Scammers use psychological tricks to dupe people online

Fraudsters play on our emotions and persuade us into making hurried decisions, says Uma Shashikant.

Our elderly aunt is now an active Internet user after discovering the joys of the World Wide Web. It surely is a web, she says, for she receives countless number of junk emails, robocalls, and online requests that leaves her baffled. It is easy to explain to her how to identify a scam and to not click on a link or take a call from an unknown number. But the concern is that she might learn the technology but the scammers may be targeting her emotions.

Research shows that online scams are a large industry and notoriously difficult to catch. Shame of being duped by a fraudster is so immense for the victim that very few report the crime. Even if they do, most trails go unearthed as scammers use fake identities or simply vanish without trace.

Technology has made it easy to reach the masses through group emailing techniques. Fraudsters leverage technology not only to mask identity and create fake emails and websites but also to reach a large number of people all over the world at a very low cost. But, the success of scammers cannot be attributed to technology alone. Scams work because of our several emotional vulnerabilities and behavioral limitations. Technology has only made it easier for the scammers to play on our emotions and speedup our responses in urgency.

Often, it is the savvy and the smart who make for an easy target for the scammers. The play is on their ability to engage assuming that the risk is small, they understand technology enough to not fall for any trick and there may actually be benefits. Once we begin to engage with the scammer, the web tightens as we refuse to believe that we can fall victim to a fraud. Even after we have sensed the scam and begin to worry that we are being fooled, we slip into denial about the loss. We cannot deal with the guilt of our decision and admit our foolishness. So, we refuse to end the communication with the scammer, hoping to recover something.

Fraudsters play on these emotions and some more. They exploit our ability to make irrational decisions under the influence of emotions. For example, an email from an ‘authority’, such as the government, the taxman, the banker or the police, will invoke fear. A warning that access to your bank account is being denied or that your debit card has been blocked will grab your attention and trigger an action arising out of fear. Names, designations and signatures of authority are traps that will make you open the email and click the link therein. From there, the slide downhill begins.

Fraud calls are meant to create a sense of higher benefit for lower cost. When you get a phone call declaring you have won a prize or that you are the chosen one, you are taken in by the praise. You let your guard down and continue to engage with the caller. But this can prompt the caller to make calls again from a position of familiarity and hence reduce your ability to say no or make an excuse or remain uninterested in the conversation. The trap thus deepens.

The most frequently used trick is to persuade us to act immediately. For instance, you get a call that is offering a hard-to-resist vacation deal. The bargaining instinct in you will invoke the fear of losing out a cheap deal if you don’t act fast. The scammer will capitalise on your wiilingness to take a good bargain home.

There have been ample cases of romance scams as well. A 62-year old Swedish widow, Maria Grette, made news in 2016 for getting duped by a scammer she met on an online dating site. The scammer after taking her into confidence in over three months of communication convinced her into sending him money on the pretext of getting mugged and lost. There is no dearth of similar frauds in India either.

What could we do? The primary step is to modify our behavioral response. Some responses are hardwired in our brain based on experiences. For instance, not looking a solicitor in the eyes on the streets, not opening the door to a stranger, not sharing our location with our co-passenger etc are some tricks we have learned based on shared experiences about safety. They are now so well incorporated into our behaviour that our response is almost automatic. Protection from scams needs similar training.

Know that your bank, card provider or tax authorities will never ask you to reveal details over the phone or click a link on a mail. Make it a habit to not open such emails, no matter how authentic they may look. Learn that verifying before action is a safe rule, always. If you receive an unnerving emergency phone call from a hospital about a dear one, don’t panic. Rather, cross check before making any rushed payments.

If a deal looks too good to be true, it probably is. Be careful to not make upfront payments or give advances, not without checking if the website is genuine. Practice to modify your immediate decisions positively. Identify quickly and dispose the offending email into trash, disconnect that phone, or tear up that snail mail. That response is something the scammer cannot prepare for.

Source & Courtesy: Uma Shashikant, ET Wealth - 22-28 Oct '2018