COMUNICADO N°016-2024-PCM/SGTD/CNSD		FECHA: 27 SETIEMBRE 2024
DIRIGIDO A:	**ENTIDADES PÚBLICAS** **Oficiales de Seguridad y Confianza Digital** **Jefes de las Oficinas de Tecnologías de la Información y Comunicaciones** **Equipos de Respuestas ante Incidentes de Seguridad Digital**	
ASUNTO:	Recomendaciones para evitar ser víctima del phishing	**TLP: WHITE**

1. ANTECEDENTES:

En el Perú, el vector de propagación más utilizado por los ciberdelincuentes para llegar hasta sus potenciales víctimas son las campañas de phishing. Este ciberataque consiste en adquirir fraudulentamente información personal y/o confidencial de la víctima, como contraseñas o detalles de la tarjeta de crédito y cuentas de redes sociales, para efectuar el engaño. Para ello, el estafador se hace pasar por una persona o empresa de confianza, utilizando una aparente comunicación oficial a través de un email falso, un sitio web clonado o una app no oficial.

Es ahí donde los delincuentes intentan convencerlo de que haga clic en esos enlaces o de revelar información confidencial (como datos bancarios). Una vez que se hace clic, puede ser enviado a un sitio web poco fiable que podría descargar virus en su computadora o robar sus contraseñas.

Algunas variantes de Phishing:

- Vishing: el término deriva de "voice" y "phishing" y se refiere al tipo de ciberdelito que combina una llamada telefónica fraudulenta con información previamente obtenida desde internet. Generalmente, se usa después de haber realizado phishing con la intención de que la víctima brinde su token digital o clave SMS para que el ciberdelincuente haga una transacción financiera.
- Smishing: se da por mensajes de texto o de WhatsApp. Aquí la víctima recibe un mensaje, donde el ciberdelincuente se hace pasar por el banco y alerta sobre una supuesta compra sospechosa con su tarjeta de crédito. Luego, le alienta a cancelar dicha compra llamando a un número de banca telefónica falso, en el cual le pedirán sus datos confidenciales.
- Carding: es una forma de estafa que tiene como objetivo conseguir los datos de la tarjeta de crédito de la víctima para que los ciberdelincuentes hagan compras online con la misma.
- Pharming: utiliza malware o software malicioso para redirigir a los usuarios desprevenidos hacia versiones falsificadas de sitios web, con el fin de que introduzcan sus datos personales.
- Keylogging: este tipo de spyware o software malicioso oculto se introduce en el ordenador o smartphone de la víctima para registrar en secreto todo lo que escribe y así obtener información de sus cuentas y otros datos personales.
- Sniffing: sucede cuando la víctima se conecta a una red Wi-Fi pública no protegida y no cifrada. Bajo esta modalidad, los hackers pueden robar los datos rastreando su tráfico de internet con herramientas especiales.

Según datos de ESET, en el Perú, de enero a mayo de 2024, se detectaron más de un millón de muestras únicas de phishing, utilizadas en múltiples ataques. Cabe mencionar que este millón de muestras se refiere a ejemplos de phishing enviados, no a la cantidad total de ataques. Cada tipo de phishing se utilizó en muchos ataques, por lo que el número real de ataques es muchísimo mayor.

Hoy en día, el Perú se ha vuelto mucho más vulnerable a los ataques de phishing, especialmente debido al retiro de los fondos de las AFP y CTS. Los ciberdelincuentes aprovechan esta situación, enviando mensajes de texto (SMS) que aparentan ser de entidades financieras.

"Felicidades, el depósito de tu AFP ha sido aprobado. Para retirar, ingresa AQUÍ", es un ejemplo de estos mensajes fraudulentos. El enlace suele redirigir a una página falsa que imita la de una entidad financiera legítima. Estas páginas están diseñadas para robar información personal y financiera de los usuarios desprevenidos.

2. RECOMENDACIONES:

- Desconfiar de los emails los cuales mencionan un pedido de actualización urgente de tus datos financieros y personales. Aunque el correo esté con una firma digital, no se puede asegurar que esta firma no haya sido burlada.
- No usar los links dentro de un correo, mensajes instantáneos, chat dentro de cualquier página web, si se puede creer que hay algo sospechoso en el mensaje. En cambio, se podría realizar una llamada a la compañía o ir a la página web tecleando directamente en el navegador la dirección web oficial.
- Rechazar o evitar rellenar cualquier formulario que se encuentren dentro de un email o correo en el cual pregunten sobre información personal bancaria. Esta información, como los números de la tarjeta de crédito o información de la cuenta, sólo se debe comunicar por una vía segura, la cual sería la página oficial y/o teléfono de estas empresas a las que se encuentra afiliadas.
- Asegurarse siempre que se está navegando en una página segura luego de haberte logueado con tus datos de tarjeta de crédito u otra información vulnerable vía web
- Verificar regularmente las cuentas bancarias, tarjeta de crédito, tarjeta de débito, y comunicarse con los que te brindan ese servicio para que puedas verificar que la transacción ese legitima. Si hay algo sospechoso o no reconoces la transacción debes contactarte con el banco al cual te encuentras afiliado.
- Aplicar parches y actualizar periódicamente el software y las aplicaciones a su última versión, así como realizar evaluaciones de vulnerabilidad periódicas.
- Considerar instalar una herramienta la cual te ayude con la protección de sitios web fraudulentos. Esta herramienta deberá defenderte y alertarte cuando detecte que estas visitando un sitio web fraudulento. Utilizar un software antimalware confiable en sus dispositivos y mantenerlos actualizados. Estos programas pueden detectar y eliminar ransomware y otro software malicioso antes de que puedan cifrar sus archivos.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Habilitar la autenticación de dos factores cuando esté disponible.
- Implementar el principio del privilegio mínimo para minimizar el impacto potencial ante cualquier intento de ataque.
- Capacitar a su equipo en las mejores prácticas de ciberseguridad y manténgalos informados sobre las últimas amenazas., trasladándoles las recomendaciones indicadas.
- Si ya ha hecho clic en un enlace (o ingresó sus datos en un sitio web), siga estos pasos:
  - Si está utilizando una computadora portátil o teléfono de trabajo, comuníquese con su departamento de TI y hágales saber.
  - Si ha sido engañado para proporcionar sus datos bancarios, comuníquese con su banco y hágales saber.
  - Si cree que su cuenta ya ha sido pirateada (es posible que haya recibido mensajes enviados desde su cuenta que no reconoce, o que haya sido bloqueado de su cuenta), abra su software antivirus (AV) si lo tiene y ejecute un análisis completo. Permita que su software antivirus limpie cualquier problema que encuentre.
  - Si ha proporcionado su contraseña, cambie las contraseñas en todas sus cuentas que usen la misma.
  - Si ha perdido dinero, informe a su banco e infórmelo como delito en su entidad regulatoria local, evitará que otros se conviertan en víctimas de delitos cibernéticos.

IMPORTANTE	Todo incidente de seguridad digital debe reportarse al Centro Nacional de Seguridad Digital (D.U. N° 007-2020), a través de cualquiera de los siguientes canales: ○ Correo electrónico incidentes@cnsd.gob.pe ○ Plataforma Facilita: https://facilita.gob.pe/t/1025 El equipo del Centro Nacional de Seguridad Digital estará alerta a las situaciones que puedan presentar en horarios 7x24x365.

Base normativa*: Decreto Legislativo N° 1412, Ley de Gobierno Digital y su reglamento aprobado mediante Decreto Supremo N° 029-2021-PCM. Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.*

CENTRO NACIONAL DE SEGURIDAD DIGITAL
Secretaría de Gobierno y Transformación Digital
PRESIDENCIA DEL CONSEJO DE MINISTROS