Cómo evitar caer en estafas por correos electrónicos falsos

10/07/2021

La seguridad en la web es todavía un tema que causa dolores de cabeza a las autoridades de casi todos los países del mundo, teniendo en cuenta las nuevas formas que casi a diario surgen con el objetivo de robar la información personal de los internautas.

Sin embargo, hay algunas que a pesar de ser tan conocidas no pierden vigencia para los ciberdelincuentes, no solo por la facilidad en su ejecución sino por su efectividad. Una de ellas es el ***spoofing* de correo electrónico**, que no es otra cosa que la creación y distribución de e-mails falsos que simulan el dominio de una empresa reconocida para que su treta pueda pasar lo más genuina posible y que así la víctima acceda a las peticiones que hace el atacante. Entre las principales están **"la descarga de malware, el acceso a sistemas o datos, el envío de datos personales o incluso, la transferencia de dinero"**, tal y como lo explicó la empresa de ciberseguridad Kaspersky, por medio de un comunicado de prensa.

"A menudo, estos correos electrónicos "falsos" parecen proceder de organizaciones de buena reputación, **lo que pone en peligro no sólo a los objetivos, sino también el buen nombre de las empresas cuyo dominio ha sido utilizado para engañar**. Es más, los correos electrónicos falsos pueden formar parte de ataques más amplios y de varias fases, como los que se realizan para difamar a las empresas. Y es un hecho que estos ataques van en aumento", añadió la compañía.

Por supuesto, este tipo de ataques no son de una sola clase, sino que existen varias formas de ejecutarlos, siempre

haciendo pensar a la víctima que en realidad está recibiendo un correo de una empresa perfectamente establecida y que sí es importante para ella. Así, por ejemplo, existe el ***"spoofing* de dominio legítimo"**, que como su nombre lo indica, en el apartado "De" de un correo, los ciberdelincuentes colocan el dominio de una organización de buena reputación, lo que hace pensar que el mismo es real.

"Sin embargo, si la empresa objetivo ha implementado uno de los nuevos métodos de autenticación de correo, los atacantes deben recurrir a otro método. Es aquí donde entra el llamado ***display name spoofing*** o "suplantación de nombre para mostrar", en el que los atacantes suplantan a la persona que envía el correo electrónico, es decir, haciendo que parezca que ha sido enviado por un empleado real de la empresa", explica Kaspersky en su comunicado.

 Ejemplo de un mensaje de suplantación. Foto: Kaspersky

¿Cómo reducir el riesgo de caer en una estafa?

Si usted es dueño de una empresa o es trabajador y desea proteger la información personal que le ha sido dada a su cuidado, solo hay que seguir estos pasos:

1. Lo más importante siempre será la pedagogía. Por esto es necesario realizar un curso de concienciación sobre seguridad, con el que se pueda reforzar los conocimientos, tanto propios como de la compañía, y así ofrecer a los empleados las herramientas necesarias para **comprobar siempre la dirección inscrita en los correos electrónicos de personas desconocidas.**

2. Proteger servicios "comunitarios" como **Drive o Microsoft 365** para así evitar la intrusión de personas ajenas a la compañía que puedan filtrar correos falsos y así robar información relevante.

3. Ahora bien, el conocimiento es importante para no caer como incautos en una red de *spoofing*, sin embargo, la ayuda de la tecnología es fundamental para este objetivo. Es importante adoptar un método de autenticación de correo electrónico, especialmente el corporativo. **Entre las mejores opciones se encuentran SPF, DKIM o DMARC.**