10 de abril de 2019

Guías y Recomendaciones

1. Phishing

El "phishing" es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. Resumiendo "todos los datos posibles" para luego ser usados de forma fraudulenta.

No sólo de banca online vive el phishing

La mayor parte de ataques de phishing van contra entidades bancarias, pero en realidad pueden utilizar cualquier otra web popular del momento como gancho para robar datos personales: eBay, Facebook, Pay Pal, etc.

¿Cómo protegerme?

- Identifica los correos electrónicos sospechosos.
    - Con la finalidad de engañarnos en ocasiones usan correos que incluyen el nombre de la institución que pretenden usar como parte del engaño. Si tienes duda si esa dirección de correo corresponde, te puedes comunicar con el área de atención a clientes y corroborar.
- Verifica la fuente de información de tus correos entrantes.
    - Ninguna institución bancaria o financiera te pedirá datos como: contraseña, código de seguridad, token o números de la tarjeta de codigo por correo electrónico. Si en el correo se te piden estos datos, probablemente es que sea phishing.
- Nunca entres a la pagina web de tu banco a través de enlaces incluidos en correos electrónicos. Accede directo de tu navegador.
    - Si aparece una dirección de internet que debes visitar para poner tus datos, revisa la dirección en el navegador, puede ser que no sea de una institución autentica.

- Refuerza la seguridad de tu dispositivo.
    - Mantén actualizados los componentes de su computador como antivirus, aplicaciones y sistemas operativos; los desarrolladores siempre se encuentran corrigiendo fallas o vulnerabilidades de los mismos.
- Introduce tus datos confidenciales únicamente en webs oficiales.
    - Si abres un enlace contenido en un correo de alguna empresa, verifica que sea un sitio seguro viendo en tu navegador si se estableció una conexión segura y si la dirección incluye "https://" al principio.
- Revisa periódicamente tus cuentas.
    - Nunca está de más revisar tus cuentas bancarias de forma periódica, para estar al tanto de cualquier irregularidad en tus transacciones online.
- Ante la mínima duda se prudente y no te arriesgues
    - La mejor forma es siempre es rechazar cualquier correo electrónico o comunicado que incida en que entregues datos confidenciales.
    - Se prudente con lo que publicas en tus redes sociales, el uso de la ingeniería social es un arma poderosa de información contra ti mismo.
    - Elimina este tipo de correos y llama a tu entidad bancaria para aclarar cualquier duda. Repórtalo también reenviando el correo a phishing@dicat.gob.do
- Infórmate periódicamente sobre la evolución del malware