OUCH! February 2025


# Sweet Talk and Empty Wallet: Romance Fueled Investment Scams

## A Story to Remember: Lisa's Experience

Lisa, a friendly and successful management professional, had a full life with a busy job. But as her work became overwhelming, she felt increasingly isolated and took to social media to connect with new people. That's when she met "Ryan" online, a man who quickly became a trusted friend and companion, though only virtually as he lived on the other side of the world. He seemed caring, sharing the same interests in travel, cooking, and eventually, investing.

Over several months as their relationship grew, Ryan suggested she invest in a crypto platform he had invested in and was growing fast. It seemed legitimate to Lisa and she started at first by investing a small amount. As she saw her investment grow and as Ryan encouraged her, she invested even more money over the following months. After six months into the relationship she at last tried to withdraw her money, however the platform "froze" her account and Ryan disappeared. Lisa discovered she lost over $175,000 to a romance and investment scam known as "Pig Butchering." The financial loss was devastating but the emotional betrayal hurt even more.

## What is Pig Butchering?

"Pig Butchering" is an elaborate scam that combines both romance and investment scams. It follows a few predictable steps, though the specifics can vary:

1. **Initial Contact**: The scammer reaches out, often through messaging apps or social media with casual messages, complimenting the victim or showing genuine interest in their life.
2. **Building a Relationship**: Over time, the scammer builds trust. They share personal stories, engage in regular conversations, and often build a romantic relationship to strengthen the bond.
3. **Introducing Investment Opportunities**: Once trust is established, the scammer mentions a "safe and lucrative" investment, often in crypto. They might claim to have insider knowledge or success with this investment, often showing fake investment results with incredible financial returns.
4. **Encouraging Small Investments**: The scammer encourages the victim to try a small investment. Initially, the victim sees what are actually fake "profits" or returns, which the scammer uses to build credibility. The scammer may even allow small withdrawals early in the relationship in order to add a facade of legitimacy.
5. **Increasing the Stakes**: As the victim sees "gains," the scammer urges them to invest more, with a sense of urgency – "Act now, or you'll miss out!"
6. **The Cut-Off**: When the scammer thinks they've taken the victim for all the money they can, they "freeze" the account or simply disappear. The platform becomes inaccessible, leaving the victim with nothing.

## Top Red Flags to Detect Pig Butchering Scams?

1. **Too Good to Be True**: Be wary of anyone promising guaranteed returns or claiming no risk. Legitimate investments always carry some risk, and rapid, consistent gains are often a warning sign.
2. **Unexpected Contact**: Be cautious of strangers initiating contact without a clear reason. Ever received a random "Hi" text message from a total stranger and wonder what that was about? It's the beginning of a scam. Do not respond in any way and consider blocking the sender.
3. **Relationship Becomes Financial Quickly**: If someone you've recently met online starts discussing investments or money matters, consider it a red flag. Scammers blend relationships with finances to manipulate trust.
4. **Pressure to Invest Quickly**: Scammers will often create a sense of urgency to get victims to invest large amounts quickly. They may claim that the "window" for this opportunity is closing or that it's a "limited-time" deal.
5. **Fake Investment Platforms**: Many scammers use fake but legitimate-looking investment websites or apps that display fabricated numbers. Be cautious of any platform that isn't widely recognized or recommended by trusted financial advisors.
6. **Difficulty Withdrawing Funds**: The final red flag is when you attempt to withdraw funds and face delays, excuses or additional costs. Any legitimate investment should allow you to access your funds without obstruction.

## How to Protect Yourself

The scammers behind these schemes are skilled manipulators. You are your best defense.

- **Be Wary**: When strangers initiate a connection to you, be very suspicious. In addition, the greater the financial deal, and the greater the pressure to invest, the more likely it is a scam.
- **Research Platforms Thoroughly**: Stick to well-known investment platforms, and avoid any platform with unclear ownership or lack of regulatory information.
- **Guard Your Personal Information**: Don't share too much about your finances or personal life online, especially with people you've never met in person.

## Guest Editor

Karen Nemani is the AWS Canadian Professional Services Commercial Security Leader and President of the WiCyS Ontario Affiliate. She is passionate about shifting cybersecurity culture to build an inclusive workforce where diverse mindsets, skillsets, and perspectives thrive. https://www.linkedin.com/in/karenbnemani/

## Resources

**Emotional Triggers: How Scammers Trick You:** https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
**Don't Let The Cybercriminals Swipe Your Savings: Lock Down Your Financial Accounts:** https://www.sans.org/newsletters/ouch/dont-let-cybercriminals-swipe-your-savings-lock-down-your-financial-accounts/
**Guard Your Heart (and Wallet) Against Romance Scams:** https://www.sans.org/newsletters/ouch/guard-your-heart-wallet-against-romance-scams/