

Newsletter

Crypto-WHAT?

The popularity of cryptocurrency, a form of digital currency, is rising; Bitcoin, Litecoin, Monero, and Ripple are just a few types of the cryptocurrencies available. With a lack of basic understanding of cryptocurrency and the risks associated with it, individuals and organizations continue to fall victim to illicit cryptocurrency mining activity.



What is cryptocurrency?

Cryptocurrency is a digital currency used as a medium of exchange, similar to other currencies. However, unlike other currencies, cryptocurrency operates independently of a central bank and uses encryption techniques and blockchain technology to secure and verify transactions.

What is cryptomining?

Cryptocurrency mining, or cryptomining, is simply the way in which cryptocurrency is earned. Individuals mine cryptocurrency by using cryptomining software to solve complex mathematical problems involved in validating transactions. Each solved equation verifies a transaction and earns a reward paid out in the cryptocurrency. Solving cryptographic calculations to mine cryptocurrency requires a massive amount of processing power.

What is cryptojacking?

Cryptojacking occurs when malicious cyber actors exploit vulnerabilities—in webpages, software, and operating systems—to illicitly install cryptomining software on victim devices and systems. With the cryptomining software installed, the malicious cyber actors effectively hijack the processing power of the victim devices and systems to earn cryptocurrency.

What types of systems and devices are at risk for cryptojacking?

Any internet-connected device with a CPU is susceptible to cryptojacking, including: Computer systems and network devices, mobile devices; and any Internet of Things devices.

How do you defend against cryptojacking?

The following cybersecurity best practices can help you protect your internet-connected systems and devices against cryptojacking:

- Use and maintain antivirus software.
- Keep software and operating systems up-to-date.
- Use strong passwords.
- Change default usernames and passwords.
- Check system privilege policies.
- Apply application whitelisting.
- Be wary of downloading files from websites.
- Recognize normal CPU activity and monitor for abnormal activity.
- Disable unnecessary services.
- Uninstall unused software.
- Validate input.
- Install a firewall.
- Create and monitor blacklists.

On the Lighter Side of Things

What do you get when you cross an elephant with a computer?

A lot of memory.

Why did the computer sneeze?

It had a virus.

What did the spider do inside the library computer?

It made a web page.

Why did the CPU go broke?

A reboot cleared out all of its cache. Now it has insufficient resources.

A Quote to Live By

NO! WE DON'T
HAVE WIFI



TALK TO EACH OTHER!

Through Service We Grow

Total is pleased to announce the addition of two new Service Team members: Chris, Helpdesk Technician - Level 2 and Justin, Helpdesk Technician.

Chris

Chris joins Total with a background in Information Technology, namely in network security, and has experience working at the helpdesk for Farmingdale State College SUNY. Over the years, he has learned to effectively communicate with clients and is extremely tech saavy when it comes to troubleshooting issues for computers and other devices.



Justin

With a passion for technology, along with his coding knowledge and previous work experience at Microsoft, Justin joins the team with an eagerness to contribute his fresh perspectives on IT solutions to our growing company.



Total is

CELEBRATING
30 years

in Business

SunriseWALKS 2018

What an amazing day at the SunriseWALKS Long Island fundraiser held on Sunday June 10. Total was able to raise \$15,768 for this charity to send children with cancer to day camp, free of charge. To date, the event raised \$934,801 but the donations keep coming in!



HEADQUARTERS: 1895 Walt Whitman Road • Melville, NY 11747 USA
631-777-7477 • 888-777-8093

www.total.us.com

Page 2