What does pig butchering have to do with an annual FBI warning about online scams during the holidays in New Mexico?

The porcine-dubbed fraud is one of several the Albuquerque FBI Division wants to inform the public about as more people hit the web looking for deals and romance.

“Scams take many forms, and criminals every year try to think up new ways to steal your money,” Special Agent in Charge Raul Bujanda of the Albuquerque FBI Division said. “But one thing stays the same: If a deal looks too good to be true, it probably is. You can protect yourself from most scams by being suspicious of unsolicited emails and making sure you secure your banking and credit accounts with strong passwords.”

More than 2,600 New Mexico victims of internet scams reported losing almost $13 million in 2021, according to the FBI’s Internet Crime Complaint Center.

More than a quarter of that loss—$3.4 million—was reported in the last two months of the year.

The FBI is calling attention to a growing investment scam known as “pig butchering,” a fraud that is heavily scripted and contact intensive.

The scammer makes contact with a victim — usually on dating and social media apps.

After building trust and rapport, the scammer will convince the victim to make investments in cryptocurrency to take advantage of the potential for high yield returns. To facilitate the investment and demonstrate the returns on investment, victims are directed to websites that appear authentic but are actually controlled by the scammer.

After the victim has made several cryptocurrency investments through these fake sites, which purport significant returns, requests by victims to withdraw or cash-out their investments are denied for one reason or another. The scammer vanishes, cutting off contact with the victim, and taking the invested sums with them.

New Mexico law enforcement has noticed an increase in another scheme that involves perpetrators informing victims—who are usually elderly—that their bank or other accounts have been compromised and “unusual transactions” are occurring.

The perpetrators will tell the victim to move all their assets to a safer “U.S. Government-protected” account and give them a link to use to transfer the funds.

In some instances, the scheme uses fake law enforcement websites that try to prove that the perpetrator is legitimate.

Other popular scams

- **Sweepstakes scams:** Victims, who are usually elderly, are notified they won a sweepstakes, but first they need to send money in order to cover taxes and other processing fees.

- **Phony Amazon scams:** Perpetrators pretending to be from Amazon notify victims that their credit card on file is no longer working and they need to supply another. Or scammers will ask victims about a “suspicious purchase” that is being investigated by the FBI or other law enforcement. The victim is told they need to pay a certain amount of money to restore their account.
- **Online shopping scams:** Criminals offer too-good-to-be-true deals via phishing emails or advertisements. Such schemes may offer brand-name merchandise at extremely low prices or offer gift cards as an incentive.

Tips to avoid being victimized

- Do your homework on the retailer/website/person to ensure legitimacy.
- Conduct a business inquiry of the online retailer on the Better Business Bureau's website.

- Be wary of online retailers offering goods at significantly discounted prices.
- Check each website's URL to make sure it's legitimate and secure. A site you're buying from should have "https" in the web address. If it doesn't, don't enter your information on that site.
- Beware of purchases or services that require payment with a gift card.
- Beware of providing credit card information when requested through unsolicited emails.
- Do not click on links contained within an unsolicited email or respond to them.
- Check credit card statements routinely.
- Verify requests for personal information from any business or financial institution by contacting them using the main contact information on their official website.
- Secure credit card accounts, even rewards accounts, with strong passphrases. Change passwords and check accounts routinely.

What to do if you are a victim

If you are a victim of an online scam, the FBI recommends taking the following actions:

- Contact your financial institution immediately upon discovering any fraudulent or suspicious activity and direct them to stop or reverse the transactions.
- Ask your financial institution to contact the corresponding financial institution where the fraudulent or suspicious transfer was sent.
- Report the activity to the Internet Crime Complaint Center at IC3.gov, regardless of dollar loss. Provide all relevant information in the complaint.


DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY