Algunos aprovechan la crisis de la Covid-19 para atacar a nuestros ordenadores, tabletas o teléfonos móviles y robarnos datos sensibles o personales. Es tiempo de confinamiento necesario y obligatorio que nos facilita pasar más tiempo conectados a la red y nos expone más de lo habitual a sus riesgos. Además, el teletrabajo incrementa los riesgos por la falta de seguridad de los dispositivos que tenemos en casa. Ofrecemos diez consejos en pos de esa seguridad informática.

David Megías y Helena Rifà, investigadores expertos en ciberseguridad del Internet Interdisciplinary Institute (IN3) de la Universitat Oberta de Catalunya (UOC), nos facilitan consejos prácticos para evitar ser víctimas de actividades maliciosas en internet en plena crisis del coronavirus.
Â
Las crisis también son situaciones para aprender. De hecho, en chino este concepto se compone de la suma del ideograma de peligro y del de oportunidad. Pero no siempre se saca provecho de oportunidades con buenas intenciones. La crisis presente puede ser un caldo de cultivo para que habituales acciones maliciosas que se propagan por la red se cobren más víctimas, ya que buena parte de la sociedad está más tiempo conectada de lo habitual. «Las campañas maliciosas funcionan por estadística. Sus autores saben que existe un cierto número de usuarios, un porcentaje aunque sea pequeño, que va a caer», indican los expertos de la UOC. «Los datos personales tienen un valor elevado en el mercado negro», añaden. Estos son algunos de los principales motivos por los que tanto los usuarios a título individual como las empresas deben tener presentes precauciones como las siguientes a fin de que los ataques informáticos que se aprovechan de la inestabilidad de este periodo no afecten sus dispositivos y la seguridad de sus datos.
Â

- **1.** Hay que informarse sobre las medidas de protección que pueden tomarse en función de cada caso. Según David Megías, director del IN3, aunque la población recibe «información sobre los riesgos y las vulnerabilidades de conectarse a internet, no cuenta con suficientes conocimientos sobre ciberseguridad». Hay que tener en cuenta que no es similar el grado de riesgo de hacer un uso lúdico de un teléfono móvil al de trabajar con datos sensibles de una empresa en un ordenador que tenemos en casa, especialmente si a raíz de la crisis debemos teletrabajar de forma intensiva. Igualmente, el confinamiento es una óptima oportunidad para aprender buenas prácticas para navegar de forma más segura. Como una de las mejores formas de evitar riesgos es obtener información de calidad, además de poder resolver las dudas que nos surgen a partir de los conocimientos de personas expertas de nuestro entorno, podemos aprovechar esta época para consultar portales de organismos oficiales que facilitan información detallada en materia de ciberseguridad. Es el caso de la Oficina de Seguridad del Internauta (OSI), adscrita a la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, que dispone de información

práctica sobre cómo navegar con protección. En cualquier caso, Megías confirma que «hace falta más formación práctica para los usuarios domésticos a fin de que puedan conocer qué opciones tienen para protegerse frente a los riesgos».

- **2.** Debemos tener contraseñas seguras. «Debemos contar con contraseñas seguras, no solo para acceder a nuestros correos o aplicaciones sensibles como las bancarias, sino también para cuando las claves se establecen por defecto, por ejemplo, en las conexiones wifi, passwords que debemos evitar mantener», puntualiza Helena Rifà, directora del máster interuniversitario de Seguridad de las Tecnologías de la Información y las Comunicaciones. Según la profesora e investigadora de la UOC, aunque los consejos son los habituales, debemos tener en cuenta que en la situación actual podemos ser más vulnerables y debemos minimizar los riesgos.
- **3.** Conviene familiarizarse con algunas de las prácticas maliciosas (malware) más comunes. Es el caso del phishing, que es la suplantación de la identidad legítima de organismos o empresas para engañar a los usuarios y pedirles datos sensibles, como los de carácter personal. El objetivo de sus impulsores puede ser desde «vender bases de datos con direcciones de correo electrónico hasta incluso conseguir datos bancarios, si son capaces de que los usuarios las revelen», apunta Megías. Otra práctica peligrosa común es el llamado ransomware o software de secuestro: los usuarios reciben un mensaje malicioso y por simplemente hacer clic en un enlace abren la puerta a la descarga de un programa que inutiliza el ordenador, lo que impide a los propietarios acceder a su información. El objetivo de sus responsables es pedir un rescate económico para solucionarlo.
- **4.** Los organismos oficiales no piden datos a los usuarios por correo electrónico. Aparte de que el correo electrónico solo suele ser un canal común para campañas publicitarias masivas, «no es la vía por la que nos solicitan nuestros datos personales», matiza el director del IN3. «Las entidades nunca nos pedirán datos por medio de un mensaje electrónico con un sencillo responder aquí, ya que la información sensible no se envía nunca de esta forma», refuerza Helena Rifà.
- **5.** Debemos sospechar de los mensajes electrónicos cuyos remitentes no conozcamos. «Además, no debemos confiar en los mensajes que tengan un remitente del que no tenemos la seguridad de que es quien afirma ser», añade Megías. Según el investigador, una de las mejores maneras de asegurarse de ello es revisar si los dominios de las direcciones de correo son los habituales, tales como .es en el caso de un organismo del Estado, en lugar de .com o .org. «Incluso hay direcciones maliciosas que tienen unos códigos numéricos largos en sus usuarios. A veces, si revisamos los nombres que acompañan a las direcciones sospechosas no nos parecen peligrosas hasta que comprobamos cómo es el email que nos contacta, con un formato alfanumérico muy extraño», puntualiza el experto.
- **6.** Hay que ser conscientes de que, aunque los filtros anti-SPAM o anti-phishing de nuestros servidores de correo funcionan bastante bien, a veces pueden fallar y no detectar algún mensaje malicioso. «Si de cada 100.000 usuarios que reciben un mensaje malicioso, solo un 1% cae en la trampa, ya tenemos 1.000 usuarios afectados. Debemos ser conscientes de que este tipo de ataques se organizan pensando en un elevado número de usuarios», apunta Megías.
- **7.** Las aplicaciones de los markets oficiales, como Google Play o Apple Store, han sido revisadas y en principio son seguras. En cambio, «si nos descargamos una aplicación fuera de un market oficial, nos exponemos a un ataque malicioso para nuestro móvil o tableta. Si no estamos seguros, no deberíamos instalar ninguna aplicación que no sea de un escaparate

oficial», confirma Megías. «A veces, la misma curiosidad con la que navegamos por internet nos hace encontrar contenidos o webs con datos interesantes, como sobre la evolución del coronavirus en tiempo real. Nos indican a continuación que existe una aplicación que podemos descargar para obtener más información, app que ingenuamente descargamos, instalamos y con la que damos permisos adicionales a acciones maliciosas que pueden afectar de manera grave nuestros dispositivos», ejemplifica Helena Rifà.

- **8.** Si teletrabajamos, debemos tratar con cuidado los datos sensibles de nuestras empresas. Los investigadores de la UOC ponen énfasis en las organizaciones que no acostumbran a trabajar de forma remota y que en pocos días no han tenido suficiente margen para implantar un plan de desarrollo del e-trabajo entre su equipo, teniendo en cuenta cómo reducir al mínimo posibles riesgos como los ciberataques. «Los atacantes aprovechan la falta de previsión del teletrabajo para introducir más malware en la red», opina Rifà. Adaptarse y estar preparados en poco tiempo para tomar las medidas necesarias a fin de evitar las vulnerabilidades no es fácil. «Uno de los principales riesgos para las empresas son los datos que manejan los equipos. Durante estos días, los trabajadores acceden a informaciones sensibles de sus empresas desde casa con los ordenadores de sus domicilios, que en muchos casos no se ajustan a los estándares de ciberseguridad fijados por las organizaciones, como ocurre con los dispositivos que usan en sus oficinas», apunta Megías.
- **9.** Al trabajar desde casa, tenemos que evitar hacer copias innecesarias de datos sensibles. Según los expertos de la UOC, tenemos que ser muy cuidadosos con los datos de la actividad profesional y guardarlos de forma temporal y excepcional en los dispositivos de nuestro domicilio. Así, tenemos que evitar hacer copias de datos en dispositivos que están fuera de la red de nuestra organización o empresa, porque no disponemos de las medidas de seguridad y los protocolos que exigen las normativas que regulan su uso, como los requerimientos del Reglamento general de protección de datos. Los investigadores ponen como ejemplo sensible los datos personales y bancarios con los que trabajan los departamentos de recursos humanos de las empresas.
- **10.** Difundiendo fake news ponemos en peligro nuestra ciberseguridad y la del resto de usuarios. Aumentar el ruido con contenido no veraz relacionado con cuestiones de interés general como la COVID-19 no solo perjudica a la sociedad con desinformación, sino que también puede propagar acciones maliciosas que contengan estas informaciones. «Antes de difundir según qué contenidos sensibles debemos estar alerta, consultar fuentes fiables y no amplificar lo que no esté contrastado», opina David Megías. Incluso, según los investigadores de la UOC, webs con nombres demasiado evidentes, que contienen el concepto coronavirus en su URL, o campañas de apoyo colectivo que afloran pueden ser foco de acciones maliciosas contra la ciberseguridad. Por ello, según los expertos de la UOC, la gran norma que hay que seguir siempre es «desconfiar de lo que no conocemos y de aquello de lo que no hemos podido comprobar la autenticidad».

Â

Expertos de la UOC en ciberseguridad

David Megías, además de director del IN3, centro de investigación de la UOC, desde 2019 es uno de los expertos de la iniciativa Uso Delictivo de la Ocultación de Información (CUIng), que coopera con el Centro Europeo de Ciberdelincuencia de la Europol (EC3). Además, es el

investigador líder del grupo de investigación K-riptography and Information Security for Open Networks (KISON), del que también forma parte Helena Rifà, profesora de los Estudios de Informática, Multimedia y Telecomunicación y directora del máster interuniversitario de Seguridad de las Tecnologías de la Información y las Comunicaciones.

* Texto remitido en el que se respeta el contenido íntegro, la redacción y la ortografía, con excepción del titular y de la entradilla del artículo
Â