Instituto Tecnológico de Reynosa

PRÁCTICA 3

Simulación de criptomonedas

Integrantes:

Pesina González Belinda Inés 24580023

Hernández Jasso Dulce Lizbeth 24580016

López Valenzuela Ana Paulina 24580277

Miranda Salinas Miguel Angel 24580021

Carrera: Ingeniería en Tecnologías de la información y Comunicaciones

Materia: Introducción a las TICS

Primer paso, debe ingresar a la página de Cryptospaniards simulador y crear una cuenta con correo electrónico y nombre de usuario, después se le pide la cantidad exacta que quiera comprar de criptomonedas, se ingresó la cantidad de $100,000. Luego del lado superior derecho hay un apartado llamado “Mercado” que contiene los tipos de moneda con su precio y porcentaje para comprar estas criptomonedas y en el mismo apartado dice buy lo cual se le da clic en esa opción de cuanto deseas comprar y dependiendo de la cantidad que deseas comprar es la cantidad de criptomonedas dependiendo del valor de cada moneda. Y se ha comprado alrededor de 5 monedas entre ellas: BTC, ETH, BNNB, DOGE, TRX, entre otras.

Después, se revisó una por una para ver cuál era buena para comprar y se compró primero BTC que tiene un precio de $66,166.79, y solo se compró la cantidad de 0.4611 que tuvo un valor de $30,511.79. Luego, ETH y se compró la cantidad de 5.00, de ahí, DOT la cantidad de 839.94.

Finalmente, al terminar de comprar las monedas en la parte de arriba en el apartado de la capital total que tienes y se va actualizando cada cierto tiempo, a lado de eso viene el historial si vas ganando o perdiendo de lo que se ha comprado, en este caso, iba bajando al principio, pero poco después de un rato empezó a subir y al final en línea recta. Por último, hay un apartado mas que es el portafolio de las monedas que has comprado con el valor, cantidad y precio.

Riesgos asociados con plataformas sin que no requieren verificación de identidad

1. Fraude y suplantación de identidad

- **Riesgo:** La falta de verificación facilita que personas malintencionadas utilicen identidades falsas o robadas para llevar a cabo actividades fraudulentas, como estafas, suplantación de identidad (phishing), y otros delitos cibernéticos.
- **Ejemplo:** Un estafador podría crear múltiples cuentas bajo identidades falsas para engañar a otras personas o realizar transacciones fraudulentas sin ser rastreado fácilmente.

2. Aumento de actividades ilegales

- **Riesgo:** Las plataformas sin verificación de identidad son más susceptibles a ser utilizadas para actividades ilegales, como la venta de productos ilícitos, la distribución de contenido ilegal, o el lavado de dinero.
- **Ejemplo:** En plataformas de comercio o criptomonedas sin controles de identidad, los delincuentes podrían hacer transacciones anónimas para ocultar actividades ilícitas.

3. Aumento de fraudes financieros

- **Riesgo:** En plataformas donde los usuarios pueden realizar transacciones sin una verificación adecuada, aumenta la probabilidad de fraude financiero, como el uso de tarjetas de crédito robadas o la realización de pagos fraudulentos.
- **Ejemplo:** En plataformas de pago sin verificación, un estafador podría realizar compras o transferencias de dinero a nombre de otra persona.

Aunque las plataformas sin verificación de identidad pueden ofrecer mayor privacidad o facilitar la accesibilidad para los usuarios, los riesgos asociados son significativos. La falta de medidas adecuadas de verificación de identidad puede generar un entorno propenso a fraudes, abuso, y actividades ilegales. Para mitigar estos riesgos, es crucial que las plataformas implementen medidas de seguridad adecuadas, como procesos de verificación de identidad, monitoreo constante y políticas claras de uso responsable.

Medidas de seguridad para proteger criptomonedas en plataformas

Con formato: Fuente: 18 pto, Negrita

1. Usar un monedero hardware (cold wallet)

- **Qué es:** Un monedero hardware es un dispositivo físico que almacena tus claves privadas de forma offline, lo que lo hace menos vulnerable a ataques en línea.
- **Por qué es importante:** Dado que los monederos hardware no están conectados a Internet, son mucho más seguros que los monederos online o en aplicaciones móviles.
- **Ejemplos:** Ledger Nano S, Ledger Nano X, Trezor Model T.

2. Activar autenticación en dos factores (2FA)

- **Qué es:** La autenticación en dos factores añade una capa extra de seguridad a tus cuentas de intercambio o billeteras en línea. Requiere tanto una contraseña como un código adicional generado por una aplicación (como Google Authenticator o Authy).

- **Por qué es importante:** Si tu contraseña es comprometida, un atacante aún necesitará el código de 2FA para acceder a tu cuenta.
- **Cómo hacerlo:** Activa 2FA en todos los intercambios y plataformas donde almacenes criptomonedas. Nunca uses 2FA basada en SMS, ya que es vulnerable a ataques de SIM swapping.

3. Usar contraseñas fuertes y únicas

- **Qué es:** Las contraseñas deben ser largas, complejas y únicas para cada cuenta que utilices.
- **Por qué es importante:** Si usas contraseñas fáciles de adivinar o las mismas en varios sitios, los atacantes pueden acceder fácilmente a tus cuentas si se filtra tu información.
- **Cómo hacerlo:** Utiliza un administrador de contraseñas para generar y almacenar contraseñas complejas y únicas. Evita usar contraseñas simples o comunes.

Tomar medidas de seguridad rigurosas para proteger tus criptomonedas es fundamental para evitar pérdidas y garantizar la seguridad de tus fondos. El uso de monederos hardware, la autenticación en dos factores y la precaución ante ataques de phishing son algunas de las mejores prácticas. Además, mantener tus dispositivos seguros y realizar copias de seguridad de tus claves y frases de recuperación son pasos esenciales para proteger tus activos digitales.