

Tenemos algo contra el phishing del Coronavirus:

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 (p.ej., su banco, PayPal) o de portales de compra en línea (p.ej., Amazon).



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 cripticos 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 encantan las crisis. Abusan deliberadamente del estado de emergencia por el Coronavirus: la actualidad del sujeto, la inseguridad de la gente y la situación laboral de teletrabajo, inusual para muchos empleados.



Pero tenga cuidado: los estafadores del Coronavirus 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.



Atentos al phishing sobre Coronavirus

Desconfíe de todo lo que se ofrece actualmente en la red en torno al Coronavirus. Y desconfíe también cuando se trata de instrucciones relacionadas con el teletrabajo.

Métodos actuales de los ciberdelincuentes para propagar malware, sustraer datos y obtener beneficios:



Información “oficial” sobre el Coronavirus como una suscripción a un boletín de noticias, en un archivo adjunto o como una opción de descarga

Ofertas de productos de alta demanda como mascarillas, pruebas para detectar el Coronavirus, aplicaciones de rastreo

Solicitud de datos para una **nueva regulación** de las prestaciones a los clientes o de servicios por el cierre de filiales/oficinas

Solicitud de una **donación**, p.ej., para el desarrollo de una vacuna

Consejos de inversión “inteligentes” como “Elevada rentabilidad en la época del Coronavirus”



Instalación de software para teletrabajo

Solicitud de contraseñas para participar en una videoconferencia

Sincronización de datos para la activación de una herramienta remota (mantenimiento a distancia)

Descarga de una actualización de seguridad para el teletrabajo

¿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 relacionados al coronavirus. **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

