Cyber Tales by Tenali

- a fortnightly series

ONLINE SHOPPING SCAM

Scan this QR Code to Download this edition:

Cyber tales by Tenali
Vol 15, July 2021, I Issue

Published by:
UCO Bank, CISO Office

Editor-in-chief
Avinash Shukla, DGM & CISO

Editor
Ruchi Agrawal, CM

What's Inside:

यूको बैंक UCO BANK
(भारत सरकार का उपक्रम) (A Govt. of India Undertaking)
सम्मान आपके विश्वास का Honours Your Trust

The internet continues to reshape the way we shop, with retail apps and social media stores adding to consumers' online options and the coronavirus pandemic driving people to shop from home in droves. Cybercriminals are taking advantage of this trend to dupe innocent people. In this edition, we will look how scammers use this latest technology to rip off unsuspecting shoppers.

RIA GOT SCAMMED

Oneday Ria saw an advertisement in Facebook which something like this:

ONLINE SHOPPING SCAM... Contd

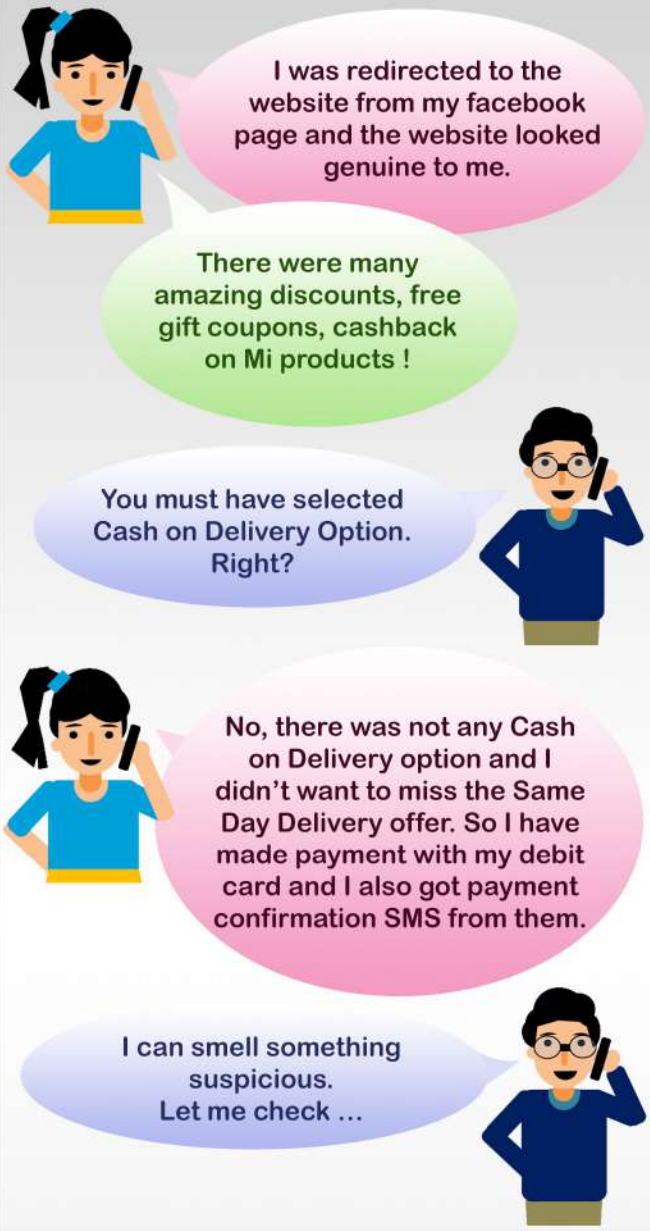
Ria was very excited to see this offer on Facebook as she was searching for this smartphone online from long time at different sites but the rates were very high. So when she found smartphone with 75% discount, she immediately clicked on 'Buy Now' option. She was redirected to a very classy looking shopping website:

In the website, Ria saw many amazing offers and free cashback gifts along with each purchase that she had never seen before. All the offers were expiring very soon. So she immediately selected her desirable smartphone and proceeded for checkout. She gave her shipping details but didn't find any 'Cash on Delivery' option for payment. All payments were only accepted via debit/credit card , UPI , Net banking etc. She completed the purchase by making the card payment.

She also received an SMS for her order confirmation:

Ria was very happy after buying the phone. She called her friend Ajay to share her experience and told him about this new website with exciting offers.

ONLINE SHOPPING SCAM... Contd



After searching for a while Ajay found the original website link as **mi.com**. But Ria has purchased her phone from **mi-home.in** which looks exactly the same as the original one. He immediately called Ria and told that she might have scammed via fake website.

Ria did not believe in Ajay's prediction, She was eagerly waiting for her order delivery. But she neither got any tracking id nor her order was delivered in 24 hours. She tried many times for contacting customer care division but she could not reach any contact person nor there was any link from where she can trace her order. Atlast she understood that she has been scammed via Fake Online Shopping

WHAT HAPPENED HERE?

This is a relatively new Modus Operandi that has been adopted by cyber fraudsters to dupe people online. Online shopping scams involve scammers pretending to be legitimate online sellers, either with a fake website or a fake ad on a genuine retailer site. Scammers use the latest technology to set up fake retailer websites that look like genuine online retail stores. They may use sophisticated designs and layouts, possibly stolen logos, and even a domain name similar to an authentic retailer.Sometimes these scams involves the use of social media platforms to advertise their fake website. Scammers open the store for a short time, often selling fake branded items. After making a number of sales the stores disappear.

ONLINE SHOPPING SCAM...

The intention of the company is to lure customers with non-existent attractive offers with quick delivery option. Thus they induce unsuspecting customer to pay online and once the payment is done, the customer never gets the ordered product or gets mostly a duplicate version of the product. Ria is one of the victims of this scam. She has fallen prey to deep discounts and didn't even search for the reviews of the website before purchasing. She trusted the website because of its genuine looks and made instant online payment for her order.

WARNING SIGNS

- *Scammers offer very low prices for costly items that actually don't esist.*
- *Pressurise you for immediate payment via online instead of 'Cash-on-Delivery'.*
- *Encourage you by offering a special discount / quick delivery of orders / very less time to get the deal / limited stocks available etc.*

SAFETY PRECAUTIONS

1. *Don't fall prey to deep discounts, especially on aspirational products. If the offer is too good to be true, it probably isn't.*
2. *Search on Internet about the credentials of the shopping portal. If a large number of reviews about the site complain about non-delivery of products, then the site is probably fake.*
3. *If the unknown site is offering Cash-on-Delivery, prefer that instead of affront payment.*
4. *Do not make payment using credit/debit card on untested e-commerce sites as it captures your debit/credit card credentials and may sell it on dark web.*

In case you have fallen prey to any such fraud -
REPORT IMMEDIATELY TO THE NEAREST CYBER CRIME POLICE STATION & NATIONAL CYBER CRIME REPORTING PORTAL
https://cybercrime.gov.in

We welcome your valuable suggestions / feedback at
ciso.office@ucobank.co.in

Cyber Guru Tenali's Mantra
KEEP EYES OPEN