

La ciberseguridad es un tema que nos afecta a todos y que ya está en todos los ámbitos, queramos o no, como usuarios debemos ser conscientes que el número de delitos informáticos ha crecido exponencialmente en los últimos años. Por este motivo para que nuestras juntas virtuales sean lo más seguras posibles, debemos seguir una serie de pautas que minimicen la posibilidad de ser víctima de un ciberdelincuente.

Debemos tener instalado un antivirus en nuestros dispositivos, tanto el móvil como nuestros PCs o tablets, si nos lo podemos permitir, instalar un antivirus de pago y mantenerlo siempre actualizado.

Del mismo modo, debemos tener actualizado tanto el sistema operativo como el software que utilicemos según nos indique el fabricante, las vulnerabilidades o brechas de seguridad surgen a diario.

No debemos conectarnos a redes wifi que no sean de confianza y por supuesto nunca conectarse a una red wifi abierta, no sabemos quiénes administran estas redes, por lo tanto, conectarnos a través de ellas podría significar que nos están robando nuestros datos.

Las convocatorias de juntas se suelen enviar/recibir por mail, como emisores no debemos incluir en el campo “para” o “con copia” a destinatarios que no se conozcan entre sí, para evitar problemas incluir a todos los destinatarios en el campo “con copia oculta”, revelar el mail de una persona a un tercero sin su autorización podría significar incurrir en un delito de la RGPD; por otro lado, como receptores, debemos asegurarnos de que el mail es lícito, para ello miraremos el mail del emisor e incluso si tenemos cierto conocimiento técnico, las cabeceras de dicho mail, aunque suene raro, es muy sencillo y nos puede evitar más de un problema.

No debemos fiarnos de mails que no esperamos, nos piden algo poco habitual y nos apremian a hacer algo, si tenemos dudas, la mejor arma es comunicarse directamente por teléfono con el emisor y verificar si dicho mail es correcto.

No debemos usar contraseñas débiles o inseguras, quedan prohibidas palabras completas, fechas o nombres de mascotas o familiares, las contraseñas deben ser robustas, mínimo 8 caracteres donde incluyamos mayúsculas, minúsculas, números y algún carácter especial.

Si la aplicación o sistema lo permite, activar el doble factor de autenticación, cuanto más difícil se lo pongamos a un ciberdelincuente antes desistirá de intentarlo y se irá a por otra víctima.

Seguir siempre la máxima, “mínima exposición, máxima seguridad”:

¿Tenemos instalado algún software que ya no usemos? Pues hay que desinstalarlo, con ello obtendremos 2 beneficios, nuestro dispositivo funcionará mejor y evitaremos posibles brechas de seguridad sobre un software que no usamos y que posiblemente se quede obsoleto. ¿Tenemos instalado un software que sí usamos en dispositivos que ya no utilizamos? Pues de igual manera, desinstalarlo, es común que por alguna urgencia instalemos plataformas de comunicación en los dispositivos de algún amigo o familiar, cuando terminemos la reunión desinstalar dicho software.

No mantener las sesiones abiertas de ninguna aplicación más tiempo del necesario, si nos levantamos de nuestro puesto de trabajo, bloquear el equipo antes de irnos, por supuesto no ceder ni comunicar nuestras contraseñas a nadie.

Por último, usemos el sentido común, si algo nos parece extraño, mejor verificarlo, perder 5 minutos en algo, puede significar no caer ante un ciberdelincuente.



Rafael García Lázaro

COO-CTO, Co-Founder

<http://www.hackbysecurity.com>