Ian Waweru

Zehra, Susan

Cybersecurity Fundamental

12/5/2022

Cryptocurrency

The increase in technology has grown over the years. Our society has benefited from this increase, and it continues to improve as the years go by. Technology has done a really good job of making our daily lives easier. For example, we can handle complicated data and other complicated tasks with the help of technological systems. Big organizations are now heavily dependent on the technology we have today. Due to the increase and improvement of technology every year it’s important to develop cybersecurity as well. Cybersecurity is very important because its purpose is to protect networks, devices, and data from cybercriminals. There are people in the world who are known as cybercriminals and their objective is to steal organizational data or corrupt systems used in an organization.

There have been all kinds of attacks have occurred over the years. For example, there have been phishing attacks, Denial-of-Service attacks, and SWL injection attacks. These attacks have occurred before and can still happen if not careful to this day. There hasn’t been a year where cybercrime would show signs of slowing down. It’s 2022 and cybercrime is still as relevant as it has always been. This year has had its fair share of cyber issues and I want to discuss a cyber-attack that has become a growing issue. Cryptocurrency has gained popularity over the years, in the year 2022 the request for crypto was at large. Some benefits come with crypto that made it grow in popularity. For example, I can get an oversized return. If I was to invest a penny, over time depending on the economy that penny can turn into thousands of dollars. Other benefits have attracted a lot of attention. All the attention is good however, it also has grasped the attention of cybercriminals. Cybercrime has stolen billions of dollars of cryptocurrency and it continues to become a problem. From the beginning of the year 2022 and into the summer of July it has been reported that almost 2 billion worth of cryptocurrency was stolen. That’s an increase from what was recorded in the previous year. The main target that bad actors want to exploit is the decentralized fiancé (Defi). Defi gets targeted because of its vulnerability. All systems have a potential vulnerability, it’s important for cybersecurity to locate the vulnerability before a hacker can exploit it. Hackers were able to locate and exploit the vulnerability of Defi programs. Hackers were able to attack its vulnerability because it used the program open-source codes. Open-source code is available to the general public, this allows a hacker to observe and learn the code and find the vulnerabilities. Cybercriminals have multiple methods they use to commit an attack. For instance, there is a new attack method that has been recently developed is the use of blockchain bridges. Blockchain bridges have been a success, its purpose is to swap tokens at a faster pace. For it to have success crypto enthusiasts must bypass a central exchange. Doing that left that system unprotected and acceptable to breeches. 1.4 billion dollars were lost due to breaches occurring on these cross-chain breaches. Another example of a crypto attack is private key theft. Some people rely on private keys to protect their bitcoin, however, this only put them more at risk for theft vulnerability. If a hacker can obtain those private keys, they can use them to steal bitcoin funds.

There are all kinds of protocols that have been created to help protect cryptocurrency users. Blockchain for example has emerged, it’s very efficient in protecting data. However, hackers have found new ways to even bypass its security mechanism. There are a couple of blockchain networks that have been exploited by hackers. For example, flaws in blockchain security have allowed hackers to obtain funds. A term for this flaw is called the exit scam. The exit scam is when a user’s fund mysteriously disappears and restricts them from recovering their payments. Another example of a vulnerability in the blockchain is emailing scams. Phishing attacks are becoming a trend in the crypto space. A cybercriminal’s objective is to study and gain information on a victim. Once they get their information, they can use their identity to customize their operation. Hackers are disrupting the vision that was had for cryptocurrency. The development of crypto has brought new benefits to our society. Its purpose is to change the future of global finance. It can change how we used to operate for example people can make transactions without the need for banks or the government. The development of crypto can make anyone who invests properly a lot of money in the long run. The need for cybersecurity increases as the popularity of crypto continues to grow. However, hackers have exploited the vulnerabilities in crypto and have made it a risk to trust. Businesses especially should be aware of the risks because they can affect the security of their business.

Our technology is only going to keep improving in our society. Cryptocurrency is an example of new technical tools that are to come in the coming. Cybersecurity will continue to battle these malicious activities and help protect systems and the people involved. Cryptocurrency has had its issues but over time these issues get solved and new protocols are set. It’s almost like a game of chess. A hacker will infect a system then a cybersecurity team will fend off the hacker with new protocols. Before it’s all set and done the hacker will find a new way to get into a system until it’s stopped by a cybersecurity team.

References:

White, Josh. “Common Ways Criminals Use to Steal Bitcoin.” *Sharecast*, 6 Dec. 2022, [www.sharecast.com/promoted/international-economic/common-ways-criminals-use-to-steal-bitcoin.html](http://www.sharecast.com/promoted/international-economic/common-ways-criminals-use-to-steal-bitcoin.html).

Sigalos, Ryan Browne, MacKenzie. “Hackers Have Stolen $1.4 Billion This Year Using Crypto Bridges. Here’s Why It’s Happening.” *CNBC*, 10 Aug. 2022, [www.cnbc.com/2022/08/10/hackers-have-stolen-1point4-billion-this-year-using-crypto-bridges.html](http://www.cnbc.com/2022/08/10/hackers-have-stolen-1point4-billion-this-year-using-crypto-bridges.html).

Nath, ojasvi. “Top Five Blockchain Attacks and DLT Vulnerabilities to Know in 2022 |.” *Top Five Blockchain Attacks & DLT Vulnerabilities to Know in 2022 | Spiceworks It Security*, 28 Mar. 2022, [www.spiceworks.com/it-security/vulnerability-management/articles/top-five-blockchain-attacks](http://www.spiceworks.com/it-security/vulnerability-management/articles/top-five-blockchain-attacks).

Lane, Aaron M. “Crypto Theft Is on the Rise. Here’s How the Crimes Are Committed, and How You Can Protect Yourself.” *The Conversation*, 3 Feb. 2022, theconversation.com/crypto-theft-is-on-the-rise-heres-how-the-crimes-are-committed-and-how-you-can-protect-yourself-176027.

Kaspersky, My. “What Is Cryptocurrency and How Does It Work?” *www.kaspersky.com*, 9 Feb. 2022, [www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency](http://www.kaspersky.com/resource-center/definitions/what-is-cryptocurrency).

May, Fulton. “How Cryptocurrency Impacts Cyber Security | Fulton May.” *Chicago’s IT Consulting & Cloud Services*, 13 Nov. 2019, /what-is-cryptocurrency-and-how-does-it-affect-cyber-security.