Components and Pattern Analysis of Online Scam Websites

[1]Rahul Verma, [2]Aman Choudhary, [3]Bharath Janardan [4]Gulshan [5]Awadhesh Kumar Shukla

[1]Student, [2]Student, [3]Student, [4]Student, [5]Assistant Professor,
Lovely Professional University, Phagwara, Punjab, India.

Abstract : Digital scams are increasing at a rapid pace year by year. Cyber scam happens due to people's mere carelessness and lack of knowledge about cybersecurity in the modern world. In this paper, we will analyze the patterns and components of online scam websites. This will throw light on how these scam websites operate in the dark to scam people online. Also, this will explain how these scam websites retain users and trick them into being a victim of cyber scams

***IndexTerms* - online-scam-website, scammer, scam-website, scam, online scam, cyber-crime, cyber-security**

I. INTRODUCTION

With the rise of online scam websites, a large population is becoming a victim of scam websites every day. Scam ranging from personal information theft to unauthorize money transfers. These scam websites use certain methodologies and patterns to lure customers into becoming a victim. Since the Internet is now a ready-to-go place for online activities like entertainment, logistics, hospitalization, business, etc, it's also home to many scam websites.

II. COMPONENTS OF SCAM WEBSITE

There are several factors that separate Internet scam websites from genuine ones. It is quite strenuous to deceive a person from an IT background. On the other hand, normal people get easily involved in such scams websites and end up with the worst outcomes. No matter what age or background, people tend to fall victim to many scam types [1] in the Terrain of Cybercrime

2.1 Credibility

The credibility of a website includes the design and all other factors that make it look trustworthy to the visitors. The look of a website is the first impression that will grab the visitor's attention. Authentic sites feature a user-friendly interface since they are dedicated to providing the best user experience.

In the case of a scam website, they come up with bad credibility and poor design. Most of these sites are built for a temporary purpose. Rather than focusing on the design, scammers give more importance to finding new ways to fool people. They will ask you to fill in your identification details, card details, payment methods, and more.

2.2 Longetability

Longetability is a crucial component of scam websites. Scam websites [2] are made to meet a particular short term goal. The culprit turns them down once they achieve their short term goal.

If a site is pretty new in the market and still pretending to give impossible deals and services, they are most probably scamming. Their ultimate goal is either to steal your identity or get your bank credentials, or there might be some other motive as well.

2.3 Impersonification

In impersonification, the scammers create websites that look similar to trusted e-commerce sites such as Amazon and Flipkart. They share false links advertising huge discounts on branded products. Once the buyer makes the payment, the scammers receive your money, but you won't ever get your delivery in the future.

2.4 Payment Handling

Most customers prefer to pay via our credit/debit cards. And this is where scammers and fraudsters find the most unquestionable path to deceive innocent peoples. Most scam websites use payment gateway which does not offer refunds or chargeback services. In such scenarios, victims pay for un-reliable service or product and never receive them in the future.

2.5 Unusual Questionable Offers/Deals

Scam websites come with questionable offers that none of the websites can give. This scam attracts many customers with unusual prices over the latest products.

III. PATTERN ANALYSIS OF SCAM WEBSITES

Average internet users are getting awakened about different types of Internet scams [3]. There is no doubt scam websites are getting advanced too. Scam websites tend to follow a pattern of luring customers into their website, offering them something out of extra, ordinary, and demanding them money or personal information in regard to the delivery of the product.

The pattern for stealing personal identification, sensitive information, or monetary value commonly involved three steps.: Attract, retain, and transaction.

3.1 Attract

In this phase, the victim disguised as a customer is shown attractive offers to buy a product or to enquire for a product. people with low self-control respond differently to deceptive online commercial offers [4] where people who are uneducated tend to fall into such traps easily.

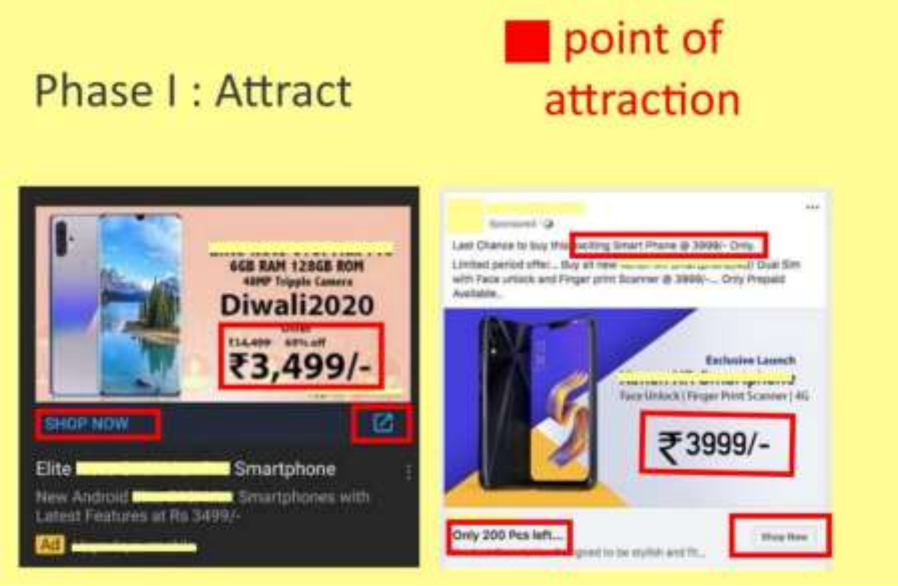

Fig 3.1.1 phase Attract - Pattern analysis of Scam websites

After attracting the victim, the scam websites tries to divert them to unsecured webpage for the next phase.

3.2 Retain

In this phase, the victim is promised for the delivery of goods or services.

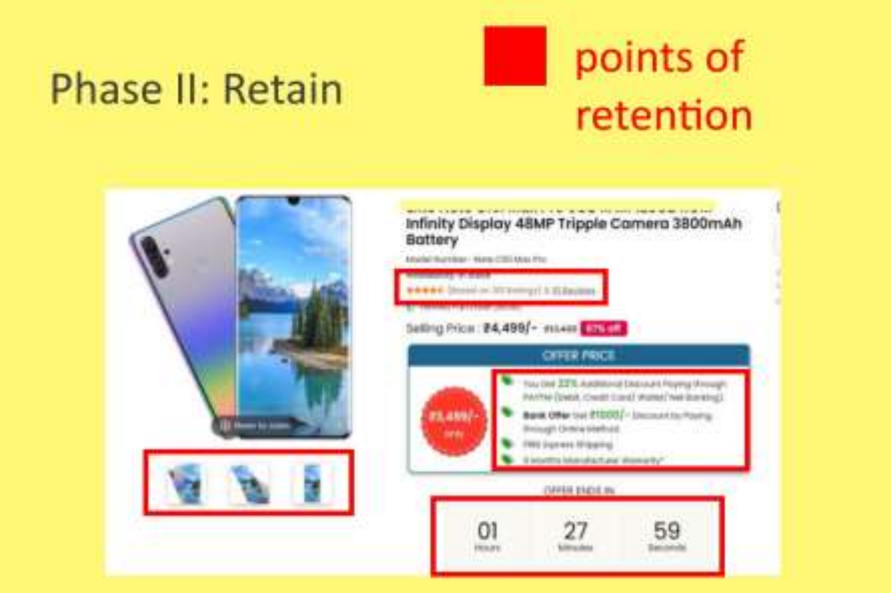
Phase II: Retain
points of retention
Infinity Display 48MP Tripple Camera 3800mAh Battery
Selling Price : ₹4,499/- ₹13,499 67% off
OFFER PRICE
₹3,499/-
OFFER ENDS IN
01
27
59

Fig 3.2.1 phase Retain - Pattern analysis of Scam websites

After retaining the victim for long time and gaining the trust, the cam websites moves to its next phase transaction where exchange of personal sensitive data or monetary values take place. Retention is done by deceptive online reviews [5] and outstanding offers.

3.3 Transaction

In this phase, the victim makes a transaction or exchange of information on fraud websites.

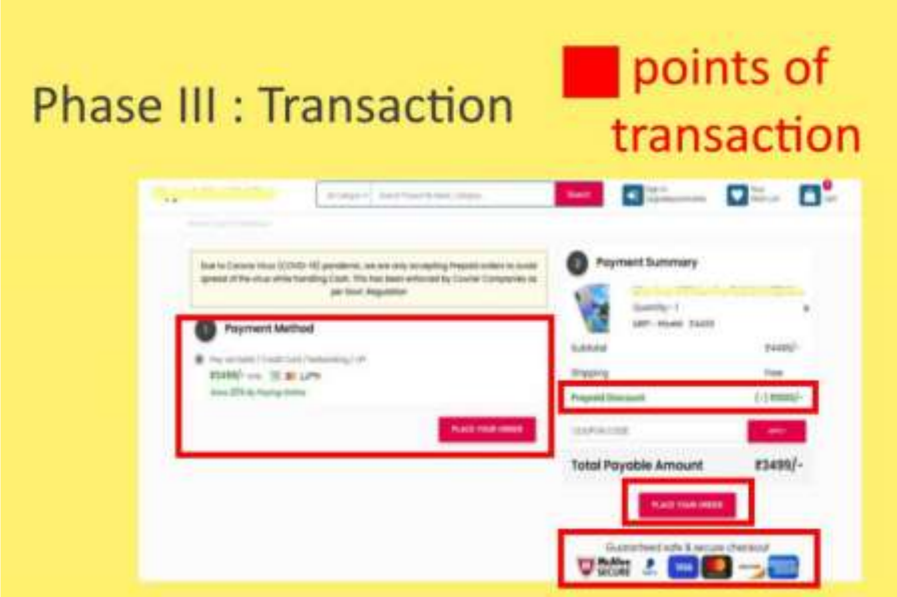

Fig 3.3.1 phase Transaction - Pattern analysis of Scam websites

After the transaction phase, the monetarily values or services promised to the victim are not delivered. And personal data or money is scammed un-ethically from the victim.

IV. CONCLUSION

Putting an end to the online scam websites is inevitable. But it can be stopped by figuring out the ways to identify such scam websites on the internet. These scam websites are operating in the dark and victimizing countless people for sensitive personal data and monetary value. After studying this pattern analysis, people will be now more aware of such online scam websites and will be able to protect themselves.

References:

[1] : A. Stabek, P. Watters and R. Layton, "The Seven Scam Types: Mapping the Terrain of Cybercrime," 2010 Second Cybercrime and Trustworthy Computing Workshop, Ballarat, VIC, 2010, pp. 41-51, doi: 10.1109/CTC.2010.14.

[2] : J. Drew and T. Moore, "Automatic Identification of Replicated Criminal Websites Using Combined Clustering," 2014 IEEE Security and Privacy Workshops, San Jose, CA, 2014, pp. 116-123, doi: 10.1109/SPW.2014.26.

[3] : M. Sharifi, E. Fink and J. G. Carbonell, "Detection of Internet scam using logistic regression," 2011 IEEE International Conference on Systems, Man, and Cybernetics, Anchorage, AK, 2011, pp. 2168-2172, doi: 10.1109/ICSMC.2011.6083998.

[4] : Johan van Wilsem, 'Bought it, but Never Got it' Assessing Risk Factors for Online Consumer Fraud Victimization, European Sociological Review, Volume 29, Issue 2, April 2013, Pages 168–178, https://doi.org/10.1093/esr/jcr053

[5] : Fraud detection in online consumer reviews https://doi.org/10.1016/j.dss.2010.08.012