

Escalation process

If you have doubts about any email or attached file, do not download, do not open it and report, follow these steps:

1. Click the button directly from Outlook
2. Call the Cibersecurity team

Noticias Banorte: Mes de la mujer 2024 ❤️

IG Para Banorte

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Responder Responder a todos Reenviar

Lunes 04/03/2024 01:37 p. m.



MANTÉN SEGURO A BANORTE

¿Crees que tu equipo puede estar infectado con *malware*? No te preocupes, nuestro equipo de seguridad está listo para asistirte.

Llama desde la red externa al 55 200 opción 3 o desde la red interna al 81 0 opción 3.

Si es sospechoso, es peligroso.



¿TE INTERESA ADQUIRIR UN INMUEBLE? BANORTE TIENE OPCIONES PARA TI

Inmuebles adjudicados con atractivos descuentos del valor comercial.

Para consultar el catálogo ingresa a la intranet de Recursos Humanos y sigue esta ruta:

Servicios en línea - Venta vivienda empleados

Noticias Banorte: el primero del 2024 📅

IG Para Banorte

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Responder Responder a todos Reenviar

Lunes 15/04/2024 10:04 a. m.



¿ERES DE LOS QUE CAEN O DE LOS QUE SI SABEN?

El *phishing* es un ataque en el que los delincuentes buscan engañar a las personas con el fin de robarles su información. Su principal arma es el correo electrónico dada la facilidad de poder usar otra identidad.

Los peligros más comunes asociados al *phishing* son:

- Robo de información personal y financiera.
- Suplantación de identidad.
- Accesos no autorizados.

Cualquier correo sospechoso repórtalo mediante el botón "Reportar *Phishing*" que está habilitado en tu herramienta de correo electrónico.



CONOCE EL PROCESO DE AUTORIZACIÓN

Si tu puesto requiere enviar información a correos externos es necesario solicitar la excepción para que tus correos no se bloqueen y asegurar que no se pretende hacer un mal uso del correo electrónico.

Da clic [aquí](#) para consultar el proceso.

Noticias Banorte: Ingenio Banorte 2024 🚀💡



Para

Banorte

Responder Responder a todos Reenviar

lunes 22/04/2024 09:04 a. m.

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

> CONTROL INTERNO / DATOS PERSONALES

> YO SOY CONTROL INTERNO



VUÉLVETE EL GUARDIAN DE LOS DATOS PERSONALES

Tu Dato necesita colaboradores expertos en la protección de datos personales, conviértete en uno de ellos.

Da clic [aquí](#) para conocer más.

MANTÉN SEGURO A BANORTE

¿Crees que tu equipo puede estar infectado con *malware*? No te preocupes, nuestro equipo de seguridad está listo para asistirte.

Llama desde la red externa al 55) opción 3
o desde la red interna al 8 pción 3.

Si es sospechoso, es *peligroso*.



¿CÓMO COMBATIR LOS ATAQUES DE PHISHING?

Aunque no existe una receta exacta, es importante conocer algunas acciones que usan los criminales en estos ataques y cómo combatirlas:

Acciones usadas por los criminales

- Manipulan nuestras emociones
- Suplantando la identidad de empresas o personas
- Fallos en la capacitación
- Volumen masivo de correos
- Falta de medidas de seguridad



¿Cómo me protejo?

- Mantenernos tranquilos y revisar primero el correo, sin hacer clic o descargar nada.
- Revisar la dirección de donde proviene, así como las imágenes que usa.
- Mantenernos informados de las campañas de seguridad y participar reportando las simulaciones de *phishing*.
- Evita pensar que "a mí nadie me atacaría" ya que estos ataques le pueden suceder a cualquiera.
- Mantener mi equipo actualizado, y no prestando mis credenciales de acceso.



Mantente alerta, y si sospechas de algún correo electrónico, repórtalo mediante el botón "Reportar Phishing" en Outlook.

1,2,3
POR LAS
CONTRASEÑAS

ASÍ ATACAN AL
CONTROL DE
ACCESOS

Escucha el audio aquí

Escucha el audio aquí

Recuerda, tú eres la primera línea de defensa contra las amenazas.
Si detectas actividades sospechosas, repórtalo a la
Mesa de Seguridad y Control de Accesos 8811-6200 opción 3
¡SI ES SOSPECHOSO ES PELIGROSO!

Tenemos unas preguntas para ti
Da clic aquí