Debido al incremento en el número de ataques de phishing (suplantación de identidad) en los últimos meses, en COBAES te recomendamos atender las siguientes acciones:

No haga clic nunca en vínculos ni datos adjuntos en correos electrónicos sospechosos.
Informar del mensaje sospechoso a la Dirección de Tecnologías de la Información para recibir asesoría y que se tomen las acciones pertinentes.
Eliminar el correo electrónico sospechoso.

Protéjase del phishing

El phishing es un ataque que intenta robar su dinero o su identidad, haciendo que divulgue información personal (como números de tarjeta de crédito, información bancaria o contraseñas) en sitios web que fingen ser sitios legítimos, empresas prestigiosas, amigos o conocidos en un mensaje falso, que contiene un vínculo a un sitio web de phishing.

Cómo detectar un mensaje de phishing

El phishing es una forma popular de ciberdelincuencia debido a su eficacia.
Los ciberdelincuentes han tenido éxito al usar correos electrónicos, mensajes de texto o mensajes directos en las redes sociales o en videojuegos para que las personas respondan con su información personal. La mejor defensa es el conocimiento y saber qué buscar.

Aquí se muestran algunas formas de reconocer un correo electrónico de phishing:

1. **Llamada urgente a la acción o amenazas**: sospeche de los correos electrónicos que afirman que debe hacer clic, llamar o abrir un archivo adjunto de inmediato, a menudo, afirman que tienes que actuar ahora para reclamar una recompensa o evitar una penalización. Crear un falso sentido de urgencia es un truco común de los ataques de phishing y estafas. Lo hacen para que no piense en ello demasiado o consulte con un asesor de confianza que pueda advertirle.
2. **Remitentes de primera vez o poco frecuentes**: aunque no es inusual recibir un correo electrónico de alguien por primera vez, especialmente si están fuera de su organización, esto puede ser un signo de suplantación de identidad (phishing). Cuando reciba un correo electrónico de alguien que no reconoce o que Outlook identifica como un nuevo remitente, examine el correo electrónico con sumo cuidado antes de continuar.
3. **Ortografía y mala gramática**: las empresas y organizaciones profesionales suelen tener un personal editorial para garantizar que los clientes obtengan contenido profesional de alta calidad. Si un mensaje de correo electrónico tiene errores ortográficos o gramaticales obvios, es posible que se trate de una estafa. Estos errores a veces son el resultado de una traducción incorrecta de otro idioma. A veces es deliberado, en un intento de sortear filtros que intentan bloquear estos ataques.
4. **Saludos genéricos**: una organización que trabaja con usted debe conocer su nombre y, hoy en día, es fácil personalizar un correo electrónico. Si el correo electrónico empieza con un mensaje genérico, como "Estimado señor o señora", es un signo de que puede que no sea realmente su banco o sitio de compras.

5. **Dominios de correo electrónico que no coinciden**: si el correo electrónico dice ser de una empresa acreditada, como Microsoft o su banco, pero el correo electrónico se envía desde otro dominio de correo electrónico como Gmail.com o microsoftsupport.ru probablemente sea una estafa. También esté atento a los errores ortográficos muy sutiles del nombre del dominio legítimo. Como micros0ft.com donde la segunda "o" se ha reemplazado por un 0 o rnicrosoft.com, donde la "m" se ha reemplazado por una "r" y una "n". Son trucos comunes de estafadores.
6. **Vínculos sospechosos o datos adjuntos inesperados**: si sospecha que un mensaje de correo electrónico es un fraude, no abra los vínculos o datos adjuntos que vea.