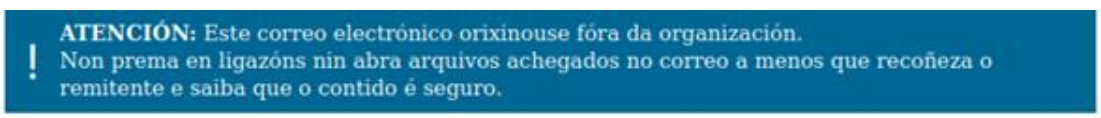
Recomendacións para previr o phishing no correo electrónico

O correo electrónico é unha das vías máis frecuentes pola que os cibercriminais tentan suplantar a unha identidade coñecida, co obxectivo de que a vítima faga clic nunha ligazón maliciosa, descargue un ficheiro adxunto con malware, envíe información sensible ou realice un pago fraudulento.

As seguintes recomendacións axudaranche a detectar correos potencialmente perigosos e non caer nas trampas dos cibercriminais:

- É posible que o teu servizo de correo electrónico corporativo identifique os correos que chegan do exterior ou con remitentes sen verificar mediante alertas visibles ao comezo das mensaxes. Se esta característica está dispoñible, as alertas deben ser o primeiro sinal para aumentar a precaución:



- As técnicas de engano están en evolución permanente, por iso é moi importante pararse a reflexionar e comprender o que se está pedindo na mensaxe, analizando os riscos que poden supoñer o que se solicita (roubo de información, pagos erróneos, apertura dun arquivo malicioso, etc.).

- Débese desconfiar sempre de todo aquilo que se salga do habitual, como mensaxes nas que se pide realizar accións dun xeito excepcional, con urxencia, adulacións, ameazas, etc.

- A inclusión de enlaces e ficheiros adxuntos maliciosos nas mensaxes é unha técnica habitual dos ciberdelincuentes.

- En caso de existir a máis mínima dúbida dunha mensaxe ou a súa procedencia, contacta co remitente por outro medio distinto do correo electrónico.

- É moi importante informar ao teu Centro de Atención a Usuarios cando se sospeite dun *phishing*. A seguridade é cousa de todos!

Lembra que podes atopar máis información e consellos sobre ciberseguridade e protección de datos no portal ciberseguridadegalicia.gal