`What is Cryptocurrency?

Bitcoin and other types of cryptocurrencies have exploded onto the market in recent years, and based on virtual currency's popularity, it seems to be here to stay. Cryptocurrencies are digital or virtual currencies secured by cryptography, with many using decentralized networks based on blockchain technology – an open, distributed ledger that records transactions in code. Crypto is stored in a digital "wallet," which can be on a website, on a computer or an external hard drive. To put it simply, cryptocurrencies as systems that allow for secure payments online, which are denominated in terms of virtual "tokens."

Bitcoin, the first cryptocurrency that launched a little over a decade ago, was created by Satoshi Nakamoto, who described it as "an electronic payment system based on cryptographic proof instead of trust." Other common types of cryptocurrencies include Litecoin, Namecoin, Dogecoin, Ethereum, Cardano and others. In March 2021, there were reportedly over 18.6 million bitcoins in circulation, with a total market cap of around $927 billion.

Unlike the U.S. dollar, there is no physical coin or bill involved in cryptocurrency. It is a type of digital currency that only exists electronically, with no backing from a government and no central authority managing the value. One advantage of cryptocurrency is that it can be easily exchanged online, using a computer or phone, usually for quick payments to avoid transaction fees charged by traditional banks. However, due to the semi-anonymous nature of the transaction, users could be opening themselves up for a host of different types of scams or even illegal activities like money laundering.

Types of Cryptocurrency Scams that affect Cybersecurity

In early May 2021, a ransomware attack struck the Colonial Pipeline. A hacker group known as DarkSide forced the company to shut down over 5,000 miles of pipeline in the south-eastern United States until the hackers received a total of $5 million in bitcoin ransom payments. Luckily, U.S. law enforcement officials were able to recover $2.3 million of the ransom paid after identifying a virtual currency wallet the hackers used to collect the payment. However, in total, DarkSide reportedly has been paid $90 million in bitcoin ransom payments from 47 victims, with the average amount being $1.9 million.

The Federal Trade Commission (FTC) states that one of the biggest signs of a cyber scam is when a cybercriminal asks an individual or company to pay by cryptocurrency. Whenever there's a request to pay by gift card, wire transfer or cryptocurrency, it's a major red flag that you're about to fall victim to a cyber- attack. Once the scammer is paid in one of those ways, it becomes nearly impossible to recover the money. Cryptocurrency can be mysterious, complicated and confusing to many people, and as it continues to grow in popularity, so does the opportunity for crypto scams. The FTC reports that between October 2020 and May 2021, Americans lost over $80 million to cyberattacks on cryptocurrency.

Investment Scams

Investment scams, for example, lure individuals to websites with seemingly legitimate testimonials and credible-looking charts and wording that make it appear an investment is growing. However, the victim is asked to send more crypto when they attempt to withdraw their profits and soon find out they get nothing in return.

Giveaway Scams

Giveaway scams are also popular cyberattacks on cryptocurrency. The hackers pose as well-known investors or even celebrity figures who offer to help small investors. However, when the victim sends their crypto, instead of growing their own investment, the money goes right into the scammer's hands.

Initial Coin Offering (ICO) Fraud

Scammers also have found ways to hack into crypto wallets or use bitcoin-stealing malware to commit their attacks. What's known as ICO (initial coin offering) fraud is also a common type of crypto scam, as victims get lured into investing in the launch of a new cryptocurrency that turns out to be fake.

Scammers generally promise that you will make a profit, offering big payouts with guaranteed returns or even promise free money. They may make big claims without any explanations or details. It's important for business owners to understand where their investment is going and how it works, so always research both the company name and the type of cryptocurrency offered.

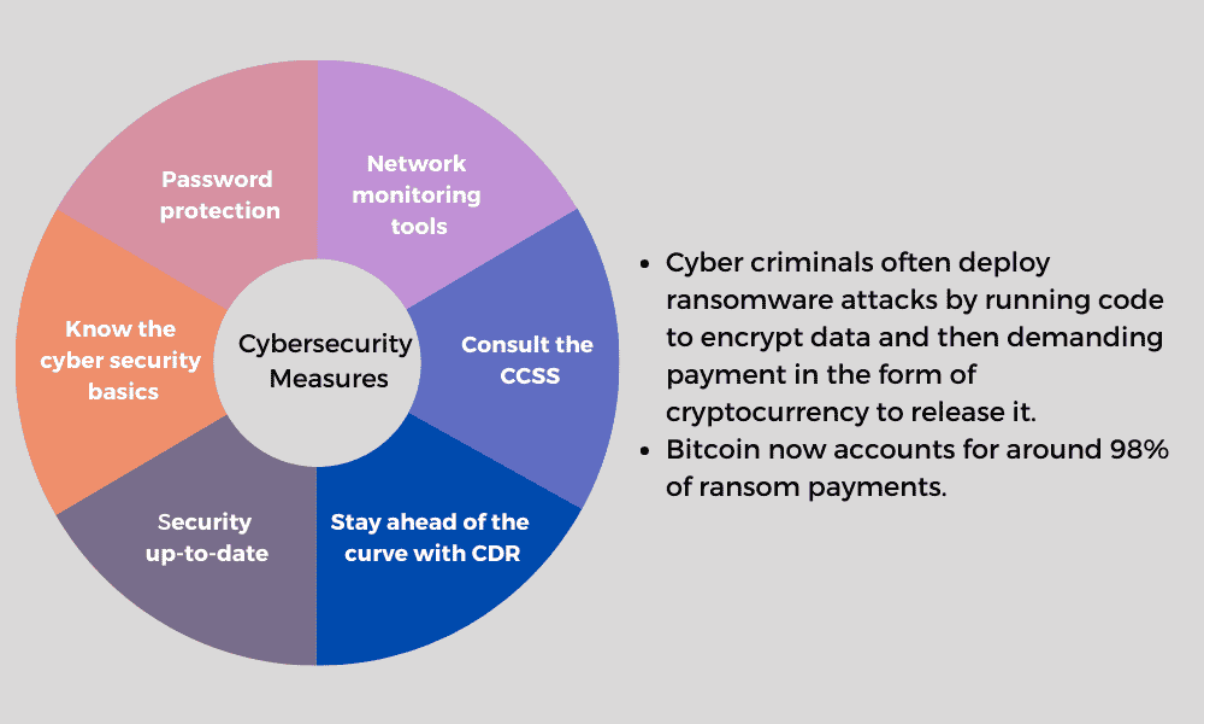
Cryptocurrency and Business's Cybersecurity

More and more public companies and major financial institutions have begun to recognize digital currencies, amplifying the need for crypto-related insurance policies. The Colonial Pipeline attack was one of the most disruptive cyberattacks in history, resulting in substantial expenses, including days of lost revenue and the $5 million ransom payment. Unlike other cybersecurity scams that target personal data, this attack had a major impact on the entire country's infrastructure and became a wake-up call to consumers everywhere.

There are pros and cons when it comes to businesses and cryptocurrency.

Cyber liability insurance is vital to protect a company from a wide range of cyberattacks. While policies specifically designed for crypto-related risks remain limited, cyber liability insurance helps cover ransomware payments, the costs associated with an investigation, data breach notifications and legal defence should there be third-party lawsuits related to the attack.

What are the measures businesses can take to protect themselves from cryptocurrency scams?



Businesses can take a few measures to protect themselves from cryptocurrency scams.

1. Educate yourself and your employees about cryptocurrency and how it works. It will help you spot red flags that indicate a scam.
2. Only deal with reputable exchanges and businesses. Do your research to make sure you're dealing with a legitimate company.
3. Keep your computer security up-to-date to protect yourself from mining malware and other attacks.
4. Be careful when accepting cryptocurrency as payment. Make sure you understand the risks involved before you agree to receive it.
5. If you use cryptocurrency to buy or sell goods and services, only deal with reputable companies. Be aware of the risks involved in doing this.