Online Shopping Frauds

Sarat K Samal

Abstract--- *CNP fraud or online shopping fraud is when a suspect enables fraudulent payment details or fraudulently acquired card cards to make online retail purchases without the consent of the account owner. Transaction scam is any type of fake or unlawful transaction by cybercriminal. The offender uses the Internet to deprive the victim of resources, personal property, interest or confidential information. Payment fraud is defined in three ways: loans that are illegal or not authorized. Missing merchandise, or robbed. The Ministry of Commerce and Industry has stated that online retail fraud has resulted in 13,873 cases since July 2016. The government has stated there is a database and a website for customers to send their concerns regarding online shopping scams. It is stated by the federal trade commission the steps that the consumer needs to follow when one opts for online shopping are getting details about the product one is buying, know about the cost of the product, beware of fake reviews etc. This paper reveals about online shopping frauds, how to identify fraudulent, how to report frauds.*

Keywords--- *Cash on delivery, customer, Frauds, Online Shopping, Seller.*

I. INTRODUCTION

The Ministry of Commerce and Industry has stated that online retail fraud has resulted in 13,873 cases since July 2016. The government has stated there is a database and a website for customers to send their concerns regarding online shopping scams. Some of the cases which are usually faced by the victims of online frauds:[1], [2]

- Consumers receiving goods late, or not at all,
- vendors receiving no payment,
- consumers receiving items which are either less expensive than those marketed or completely different from the original description,
- Failure to disclose relevant information about the product or terms of sale.

Department of Management, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, saratksamal@soa.ac.in

Received: September 2019 | Revised: October 2019 | Accepted: November 2019

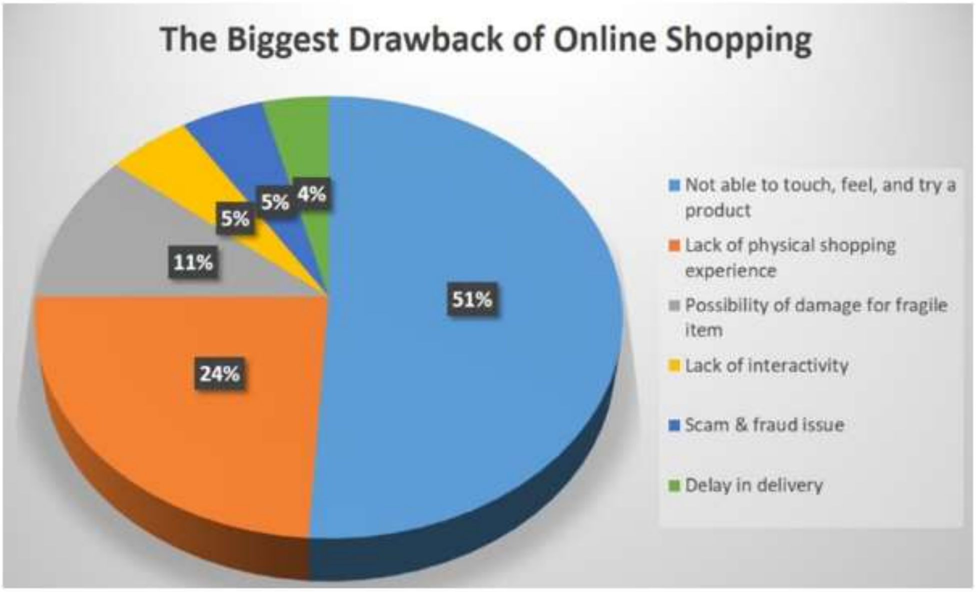


Fig.1 Drawbacks of online shopping

II. IT IS STATED BY THE FEDERAL TRADE COMMISSION THE STEPS THAT THE CONSUMER NEEDS TO FOLLOW WHEN ONE OPTS FOR ONLINE SHOPPING:

II.I. Get the Details (Know from whom you are buying a product from)

Anyone can create a fake profile by using any name. Confirm the registered address and telephone number of the online retailer in case one have any query or issues. And if one is receiving a mail or pop-up notification asking for one's financial information while surfing, don't respond or follow the link. Trusted sellers doesn't ask for information.[3]–[5]

II.II. Get details about the product one is buying

Read closely product description by the seller, especially the fine print. Terms such as refurbished, vintage or close-out can suggest that the merchandise is in too little-than-mint quality, while titled-brand items with fire sale prices may be counterfeit.

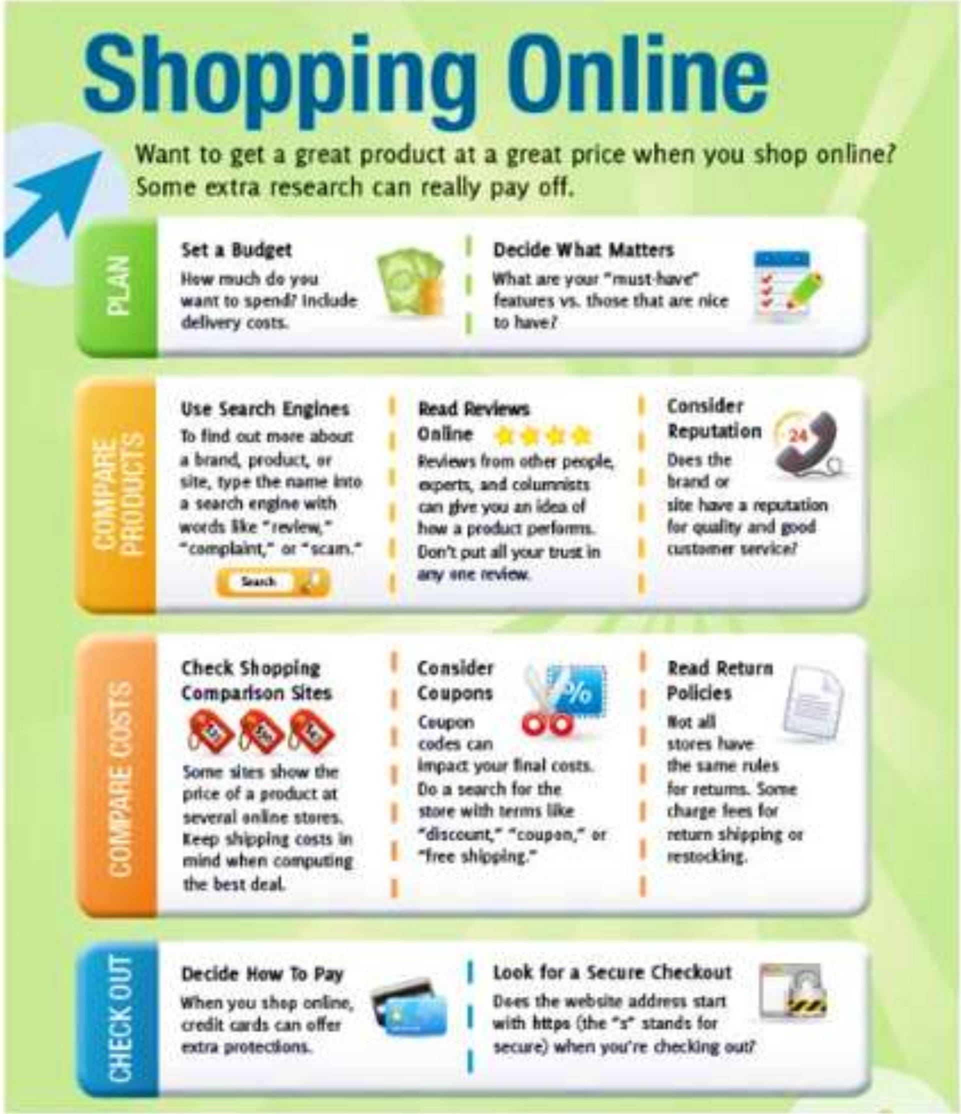
II.III. Know about the cost of the product

Search databases that provide price comparisons and then evaluate "oranges to oranges." Shipping and handling figure in the total cost of your order. Under no conditions one should send the cash or money transfers.

II.IV. Know about the terms and conditions of the product

If you aren't satisfied, can you return the product for a refund or replacement? When someone buy it, who bears the cost of delivery or restocking fees and when do one get his/her order? A Federal Trade Commission (FTC) rule requires retailers to send goods as agreed or, if no specific date is specified, within 30 days after the request. Many stores offer tracking options, so one will be able to see exactly where your order is an estimate when you will get it.[6]–[8]

Received: September 2019 | Revised: October 2019 | Accepted: November 2019



Shopping Online

Want to get a great product at a great price when you shop online? Some extra research can really pay off.

PLAN

Set a Budget
How much do you want to spend? Include delivery costs.

Decide What Matters
What are your "must-have" features vs. those that are nice to have?

COMPARE PRODUCTS

Use Search Engines
To find out more about a brand, product, or site, type the name into a search engine with words like "review," "complaint," or "scam."

Search

Read Reviews Online
Reviews from other people, experts, and columnists can give you an idea of how a product performs. Don't put all your trust in any one review.

Consider Reputation
Does the brand or site have a reputation for quality and good customer service?

COMPARE COSTS

Check Shopping Comparison Sites
Some sites show the price of a product at several online stores. Keep shipping costs in mind when computing the best deal.

Consider Coupons
Coupon codes can impact your final costs. Do a search for the store with terms like "discount," "coupon," or "free shipping."

Read Return Policies
Not all stores have the same rules for returns. Some charge fees for return shipping or restocking.

CHECK OUT

Decide How To Pay
When you shop online, credit cards can offer extra protections.

Look for a Secure Checkout
Does the website address start with https (the "s" stands for secure) when you're checking out?

Fig.2 online shopping

II.V. Always check for HTTP and HTTPS

Fig. 3 HTTP and HTTPS

The main difference between HTTP and HTTPS is that HTTP is not safe, while HTTPS is a protected protocol that

Received: September 2019 | Revised: October 2019 | Accepted: November 2019

utilizes TLS / SSL certificates for security purposes. These are the domain alpha privative for URL and used for web server encryption of web pages.

These guidelines are fairly simple, a user (typically a browser) sets a TCP connection to the server (HTTP or HTTPS), sends an ASCII string request and expects a response. The response is also often encoded as an ASCII string, though the server may return many other data formats (for example, pictures are sent as binary data).

If someone use the HTTP protocol, it is simpler to break the encryption, as it is in plain text for information and data sharing. But while using HTTPS protocol, violating protection is hard as the information and data is sent in encrypted form. HTTPS policy is highly recommended if the recipient shares his / her personal and sensitive data.[9]–[11]

II.VI. Real Website Vs Fake Website

Know the difference between real website and fake website as one can tell the difference by looking at the structure and functioning of website·

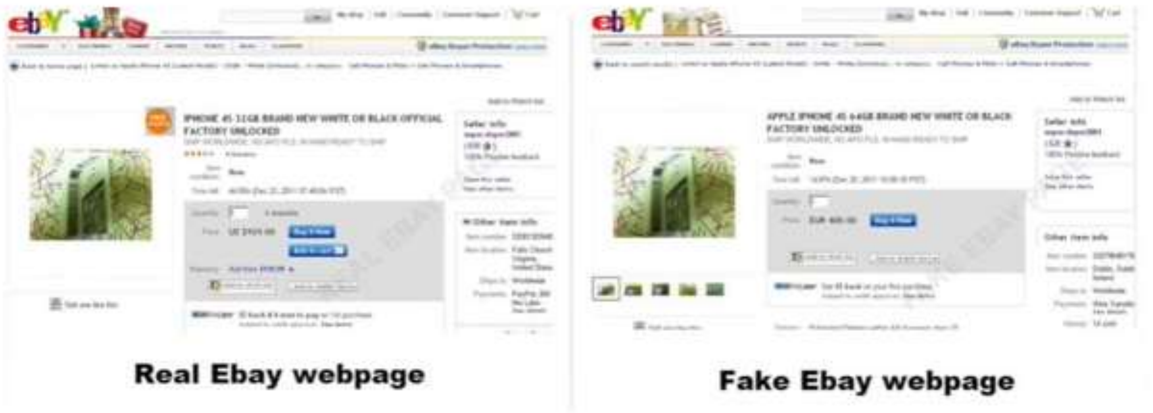


Fig.4 Real vs Fake Websites

Real website link – www.ebay.com
Fake website link – www.ebay.123.com

II.VII. How to check whether the seller is verified or not?

While using the trusted websites like amazon, flipchart one should take a look at the names of the sellers, those having fulfilled or prime logo on amazon are trusted sellers and those having assured logo are trusted sellers. Having these logos under the name of the sellers means that the website owner verifies that the seller is authenticated and trustworthy.

II.VIII. Fake Reviews:

If those wireless earphones costing $10 dollars of 11,999 five-star reviews seem too tempting, they actually do. One of the many dangers of online shopping in 2019 is being duped into buying an inferior product through misleading or false ratings.

- In every field of e-commerce, fake reviews have gained popularity, from appliances to shoes, books and children's toys.
- Customer tracking site Fake spot, which examines feedback from prominent e-commerce platforms, reports that one-third of reviews on sites such as Walmart.com, Amazon.com and Sephora.com are false.

- To make things more difficult for potential buyers, most of these fake reviews are written by people, not by bots.
- Buzz feed profiled an individual last week who invested more than $14,000 on Amazon goods during 2019, all of which was in return for 5-star ratings.

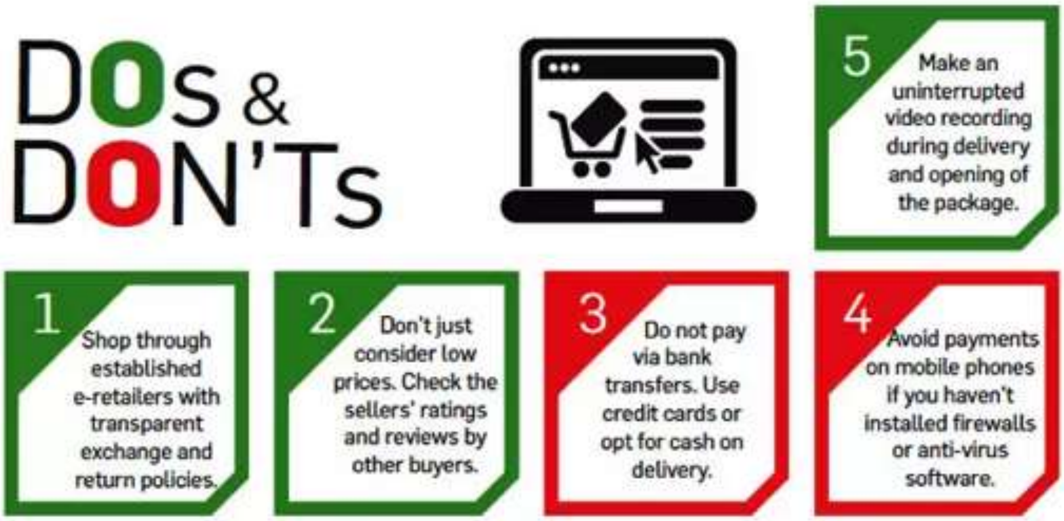

DOs & DON'Ts
5 Make an uninterrupted video recording during delivery and opening of the package.
1 Shop through established e-retailers with transparent exchange and return policies.
2 Don't just consider low prices. Check the sellers' ratings and reviews by other buyers.
3 Do not pay via bank transfers. Use credit cards or opt for cash on delivery.
4 Avoid payments on mobile phones if you haven't installed firewalls or anti-virus software.

Fig. 5 Do's and Don'ts

III. HOW TO REPORT ONLINE SHOPPING FRAUD?

Try to work them out directly with the vendor, customer, or web page operator if you have any issues during a transaction. If this is not working, please lodge a report with:

- At the Federal Trade Commission website (www.ftc.gov/complaint)
- To one's state Attorney General, with contact information at (naag.org)
- Visit consumeraction.gov find out "Where to File a Complaint."

IV. CONCLUSION

CNP fraud or online shopping fraud is when a suspect enables fraudulent payment details or fraudulently acquired card cards to make online retail purchases without the consent of the account owner. Transaction scam is any type of fake or unlawful transaction by cybercriminal. The offender uses the Internet to deprive the victim of resources, personal property, interest or confidential information. Payment fraud is defined in three ways: loans that are illegal or not authorized. Missing merchandise, or robbed. The Ministry of Commerce and Industry has stated that online retail fraud has resulted in 13,873 cases since July 2016. The government has stated there is a database and a website for customers to send their concerns regarding online shopping scams. It is stated by the federal trade commission the steps that the consumer needs to follow when one opts for online shopping are getting details about the product one is buying, know about the cost of the product, beware of fake reviews etc. When someone opts for online shopping he/she should be alert and should consider above mentioned points while shopping online.

Received: September 2019 | Revised: October 2019 | Accepted: November 2019

REFERENCES

[1] D. M. S. J. D. J. S. Nath, “Credit Card Fraud Detection Using Neural Network,” Int. J. Soft Comput. Eng., 2014.

[2] K. Kim, Y. Choi, and J. Park, “Pricing fraud detection in online shopping malls using a finite mixture model,” Electron. Commer. Res. Appl., 2013.

[3] C. V. Amasiatu and M. H. Shah, “First party fraud: A review of the forms and motives of fraudulent consumer behaviours in e-tailing,” Int. J. Retail Distrib. Manag., 2014.

[4] K. Yoshida, K. Tsuda, S. Kurahashi, and H. Azuma, “Online Shopping Frauds Detecting System and Its Evaluation,” in Proceedings - International Computer Software and Applications Conference, 2017.

[5] M. Levi, “Assessing the trends, scale and nature of economic cybercrimes: overview and Issues: In Cybercrimes, Cybercriminals and Their Policing, in Crime, Law and Social Change,” Crime, Law Soc. Chang., 2017.

[6] S. Verma, A. Singh, D. Singh, and V. Laxmi, “Computer forensics in IT audit and credit card fraud investigation - For USB devices,” in 2014 International Conference on Computing for Sustainable Global Development, INDIACom 2014, 2014.

[7] M. Cremonini, C. Braghin, and C. Agostino Ardagna, “Privacy on the Internet,” in Computer and Information Security Handbook, 2013.

[8] R. Shafei, “Effect of customers’ emotions on perceived damage of the probability of fraud in online shopping,” Int. J. Inf. Sci. Manag., 2013.

[9] K. Prathyusha, T. Anuradha, R. Sai, and N. K. Meghana, “Detecting Frauds In Online Auction System,” Int. J. Adv. Res. Comput. Sci. Softw. Eng., 2013.

[10] SandeepPratap Singh, S. S. P.Shukla, N. Rakesh, and Vipin Tyagi, “Problem Reduction in Online Payment System Using Hybrid Model,” Int. J. Manag. Inf. Technol., 2011.

[11] K. Yoshida, “Mining Online Shopping Frauds—A Non-Data Mining Approach,” Int. J. e-Education, e-Business, e-Management e-Learning, 2013.

Received: September 2019 | Revised: October 2019 | Accepted: November 2019