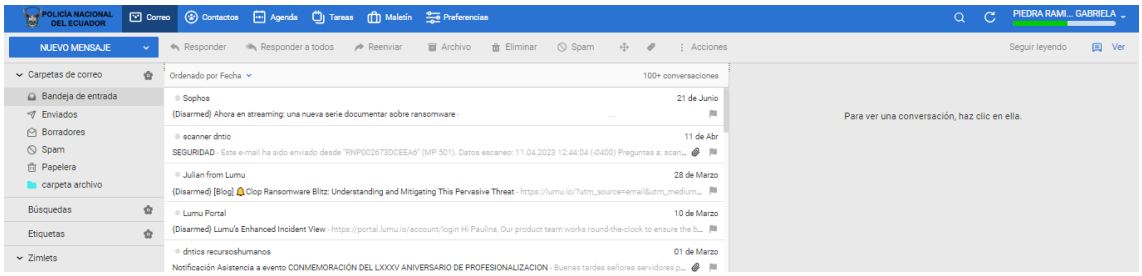
BUENAS PRACTICAS DEL USO DEL CORREO ELECTRONICO INSTITUCIONAL



¿Sabías cuáles son los métodos de ataque?

TIPS

- El atacante hace creer a la víctima que el fichero adjunto es legítimo porque le asigna un icono representativo de determinado software conocido.
- No se debe incluir macros en un documento de office porque el atacante consigue ejecutar código dañino en el equipo de la victima
- Detectar que el archivo adjunto que envía el atacante no contenga espacios justo antes de la verdadera extensión.
- Antes de enviar cualquier mail, los atacantes tratan de obtener la mayor cantidad posible de información acerca de sus víctimas.
- No confíe únicamente en el nombre del remitente. Debe comprobar que el propio dominio del correo recibido es de confianza.
- Antes de abrir cualquier fichero descargado desde el correo, asegúrese de la extensión del mismo.
- Es importante que el usuario no ejecute ningún fichero cuya extensión sea extraña o desconocida.
- El sistema operativo, las aplicaciones ofimáticas, así como el navegador y cada uno de sus componentes, deben de estar actualizados a la última versión en cada una de las estaciones del cliente final.

Telf. 2236-092 / Conmutador 3955-900
dntic.direccion@policiaecuador.gob.ec
Dirección Nacional de Tecnologías de la Información y Comunicación
Departamento de Seguridad de las TIC

BUENAS PRACTICAS DEL USO DEL CORREO ELECTRONICO INSTITUCIONAL

Cómo debemos actuar en estos casos:

- El usuario debe comprender que el proceso de enviar un correo electrónico comprende numerosos pasos en los cuales se ven involucrada información considerado sensible o confidencial.
- Evite hacer clic directamente en cualquier enlace desde el propio cliente de correo. Si el enlace es desconocido es recomendable buscar información del mismo en motores de búsqueda como Google o Bing.
- Utilice contraseñas robustas para el acceso al correo electrónico. Las utilice doble autenticación.
- Cifre los mensajes de correo que contengan información sensible.
- Si se va a enviar un mensaje a varias personas y se quiere evitar que los destinatarios puedan ver el resto de direcciones, utilice la función de copia oculta (CCO)
- Debe informarse inmediatamente al responsable de seguridad de la organización en el caso de recibir un correo sospechoso (las faltas de ortografía suelen ser una señal bastante reveladora).
- No debe hacerse clic en ningún enlace que solicite datos personales ni bancarios (los bancos nunca solicitarán las credenciales o datos personales del cliente por medio del correo electrónico).

REFERENCIAS:

https://www.proofpoint.com/us/security-awareness/post/2020state-phish-security-awareness-training-email-reporting-morecritical

https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl2020-phishing/at_download/file

https://computerhoy.com/noticias/tecnologia/ransomwarenegocio-lucrativo-sigue-creciendo-668142

Telf. 2236-092 / Conmutador 3955-900
dntic.direccion@policiaecuador.gob.ec
Dirección Nacional de Tecnologías de la Información y Comunicación
Departamento de Seguridad de las TIC