FBI warns of increased use of cryptocurrency ATMs, QR codes for fraud

By
Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)

November 5, 2021 09:55 AM **0**

The Federal Bureau of Investigation (FBI) warns that victims of various fraud schemes are increasingly asked by criminals to use cryptocurrency ATMs and Quick Response (QR) codes, making it harder to recover their financial losses.

The warning was published as a public service announcement on the Bureau's Internet Crime Complaint Center (IC3) on Thursday.

"The FBI has seen an increase in scammers directing victims to use physical cryptocurrency ATMs and digital QR codes to complete payment transactions," the federal law enforcement agency said.

This tactic is used by criminals behind various fraudulent schemes, including online impersonation where the scammer claims to be a government, law enforcement, a legal office, or utility company representative.

Fraudsters will also use it in romance schemes where they first establish an online relationship with their victims before asking for money or in other common scams and frauds (https://www.usa.gov/common-scams-frauds).

The scammers will use the same general steps to make sure law enforcement loses track of the fraudulent payments:

- they provide a QR code associated with the scammer's cryptocurrency wallet for the victim to use during the transaction
- direct the victims to a physical cryptocurrency ATM to insert their money, purchase cryptocurrency, and use the provided QR code to auto-populate the recipient address.
- keep constant online communication with the victim and provide step-by-step instructions until the payment is completed.

Cryptocurrency makes it harder to avoid financial loss

This way the criminals make sure the targets will deliver on their promises to pay various sums of money as a favor or in exchange for non-existent fines, depending on the fraud scheme they fall victims to, and they can get away with all the money.

"Cryptocurrency's decentralized nature creates challenges that makes it difficult to recover. Once a victim makes the payment, the recipient instantly owns the cryptocurrency, and often immediately transfers the funds into an account overseas," the FBI added (https://www.ic3.gov/Media/Y2021/PSA211104).

"This differs from traditional bank transfers or wires where a payment transaction can remain pending for one to two days before settlement. It can also make law enforcement's recovery of the funds difficult and can leave many victims with a financial loss."

The FBI urges all those who believe they've been the victim of a cryptocurrency ATM or QR code scam to report the fraud to their local FBI field office to get help from specially trained Victim Specialists (https://www.fbi.gov/resources/victim-services).

The federal agency also encourages victims to report any fraudulent or suspicious activities they observe to the FBI IC3 at www.ic3.gov (https://www.ic3.gov/).

The FBI shared the following tips to help those targeted in such scams protect themselves:

- *Do not send payment to someone you have only spoken to online, even if you believe you have established a relationship with the individual.*
- *Do not follow instructions from someone you have never met to scan a QR code and send payment via a physical cryptocurrency ATM.*
- *Do not respond to a caller, who claims to be a representative of a company, where you are an account holder, and who requests personal information or demands cryptocurrency. Contact the number listed on your card or the entity directly for verification.*
- *Do not respond to a caller from an unknown telephone number, who identifies as a person you know and requests cryptocurrency.*

- *Practice caution when an entity states they can only accept cryptocurrency and identifies as the government, law enforcement, a legal office, or a utility company. These entities will likely not instruct you to wire funds, send checks, send money overseas, or make deposits into unknown individuals' accounts.*
- *Avoid cryptocurrency ATMs advertising anonymity and only requiring a phone number or e-mail. These cryptocurrency ATMs may be non-compliant with US federal regulations and may facilitate money laundering. Instructions to use cryptocurrency ATMs with these specific characteristics are a significant indicator of fraud.*
- *If you are using a cryptocurrency ATM and the ATM operator calls you to explain that your transactions are consistent with fraud and advises you to stop sending money, you should stop or cancel the transaction.*

Related Articles:

FBI: Ransomware gangs hit several tribal-owned casinos in the last year (https://www.bleepingcomputer.com/news/security/fbi-ransomware-gangs-hit-several-tribal-owned-casinos-in-the-last-year/)

FBI: Ransomware targets companies during mergers and acquisitions (https://www.bleepingcomputer.com/news/security/fbi-ransomware-targets-companies-during-mergers-and-acquisitions/)

FBI: Ranzy Locker ransomware hit at least 30 US companies this year (https://www.bleepingcomputer.com/news/security/fbi-ranzy-locker-ransomware-hit-at-least-30-us-companies-this-year/)

FBI warns of fake govt sites used to steal financial, personal data (https://www.bleepingcomputer.com/news/security/fbi-warns-of-fake-govt-sites-used-to-steal-financial-personal-data/)

US links $5.2 billion worth of Bitcoin transactions to ransomware (https://www.bleepingcomputer.com/news/security/us-links-52-billion-worth-of-bitcoin-transactions-to-ransomware/)