TELECOMSYSTEM
R.U.C. 1104728611001
Dir. Matriz: 18 de noviembre
entre Miguel y Azuay.
Ciudad de Loja
0995702265
crismajovi@gmail.com

RECOMENDACIONES DE SEGURIDAD INFORMÁTICA

- **Mantener el ordenador actualizado**

Esto es algo que los expertos en seguridad no se cansan de repetir y muchos consideran que lo más importante para la seguridad de un ordenador es mantener el sistema operativo (Windows, OS X, Linux, etc.) del ordenador y los programas que se utilicen **actualizados con los últimos parche de seguridad**. Esto se debe a que en cuanto se conoce un problema de seguridad en un sistema operativo o en un programa los ciberdelincuentes lo analizan y buscan rápidamente la manera de explotarlo para conseguir sus fines. Si instalamos las actualizaciones antes de que un posible programa malicioso aproveche un fallo de seguridad e infecte nuestro ordenador estaremos mejor protegidos.

- **Utilizar un antivirus en el ordenador**

Cada día obtenemos mayor información externa, descargamos ficheros y navegamos mucho por internet. Por tanto es esencial que el ordenador tengo un antivirus instalado que haga de guardián ante tantas posibles amenazas. Existe el falso mito de que los Mac no necesitan antivirus, pero es simplemente un mito. Es cierto que al estar su uso menos extendido que el de los ordenadores con Windows los ciberdelincuentes les prestan menos atención a los Mac, pero también necesitan antivirus.

- **Desconfiar de soportes de información externos**

Es habitual recibir información en memorias **USB, CD, DVD o discos duros externos**. Si es posible se debe evitar. Estos soportes hay que tratarlos con precaución y por tanto hacer que sean analizados por un antivirus antes de ser utilizados. En el caso de las memorias USB o las unidades lectoras de DVD es importante configurarlas para que no se ejecuten o utilicen de forma automática, de tal forma que se puedan

analizar y que sea el usuario quien decida qué hacer con ese soporte de información. Existe software malicioso que si ha infectado una memoria USB y se inserta en un ordenador que ejecuta automáticamente el contenido de la memoria USB el ordenador se estará infectando. Los sistemas antivirus suelen protegen contra esta amenaza. Tan peligroso es que nos den una memoria USB desconocida como que prestemos una nuestra, se utilice en otro ordenador y que posteriormente la insertemos en nuestro ordenador. Si es posible evita el uso de memorias USB para transferir información de terceros.

- **Bloquear un ordenador desatendido**

Cuando nos alejemos de nuestro ordenador por un momento es importante bloquearlo. Es una operación que cuesta un par de segundos y evita que alguien pueda utilizar el ordenador mientras estamos ausentes. Si dejamos el ordenador operativo en nuestra ausencia alguien podría robar información mediante una memoria USB, infectar nuestro ordenador, enviar un mensaje de correo electrónico (y luego borrarlo para retrasar su detección) del que nosotros seremos responsables o borrar/modificar información importante.

- **Utilizar conexiones a internet de confianza**

Cuando se está con un portátil o tableta fuera de nuestra oficina a veces se utilizan **redes WiFi** públicas, lo cual supone un alto riesgo para la seguridad de nuestra información y la de la empresa. Si aun así consideramos absolutamente inevitable conectarnos a una red WiFi pública, al menos deberíamos **utilizar conexiones cifradas** (por ejemplo, utilizando sitios web cuya dirección empieza por 'https' en vez por 'http'). Lo ideal sería que utilizáramos el portátil o tableta con la conexión a internet de **nuestro propio teléfono móvil** (mejor con un cable que por la WiFi del teléfono). Todavía mejor sería utilizar una servicio **VPN** (Red Privada Virtual) que garantizase la confidencialidad de las comunicaciones cifrando toda conexión a internet.
Especial atención a esta norma se debe tener en lugares muy concurridos como ferias o aeropuertos, donde es habitual que ciberdelincuentes espíen las comunicaciones por WiFi. Una práctica habitual que utilizan es crear una red WiFi con el mismo nombre que un restaurante o cafetería cercano, con gran potencia, y dejándola de libre acceso. Muchas personas considerarán que se trata de la WiFi propia de esos establecimientos y pensarán que es segura, cuando en realidad alguien está espiando todo el tráfico que circula por esa red WiFi.

- **Uso de dispositivos personales en la empresa**

Me parece importante destacar la información contenida en un artículo que escribí hace unos meses, 'Estrategia móvil para las empresas (3): BYOD y aplicaciones privadas', donde se revisan aspectos tan importantes como almacenamiento en la nube, pérdida o robo de dispositivos, privacidad, aplicaciones permitidas y prohibidas o qué sucede cuando un empleado deja la empresa, todo ello analizado desde la perspectiva del uso de dispositivos propios en la empresa (BYOD: Bring Your Own Device = Trae Tu Propio Dispositivo).
Contraseñas

Deseo terminar esta serie de medidas hablando de algunos hábitos en el uso de contraseñas que si los practicas conseguirás el más ferviente agradecimiento por parte de los cibercriminales:

- Si utilizas una de las contraseñas más comunes, como por ejemplo '123456′, 'password' o 'qwerty' te querrán toda la vida.
- Si utilizas información personal en la contraseña, como por ejemplo la fecha de nacimiento, número de teléfono, nombre de una mascota, etc. debes saber que existe tanta información pública sobre nosotros que esta práctica supone un alto riesgo. Si sigues esta práctica los cibercriminales te van a hacer la ola.
- Si reutilizas una misma contraseña para múltiples usos no te imaginas cómo te querrán los cibercriminales, porque una vez que la conozcan será la llave que abrirá todas las puertas que necesitan sin ningún esfuerzo adicional. Si no fuese por el riesgo que supone estoy seguro de que te enviarían una postal navideña de felicitación todos los años.
- Si quieres hacer feliz a un cibercriminal debes utilizar contraseñas muy cortitas (menos de 8 caracteres) o que sean palabras que se puedan encontrar en un diccionario para que así les sea muy fácil ir probando las distintas posibilidades y dar con la tuya.
- Por último, si alguna vez te encuentras un precioso regalo con un lazo rojo en tu escritorio y eres de los que escriben las contraseñas en un post-it, puedes estar casi seguro de que ambas cosas están relacionadas.

Creo que el humor es una buena herramienta didáctica, pero quiero dejar claro que no trato de frivolizar sobre este tema porque la seguridad informática es realmente un asunto muy serio. Por tanto, no olvides actualizar tu sistema operativo y tus programas, instala en tus equipos un antivirus, intenta evitar o manejar con cautela dispositivos de almacenamiento externo, si vas a ausentarte de tu ordenador deja tu sesión bloqueada, utiliza exclusivamente conexiones a internet seguras y de confianza, implanta y cumple en tu empresa una política adecuada en el uso de dispositivos móviles personales y cuida la fortaleza de tus contraseñas, y si fuese posible utiliza un segundo factor de autenticación.

Atentamente,

Ing. Cristian Villamagua.

GERENTE TELECOMSYSTEM