

How scammers use psychology to create some of the most convincing internet cons—and what to watch out for

June 22 2023, by Stacey Wood and Yaniv Hanoch



Credit: AI-generated image ([disclaimer](#))

[Online fraud is today's most common crime](#). Victims are often told they are foolish for falling for it, but fraudsters use psychological mechanisms to infiltrate the defenses of their targets, regardless of how intelligent they are.

So it's important to keep up with the latest scams and understand how they work.

Recently, consumer protection magazine Which? [identified some of the most convincing scams of 2023](#). These scams all have one thing in common—they insidiously take advantage of people's cognitive biases and psychological blind spots.

They included "pig butchering" a way of fattening up [victims](#) with affection, the missing person [scam](#) which involves posting fake content on social media pages, the traditional PayPal scam, and a new scam called the "fake app alert" in which malware is hidden on apps that look legitimate.

Pig butchering

In our work as fraud psychology researchers we have noticed a trend towards hybrid scams, which combine different types of fraud. Hybrid scams often involve crypto investments and [sometimes use trafficked labor](#) In the US alone, [the FBI recently reported](#) that people lost US \$3.3 billion (£2.6 billion) in 2023 to investment fraud.

Pig butchering is a long-term deception. [This type of scam](#) combines elements of [romance scams](#) with an investment con. The name comes from the strategy of ["fattening up" a victim with affection before slaughter](#).

It will usually begin with [standard scam approach like a text](#), social media message, or an introduction at a job board site.

Victims may have their guard up at first. However, these scams can unfold over months, with the scammer slowly gaining the victims' trust and initiating a romantic relationship all the while learning about their

vulnerabilities.

For example, details of their financial situation, job stresses, and dreams about the life they want. Romance scammers often saturate their targets with affection and almost constant contact. Pig butchering sometimes involves several trafficked people working as a team to create a single persona.

Once the victim depends on the scammer for their emotional connection, the scammer introduces the idea of making an investment and uses fake crypto platforms to demonstrate returns. The scammers may use legitimate sounding cryptocurrencies and platforms. Victims can invest and "see" strong returns online. In reality, their money is going directly to the scammer.

Once a victim transfers a substantial amount of money to the con artist, they are less likely to pull out. This phenomenon is known as the "[sunk cost fallacy](#)". Research has shown people are likely to carry on investing money, time and effort in activities they have already invested in and ignore signs the endeavor isn't in their best interests.

When the victim runs out of money or tries to withdraw funds, they are blocked.

The victim is left with not only financial devastation, but also the loss of what they may imagine to be their most intimate partnership. They are often [too embarrassed to discuss the experience](#) with friends and family or to report to the police.

PayPal scams

Fake payment requests are a common attack that works by volume rather than playing the long game. Payment requests appear to come from a

genuine PayPal address. Fraudulent messages typically begin with a generic greeting, an urgent request and a fake link.

For example, Dear User: You've received a payment, or you have paid too much. Please click link below for details. Users are directed to a spoofed website with a legitimate sounding name such as www.paypal.com/SpecialOffers and asked to enter their account information and password.

Both of us have received these scam requests—and even we found them difficult to discern from legitimate PayPal request emails. These scams work through mimicry and play on the human tendency to trust authority. Legitimate PayPal correspondence is usually automatic bot language, so it is not difficult to imitate.

But remember, genuine messages from PayPal [will use your first and last name](#).

The missing person scam

This seems to be a new scam that exploits a person's kindness. In the past, charity scams involved posing as charitable organization responding to a [recent, real calamity](#).

The new missing person scam is more sophisticated. The initial plea is a [fake missing person post](#) that generates likes and shares, increasing its credibility and exposure. Then the fraudster edits the content to create an investment scheme which now has the veneer of legitimacy.

This scam may work because the initial consumers are unaware that the content is fraudulent, and there is no obvious request. In psychology, this type of persuasion is known as "[social proof](#)"—the tendency of individuals to follow and copy behavior of others.

Fake app alerts

People post mobile apps, designed to steal users' personal information, on the Google Play or Apple app store.

The app often has a [legitimate function](#), which gives it a cover. Consumers unknowingly jeopardize their private information by downloading these apps which use malware to access additional information.

Although there has been [media coverage of Android security issues](#), many users assume malware [cannot bypass app store screening](#). Again, this scam plays on people's [trust in authority figures](#) to keep them safe.

Discuss any investment opportunities with friends, family members or professionals. It's much easier said than done, but exercising caution one of the best strategies to reduce the chance of becoming a fraud victim.

Scammers count on people paying little to no attention to their emails or messages before clicking on them or providing valuable information. When it comes to scams, the devil is in the missing details.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

Citation: How scammers use psychology to create some of the most convincing internet cons—and what to watch out for (2023, June 22) retrieved 2 May 2024 from <https://techxplore.com/news/2023-06-scammers-psychology-convincing-internet-consand.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private

study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.