

Tenemos algo contra el phishing:

# Guía Anti-Phishing de Retarus

---

Los mensajes de phishing que han llegado a su bandeja de entrada todavía se encuentran con un duro oponente: usted mismo.

Descubra cómo puede mejorar ahora su protección frente a fraudes online.



# No baje la guardia.

---

Espere encontrar intentos de fraude online en todo momento. Solo estando alerta podrá reducir considerablemente la probabilidad de caer en una trampa de phishing.

 El phishing es una forma de fraude online con la que los ciberdelincuentes intentan propagar programas maliciosos, sustraer datos y obtener beneficios económicos. Para ello, trabajan con identidades falsas y mensajes manipuladores que se aprovechan de características propias de la naturaleza humana como la buena fe, la disposición para ayudar o el miedo (Ingeniería social).



## A los ciberdelincuentes les gusta camuflarse de buenos amigos.

Los ciberdelincuentes se hacen pasar por amigos y familiares, adoptan el papel de compañeros, superiores o socios comerciales y se dirigen a usted en nombre de instituciones oficiales, proveedores de servicios financieros conocidos o de portales de compra en línea (p.ej., su banco, PayPal, Amazon, etc.).



Esto significa que un mensaje de correo electrónico de un remitente “conocido” también puede tratarse de un intento de phishing.

## La calidad del phishing ha mejorado en técnica, contenido y aspecto.

Cada vez son más escasos los mensajes de correo de phishing con interminables enlaces crípticos y torpes instrucciones usando un castellano mediocre y un mal diseño. Los mensajes de phishing de nueva generación se han sofisticado técnicamente, están perfectamente formulados y su diseño es profesional.



Los mensajes de correo fraudulentos, los remitentes manipulados, los archivos adjuntos, las descargas y los sitios web suelen tener un aspecto engañosamente genuino y no son necesariamente reconocibles como falsos, ni siquiera después de un segundo vistazo.

# Actúe con prudencia.

---

Si tiene la sensación de que algo no encaja en un correo electrónico o un sitio web, actúe con prudencia.

Si se trata de un ataque de phishing, la mejor defensa es no hacer absolutamente nada.

 Los ciberdelincuentes introducen programas maliciosos (malware) en archivos adjuntos, enlaces y opciones de descarga que pueden paralizar su ordenador y, en el peor de los casos, toda la estructura de IT.



---

**N.º 1** No haga clic nunca en los enlaces de mensajes de correo sospechosos (ni en los enlaces para cancelar una suscripción\*).

---

**N.º 2** No abra/descargue los archivos adjuntos (malware) de mensajes de correo sospechosos.

---

**N.º 3** No responda\* a un mensaje de correo sospechoso ni lo reenvíe.

---

**N.º 4** No proporcione nunca nombres de usuario, contraseñas y otros datos personales en sitios web sospechosos.

---

\*De esta forma confirmaría su dirección de correo electrónico al ciberdelincuente.

### **Aviso a directivos: cuidado con el fraude del CEO (CxO Fraud)**

El fraude del CEO es un método de phishing especialmente audaz en el que los ciberdelincuentes se hacen pasar por directivos y presionan a los empleados para realizar determinadas acciones (p.ej., una transacción financiera, la revelación de información confidencial) mediante falsos pretextos (p.ej., una situación de emergencia).

Los rasgos típicos de este tipo de mensaje de phishing son una gran urgencia y la petición de un tratamiento confidencial.

### **¿Conoce al remitente de un mensaje de correo con contenido dudoso?**

Confirme la autenticidad del mensaje de correo electrónico mediante una conversación personal o una llamada con el remitente.

### **¿Cree que ha caído en una trampa de phishing?**

No dude ni un segundo en informar a sus superiores y/o a los compañeros del departamento informático. Ellos saben cómo proceder.

# Sea desconfiado.

---

A los ciberdelincuentes les encanta todo aquello que conmueve o preocupa a la gente. Por este motivo suelen contar con “elaborados” señuelos de phishing, con temas que nos afectan personalmente, que son cubiertos ampliamente por los medios de comunicación, o que nos llenan de preocupación o alegría.

 Pero tenga cuidado: los estafadores no solo actúan mediante correo electrónico y sitios web, sino que también pueden aparecer en redes sociales, SMS, teléfono y hasta al abrir la puerta.



Desconfíe cuando una oferta llega “como si fuera una señal”, cuando un mensaje parece atraerle especialmente, o cuando se trata de instrucciones relacionadas con el teletrabajo. Lo mejor es tomarse un momento y reflexionar sobre lo que puede provocar o desencadenar ese mensaje. ¿Le “está hablando” una autoridad? ¿Está aludiendo al miedo o generando preocupación? ¿Parece una oportunidad demasiado perfecta? Si es así, respire profundamente, piense nuevamente, posiblemente investigue un poco, y sólo entonces reaccione. O no.

## Métodos de los ciberdelincuentes para propagar malware, sustraer datos y ganar dinero:

**Información oficial, indispensable o exclusiva mediante** una suscripción a un boletín de noticias, en un archivo adjunto o como una opción de descarga

**Oportunidades únicas** como ofertas de productos de alta demanda o sólo disponibles durante un tiempo limitado, altas posibilidades de ganar, consejos de inversión “inteligentes”, ...

**Consulta y/o revisión de datos de cuentas online** (empleados, clientes, usuarios, miembros, pacientes, ...)

**Instrucciones** y demandas que ponen al receptor **bajo presión** (refiriéndose a emergencias, omisiones, peligros, ...)

**Descarga o instalación** de software o actualizaciones de seguridad

**Solicitud de contraseñas** para participar en una videoconferencia

**Consulta y/o revisión de datos** para la activación de una herramienta remota (mantenimiento a distancia)

---

**¿Tiene dudas sobre una instrucción informática relacionada con el teletrabajo?** Contacte con sus compañeros del departamento de IT.

## La única solución contra el phishing: una buena seguridad del correo electrónico y usted mismo

No baje la guardia: espere encontrar intentos de fraudes online en todo momento. Actúe con prudencia: evite los clics espontáneos y las descargas. Sea desconfiado: cuestione los mensajes, utilice su sentido común y más de una fuente de información.

---

### Retarus Email Security

Para que el correo electrónico de su empresa siga funcionando y no se detenga.

[retarus.es/email-security](https://retarus.es/email-security)

