Publicado en Madrid el 28/11/2019

# [IMF Business School ofrece 9 claves para ganar la batalla al ciberdelito](http://www.notasdeprensa.es)

## El 36% de las empresas españolas ha sido víctima de algún ciberataque durante los primeros siete meses de 2019. Además, más de la mitad de los ciberataques se llevan a cabo a través de ‘phishing’, aquellos emails en los que el remitente se hace pasar por una empresa de confianza para pedir datos personales como contraseñas o información bancaria al usuario

 A mediados de enero fue la denominada Collection #1, una operación en la que cerca de 800 millones de direcciones de correo electrónico fueron hackeadas. Esta semana, 10 meses después del considerado como el mayor robo de datos de la historia, se ha conocido una nueva filtración de información personal que ha afectado a 1.200 millones de usuarios en la Dark Web, como ha asegurado el investigador de ciberseguridad Vinny Troia y que, aunque ya eliminada, resultaba fácilmente accesible. Ante este nuevo ciberataque y coincidiendo con la celebración del Día Internacional de la Ciberseguridad (Computer Security Day) el próximo 30 de noviembre, desde IMF Business School han analizado las 9 vulnerabilidades más aprovechadas por los ciberdelincuentes y las claves para superar estos fallos de seguridad que afectan tanto a particulares como empresas. De hecho, el 36% de las empresas españolas ha sido víctima de algún ciberataque durante los primeros 7 meses del año, según BitDefender. Correos electrónicos. ¡Has ganado 3.000 euros! Este tipo de emails, en los que el remitente se hace pasar por una empresa de confianza para pedir datos personales como contraseñas o información bancaria al usuario, son cada vez más comunes. Esta técnica, conocida como ‘phishing’, representa el 53% de todos los ciberataques, según un estudio de Sophos. Para afrontar este problema, lo mejor es leer los correos con sentido común y no abrir ningún mensaje de direcciones desconocidas o sospechosas. Seguridad en dispositivos móviles. Muy relacionado con el anterior punto son aquellas cadenas de WhatsApp que, valiéndose de mensajes sensacionalistas, consiguen que cientos de usuarios pinchen en un link que puede estar cargado de virus. Una vez más, la mejor defensa es el sentido común: tratar al smartphone como si se tratase de un ordenador y no acceder a enlaces sospechosos. Atención a los ‘softwares’. Es muy común que dependiendo del trabajo se utilicen programas informáticos específicos, pero, independientemente del software, siempre ha de ser descargado o adquirido de proveedores oficiales para evitar sitios de descargas con virus. Lo mismo ocurre a la hora de descargarse apps para el smartphone, ya que es vital que éstas se adquieran en mercados oficiales como App Store o Play Google. Solo formularios estrictamente necesarios. Los formularios online que se rellenan para iniciar sesión o para comprar se han convertido en otra de las vías de acceso preferidas de los ciberdelincuentes. Se estima que el 60% de todos los robos relacionados con tarjetas de crédito utilizan esta técnica, según F5 Labs. Asimismo, la compañía especializada en servicios de aplicación y redes de entrega de aplicaciones ha detectado un total de 83 incidentes este año que utilicen esta técnica, afectando a un total de 1,4 millones de tarjetas de crédito. Siempre hay que actualizar. Una situación cotidiana para muchos al acabar la jornada es ver como el ordenador solicita actualizar antes de apagar. Sin embargo, las prisas pueden ser malas consejeras y lo recomendable es tener paciencia y esperar a que acaben las actualizaciones, ya que siempre incluyen parches a vulnerabilidades del sistema que, de no arreglarse, podrían ser aprovechadas por los cibercriminales. Proteger el router. Son la puerta de entrada y salida de los datos a Internet y, por lo tanto, también tienen sus vulnerabilidades como otros hardwares. De hecho, se calcula que el malware VPNFilter consiguió infectar entre 500 mil y 1 millón de routers durante el 2018. Ponles freno a los hackers cambiando la contraseña de acceso a la red que viene por defecto. Antivirus y cortafuegos. Los antivirus y cortafuegos deberían ser el salvavidas por si todo lo demás falla, pero se ve que no es así. Muchos usuarios cometen el error de descuidar muchos comportamientos de seguridad básicos solo por el hecho de tener un buen antivirus u optan por programas gratuitos de protección básica por encima de softwares de pago más completos. En la nube, protegerse Hasta junio de este año, se produjeron más de 15 millones de ciberataques en la nube, de los cuales más de 400.000 fueron completados con éxito, según un análisis realizado por la compañía Proofpoint a 20 millones de cuentas de usuario. Copias de seguridad. Si todo lo anterior falla y los ciberdelincuentes consiguen hacerse con información sensible del usuario o la empresa, es vital que se cuente con una copia de seguridad para recuperarlos con facilidad. Eso sí, de nada sirve hacer un backup de estos datos si se van a almacenar en el mismo equipo que los datos originales. Según Gartner, se calcula que en 2021 habrá 3,5 millones de vacantes en el sector de la ciberseguridad. Asimismo, cada vez más empresas son conscientes de la dificultad de mantener los datos empresariales a salvo. Conscientes de esta necesidad, IMF Business School ofrece entre su oferta educativa un Máster en Ciberseguridad codesarrollado con Deloitte, tanto online como presencial, para responder a este aumento en la demanda de profesionales expertos en esta materia.

**Datos de contacto:**

Redacción

91 411 58 68

Nota de prensa publicada en: [https://www.notasdeprensa.es/imf-business-school-ofrece-9-claves-para-ganar](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorias: Nacional Ciberseguridad Recursos humanos



[**http://www.notasdeprensa.es**](http://www.notasdeprensa.es)