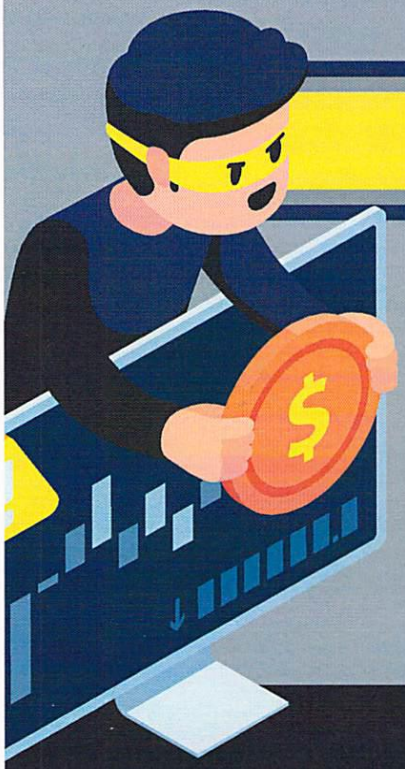


CRYPTO

ABA FOUNDATION

INVESTMENT SCAMS

WHAT YOU SHOULD KNOW

Crypto* investment scams, commonly referred to as "pig butchering" by scammers, cost consumers billions of dollars. Criminals befriend people to entice them to make crypto investments through phony apps and websites. The investments may start out slowly with small sums of money, but it's a scam aimed at stealing tens of thousands to millions of dollars.

*Crypto is also referred to as cryptocurrency by users

HOW DO CRIMINALS TARGET PEOPLE & HOW DOES THE CON START

HOW DOES THE CON START?

Criminals often pose as people interested in:

- Friendship,
- Romantic relationships, or
- Business investments.

Using fake profiles, they take time and build connections with their targets. They claim to be, or to know, experts who can help investors make money. To mask their identities, they:

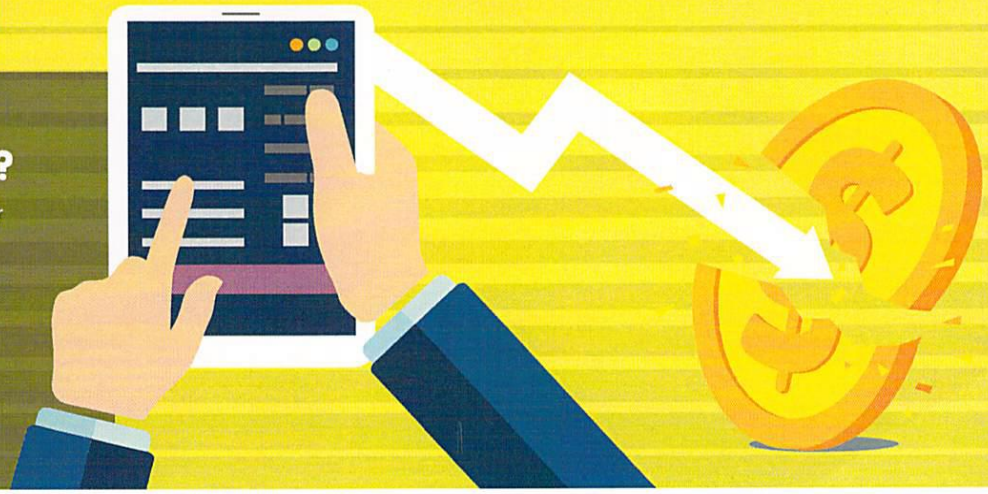
- Use fake phone numbers (spoofing)
- Rely on deepfake videos, voices or images
- Employ artificial intelligence

They target people through texts, dating sites, social media channels, professional networking platforms and/or other apps. After establishing trust with their victims, criminals move conversations to encrypted messaging apps and introduce crypto.

They coach victims into investing using fake platforms. Websites might look legitimate, but it's all phony and controlled by criminals. Once people begin "investing," criminals manipulate the sites/apps to show fake profitable returns. Victims might even be allowed to make initial withdrawals, but it's a ploy to encourage further investments.

HOW DOES IT END?

When victims try to withdraw larger sums of money, they are told they need to pay a fee or taxes. But there's no getting the money back, even if they pay the supposed fees or taxes. In the end, victims lose everything they invested.



PROTECT YOURSELF

- Research before you invest in anything.
- Recognize that pressure to "act fast" might be a sign of a scam.
- Do not send money to anyone you meet online or via apps, and don't make investments based on their advice.
- Do not download or use any unfamiliar apps.
- Do not pay for services that claim they can recover lost funds.
- Do not trust anyone who offers a "sure bet." All investments involve risk.
- Recognize that even video chats and online trading platforms which appear real can be fake.

WARNING SIGNS

- Unexpected contact by an unknown person.
- Requests to limit contact with financial institutions or advisors.
- New online friends sharing "can't-miss" investment opportunities.
- Sense of urgency to invest more money or pay fees.
- Misspelled web links.

IF YOU HAVE BEEN VICTIMIZED

Stop sending money to the criminals.

Contact your bank.

Keep records and communications relating to the scam.

File a report with the FBI Internet Crime Complaint Center at IC3.gov.

ABA Foundation is proud to work with:

Commodity Futures Trading Commission

Department of Justice Federal Bureau of Investigation

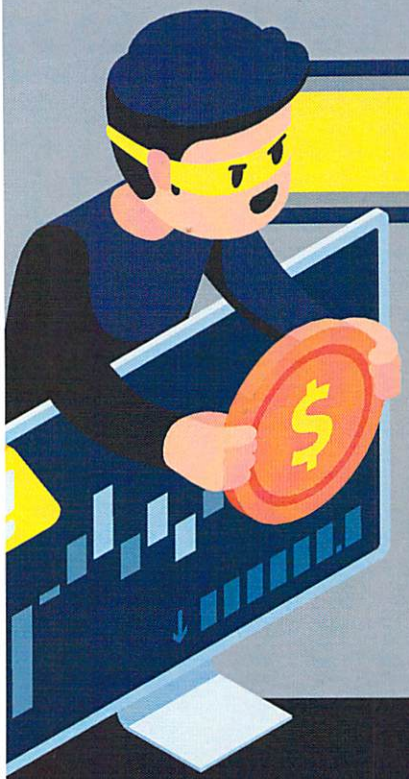
U.S. Treasury Financial Crimes Enforcement Network

FINRA

Homeland Security Investigations

IRS-CI

Investor.gov



CRYPTO

ABA FOUNDATION

INVESTMENT SCAMS

WHAT YOU SHOULD KNOW

Crypto* investment scams, commonly referred to as "pig butchering" by scammers, cost consumers billions of dollars. Criminals befriend people to entice them to make crypto investments through phony apps and websites. The investments may start out slowly with small sums of money, but it's a scam aimed at stealing tens of thousands to millions of dollars.

*Crypto is also referred to as cryptocurrency by users

HOW DO CRIMINALS TARGET PEOPLE & HOW DOES THE CON START

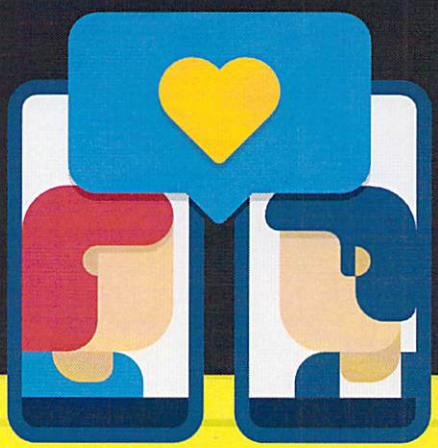
HOW DOES THE CON START?

Criminals often pose as people interested in:

- Friendship,
- Romantic relationships, or
- Business investments.

Using fake profiles, they take time and build connections with their targets. They claim to be, or to know, experts who can help investors make money. To mask their identities, they:

- Use fake phone numbers (spoofing)
- Rely on deepfake videos, voices or images
- Employ artificial intelligence



They target people through texts, dating sites, social media channels, professional networking platforms and/or other apps. After establishing trust with their victims, criminals move conversations to encrypted messaging apps and introduce crypto.

They coach victims into investing using fake platforms. Websites might look legitimate, but it's all phony and controlled by criminals. Once people begin "investing," criminals manipulate the sites/apps to show fake profitable returns. Victims might even be allowed to make initial withdrawals, but it's a ploy to encourage further investments.

HOW DOES IT END?

When victims try to withdraw larger sums of money, they are told they need to pay a fee or taxes. But there's no getting the money back, even if they pay the supposed fees or taxes. In the end, victims lose everything they invested.