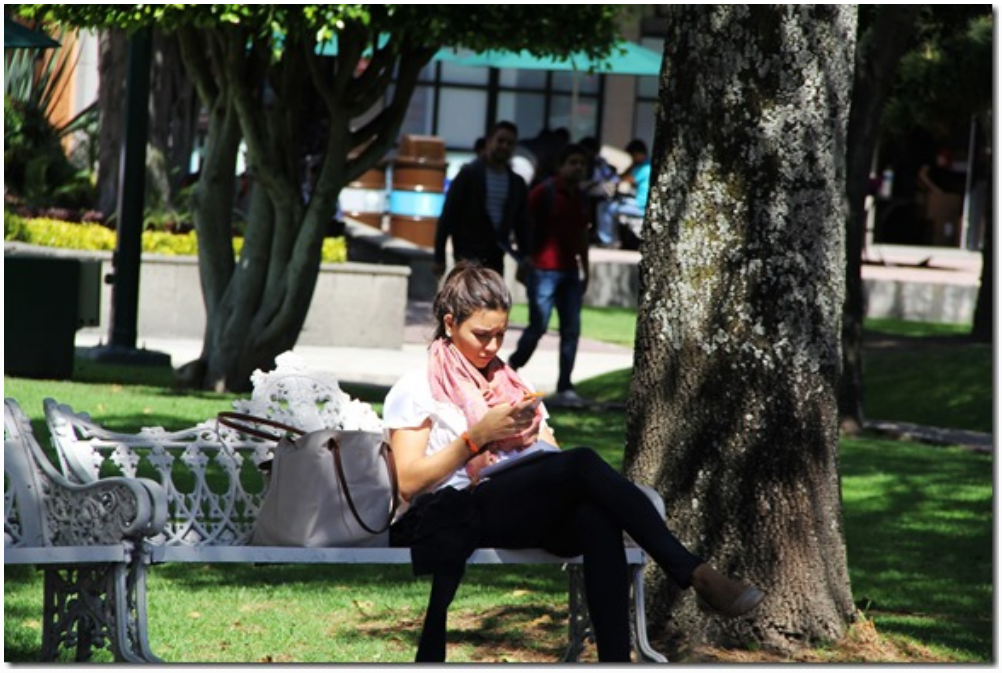
Lo que no conocías sobre seguridad para tu Smartphone



Es difícil pensar en un día encontramos con un aviso de amenaza de virus mientras navegamos en nuestro Smartphone o abrimos algún archivo adjunto en él, sin embargo, si reflexionamos un poco sobre la naturaleza de los virus y cómo afectan a las computadoras nos damos cuenta que todo aquello con un sistema operativo corre el riesgo de ser infectado, sin importar si se trata de Mac o PC o este caso, iOS, Android o Windows Phone.

Diariamente, utilizamos nuestros teléfonos para ver, recibir y transmitir todo tipo de información, links, fotografías, archivos de música, video, etc., es solamente lógico que alguno de estos, alguna vez, pueda contaminarse con un virus o malware. Incluso sólo al dar clic en un link en Twitter.

Aunque los dispositivos móviles son más populares que nunca, los usuarios suelen subestimar el peligro que podrían enfrentar. Según una encuesta realizada por Kaspersky Lab y B2B International, se sabe que el 28% de los usuarios no sabe nada o muy poco acerca del malware móvil.

También destacó que el 58% de los Smartphone con Android y el 63% de las tabletas Android están protegidos por un antivirus, mientras que el 31% de los Smartphone y el 41% de las tabletas ni siquiera están protegidos con una contraseña. Los usuarios de dispositivos con Android enfrentaron amenazas en línea con más frecuencia que los usuarios de dispositivos con Windows (curiosamente, es el sistema operativo móvil más seguro, aunque no invulnerable). Y Apple no se queda atrás, Wirelurker, un troyano descubierto hace poco, es un claro ejemplo de malware diseñado específicamente para atacar a los usuarios de Apple.

Guardamos toda cantidad de información personal y perjudicial (en las manos equivocadas) en la memoria de nuestros Smartphone, ¿te imaginas qué pasaría si te los robaran o los perdieras a causa de un virus? Para que no pierdas todos los datos de tu teléfono o incluso el mismo dispositivo, este Jueves de Tecnología te damos algunos consejos para mantenerlo seguro:

Mantenlo bloqueado

Asegúrate de que la pantalla del teléfono siempre está bloqueada; así reducirás los riesgos si el teléfono cae en manos de un cibercriminal.

Cifra la información confidencial

Si el teléfono incluye funciones de cifrado de datos, asegúrate de utilizarlas. En el caso de te roben el teléfono, los cibecriminales no podrán acceder a la información personal almacenada en él, si dicha información se ha cifrado previamente.

Supervisa el comportamiento de las aplicaciones en tu teléfono

Duda de las solicitudes de permisos de las aplicaciones que se ejecutan en tu teléfono. Ante esta situación, los dispositivos Android son los que se han mostrado más afectados.

Protege el teléfono y tus datos

Muchas personas que usan antivirus olvidan que los smartphones actuales son ordenadores potentes, y que son vulnerables a los mismos riesgos. Asegúrate de contar con un antivirus en todos tus dispositivos móviles y de que las bases de datos de virus se actualizan regularmente.

Desactiva la conexión Bluetooth cuando puedas

Si no estás utilizando la conexión Bluetooth, es mejor desactivarla. De esta forma, conseguirás que tu teléfono sea menos vulnerable a los ciberataques y gastarás menos batería.

Elige una solución de seguridad para Smartphone con funciones antirrobo

Algunos productos de seguridad para Smartphones incluyen una gama de funciones antirrobo que proporcionan acceso remoto al teléfono en caso de pérdida o robo, y con las que puedes bloquearlo, borrar sus datos y buscar su ubicación.

Respalda

Es esencial mantener tanto una copia de los archivos como una copia de seguridad de arranque de tus dispositivos móviles en un disco separado y en una ubicación diferente.

Lo más importante es ser un poco más cuidadoso con la información que permitimos que se comparta en nuestro teléfono. Ten cuidado en descargar archivos poco confiables, abrir páginas desconocidas o descargar aplicaciones dudosas. Perder tu información, especialmente aquella que se refiere a datos personales o trabajos académicos únicos, nos es algo que se le desea a nadie.

Recuerda que, si como alumno necesitas una revisión de tus dispositivos móviles, la UDLAP puede instalarte apoyarte; sólo debes acudir a IA110 en horario de 9 a 18 h.

¿Te pareció útil esta información? No olvides seguirnos el próximo Jueves de Tecnología y compartir con nosotros tus opiniones y experiencias personales.