DigiKnow
CYBER SECURITY DEPENDS ON YOU

CRYPTO CURRENCY AND CRIMES

July 2024| Issue 2024:7

IT HAPPENS IN DELAWARE TOO

Crypto ATM and QR Code Scams: In 2022 the Delaware State Police issued a warning about an increase in scams involving cryptocurrency (or “crypto”) ATM machines and quick response (QR) codes. In these schemes, victims are directed to local crypto ATMs or stores that authorize QR crypto payments. Criminals often impersonate government agencies (such as the DEA, ATF, or local police) or use romance scams to manipulate victims. Once funds are sent via crypto transfers, recovery becomes extremely challenging due to the instantaneous nature of these transactions.

DECIPHERING CRYPTO SCAMS

According to the Better Business Bureau these are the most common cryptocurrency scams:

Government Impersonators: Contact by phone, email or text claiming that you owe taxes or fines.

Online Dating Scams: A new online love interest asks for money to help with an "emergency" that you can resolve by sending cryptocurrency.

Job Scams: Requesting payment for job-related expenses.

Investment Scams: Promising guaranteed returns with little to no risk.

Blackmail/Sextortion Threats: Sextortion is when someone online poses as a young person, convinces a real teenager to send them explicit photos and then once they have the photos, the scammer blackmails the young person for money. The threats have become so intense that

“Pig Butchering” Scam: Recently, the Delaware Department of Justice froze funds in accounts containing fraudulently obtained cryptocurrency. This action was part of a scam known as “pig butchering.” Scammers groom individuals over time, encouraging them to invest in crypto holdings. However, victims ultimately end up losing their investments to these deceptive schemes.

Protecting Investors: A distressing incident involving a senior citizen losing $275,000 to a cryptocurrency scam prompted the Delaware Department of Justice to take action against crypto fraud. Authorities are actively combatting fraudulent activities to safeguard investors from further harm.

Remember to stay vigilant and report any suspicious crypto-related activities to the appropriate authorities. If you encounter such scams, you can report them to the FBI via their website at www.ic3.gov.

Solomon Adote

Chief Security Officer

the FBI says sextortion has led to at least 20 suicides nationwide.

Scammers increasingly demand payments in cryptocurrency. Here’s why:

Lack of Legal Protections: Unlike credit cards, cryptocurrency payments don’t offer legal safeguards.

Irreversible Payments: Once you send money via Bitcoin or other cryptocurrency, it is almost impossible to get it back.

Public Confusion: Many people still don’t fully understand how cryptocurrency works, making them susceptible to scams.

TIPS TO AVOID FALLING FOR CRYPTO SCAMS

Don't Send Cryptocurrency. Only scammers demand crypto. Legitimate businesses and government agencies never ask for cryptocurrency payments (unless you are buying cryptocurrency).

Avoid Job-Related Fees: Don’t ever pay any fees to secure a job.

Be Cautious with Online Romances: If someone you meet online asks for money, it’s likely a scam.

No Guarantees in Investments: Be skeptical of anyone guaranteeing profits or big returns, especially with cryptocurrencies. It is a very volatile investment vehicle.

Don't Transfer Money on Demand: Your money is safe where it is. Don’t move it based on a call or urgent demand.

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Technology & Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links or want to print a PDF copy, go to:https://digiknow.dti.delaware.gov/news/index.shtml?dc=newsletters

Department of Technology and Information

Contact us at **esecurity@delaware.gov**