

## E-Mail Scam: Awareness level of e-mail users in Palakkad District

<sup>1</sup>Anjusha K, <sup>2</sup>Deepika C

Assistant Professor on Contract, PG Department of Commerce and Management, Sreekrishnapuram VTB College, Mannampatta, Palakkad

### Abstract

Internet has become a part of our life and we cannot think a day without internet. Now the world wide communication is within the hands of internet. With its wide popularity and use, email box became the target of scammers and provide online criminals an opportunity to commit different scams. Scams and phishing are the most reported cybercrimes now. As E-mail scams are the target of scammer, they take the form of unsolicited e-mails which may ask for personal and confidential information or to pay some amounts or invite victims to a website or for business with a detailed pitch. E-mail is a platform for online criminals to theft identity, acquire money from individuals or lead the people to certain sites. Most of the e-mail users are unaware about these scams and traps. They haven't enough knowledge to differentiate the legitimate e-mails and scam e-mails. The scammers exploit the unawareness and carelessness of people to make financial benefits. The scammers creates e-mail messages as same as genuine and legitimate to lure the users. The present study aims to study the awareness level of e-mail users to identify e-mail scams. The study seeks to explore factors influencing identification of scams. The research study is a descriptive one. For this study data is collected from both primary and secondary sources. This survey is conducted among 70 e-mail account holders in Palakkad district. A structured questionnaire was directed to collect the primary data. The study examines how well the users are aware of e-mail scams in Palakkad District.

**Keywords:** E-mail scams, awareness level, scam victimization.

### 1. Introduction

The internet has become a part of our life and we cannot think a day without internet. Now the worldwide communication is within the hands of internet. Email was the most popular application of internet since its infancy. It is one of the internet's "killer" applications to date. Now most of the personal and business communication is done through emails. Persons, banks and companies consider e-mail as their convenient way to communicate with others. With the growth of its popularity and use, email box became the target of scammers and provide online criminals an opportunity to commit different scams. Scams and phishing are the most reported cybercrimes now. As E-mail scams are the target of scammers taking form of unsolicited e-mails which may ask for personal and confidential information or to pay some amounts or invite victims to a website or for business with a detailed pitch. The scammers acquire the confidence of users by providing standard format, using names of reputed companies or banks, mirroring websites and web pages. If the 'fish' takes the 'bait' they are hooked- then their personal information will be in the hands of scammers. Bank scam emails, PayPal scam emails, tax rebate scam, scams from HM revenue & customs and scam mails seeking money for service are the top five email scams reported. The scammers exploit the inherent greed and dishonesty of their victims. The number of scams and phishing are increasing day by day. People are unaware about the traps of scammers and don't make any actions to avoid these scams. It is very difficult to differentiate between the genuine and fake e-mails. Many of them are the victims of scammers and many people have little knowledge but they ignore or delete such scam messages from their mailbox. Only a small no. of persons can identify the

scams correctly and ready to report to the concerned authority. Moreover, E-mail scam alert has been an initiative from National Consumer Protection Agency to protect the users from the hands of scammers.

### Significance of the Study

Now a day, it is very difficult to find a person who doesn't have an email account. It is one of the primary ways to communicate. We are using e-mails not only for daily works but also to keep in touch with our intimates. In addition email is an important facility used by the companies to provide goods and services, confirmation of online purchases or updates to our bank account. The banks also use e-mails to inform and maintain relationship with customers. So many people around the world select e-mail as their communication medium. Thus, it has also become one of the primary methods to attack people by cyber criminals. Most of the email users have no idea about the traps hidden in these email messages. There may not any e-mail account holder who hasn't received at least a scam message. So it is relevant to study the awareness level of e-mail users about email scams, factors influencing identification of scams, different types of scams and the actions to handle these scams.

### Statement of the Problem

E-mail is a platform for online criminals to theft identity acquire money from individuals or lead the people to certain sites. Most of the e-mail users are unaware about these scams and traps. They haven't enough knowledge to differentiate the legitimate e-mails and scam e-mails. The scammers exploit the unawareness and carelessness of people to make financial benefits. The scammers creates e-mail messages as same as

genuine and legitimate to lure the users. The present study is an attempt to study the awareness level of e-mail users to identify e-mail scams. The study seeks to identify factors influencing identification of scams.

### Objectives of the Study

The Primary objective of the study is to determine the awareness level of e-mail users to identify e-mail scams. To fulfill this, following secondary objectives were formulated.

- To know different forms of e-mail scams experienced by the users.
- To identify factors that influence user's ability in identifying e-mail scams.
- To determine the actions taken in case of scam victimization.

### Research Methodology

The research study is a descriptive one. For this study data were collected from both primary and secondary sources. Primary data is collected by framing a questionnaire to know in detail the awareness level of e-mail users about e-mail scams, factors influencing scams, different types of scams and the actions to handle these scams. This survey is conducted among 70 e-mail account holders in Palakkad district. Secondary sources include Websites, Research Articles and Books. Nonrandom sampling method is used and the statistical tools applied for analysis of data include percentage analysis, multiple regression and Friedman test.

### Results and Discussion

#### Awareness level of e-mail users regarding e-mail scam

**Table 1:** Awareness level of e-mail users regarding e-mail scam

Response	No. of respondents	Percentage
Yes	50	71.43
No	20	28.57
Total	70	100

Source: Primary data

Table 1 shows the awareness level of e-mail users regarding e-mail scam. 71.43% of the respondents have awareness regarding e-mail scam. 28.57% respondents are not aware about e-mail scams. It reveals that majority of them are aware about e-mail scams.

#### E-mail scams experienced by the users

**Table 2:** E-mail scams experienced by the users

Sl. No	Scams Experienced	Mean Value	Ranks
1	Tax refund scam	2.02	VI
2	Pay Pal Scams	3.97	II
3	Money for help	3.58	IV
4	Tax rebate Scams	3.29	V
5	Lottery and award Scams	3.79	III
6	Bank Scams	4.35	I

Source: Primary Data

**Table 3**

Chi-Square	69.659
Df	5
Asymp. Sig.	.000
a. Friedman Test	

The above tables reveal the result of Friedman Test. Table 2 shows the mean rank on the scams experienced by the users. The highest mean rank is assigned to Bank scam and the mean is 4.35. The second rank is secured by Pay Pal Scam. Followed by this, the other scams are ranked in the order Lottery and award Scams, Money for help, Tax rebate Scams, Tax refund scam. Table 3 shows the result of Chi-square analysis in Friedman Test. It was found that the p-value (0.000) is less than  $\alpha$  (0.05), therefore the result is significant.

#### Factors that influence user's ability in identification of e-mail scams

**Table 4:** Model Summary<sup>b</sup>

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.967 <sup>a</sup>	.934	.921	2.90337
a. Predictors: (Constant), action, common practice, received scam, other media, scam victim, e-mail usage				
b. Dependent Variable: level of awareness				

**Table 5:** ANOVA<sup>a</sup>

Model	Sum of Squares	df	Mean Square	F	Sig.	
1	Regression	4912.009	8	614.001	72.839	.000 <sup>b</sup>
	Residual	345.611	41	8.430		
	Total	5257.620	49			
a. Dependent Variable: level of awareness						
b. Predictors: (Constant), action, common practice, received scam, other media, identify scam, scam victim, e-mail usage						

**Table 6:** Coefficients<sup>a</sup>

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	
	B	Std. Error	Beta			
1	(Constant)	1.280	2.447		.523	.604
	e-mail usage	.643	.633	.080	1.016	.001
	Awareness of scam	2.499	.833	.243	2.999	.005
	Common practice	1.696	.388	.182	4.371	.000
	Received scam	1.855	.483	.237	3.842	.000
	Scam victim	2.912	.827	.247	3.523	.001
	Other media	.833	.574	.081	1.451	.154
	action	1.826	.532	.237	3.434	.001

Table 4 shows R square value of .934 which means 93.4 percent extend of determination. Table 5 shows the result of Anova test. It shows that the result is significant as the P value (0.000) is less than 0.05. Table 6 shows the Co-efficient of determination. It reveals the factors those influences the user's ability in

identification of e-mail scams and those factors are e- mail usage, Common practice, Received scam, Scam victim.

**Actions taken in case of scam victimization**

**Table 7:** Actions taken in case of scam victimization

Actions Taken	Frequency	Percentage
Delete/ignore it	20	40
Report to authorities	6	12
Click on the links in the e-mail	2	4
Research online	4	8
Running anti-virus Scan	10	20
Contact the authorities	8	16
Total	50	100

**Source:** Primary data

Table 7 shows the actions taken by the users in case of scam victimization. 40% of the respondents used to delete/ignore the scam. 20% go for running anti-virus scan. 16% Contact the authorities, 12% Report to authorities and 8% conduct research online and 4% click on the links in the e-mail.

**Findings of the Study**

- Majority of e-mail users are aware about e-mail scam.
- Majority of the respondents experienced Bank e-mail scam.
- The factors those influence the user’s ability in identification of e-mail scams are e- mail usage, Common practice, Received scam, Scam victim.
- Deleting/ignoring the scam e-mail is the action taken by majority of the users.

**Conclusion**

The study concluded that majority of the respondents have awareness in identification of e-mail scams by the users. The users experienced bank scams as the most important one among e-mail scams. Most of the users are victims of e-mail scams. In case of scam victimization they either delete the scam or ignore it. Even though the users are aware of scam e-mails, they are not ready to take necessary actions. Thus necessary steps need to be initiated to alert the users against e-mail scams. Recently E-mail scam alert has been initiated as a tip from National Consumer Protection Agency and more steps could be forwarded in this regard.

**References**

1. Kurose JF, Ross KW. Electronic Mail in the Internet Computer networking: A Top-Down Approach Featuring the Internet, Pearson Education. 106.
2. Tejashree D. Datar, Kelly Anne Cole, Marcus K. Rogers. Awareness of scam e-mails: an exploratory research study, ADFSL Conference on Digital Forensics, Security and Law, 2014, 11-22.
3. <http://www.consumeraffairs.com>
4. <http://www.consumerftc.org>
5. <http://www.lovemoney.com>