



# ¿Por qué proteger tu equipo?

Por Fernanda Cisneros Landín

En los últimos años, las amenazas hacia los usuarios de computadoras ha ido en aumento: malware, bots, phishing, ataques distribuidos e ingeniería social, son sólo algunos ejemplos de estos peligros. Debido a esto, la Secretaría de Telecomunicaciones e Informática del Instituto de Ingeniería organizó una serie de pláticas sobre seguridad informática.

En la primera plática, “¿Por qué proteger tu equipo?” el Mtro. Cuauhtémoc Vélez dijo que en Internet hay 3,574,465,680 usuarios, es decir, que 47.7% de la población mundial hace uso de Internet. Agregó que cada segundo surgen catorce nuevos malware y que hay registros de 431 millones sólo en el 2015.

“La intención no es espantar, es educar” dijo citando al director de Norton Security Response, Kevin Haley. “La intención no es preocuparnos, es ocuparnos. De lo que se trata es que conozcamos y aprendamos a usar la computadora como debe ser y aplicar las medidas de seguridad necesarias para minimizar la presencia de posibles riesgos” apuntó.

El Mtro. Cuauhtémoc Vélez explicó que el “dumpster diving” es una forma de hacer robo de identidad, mediante la búsqueda de información personal en la basura. También, la ingeniería social, un conjunto de técnicas en la cual se basan en la confianza de la persona para obtener información.

“Esto puede sonar increíble, pero se da, y se da con más frecuencia de lo que creemos” aseguró el Mtro. Vélez. “Hoy estamos viviendo una verdadera guerra informática, no lo vemos sino hasta que realmente nos vemos afectados por ello”.

Aseguró también que 65 millones de usuarios mexicanos acceden a Internet. En teléfonos celulares con sistema Android, las nuevas variantes de malware aumentaron un 77% en 2015, de acuerdo con el reporte de Internet Security Threat Report.

En cuanto al IIUNAM, el Mtro. Vélez aseguró que uno de los problemas más comunes es el Ransomware, que mediante un correo electrónico con un archivo anexo se ejecuta un script. “Ese programa va a hacer dos cosas: mostrar una pantalla, que puede ser del FBI o de la Policía Federal o puede simplemente decir ‘tu información está raptada’.

“Mientras ustedes están leyendo ese mensaje se está ejecutando un programa que encripta la información”. Ante esta situación, comentó, “es mejor tener un respaldo de información para no tener que pagar un rescate, porque se estaría fomentando un delito”.

Finalmente, el Mtro. Cuauhtémoc Vélez dijo que con cualquier dispositivo con acceso a internet existe la posibilidad de que pueda ser hackeado y los proveedores no lo están considerando, por lo que es importante tener un respaldo de información. Invitó también a seguir las pláticas de seguridad informática que organiza la Secretaría de Telecomunicaciones e Informática.

