



## Academia de Diplomacia “Antonio José de Irisarri” imparte conferencia sobre medidas de seguridad en el uso del internet



A la presente fecha esta herramienta es indispensable para el desarrollo de las actividades de los usuarios. Sin embargo, se debe tomar en cuenta sobre los riesgos y medidas de seguridad para protegerse de posibles amenazas informáticas. Es por ello, que la Academia de Diplomacia “Antonio José de Irisarri” del Ministerio de Relaciones Exteriores de Guatemala, presentó la conferencia “Ciberseguridad” a funcionarios diplomáticos y trabajadores de la Cancillería el cual fue impartida por el Ingeniero Juan Pedro Cáceres, catedrático de la Universidad del Valle de Guatemala.

Durante su disertación, el experto detalló la conducta de la red informática al momento de la navegación, pues es necesario proteger los sistemas, aplicaciones, dispositivos informáticos, datos confidenciales y activos financieros contra los virus que pueden infiltrarse en los dispositivos que son de apariencia simples y molestos, dijo.

Además, Cáceres recomendó tener precaución en la instalación y uso de aplicaciones que pidan permisos excesivos, pues son las vías para vulnerar la seguridad del usuario convirtiéndolos en víctimas de robo de identidad, principalmente con archivos que contengan

malware, un software malicioso para atacar u obtener información privada de sus víctimas.

### **Prevención en el trabajo diplomático**

En el caso de la diplomacia, la ciberseguridad en las relaciones internacionales es importante que no está exenta dentro de un mundo en el que este tipo de ciberataques parecen estar cada vez más generalizados, donde no está tan lejos de las reacciones diplomáticas al máximo nivel, y por ello se debe prestar atención en el envío de las comunicaciones electrónicas como correos, uso aplicaciones y otras formas para el desempeño de las labores en las embajadas y consulados.

“Se debe tener precaución en el uso de estas herramientas, pues deben tener el respaldo de sitios oficiales. Por ejemplo, al realizar las traducciones no se emita un mensaje equivocado que perjudique el trabajo diplomático. Otro punto importante es hacer uso de herramientas antispam en los correos electrónicos de los funcionarios diplomáticos para que no adjunte enlaces sospechosos donde se puede originar un ataque entre embajadas”, advirtió el experto.



Otro de los puntos, es evitar conectarse a redes wi fi públicas o bluetooth, pues algunas de ellas no suelen contar con elementos de protección como contraseñas, debido a que cualquiera puede conectarse de manera anónima, ante esa ausencia de seguridad que se fusiona con la creatividad de los cibercriminales para obtener información o dinero de sus víctimas.

Por último, el expositor recomendó no usar aplicaciones que solicitan datos específicos más de lo necesario con la justificación de un mejor funcionamiento.

Por ejemplo, si vamos a instalar una aplicación para editar fotos y vídeos, es lógico que nos pida permisos para acceder a la cámara. Pero, una aplicación destinada a información climática exija accesos a sus contactos, ubicaciones o utilizar sus redes sociales como punto de inicio no tendría sentido que solicitara esa autorización. Por lo tanto, es importante descargar exclusivamente herramientas que pidan permisos que tengan sentido, recomendó.

