Roldanillo,Valle Del Cauca -Mayo 2024-https://www.intep.edu.co/Es/

INGENIERÍA E INNOVACIÓN INTEP

2 paginas\2 secciones- @daniel garcia, @ santiagomejia863

PHISHING

¿Qué información posee sobre la suplantación de identidad o phishing?

El phishing,un ataque dedicado al robo de bienes y de datos además de engañar a sus vìctimas

Daniel alejandro Garcìa-Santiago Mejìa

El phishing es uno de los ataques más frecuentes de ciberdelincuentes a los bienes de las personas, además de ir acompañado de la suplantación de identidad, que le facilitan al ciberdelincuente engañar a sus víctimas, haciéndose pasar por grandes empresas como bancos,con los que la víctima tiene convenio, atrayendo a las personas a sus redes de robo hasta lograr sus cometidos.

KASPERSKY, una aplicación y página brindadora de información para acceder a una mejor seguridad de los datos, (Kaspersky, 2023) “logro rechazar 709 ataques a la seguridad de los datos, bloqueando sitios webs fraudulentos en pleno 2023, esta página nos informa que las cifras de ataques de suplantación de identidad en el 2023, crecieron un porciento abismal, más del “40% de ataques fueron registrados por aplicaciones de mensajería, plataformas de inteligencia artificial, servicios de redes sociales y bolsas de criptomonedas, fueron las vías más utilizadas para llevar a cabo las estafas por parte de los ciberdelincuentes”,

¿Protocolo para prevenir ataques de phishing?
Hay múltiples formas de evitar o prevenir ser una víctima más del PHISHING, y en su gran mayoría fáciles de aplicar, según (Pinedo (Lizarraga, 2019). Estas son algunas formas de prevenir este ataque:
DISTINGUE E IDENTIFICA CLARAMENTE LOS CORREOS ELECTRÓNICOS SOSPECHOSOS, YA QUE PUEDEN SER FRAUDULENTOS. hay aspectos que, inequívocamente, identifican este tipo de ataques a través de correo electrónico. •Se utiliza el nombre y optan por utilizar la imagen de una empresa,además de que se disfrazan como empleados de la empresa, utilizando uniformes o insignias oficiales de la misma, incluyendo una web fraudulenta, pero que tiene mucha apariencia con la pagina original.
VERIFICA QUE LA FUENTE DE INFORMACIÓN DEL CORREO ENTRANTE SEA VERDADERA •Tu banco no te puede pedir tus datos personales, es típico que pensemos que una empresa de esas soliciten nuestros datos, pero no es así, es el mismo engaño que siempre ocurre, no des tus datos personales a una supuesta empresa y menos por internet, para verificar que todo esté bien, llama directamente al banco y solicita información.
NO ENTRES A LA WEB DE TU BANCO PULSANDO EN LOS LINKS INCLUIDOS EN CORREOS ELECTRÓNICOS •No entres en los enlaces adjuntos ya que posiblemente puede que te dirijan a una web de dudosa procedencia.
REFUERZA LA SEGURIDAD DE TU ORDENADOR •Aquí entra en juego un buen antivirus además de una actualización constante de tu ordenador y de las páginas webs.
DILIGENCIA. TUS DATOS CONFIDENCIALES SOLO EN LAS WEBS QUE SON SEGURAS, QUE Tú RECONOZCAS•Para reconocer una página segura debe aparecer con ‘https://’ al igual que debe tener en tu navegador un icono de un candado pequeño y cerrado.
REVISA PERIÓDICAMENTE TUS CUENTAS•El revisar de vez en cuando tu cuenta te permite ver o mantener prevenido de alguna irregularidad, en las transacciones que hayas hecho en línea.
INFÓRMATE DE VEZ EN CUANDO SOBRE EL MALWARE Y SUS EVOLUCIONES.

https://canal.uned.es/video/5a

Malware es la abreviatura de “Malicious software”, término que engloba a todo tipo de programa o código informático cuyo objetivo es dañar un sistema o causarle un mal funcionamiento.

Roldanillo,Valle Del Cauca -Mayo 2024-https://www.intep.edu.co/Es/

INGENIERÍA E INNOVACIÓN INTEP

2 paginas\2 secciones- @daniel garcia, @ santiagomejia863

¿QUÈ OTROS ATAQUES EXISTENEN A LA SEGURIDAD DE LOS DATOS?

Pérdida de documentos personales, que pueden ser utilizados por terceras personas con fines comerciales.

El phishing es un ataque muy típico pero también está el phishing,que tiene mucha similitud, solo que este se da mayormente con correos electrónicos. (Mishra 2020), dice:

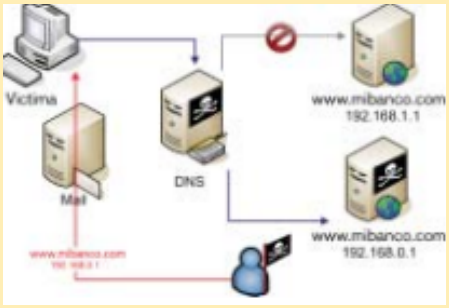
Que el“Smishing y el Phishing, es una forma combinada de mensajes,que envian los invasores con contenido malicioso a sus víctimas. Este contenido a veces incluye enlaces que redirigen al usuario a sitios web que contienen aplicaciones e interfaces de usuario falsas“(...)
(parr,1)

https://latam.kaspersky.com

El robo de datos o también robo de información, es la apropiación ilegal de información personal,con el objetivo de obtener también datos o informaciones financieras.

(“De acuerdo con (Barboza Coto y AlvaradoFonseca(s.f). hay Diferentescortafuegos que tienen el fin de evitar el robo de datos, pero estos con frecuencia tienen fallas de configuración y ahí es donde entra el delincuente llamado “Hacker” o “Cracker”. Estos últimos tipos de delincuente cibernético tienen distintas características; el “cracker” es más peligroso ya que este no tiene límites, usualmente no ocupa la información relevante del sistema, este individuo personaliza dicho sistema y lo hace a su disposición.”)

Los usuarios de internet cada vez más nos vemos afectados con los plagios, robo de identidad, de documentos, que se generan a través de correos, textos o links, los cuales ofrecen beneficios o solicitan información de nuestra cuenta de banco. Al respecto, Callegari, (s.f), un (analista en sistemas),” Se denomina pharming a la manipulación de la “resolución de nombres en Internet” producida por un código malicioso.” (pág. 1) (Pàrr,4)



El “Pharming”, el cual resulta muy difícil de detectar y/o identificar

Fuente: Daniel Garcia

Entrevista al ingeniero en sistemas Miguel Eusebio Posso.
Menciona Miguel (2024). El robo cibernético ocurre atrevés de un enlace, mensaje o llamada fraudulenta, el cual llama la atención del usuario, haciendo que este acceda a dicho link, mientras que el ciberdelincuente extrae toda la info del usuario.
En este momento se están haciendo campañas de prevención, por parte de los bancos, las cuales están educando al usuario para evitar que accedan a enlaces, abran mensajes o atiendan llamadas, donde se les exijan datos personales o bancarios.
Gracias a la evolución de la tecnología, ahora contamos con la IA (inteligencia artificial) capaz de analizar grandes cantidades de información, pudiendo detectar más.
rapidamente, anomalías que puedan indicar un robo o ataque cibernético.
A medida que la tecnología evoluciona, los ciberdelincuentes se hacen más expertos en el tema, por ende nuestros datos e información nunca estarán 100% seguros.

kaspersky. (2024). Aumentan un 40% los ataques de phishing en 2023.
https://www.kaspersky.es/about/press-releases/2024_aumentan-un-40-los-ataques-de-phishing-en-2023

(Pinedo Lizarraga, 2019)D. E. (2019). PROTOCOLO PARA LA PREVENCIÓN DE ATAQUES DE PHISHING. Revista Digital De Tecnologías Informáticas Y Sistemas, 3(1). Recuperado a partir de https://www.redtis.org/index.php/Redtis/article/view/34

Mishra, S. (2020). Smishing Detector: un modelo de seguridad para detectar smishing mediante análisis de contenido de SMS y análisis de comportamiento de URL.
https://www.ru.tic.unam.mx/handle/123456789/1684

https://www.sciencedirect.com/science/article/abs/pii/S0167739X19318758