# Kaspersky Security for Microsoft Office 365

# ¿Emigrando a la nube? Asegúrela.

Con más de 100 millones de usuarios al mes, Microsoft Office 365 es oficialmente más popular en empresas que su versión tradicional [1].

Pero el hecho de aligerar la carga de la infraestructura y los recursos no reduce el riesgo de ciberamenazas, especialmente al hablar del servicio de email de Office 365.

Spam, archivos adjuntos maliciosos, phishing (incluyendo spear phishing/ business email compromiso BEC), ransomware y el robo de datos son un gran problema para el email de Office 365.

Y ¿qué hay de los recursos que consumen? Desde la presión de banda ancha hasta la pérdida de productividad, el spam continúa tapando las arterias de las empresas por todo el mundo: más de la mitad del tráfico de email global es spam.

Para las PyMES es un gran desafío mantener la fluidez de comunicación y productividad con las ciberamenazas.

**+600%** El malware dirigido en Microsoft Office 365 aumentó en 2016 [2].

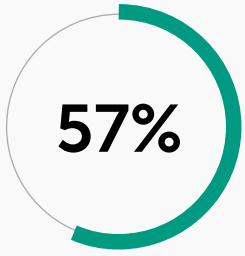
# ¡Click, click, BUM!

Ya sabe cómo funciona: el servicio de email es el vector de malware número uno en las amenazas de seguridad para empresas [3].

Entonces ¿por qué los usuarios siguen haciendo click?

A pesar de los esfuerzos, uno de cada dos hace click en un mail desconocido, aunque el 78% dice entender los riesgos [4].

No es de sorprenderse que esta siga siendo la herramienta elegida por los cibercriminales; la ruta más rápida al corazón de su empresa es la bandeja de entrada de los usuarios. Y cuando los cibercriminales diseñan los emails para parecer legítimos, son más difíciles de detectar y bloquear, ahora imagínese para los usuarios.



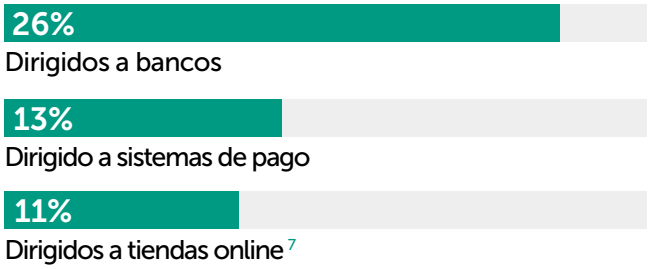

de usuarios de Microsoft Office 365 tenían al menos una copia del ataque de ransomware Cerber basado en spam en su bandeja de entrada en 2016 [5].

1. *Satya Nadella, Microsoft Q3 2017 earnings call. In 2017, Microsoft Office 365 license sales outstripped the on-premises version for the first time.*
2. *https://redmondmag.com/articles/2017/06/01/office-365-security.aspx*
3. *Verizon Data Breach Investigation Report 2017*
4. *Friedrich-Alexander Universitat: https://www.fau.eu/2016/08/25/news/research/one-in-two-users-click-on-links-from-unknown-senders/*
5. *https://www.scmagazine.com/microsoft-office-365-hit-with-massive-cerber-ransomware-attack-report/article/529295/*

# ¿Algo phishy?

La mayoría de las empresas han invertido tiempo en educar usuarios ante las amenazas a través de emails. Pero ¿qué se puede hacer cuando los cibercriminales logran atacar departamentos específicos y usuarios con emails diseñados para parecer provenientes del jefe, el proveedor o un solicitante de empleo?

Se registró alguna forma de phishing en un 21% de los incidentes[6] y más de la mitad de todos los ataques fueron dirigidos al sector financiero:



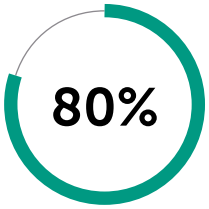

Los ataques de phishing suelen hacerse a gran escala para robar contraseñas, datos bancarios, números de tarjetas de crédito o expandir código malicioso como el ransomware en la computadora de las víctimas. Suelen parecer normales a primera vista, y son enviados en grandes cantidades para alcanzar la posibilidad de que alguna persona caiga. Antes de pensar que usted nunca caería, piénselo:

Alguien del departamento de cuentas recibe un email a final de mes con un asunto como: "ÚLTIMO AVISO DE PAGO URGENTE". Está ocupado, parece legítimo e incluye un PDF adjunto, algo que está acostumbrado a ver en un email. Así que hace click... y el malware se ejecuta.

## "¿Cómo pasó esto?"

Como el usuario tenía prisa no se dio cuenta que el archivo terminaba en .exe en vez de .pdf. O tal vez sí lo vio, pero los cibercriminales escondieron la extensión. A veces, es tan fácil como olvidarse de cambiar un ajuste de Windows que esconde las extensiones de archivo por defecto. De cualquier forma, bloquear estos emails de la bandeja de entrada podría ahorrarle muchos problemas a la compañía. El reconocimiento de archivos reales y el filtrado de adjuntos por extensión solo son dos tecnologías de seguridad que pueden ayudar a detectar y bloquear archivos que se hacen pasar como legítimos.

**En Windows, puede desactivar la opción de esconder extensiones de archivos desconocidos en la sección de carpeta de opciones del control de pestañas. Esto hará que sea más fácil para los usuarios descubrir un archivo que no es lo que parece.**




de las brechas de datos involucra el uso de contraseñas débiles o robadas, la mayoría obtenidas a través de emails de phishing [8].

## Spear phishing: especialmente para usted

Pero ¿qué pasa cuando los cibercriminales llevan las cosas a otro nivel y a otros objetivos específicos de una compañía con emails y archivos adjuntos que parecen legítimos?

El spear phishing puede hacer caer incluso al empleado más cuidadoso: con una "aplicación de trabajo" enviada a un reclutador utilizando una dirección de correo electrónico que haga referencia a una compañía que ya trabaja actualmente con su empresa. O con una factura enviada a la persona de cuentas haciéndose pasar por un socio. A veces, incluso la dirección de correo está retocada para parecer legítima, por lo menos a primera vista o para una persona que no sabe mucho sobre tecnología. Estos correos suelen adjuntar archivos maliciosos o enlaces a un sitio web malicioso, desde donde pueden implementar un ataque o robar credenciales.

6. *Verizon Data Breach Investigation Report 2017.*
7. *Kaspersky Lab: https://latam.kaspersky.com/about/press-releases/2017_kaspersky-lab-detecta-una-disminucion-de-5000-veces-en-los-envios-del-botnet-de-spam-mas-grande-del-mundo*
8. *Verizon Data Breach Investigation Report 2017.*

Algo recientemente añadido a la familia de phishing es el "email del Director Ejecutivo" que autoriza una transferencia de dinero urgente. Conocido como "Business Email Compromise" (BEC), estos correos contienen una solicitud convincente y una dirección remitente modificada para parecer legítima. Están tan bien diseñados que suelen pasar los filtros de spam, no son enviados en grandes cantidades de email y normalmente los envían solo a un par de empleados.

Con BEC es fácil entender por qué la gente comete el error de hacer click. Una vez más, la mejor defensa es detectar y filtrar estos correos antes de que lleguen a los usuarios. Las soluciones de seguridad que permiten la detección de los archivos de Microsoft Office con macros, por ejemplo, pueden incrementar la protección contra archivos adjuntos maliciosos. La habilidad de analizar archivos adjuntos previsualizados añade una capa extra de protección en caso de contenidos de phishing. Mientras tanto el soporte de email autorizado puede reducir significativamente las oportunidades de que un correo falso llegue al usuario final. Desde un punto de vista web, la actualización continua de las bases de datos de URLs maliciosas y de phishing ayudarán a que incluso si un usuario hace click, el sitio estará bloqueado.

**Antes de hacer click en cualquier link, siempre revise la URL: ej. kaspersky.com vs Kaspersky.com. Y nunca introduzca su contraseña o datos a través de un botón. Siempre visite el sitio web legítimo escribiendo la dirección en el navegador.**


El FBI declaró que se perdieron más de $2.3 mil millones de dólares a través de fraudes de emails provenientes de supuestos jefes directivos [9]. Dentro de las víctimas de alto perfil existen firmas globales como Mattel, SnapChat y FACC.

9. *https://krebsonsecurity.com/2016/04/fbi-2-3-billion-lost-to-ceo-email-scams/*

# Spam: el vampiro de la productividad

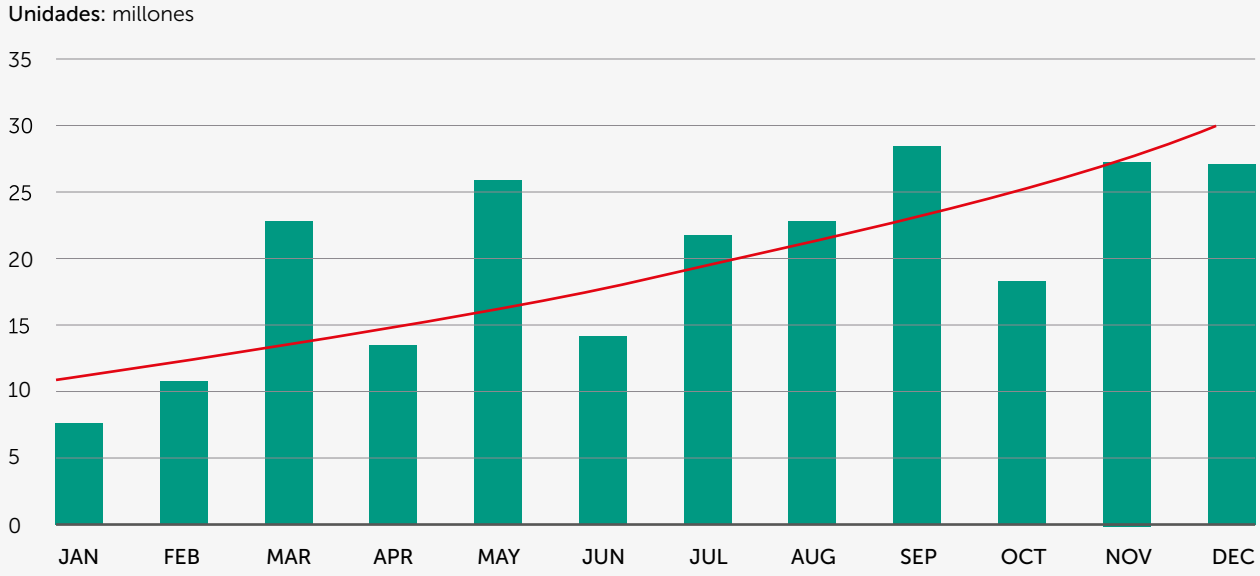
Más del 58% del tráfico de email es spam[10]. Y además de que muchos incluyen malware, también roban productividad y recursos: un trabajador pasa un promedio de 13 horas al año escaneando y eliminando spam, por un costo estimado de $1250 al año[11]. No solo el empleado pierde tiempo, más de la mitad de los costos de energía dedicados a spam están asociados a su eliminación y la búsqueda de email legítimo[12].

Cuando todo el dinero, recursos y dinero que ha ahorrado pasando todo a la nube se ve consumido por spam que nadie quiere, es entonces cuando se enfrenta a un problema.

Pero ¿qué hay de todo el email legítimo que se puede perder por confundirlo con spam? El 35% de los usuarios de empresas dicen que por bloquear emails legítimos se han tardado en responder los correos importantes un promedio de 2-3 veces al año; el 19% dice que les pasa entre 4 y 6 veces al año[13].

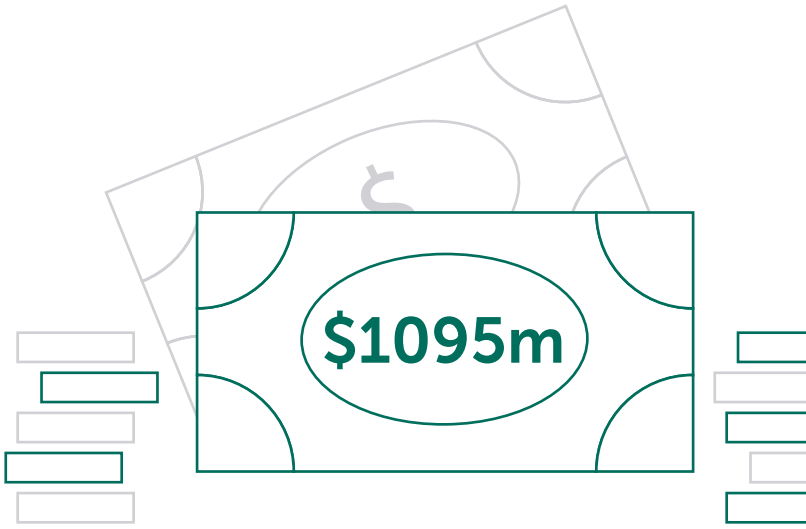
El bloqueo de emails de trabajo es una pérdida de tiempo, pero es incluso peor cuando el mail legítimo se elimina automáticamente antes de que el administrador o usuario final lo decidan, haciéndoles perder tiempo y recursos buscando, o duplicando trabajo.

**La investigación de Kaspersky demuestra un aumento masivo en el volumen de spam malicioso durante 2016**




10. *Kaspersky Security Bulletin: Spam y Phishing en 2016.*
11. *Fuente: Atlassian, Time Wasting at Work*
12. *http://www.brighthub.com/environment/green-computing/articles/33434.aspx*
13. *https://techtalk.gfi.com/survey-spam-email-disrupts-two-thirds-of-businesses-each-year-infographic/*

¿No está seguro de un sitio web que parece legítimo, pero le apareció inesperadamente listo para introducir su contraseña? Invente una, el sitio web real la rechazará. O incluso mejor, busque el prefijo "https" en la ULR, el cual indica que es seguro. Un sitio web sin https es sospechoso, especialmente si es una página financiera o comercial.




El mercado del spam tiene un costo estimado de $1095 millones de dólares anuales [14].

## Malware: la amenaza en el corazón de tu empresa

Mientras muchos cibercriminales se concentran en robar credenciales o engañar usuarios para que hagan pagos, es importante destacar que el 66% de todo el malware que se instala entra a través de archivos adjuntos maliciosos [15]. El 95% de los ataques de phishing que conllevan a una brecha se producen a raíz de la instalación de un software [16].

*Pero usted educó a sus usuarios finales y activó la seguridad que viene incluida en la instalación de su Office 365, ¿cómo pudo pasar esto?*

Algunos criminales son igual de persistentes que los cibercriminales. Siempre están buscando nuevas formas de evadir la detección y nuevas vulnerabilidades en software populares que puedan explotar antes de ser solucionados.

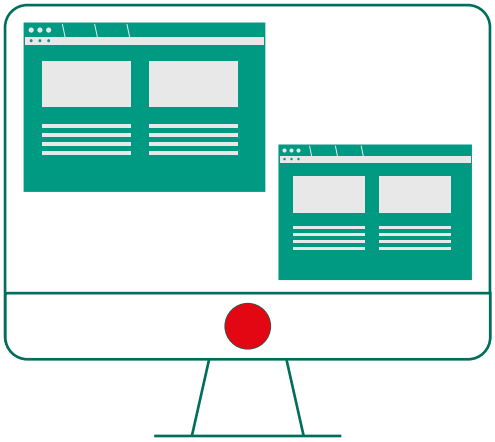
Algunos criminales son igual de persistentes que los cibercriminales. Siempre están buscando nuevas formas de evadir la detección y nuevas vulnerabilidades en software populares que puedan explotar antes de ser solucionados.

Aquellas vulnerabilidades son llamadas "de día cero", son huecos peligrosos en el software que solo han sido descubiertos, pero para los que aún no existe protección.

Estas amenazas en constante crecimiento, que suelen ser desconocidas y avanzadas se combaten mejor con tecnologías de seguridad que utilizan el aprendizaje de máquina y que actualizan constantemente su inteligencia de amenazas (en inglés, threat intelligence). Con esta combinación, su seguridad aprende constantemente de los modelos de amenazas que analiza, y de los ataques que ocurren en el mundo real.

Todo esto quiere decir que la detección antimalware y la tecnología de mitigación es un componente base para asegurar el servicio de correo electrónico, y protegerse de amenazas como spam y phishing.

14. *Kaspersky Lab, Securelist.*
15. *Informe de investigación de brechas de datos 2017 (Data Breach Investigation Report 2017)*
16. *Informe de investigación de brechas de datos 2017 (Data Breach Investigation Report 2017)*



# Amenazas constantes a Office 365

Cuando se trata de proteger su servicio de correo electrónico de Microsoft Office 365, la mejor estrategia es asegurar que las amenazas sean detectadas y bloqueadas antes de convertirse en un problema.

**Instale Kaspersky Security for Microsoft 365. Esta solución combina la protección antimalware de nueva generación con un antispam y antiphishing líderes en la industria para proteger su email y a usuarios finales contra amenazas conocidas, desconocidas y avanzadas.**

Para ser realmente efectivo necesita ser capaz de hacerlo sin ralentizar o accidentalmente eliminar el tráfico del correo electrónico legítimo. Necesita mantener la fluidez de la comunicación, pero a las ciberamenazas fuera. Y si es realmente proactivo, puede usar la información que obtenga de las amenazas bloqueadas para tener una perspectiva sobre el tipo de amenazas a las que su empresa se enfrenta.

**Kaspersky Security for Microsoft Office 365** está diseñado específicamente para hacer esto por su empresa. Al igual que su Microsoft Office 365, está alojado en la nube. Y al igual que las soluciones de Kaspersky Lab, viene incluida en la protección más premiada y probada del mundo[17].

**Kaspersky Security for Microsoft Office 365** utiliza heurística avanzada, aislamiento de procesos, aprendizaje de máquina y otras tecnologías de nueva generación para proteger el servicio de email de los peligros del ransomware, archivos adjuntos maliciosos, spam, phishing y amenazas desconocidas.

También gestiona falsos positivos de una forma más efectiva: los administradores tienen el control total sobre lo que pasa con los emails sospechosos. Los correos se almacenan en copias de seguridad que se pueden buscar y restaurar fácilmente. Nuestra tasa de detección de spam del 99% quiere decir que sus usuarios tardarán menos en gestionar aquellos emails irrelevantes, no deseados y potencialmente peligrosos.

Y ya que usted usa la nube por comodidad, eficiencia de recursos y rentabilidad, Kaspersky for Microsoft Office es muy fácil de usar: puede gestionar todo desde una sola consola y tener acceso a la información de amenazas detectadas y estadísticas. No hay necesidad de un hardware o capacitación adicional, ni distribución para su instalación.

Descubra cómo nuestras tecnologías de seguridad de nueva generación pueden facilitar la gestión y proteger su servicio de email de Microsoft Office 365.

17. *En 2016, los productos de Kaspersky Lab participaron en 78 pruebas y análisis independientes. Nuestros productos obtuvieron 55 primeros lugares y fueron finalistas 70 veces.*
*https://latam.kaspersky.com/top3*