

## INCIBE – INSTITUTO NACIONAL DE CIBERSEGURIDAD

León, 25 de septiembre de 2020.- El Instituto Nacional de Ciberseguridad (INCIBE) es un organismo dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, consolidado como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos y empresas. Además, es un instrumento para la transformación social y oportunidad para la innovación, fomentando la I+D+i y el talento.

INCIBE centra sus esfuerzos en la prestación de servicios públicos de prevención, concienciación, detección y respuesta ante incidentes de seguridad, adaptándose a cada público específico (menores, ciudadanos y empresas), así como al desarrollo de tecnología y herramientas que permiten identificar, catalogar y analizar dichos incidentes.

### Phishing suplantando a la Agencia Tributaria que puede provocar descarga de malware

Esta semana, INCIBE, desde la Oficina de Seguridad del Internauta (OSI), ha detectado una campaña fraudulenta a través del correo electrónico suplantando a la Agencia Tributaria, cuyos mensajes contienen enlaces que descargan *malware* en el dispositivo.

Los mensajes utilizan diferentes argumentos para conseguir que el usuario pulse sobre el enlace y descargue un archivo malicioso, como por ejemplo un documento que se anexa a un comprobante fiscal digital o un comprobante de transferencia.

Más información en: <https://www.osi.es/es/actualidad/avisos>.

### Campaña de correos fraudulentos suplantando al Ministerio de Trabajo y Economía Social

Además, INCIBE, a través de Protege tu Empresa, ha detectado una campaña masiva de envío de correos fraudulentos que tratan de suplantar al Ministerio de Trabajo y Economía Social con el propósito de difundir *malware*.

Más información en: <https://www.incibe.es/protege-tu-empresa/avisos-seguridad>.

Esta información puede ser usada en parte o en su integridad citando la fuente.

### **OnlyFans: la nueva red social para vender tu “privacidad”**

OnlyFans es una plataforma creada en 2016 donde se puede pagar por contenido exclusivo (fotografías, vídeos, transmisiones en vivo, etc.) de otros usuarios a través de suscripciones. Aunque el contenido es muy variado, incluyendo a ciudadanos que comparten sus conocimientos sobre *fitness*, nutrición, consejos del día a día, etc., hay un gran número de personas que lo emplea para publicar y consumir contenidos para adultos. ¿Cuáles son los peligros de esta plataforma? ¿Qué medidas pueden aplicar los usuarios para protegerse?

Más información en: <https://www.osi.es/es/actualidad/blog>.

### **El Día Mundial del Turismo: no olvides incluir la ciberseguridad en tu equipaje**

En 1979, la Organización Mundial del Turismo (OMT), dependiente de las Naciones Unidas, proclamó el 27 de septiembre como el Día Mundial del Turismo. Desde entonces, su objetivo es promover esta actividad de forma responsable, sostenible y accesible para todos abogando por un turismo de calidad que contribuya al crecimiento económico, al desarrollo incluyente y a la sostenibilidad ambiental.

Sin embargo, el turismo está considerado como uno de los sectores más ciberamenazado, ocupando los primeros puestos entre los objetivos de los ciberdelincuentes. ¿Qué recomendaciones hay que tener en cuenta para crear un ambiente ciberseguro?

Más información en: <https://www.incibe.es/protege-tu-empresa/blog>.

### **Botnets o redes zombi: una red de equipos infectados**

Los dispositivos inteligentes cada vez están más presentes en la vida de los usuarios. Tanto los *smartphones*, como los electrodomésticos inteligentes y otros dispositivos con sensores, son capaces de localizarnos en todo momento o percibir nuestro estado de salud. Son muchas las ventajas que ofrecen, pero si se deja la seguridad de estos dispositivos en un segundo plano, se puede correr el riesgo de ser víctimas de las redes zombi o *botnets*. ¿Qué son y cómo pueden afectar a los usuarios?

Más información en: <https://www.youtube.com/watch?v=S-8tfS0uK98>.

### **Recomendaciones y pautas para proteger tu puesto de trabajo**

Actualmente, con el auge del teletrabajo, se ha trasladado el puesto desde la oficina al hogar, provocando un cambio en la percepción de la seguridad y la privacidad, al no delimitar los espacios entre ambos.

Esta información puede ser usada en parte o en su integridad citando la fuente.

A pesar de seguir las indicaciones de seguridad, en ocasiones, se pueden realizar acciones que pueden comprometer la seguridad y la privacidad del puesto de trabajo dando lugar a situaciones que son aprovechadas por los ciberdelincuentes para llevar a cabo sus ataques de manera exitosa.

En esta infografía se resumen los aspectos más importantes en materia de seguridad y privacidad que se deben tener en cuenta a la hora de realizar las tareas en el puesto de trabajo.

Más información en: <https://www.incibe.es/protege-tu-empresa/blog>.



Para más información en materia de ciberseguridad visite INCIBE [www.incibe.es](http://www.incibe.es), Protege tu Empresa <https://www.incibe.es/protege-tu-empresa>, OSI [www.osi.es](http://www.osi.es) e IS4K [www.is4k.es](http://www.is4k.es).

Esta información puede ser usada en parte o en su integridad citando la fuente.