The Psychology of Scams

BY **HO YEW KEE,** Professor of Accounting, Singapore Institute of Technology

Social connectivity has introduced a myriad of utility applications and conveniences, fundamentally altering our way of life. However, like many groundbreaking inventions, the Internet is not without its drawbacks, particularly in the realm of online scams. Understanding the psychology of how people fall prey to phishing and other scam tactics can be a first step to not getting "fished".

According to the latest report by the Singapore Police Force, 2023 witnessed a significant surge in reported online scams, almost 50 per cent more than the previous year. And it is worth noting that these statistics only account for reported scams.

Beyond the financial toll, online scams can erode trust and confidence in both the Internet and society at large. Additionally, the psychological and mental distress inflicted on scam victims can substantially diminish their overall quality of life.

This article focuses exclusively on online scams targeting individuals, excluding cyber security breaches involving corporations. It delves into the structure of online scams and examines the factors influencing one's susceptibility to falling prey to scams, and explores the mental aftermath of a scam.

Phishing psychology

The unique nature of online scams lies in their requirement for the target to respond to an invitation, facilitating the execution of the scam. It is often said that no one is immune to online scams, as the human element is considered the weakest link in any secure online environment.

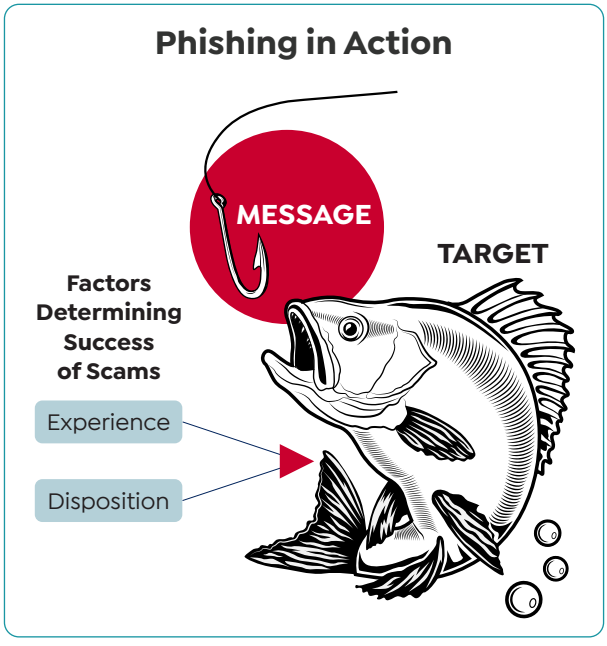
Some say the term "phishing" derives from the word fishing. Analogous to fishing, phishing is a technique to "fish" for usernames, passwords and other sensitive information (See box, "Phishing in Action").

The success of a scam is influenced by the target's experience and disposition, underscoring the critical role of the human factor in these schemes.

In essence, a scam comprises two key components: the message and the target (see box, "How a Scam Works").

Scam compliance

External life events or circumstances can contribute to scam compliance. These include significant life events (e.g., loss of a loved one, financial distress, unemployment), limited time to respond to a message, influence from individuals with high social



standing or peer pressure, compliance with authority, lack of community support for seeking help or advice, loneliness, dissatisfaction with one's present circumstances, illness, among others.

Potential scams can be mitigated by deliberate countermeasures, such as evaluating an offer rather than acting impulsively, and considering the consequences of one's action. Having a support network to check with, when faced with propositions that seem too good to be true, can also be helpful.

Scam aftermath

Scam victims typically endure profound effects, including financial losses, humiliation, loss of self-confidence, lingering feelings of anger and resentment, and a burning desire for justice. The impact on their well-being is further exacerbated when authorities redirect them to bureaucratic processes that entail filling out numerous forms without offering concrete resolutions.

These negative emotions can have a devastating impact on a victims' quality of life, profoundly affecting trust, self-esteem and online interactions. Having sympathetic and understanding support from friends and family members is a good way to recover from the trauma. For some victims, it may be helpful

How a Scam Works

The Message

The message invites the target to engage in a conversation centred around an alluring proposition or the avoidance of potential negative consequences. Social engineering is used to manipulate the individual into disclosing confidential information by targeting their individual's emotions, unique circumstances or fears. These messages take various forms: phishing emails, phishing websites and social media chats that act as platforms.

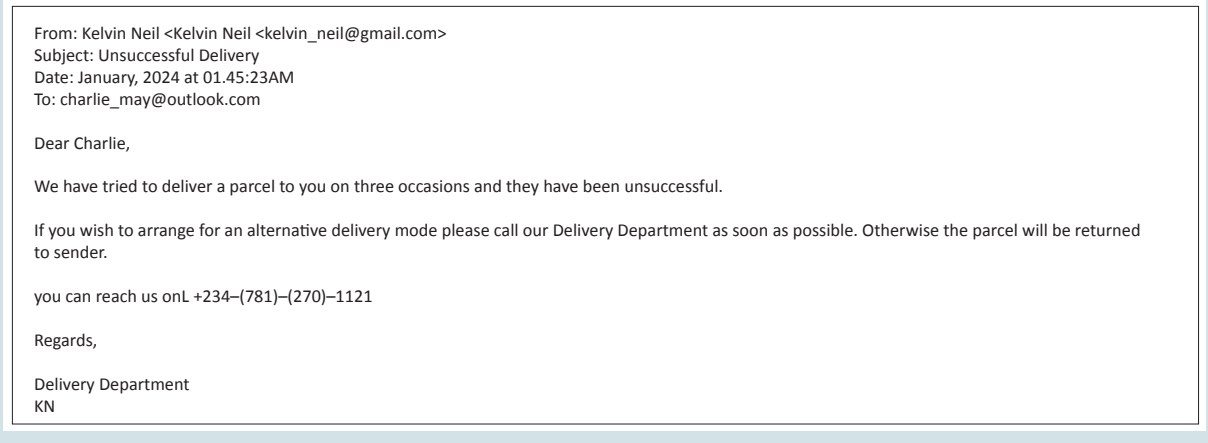
The content of the message may provide seemingly genuine, relevant and specific information, offering the target products or services, such as investment propositions, free gifts, friendships and more. It can take the form of a bulk phishing email or a more personalised spear-phishing attempt, where an individual's attributes are gathered from sources like the Internet, social media, or the dark web.

For instance, a general phishing email might impersonate a well-known company, congratulating the target on winning a prize and prompting them to click on an attached link to claim the prize. Subsequently, the target is directed to provide personal information on a fake website.

Spear-phishing is more intricate, involving a personalised disguise that incorporates the individual's information. For example, an email might address the target by name, referencing recent experiences or contacts, such as a message from the IT department requiring a password change or the collection of an expected parcel.

The key attributes of a successful scam message to obtain trust include sincerity, genuineness, relevance, relatedness and appropriateness to the potential victim's circumstances. An enticing prize can increase the appeal of the phishing email.

To defend against these scams, scrutinising the message is the best line of defence. Defensive techniques may involve seeking advice from others, delaying replies, spotting phishing's traits like spelling errors or poor grammar, and using anti-phishing software on one's device.



From: Kelvin Neil <Kelvin Neil <kelvin_neil@gmail.com>
Subject: Unsuccessful Delivery
Date: January, 2024 at 01.45:23AM
To: charlie_may@outlook.com

Dear Charlie,

We have tried to deliver a parcel to you on three occasions and they have been unsuccessful.

If you wish to arrange for an alternative delivery mode please call our Delivery Department as soon as possible. Otherwise the parcel will be returned to sender.

you can reach us onL +234–(781)–(270)–1121

Regards,

Delivery Department
KN

to seek professional counselling or psychological help to overcome the pent-up anguish.

In response, scam victims may adopt various avoidance strategies to shield themselves from falling prey again. Some opt to avoid online transactions altogether, resorting to white lies to evade commitments. Others may choose to live in a state of estrangement and indifference to others to avoid becoming victims again. A better response is to be more aware of scam tactics and to stay vigilant with good community support.

The primary need of a scam victim is to find closure, whether it be moving forward in life despite the scam or obtaining a satisfying resolution. However, clinging to a victim mentality does not serve the victim's well-being.

The Target

Why are some individuals more susceptible to scams?

Age is generally acknowledged to have a positive correlation. The US Federal Bureau of Investigation issued a public warning in November 2023 about scammers specifically targeting senior citizens. Increasingly, however, the young and technology-savvy are not spared, possibly due to over-confidence and impulsiveness.

Some evidence suggests that gender may be a factor. In Japan, for instance, older women who live alone and have smaller social networks tend to have higher vulnerability scores in relation to scams.

In general, the target's experience and disposition influence the success rate of a scam.

Experience

There is general consensus that individuals with higher levels of education, greater financial literacy, enhanced technological savviness, extensive experience using the Internet, heightened awareness of Internet safety, and staying abreast of developments in Internet security and scams are better equipped to guard against falling victim to scams.

Consequently, there are substantial benefits for individuals to pursue additional education and training in online usage. Complacency and pride, however, often manifest in the belief that "it-will-not-happen-to-me", leading to an individual's downfall.

Interestingly, the debate over the amount of time spent online persists. While a longer duration of online activity may expose individuals to a higher risk of scams, it is also acknowledged that experience is gained over time. Conversely, too little time spent online may result in insufficient experience to identify potential scams.

Disposition

There is no cause-and-effect relationship between one's inherent temperament and the likelihood of being a scam victim because mitigating circumstances always play a role. Even individuals with similar dispositions may react differently to a phishing email. However, there are documented propensities towards scam compliance for individuals with certain inherent temperaments.

Individual traits that are more prone to falling for scams are depicted in the diagram below.

As can be seen, the traits can be either positive or negative. An open and trusting person, especially one insistent on honoúring commitments and who is generally agreeable, may also be susceptible to scams.

Prevention vs recovery

Trust in fellow citizens (or netizens) and authorities is the bedrock of every community and business. When this trust is eroded through scams, the systemic trust essential for a society to function efficiently and effectively is compromised. This can lead to significant friction and increased transaction costs.

To reduce the incidence of scams, gaining a good understanding of scam mechanisms and employing various anti-scam measures is crucial. In the aftermath of a scam, victims seek resolution to address their pain, which can result in a substantial mental and psychological burden if not handled appropriately. No one is immune, and the key defence lies in exercising due diligence in handling any scam attempt. ●