Estimado cliente.

Como usted probablemente conoce por los medios de información y difusión, la inestable situación geopolítica actual ha incrementado las amenazas y **riesgos relacionados con la ciberseguridad.**

Estas amenazas afectan a la generalidad de los dispositivos y terminales, a las credenciales de usuario, a los datos almacenados, a los servicios de correo y a los dominios de INTERNET.

Concretamente, queremos alertarle acerca de los muchos intentos de suplantación de identidad que se vienen produciendo en los distintos medios y canales de comunicación:

- Llamadas de teléfono
- SMS con enlaces maliciosos
- Chats y Redes Sociales
- Correos electrónicos con nombres simulados

Como sabe, hay un incremento en el fraude mediante la utilización de nombres de dominio similares al de las empresas y Web falsas -(cybersquatting) y (pharming)- de lo que se sirven los potenciales defraudadores para registrar y utilizar un determinado nombre de dominio muy similar a uno legítimo, o para simular páginas Web, sirviéndose de internet para conseguir correos del emisor legítimo que les permita manipular o incorporar un texto con el ánimo de conseguir de un tercero mediante tales engaños un beneficio propio ilícito.

A este respecto, y con el fin de que no prosperen tales intentos de fraude, les aconsejamos que extremen las precauciones y comprueben siempre la identidad de los correos que les puedan llegar a sus buzones electrónicos, comprobando:

- que se ha enviado desde la dirección legítima. ***En nuestro caso, siempre debe figurar @saint-gobain.com***

- que el remitente o contactos son veraces. *Ante la más mínima duda, le sugerimos que* ***contacte con nosotros para contrastar la información.***

Tengan en cuenta que, en el caso de una posible comunicación nuestra, sobre modificación de datos de pago, SAINT-GOBAIN siempre les adjuntará el preceptivo certificado bancario, o el documento necesario para validar la información adjuntada.

Adicionalmente a lo anterior ***SAINT-GOBAIN siempre establecerá un contacto telefónico para confirmar el cambio solicitado.***

Igualmente, ante cualquier sospecha de un correo fraudulento, les sugerimos que contacten con nosotros antes de modificar una cuenta bancaria, enviar información sensible, compartir credenciales, abrir archivos adjuntos, o consultar información en plataformas o links de INTERNET.

Atentamente, Saint-Gobain