Los móviles: el principal objetivo de los hackers

Las grandes empresas de ciberseguridad ya lo advertían hace solo unos meses: los *hackers* estaban situando en el punto de mira el ataque a dispositivos móviles. Así lo afirmaba Kaspersky en su boletín de seguridad de noviembre de 2019 y también lo hacía McAfee en su informe sobre amenazas móviles de 2020, en el que alertaba de que las aplicaciones móviles ocultas serían una gran amenaza para los usuarios este año. «**El objetivo de los *hackers* son ordenadores y móviles, pero cada vez más estos últimos, porque los tenemos más descuidados y sin embargo los usamos más.** Por eso a los *hackers* les resulta más fácil penetrar en ellos», afirma Helena Rifà, profesora de los Estudios de Informática, Multimedia y Telecomunicación de la UOC.

De hecho, uno de los últimos ciberataques de los que advirtió la Guardia Civil mediante Twitter circuló por WhatsApp entre teléfonos móviles de todo el país. Se trataba de una falsa promoción para suscribirse gratuitamente a Netflix durante el confinamiento por COVID-19. «Era un ataque de *phishing*, ya que el formulario

que rellenabas no iba a Netflix, sino a una página web trucada con un aspecto similar al de esta plataforma», recuerda Rifà, que también es miembro del grupo de investigación K-ryptography and Information Security for Open Networks (KISON) de la UOC.

El objetivo de este tipo de cibercrímenes es obtener nuestros datos bancarios de manera directa. Aunque abundan, no son el único tipo de amenaza ante la que debemos estar alerta. «**Aproximadamente un 40 % de los ataques buscan nuestros datos financieros, pero otros tienen como fin recabar información en general del perfil de los usuarios para vender esos datos privados** a terceras empresas u obtener más información personal por si más adelante hacen ataques focalizados», advierte la profesora de la UOC, que recuerda que, en las últimas semanas, uno de los más comunes ha tenido como «gancho» los mapas de seguimiento del coronavirus. «Nos los descargábamos para saber en qué zonas estaba más activo el virus y muchos de esos mapas llevaban *malware*», advierte Helena Rifà.

Con ese software malicioso es posible que los ciberdelincuentes hagan un seguimiento de dónde estamos y de las trayectorias que seguimos o incluso que incluyan *spyware* para saber qué tecleamos y qué llamadas telefónicas hacemos, de modo que tienen un acceso casi total a nuestros datos privados.

Además, hay un tercer tipo de amenaza frecuente dirigida a móviles y está relacionada con aplicaciones no oficiales. Aunque con el ordenador solemos ser más precavidos, en el móvil nos bajamos bastantes aplicaciones: según el *Informe mobile en España y en el mundo 2017* elaborado por Ditrendia, en España cada usuario de móvil tiene una media de 17,8 aplicaciones instaladas en su dispositivo. **En la mayoría de los casos el problema no son esas aplicaciones en sí, sino los permisos que damos al instalarlas.**

«Solemos decir que sí a todo, y damos permisos que muchas veces no están relacionados con la aplicación que estamos instalando, y es ahí donde podemos desconfiar. Por ejemplo, al instalar una aplicación de retoque fotográfico que nos pide acceso a nuestro servicio de voz», señala Helena Rifà, que afirma que si vemos estas incongruencias, podemos sospechar. Otra manera de protegernos frente a los *hackers* que tienen nuestro móvil como objetivo es instalar antivirus. Aunque pueden ralentizar un poco el funcionamiento y gastar batería, según los expertos resultan recomendables.

Ingeniería social en tiempos de pandemia

Las consecuencias de los ciberataques, ya sean a nuestros dispositivos móviles o al ordenador, se traducen en miles de millones de euros. Según un informe de la empresa de ciberseguridad RiskIQ, en 2019 cada minuto se perdieron 2.646.000 euros por el cibercrimen. En 2020 la cifra puede ser aún más alta, ya que el número de ataques se ha disparado desde el comienzo del estado de alerta, señala la profesora Helena Rifà. No es la única novedad que han detectado los expertos en ciberseguridad. También **ha cambiado el objetivo de esos ataques, que ahora se ha desplazado. «En lugar de ir directamente dirigidos a las empresas ahora van hacia los usuarios finales porque el trabajo se ha desplazado de las compañías a las casas»**, recuerda Rifà.

Muchos de esos ataques se basan en la ingeniería social, que acude a la parte emocional de los usuarios para poner en marcha la operación. Según explica la profesora de la UOC, en el contexto actual es mucho más fácil que los ataques basados en ingeniería social tengan éxito porque el *hacker* sabe que el usuario está preocupado por un tema en concreto, en este caso el coronavirus, y por lo tanto puede atacar usando ese tema como gancho enviando noticias sobre la COVID-19. «**Al conocer el interés del usuario, las posibilidades de éxito del *hacker* se multiplican. Siempre que se intensifica el valor de cierta información** es más fácil penetrar en los usuarios a través de esta información. Somos más vulnerables», señala.

Precisamente de los ciberataques que ha habido durante el estado de alarma y de cómo se han perpetrado tratará la primera jornada del congreso especial UOC-Con, que tendrá lugar el próximo 27 de mayo. En la primera jornada de este encuentro *online*, «Ciberseguridad y ciberataques durante el estado de alarma», los expertos hablarán de las medidas de seguridad frente a estas amenazas.

Además, en la segunda jornada, «Medidas de control durante la COVID-19: ¿una amenaza a nuestra privacidad?», se debatirá la privacidad de **aplicaciones que tienen como objetivo controlar la pandemia mediante el seguimiento de los ciudadanos.** «Se tratará este tema no solo desde el punto de vista del derecho, sino también desde el de la tecnología: si hay soluciones y herramientas para poder lograr el mismo objetivo pero preservando la privacidad», afirma Helena Rifà, que recuerda que ya existen iniciativas que pueden salvaguardarnos de ese abuso de privacidad.

Un ejemplo de ello es la aplicación COVIDSafe que se está usando en Australia, que incorpora algunas ideas de diseño pensando en la privacidad. Aunque según los expertos tampoco está exenta de ciertos problemas, no utiliza datos de geolocalización GPS, por lo que al no revelar la localización de los usuarios, resulta menos invasiva.