CIBER SEGURIDAD

Manual Práctico para todos los niveles

La idea es crear un manual elemental para evitar en la medida de lo posible los cripto_robos (lo que hay que hacer y lo que no hay que hacer)

En primer lugar quiero aclarar que los nombres comerciales que aparezcan en este turorial son solamente para ayudar a los que no conocen o bien para ayudar a entender el concepto en las explicaciones y logicamente cada uno es libre de elegir la aplicacion que desee ya sea de codigo abierto o privativa. Dicho esto y ...

...Hasta donde yo llego y con la intención de ampliar y mejorar con la ayuda de la inteligencia colectiva del foro, me animo a desarrollar un plan de seguridad polivalente para no cometer los errores que ya han cometido otros. Contrastaré y analizaré los aportes de los foreros para mejorar el plan de seguridad. por lo tanto estamos hablando de un plan de "cripto ciber seguridad" Alfa

Por el momento este tutorial de seguridad estará pensado para el SO Windows o linux(respecto a linux hay que decir que aporta una capa de seguridad extra por multiples razones que no vamos a explicar aquí quien quiera encontrará información de sobra en la red) o ambos ya bien sea con arranque de tipo dual boot donde seleccionaremos el sistema que queremo arrancar en la máquina o tambien podriamos utilizarlos dentro de un espacio virtual tipo Virtual Box.

Algo que también deberemos tener en cuenta es cuantos dispositivos utilizaremos para trabajar con los criptoactivos, (logicamente cuantos menos dispositivos menos vulnerables seremos) supongo que lo lógico es un pc o laptop + 1 celular ya que el celular con aplicaciones de autenticación tipo google son muy importantes en la seguridad aportando lo que es más conocido como "doble autenticación" fijaros que cuando digo movil o celular me refiero como herramienta de seguridad complementaria pero no como dispositivo para operar.

Bien ! , Una vez resuelto que dispositivos vamos a utilizar que función le vamos a dar a cada uno y que sistema operativos utilizarán (no utilizar jamas SO con validadores Fraudulentos ya que no sabemos ni la procedencia ni la intención de quienes los han programado así cómo la medida en que puede afectar a las actualizaciones de seguridad del propio SO lo cual comprometería la seguridad de tu dispositivo y por ende de tus datos) aclarado esto vamos a pasar a hablar de las conexiones:

Lo primero de todo antes de empezar a instalar software, hardware, webs o nubes trazaremos un plan de seguridad en 2 niveles que llamaremos al primer nivel: seguridad perimetral y al segundo nivel: seguridad interna pudiendo dentro de cada

una de ellas instalar subcapas de protección adicionales tantas como consideremos necesarias

Me veo obligado a tener que decir la importancia que va a tener que este dispositivo sea de tipo dedicado y no lúdico hay que evitar a toda costa descargar archivos de tipo P2P (peliculas,juegos,software... Evitar el mundo warez es de vital importancia ya que estos lo utilizán para filtrar troyanos. no paginas de pornografia etc... etc...

1 - Seguridad Perimetral (antes de empezar a operar)

Conexión a la red internet: (nunca conectarse desde redes públicas ya que estaremos comprometiendo información tan valiosa como la introducción de claves) asegurarse si estais con el movil de utilizar vuestros datos moviles y no un wifi publico menos aun de una fuente desconocida o abierta. (Podriais ser victimas de un "Man in the midle") y si os conectais desde casa la conexión será desde vuestro wifi privado y vuestro equipo dispondra de un apoyo de seguridad tipo pack antivirus tan conocidos como bitdefender, nod32, kapersky ... Yo aquí si que no ultilizaria jamas un antivirus gratuito ... me parece algo importantísimo!

Utilizad la autenticación que nos ofrecen los dispositivos al iniciarlos, es decir poner la clave al inicio de sesión tanto en pc como en dispositivos móviles complementarlo si se quiere con un autenticador por huella digital en algunos moviles ya viene incorporado en pc deberiamos agregarle el hardware y software (esto da una importante protección en caso de estraviar el dispositivo o directamente ser urtado)

2 - seguridad Interna (una vez que empezamos a operar con nuestro dispositivo)

Quizas la pieza más importante de la columna vertebral cripto será vuestra cuenta de correo electrónico es muy recomendable utilizar un correo dedicado a nuestro proposito cripto y es muy recomendable utilizar un proveedor de correo electronico que nos aporte seguridad entre todos hay uno que yo consideraría por encima de los demas "Protonmail" tiene una versión gratuita y es un proveedor que se ha ganado la reputación entre los que buscan un extra de seguridad y cómo no puede ser de otra manera tengo que advetiros de lo extremadamente importante que es utilizar un password fuerte largo con números, letras y algún símbolo, Este password deberá ser sustituido periodicamente por razones de seguridad.

Donde puedo guardar los passwords?, Para no olvidarlos ni perderlos ni comprometerlos : Existen unas máquinas de rotulación

conocidas como DYMOS con las que podemos construir las palabra o frases de nuestros passwords o semillas con una garantía bastante elevada ante desastres (no contra fuego) de esta manera podremos tener seguridad de que no se va a correr la tinta o a desgastar etc... El lugar donde deben guardarse logicamente será de tipo offline ya bien debajo el fondo de un cajón o detras de un cuadro ... cada uno que elija el lugar secreto también es muy recomendable una caja fuerte ya que esta si que aportaría una protección ignífuga hasta cierta medida.

Las VPN no són recomendables en el caso de las echanges ya que estas utilizan nuestra IP y zona geografica como medida de seguridad y esto es muy importante que siga siendo así para otro tipo de operaciones quien lo considere nevesario que utilice La VPN que solo le aportará un grado superior de anonimato y nada más.

Cifrado de claves: Será de vital importancia el cifrado de los passwords que vamos a necesitar para interactuar en el mundo cripto (que no són pocas veces) aquí nombrare uno que me recomendaron desde la plataforma de echange KRAKEN y otro más

Wallet fria: Personalmente aun no dispongo de ningun dispositivo de hardware wallet y por esa razón no puedo aportar mi experiencia pero es obvio lo importante que puede llegar a ser no solo a efectos de ciber delincuencia si no también de sustracción o pérdida de dispositivos, accidentes ... etc. se que en el foro encontarreis hilos dedicados a muchos de los puntos aqui nombrados que podriamos utilizar como hashtags. Sobra decir que la wallet fria nos aporta un grado más de seguridad ya que el volumen importante de criptos que no usemos a diario podemos tenerlo guardado allí de manera muy segura y dejar en los echange y monederos solo las cantidades necesarias para manejarnos en lo rutinario

Si utilizamos billeteras en web3 acordarse antes de cerrar la sesion en el pc de bloquear las billeteras tipo metamask, phantom ... etc aunque he podido comprobar que se cierran de manera autómática por defecto seguramente en la configuración de cada monedero tipo Metamasl, Phantom etc. podemos ajustar esta opción igualmente sucede con las echanges hay que acordarse a cerrar sesión o configurar su temporización.

INGENIERÍA SOCIAL: ¿Por qué lo escribo en mayúsculas ? ... Si! este es el punto debil de los humanos y por donde llegan el 99% de los ciberdelitos aquí es donde debermos listar casos prácticos o sucesos para aprender de los errores ya cometidos para que no vuelvan a sucedernos.

Para evitar ser victimas de paginas clonadas donde podriamos estar ingresando nuestras credenciales sin darnos cuenta de que se trata de un phishing lo que hay que haces es localizar la pagina oficial, verificarla y enviar el enlace o ya bien en icono en el escritorio o en nuestro navegador en favoritos de manera ordenada para no cometer errores y de esta manera evitaremos poder caer en las webs fraudulentas que utilizan este tipo de tecnicas para el robo de credenciales.

Otra de las artimañas de ingeniería social se dan en foros o plataformas sociales como facebook,twitter... donde alguién puede hacerse pasar por un técnico del soporte o querer hacerse amigo nuestro con la intención de obtener información relevante.

Bien!, una vez leido hasta aquí sólo cabe decir que la clave, de la seguridad, reina en el sentido común!