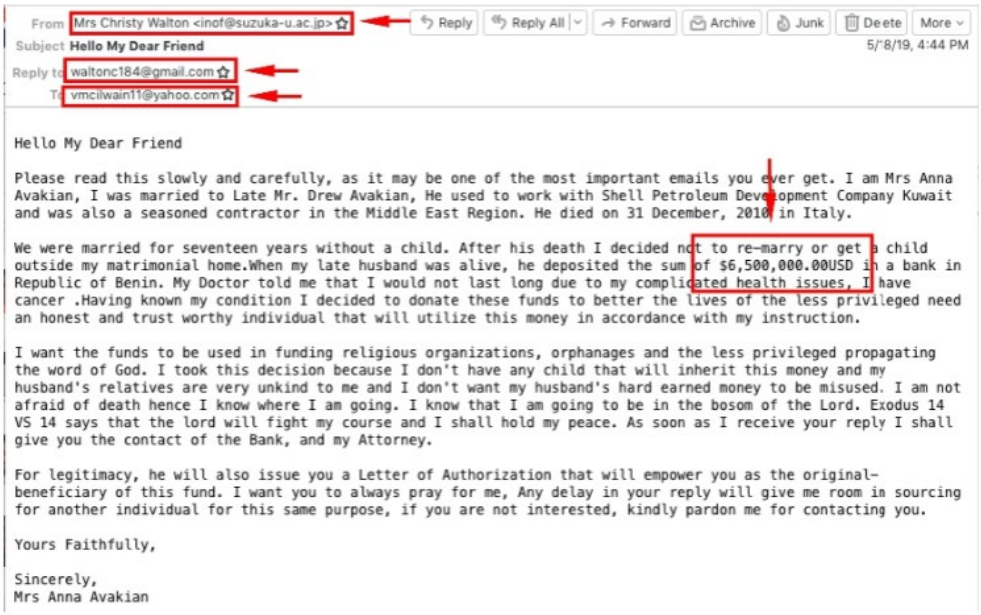
Estos son solo algunos ejemplos; desafortunadamente, la creatividad maligna de los(as) delincuentes no tiene límites, así que siempre debe estar alerta, recordar que NUNCA se va a ganar una lotería que no compró o un sorteo en el cual no participó; que, si usted no tiene vehículo, no va a recibir una multa de tránsito, entre otras situaciones.

Recomendaciones de seguridad en el manejo del correo electrónico

1. **SIEMPRE** revise con detenimiento la dirección de origen del correo electrónico; no es lógico que un banco tenga como dirección una cuenta de *Gmail*, *Hotmail*, *Yahoo* o un nombre diferente al del dominio del banco. Por ejemplo:



La siguiente imagen es un ejemplo de un tipo de estafa nigeriana, en la cual una viuda quiere depositar $6 500 000…¡sería maravilloso!, pero **es una estafa**.



2. Los(as) delincuentes compran dominios que pueden usar fácilmente para engañar. Por ejemplo, compran *"alerta.com"* y luego crean direcciones como alerta@banconacional.alerta.com.

3. Si el correo viene de un supuesto banco, pero se dirige de forma impersonal, **desconfíe**. Un banco o una entidad real donde usted sea cliente(a) va a dirigirse a usted por su propio nombre y apellidos. Los(as) delincuentes se dirigen a sus víctimas de forma impersonal, como "*Estimado cliente"*, "*Apreciado deudor"*, "*Sr./Sra."*, "*A quien corresponda",* entre muchas otras opciones.

4. Desconfíe si la persona que se quiere comunicar es demasiado afectuosa y ni siquiera le conoce.

5. Si el correo viene con una redacción difícil de entender o ilógica, errores ortográficos u otros, **desconfíe**. Un banco o una institución real va a tener cuidado en su redacción y la comunicación con su clientela.

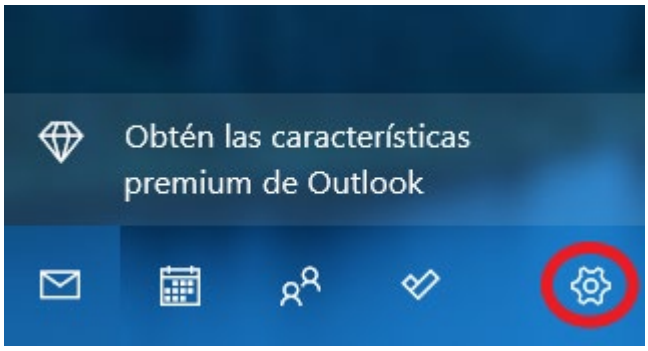
6. Cuando reciba un correo que tenga un enlace, **NO haga clic sobre el enlace**. Antes de hacerlo, posicione su *mouse* sobre el enlace y mire en la parte inferior del correo adónde le lleva realmente.

7. Los(as) delincuentes pueden enviar correos solicitándole datos personales. **NUNCA** suministre datos si no está totalmente seguro(a) del origen de la solicitud.

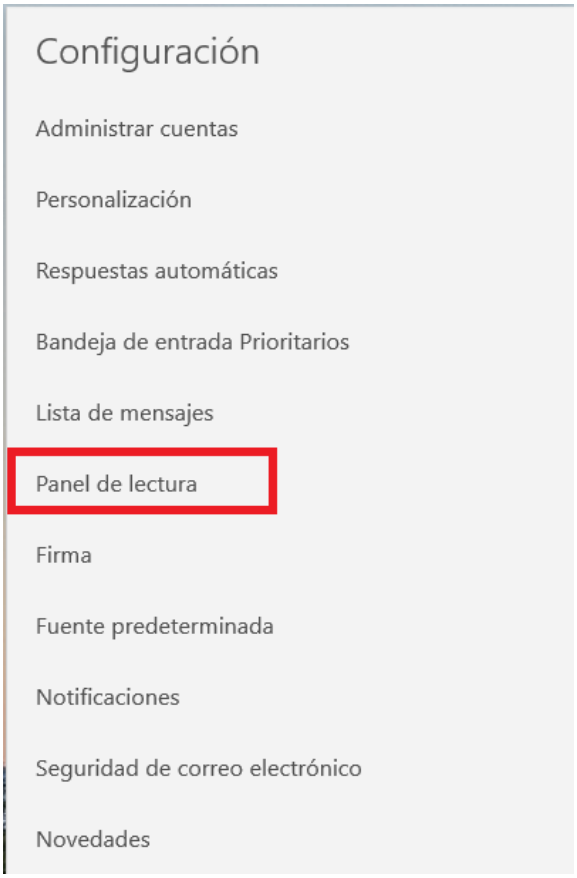
8. Desactive la previsualización automática del contenido. Dependiendo de qué herramientas use como cliente(a) de correo, pueden bloquear esos contenidos.

Desactivar la descarga automática de imágenes en *Windows 10*

Para desactivar la descarga automática de imágenes en la aplicación de correo en *Windows 10*, abrimos la aplicación de correo y en la barra de la izquierda, seleccionamos el ícono de *Configuración de la herramienta*. Hacemos clic sobre él y nos aparece el menú de configuración.

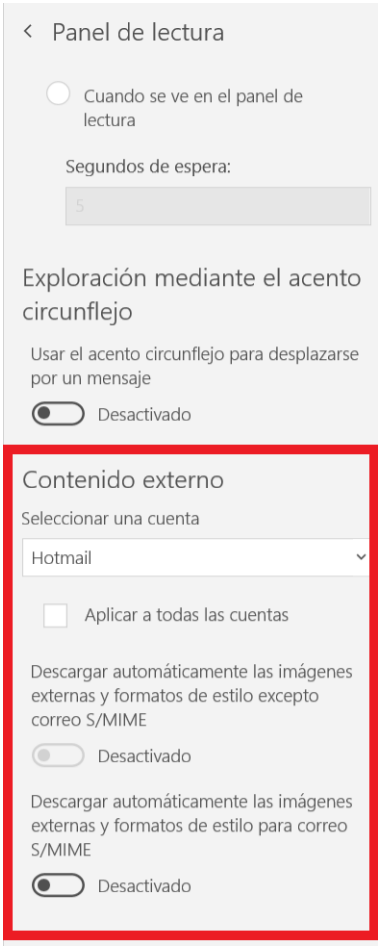


En el menú de configuración al lado derecho, buscamos la opción **Panel de lectura** y hacemos clic.



Vamos a obtener una pantalla como la siguiente, en la cual debe desplazarse hacia abajo, para encontrar **Contenido externo**.

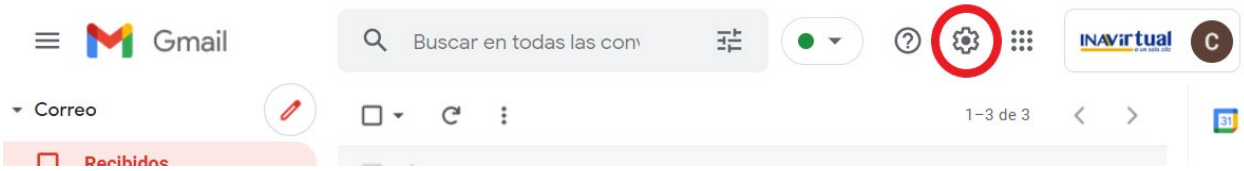
Cuando encontramos esta información, se debe desactivar la opción "**Descargar automáticamente las imágenes externas y formatos de**…". Esta opción *por defecto* viene activa; con un simple clic se desactiva.



Cuando se ha desactivado la descarga automática de imágenes en el correo, los mensajes van a aparecer un poco diferentes donde hay imágenes, no obstante, si quiere descargar todas las imágenes porque confía en el origen del correo, puede bajar al final del mensaje y seleccionar "**Descargar mensaje e imágenes**".

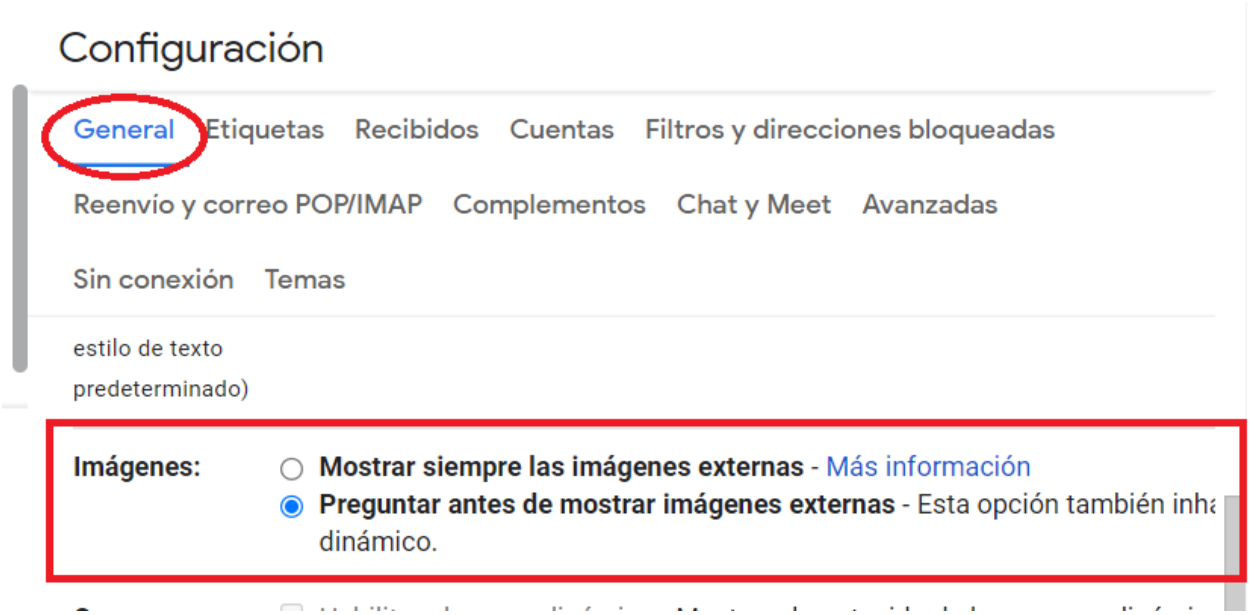
Desactivar la descarga automática de imágenes en *GMAIL*

En nuestra cuenta de *Gmail*, buscamos el ícono del engrane que nos permite ir a la configuración de la cuenta y hacemos clic sobre él.



En la ventana que se despliega seleccionamos **“Ver todos los ajustes”**.

En la pestaña **General**, bajamos en las opciones hasta donde se encuentra **Imágenes** y seleccionamos la opción "**Preguntar antes de mostrar imágenes externas**".



Para devolvernos a nuestro correo, solo hacemos clic sobre el ícono de ***Gmail*** en la parte superior izquierda.


Gmail
Buscar en todas las con
INAVirtual
Correo
Recibidos
Destacados
Pospuestos
Enviados
Borradores 2
Chatear
Configuración
General Etiquetas Recibidos Cuentas Filtros y direcciones bloqueadas
Reenvío y correo POP/IMAP Complementos Chat y Meet Avanzadas
Sin conexión Temas
estilo de texto
predeterminado)
Imágenes:
Mostrar siempre las imágenes externas - Más información
Preguntar antes de mostrar imágenes externas - Esta opción también inh
dinámico.