¿Que es PHISHING?

El phishing es una forma de fraude muy utilizada en internet para obtener información personal de los usuarios. Roba nuestros datos personales y bancarios a través de páginas web falsas de alguna institución oficial, la más utilizada es la de bancos o cualquier empresa o tienda que consideraríamos de total confianza.
Los peligros y riesgos que pueden causar a las personas estafadas pueden llegar a ser realmente serios, como robo de identidad, de dinero, o utilización de sus cuentas para actividades delictivas.

¿Cómo funcionan estos ataques?

Hasta ahora los hackers han utilizado los correos electrónicos para lanzar este tipo de ataques, pero con el uso masivo de redes sociales y smartphones con conexión a internet, las vías de ataque se están multiplicando.
Estos correos electrónicos o mensajes incluyen un enlace que lleva al usuario a un sitio web en teoría conocido, pero que es una copia del original donde se solicita información confidencial.
De esta manera, usuarios demasiado confiados y que no dispongan de una protección antivirus adecuada, podrían verse involucrados en este tipo de ataques que tienen como principal objetivo el robo de datos personales.

¿Cómo podemos evitar ser engañados?

Acá te dejamos algunos consejos para prevenirlos:

Aprendé a identificar claramente los correos electrónicos sospechosos de ser ‘PHISHING’

Existen algunos aspectos que inequívocamente, identifican este tipo de ataques a través de correo electrónico:
Utilizan nombres y adoptan la imagen de empresas reales
Llevan como remitente el nombre de la empresa o el de un empleado real de la empresa
Incluyen webs que visualmente son iguales a las de empresas reales
Como gancho utilizan regalos o la perdida de la propia cuenta existente

Verificá la fuente de información de tus correos entrantes

Tu banco nunca te pedirá que le envíes tus claves o datos personales por correo. Nunca respondas a este tipo de preguntas y si tienes una mínima duda, llama directamente a tu banco para aclararlo.

Nunca entres en la web de tu banco pulsando en links incluidos en correos electrónicos

No hagas clic en los hipervínculos o enlaces que te adjunten en el correo, ya que de forma oculta te podrían dirigir a una web fraudulenta. Teclea directamente la dirección web en tu PC o utiliza marcadores/favoritos si quieres ir más rápido.

Ingresá tus datos confidenciales únicamente en webs seguras

Las webs ‘seguras’ han de empezar por ‘https://’ y debe aparecer en tu navegador el icono de un pequeño candado cerrado.

Ante la mínima duda se prudente y no te arriesgues

La mejor forma de acertar siempre es rechazar de forma sistemática cualquier correo electrónico o comunicado que incida que facilites datos confidenciales. Eliminá este tipo de correos.

Protegé tus datos. Evitá el phishing.

SPD
SOFTWARE PRO DATA S.A.

Información confeccionada y
distribuida por Software Pro Data S.A.

Ayudando a hacer un uso seguro de nuestros recursos de Internet