Publicado en Madrid el 16/10/2023

Estos son los ciberpeligros de usar el email del trabajo para registrarse en Tinder

La compañía de ciberseguridad S2 Grupo advierte de que cuando se usa el correo corporativo para darse de alta en cualquier red social, se pone en ciberriesgo a la empresa, a los compañeros y a uno mismo

Según ha indicado en un comunicado la empresa S2 Grupo, especializada en ciberseguridad y gestión de sistemas críticos, es "una práctica común" que se utilice el correo corporativo para registrarse en redes sociales. Esta práctica puede acarrear problemas de ciberseguridad en las empresas y organizaciones de todo tipo.

"Uno de los casos donde esto sucede es en Tinder, por ejemplo. Y aquí el peligro se ve muy fácilmente. Damos mucha información sobre uno mismo, que incluso se puede pensar que es privada, y todos esos datos en realidad no se sabe a quién se los estamos ofreciendo. Es más, puede que no se los estemos dando a una persona y sea un bot. Cualquier ciberdelincuente puede hackearnos el perfil de Tinder, descubrir dónde trabajamos y atacar la cuenta profesional", ha afirmado José Rosell, socio-director de S2 Grupo.

En este contexto, el equipo de la empresa de ciberseguridad ha destacado que 5 peligros de utilizar la cuenta de correo en esta red social son los siguientes:

1.- Tinder tiene demasiada información sobre sus usuarios >> Al descargar Tinder y aceptar su política y condiciones de uso, se permite que acceda a información no sólo del dispositivo desde el que se va a utilizar la app, sino también del perfil de usuario que va ser creado. Si este usuario utiliza una cuenta de correo profesional, Tinder la recoge en sus bases de datos, vinculándola a un perfil determinado y, dependiendo del caso, a datos bancarios.

2. No se sabe quién hay detrás de la pantalla >> La falsa sensación de seguridad que aporta hablar a través de la pantalla con gente desconocida, hace que las personas se vuelvan más confiadas y establezcan contacto con cualquier persona con la que se haga match, independientemente de si se la conoce realmente o no. Es más, puede que incluso estemos en comunicación con un bot sin percibirlo. En estos casos, las posibilidades de ser víctimas de cualquier ataque de ingeniería social (phishing, catfishing, chantaje, estafas, robo de información personal o cuentas, infección del dispositivo mediante virus) se multiplican.

3. El campo de actuación de los ciberdelincuentes es mayor >> El hecho de no separar la esfera profesional de la personal proporciona información más completa sobre uno mismo, ampliando el campo de actuación de los ciberdelincuentes y aumentando el posible daño de los ciberataques. Cuanto más ser reserven datos relevantes sobre uno mismo, más ciberseguro se estará. Es importante aprender a separar el aspecto personal del laboral porque de cara al uso de servicios en Internet ya que garantiza mayor protección.

4. Se puede comprometer la información de la organización profesional, la de los compañeros y la propia >> Si el correo utilizado para crear el perfil es el mismo que el del puesto de trabajo, el peligro es evidente, porque si hackea el perfil de un usuario se puede acceder a la cuenta profesional. La suplantación de identidad (tanto personal como laboral), la extorsión, el acceso y difusión de información confidencial y el hackeo de sistemas de seguridad del lugar de trabajo, son algunos de los riesgos si se vincula la cuenta profesional a una app de carácter personal.

5. Falta de profesionalidad >> Utilizar la cuenta de correo corporativa para fines personales también puede interpretarse como falta de profesionalidad. El email es una herramienta de trabajo indispensable proporcionada por la corporación a la que se pertenece para poder realizar funciones correctamente y que, por tanto, no es privada. Si este recurso se utiliza para fines particulares, con el riesgo que ello conlleva, se está demostrando falta de compromiso y seriedad con el trabajo, y atentamos contra la confianza depositada.

En conclusión, la recomendación del equipo de S2 Grupo para no incurrir en este tipo de ciberpeligros en el uso de una red social como Tinder es crear una cuenta de correo personal y específica para esto y limitar la cantidad de información que se comparte porque una sobre exposición de los datos personales puede situar en una posición de desventaja.

Datos de contacto:
Luis Núñez Canal
S2 Grupo
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional Sociedad Ciberseguridad Recursos humanos