

MONDAY | FEBRUARY 19, 2018

**B4**

# Public cautioned to be careful of online cryptocurrency schemes

By IRIS GONZALES

Trend Micro Inc., a global leader in IT security, cautioned the public to be careful of online schemes that are hitching a ride on the hype around cryptocurrencies.

Trend Micro director for technology marketing Myla Pilao said cybercriminals are taking advantage of investor interest in cryptocurrencies or the so-called digital money.

"The hype around cryptocurrencies as an investment has emerged as another opportunity for cybercriminals to victimize people looking to make a fast buck," Pilao said.

She said that while digital currencies have become a hot investment and a valuable innovation in online commerce, the innovation has become a new target for cybercriminals.

"The technology behind cryptocurrencies is actually

revolutionary from a cyber-security standpoint because it allows digital information to be distributed without being altered," Pilao said.

According to Trend Micro, cryptocurrency is a medium of exchange that uses cryptography to secure transactions and control the production of additional units.

Some samples of digital currencies are Bitcoin, Ethereum,

Ripple, Litecoin, and Monero.

Cryptocurrencies are built on blockchain technology, a secure ledger of transactions processed and validated by a distributed network of computers or specialized hardware.

This operation is run by so-called miners who receive cryptocurrencies from vendors or merchants in return.

This so-called blockchain technology was invented to prevent double-spending in the system. It is the first type of

currency that is decentralized.

This means that control is taken away from central banks or government to inflate or deflate the value by manipulating the supply.

In recent years, the value of cryptocurrencies has surged, making digital currencies a major target of online hackers.

Just recently, attackers capitalized on the hype to market a dummy cryptocurrency called Sprite coin online, according to Trend Micro.

However, some users were duped into investing in the initial coin offering by downloading a wallet application that turned out to be a ransomware. Criminals successfully went after the victims' files and demanded money in exchange.

"The security landscape is constantly evolving, as cybercriminals adapt to innovations and take advantage of the loopholes or vulnerabilities,"

Pilao said.

She said enterprises and consumers must reevaluate their approach to security and remain a step ahead.

Users must take caution against well-known schemes such as socially engineered links, attachments or files from suspicious websites, dubious third-party software/applications, and unsolicited emails, according to Trend Micro.

In cases of illegal mining, updating devices helps deter the ploy of cybercriminals. Securing the devices with passwords also makes them less prone to unauthorized access. In home networks, firewall of routers should be enabled.

"There is no quick all-in-one solution to cyberattacks, but we can always start with the best security practices to make our world safe for enterprises and consumers to exchange digital information," Pilao also said.

\* money