

Chapter 2

Identifying Scams and Trends

Abstract This chapter focuses on the taxonomy of scam emails collected from various sources and investigates long-term trends in scam emails. We first describe a large-scale compendium of scam emails collected from various sources, and then present an analysis regarding what kind of scams exist, what their structures are, and how they are related to each other. We then describe a machine learning classifier built based upon the taxonomy analysis, and use it to cluster scam emails into major scam categories. Then an analysis of different trends from each scam category is presented. Our analysis shows a clear trend that spam-like *non-targeted scams* are decreasing continuously while *targeted scams* with specific victims have been getting more prevalent over the last 10 years.

2.1 Gathering Hundreds of Thousands of Scam Messages

To analyze the trends in scams, we collected extensive scam emails from several sources including scam reporting sites and a government report on internet crimes.

Scam emails collected from scam reporting sites, wherein anonymous users post scam emails they received, comprise the first data set. Amongst the many scam reporting sites, we selected four major ones with relatively large scam email databases, with more than thirty thousand scam emails in each site. We examined scam emails reported between 2006 and 2014, that is, more than ten thousand scam emails each year. Overall we collected about 220 thousand scam emails over the four scam reporting sites. Table 2.1 represents the summary of our scam email dataset.

A second source of scam data is the *FBI/IC3 annual reports* [3]. We refer to the FBI/IC3 annual reports to look at frequency of reporting and resulting financial loss to determine how harmful each type of scam has been.

2.2 Taxonomy of Scam Emails

In this section, scam email taxonomy is analyzed based on the scam email dataset described in Sect. 2.1. Since no de facto standard of scam categorization exists, the major scam categories frequently reported from users requires definition.

Table 2.1 Dataset summary

Source	URL	Start date	End date	# Scam emails
Anti fraud international	Antifraudintl.org	02/2007	12/2014	57,338
Scam Warners	Scamwarners.com	07/2008	12/2014	54,352
Scamdex	Scamdex.com	01/2006	12/2014	75,943
419baiter	419baiter.com	06/2008	02/2012	31,847
Total				219,480

Summary of scam email dataset between 2006 and 2014

Although a few fraud taxonomies have been proposed [1, 3], and scam reporting sites have their own categorization rules, these classifications are not mutually consistent and do not cover all the types of scam present in our combined dataset. Also, each scam reporting site uses different scam categories. For example, the scam reporting site *anti fraud international* has twenty scam categories while the scam reporting sites *419baiter* and *scammed.by* do not categorize scam emails at all. Hence we built our own scam categorization as described in Table 2.1. Scam emails are categorized based on (1) whom scammers are pretending to be and (2) how scammers try to persuade their victims. Through the in-depth investigation of the collected scam emails and a survey of literature, we find ten scam categories (15 if counting subcategories) commonly used or frequently reported to the scam reporting sites. Table 2.2 gives a brief description of each of the 9 scam categories in our taxonomy of scam emails. This scam categorization result is used throughout Chap. 2.

2.2.1 Non-Targeted Scams

Our taxonomy of email scams first divides scams into three Types (see Table 2.2) depending on whether the email is *non-targeted*, *targeted* or *both*. A non-targeted scam is a traditional and typical form of email fraud where scammers do not set any designated victims; instead, like spammers, they send out as many scam emails as possible to anonymous users. A targeted scam aims at a specific victim based on a certain context (e.g., the victim is looking for a rent on Craigslist). Hence this type of scam can be more plausible. A few types of scam emails can be both non-targeted and targeted depending on the situation. For example, *Phishing* scam email can be delivered to many number of anonymous users just like spam emails, or it can be targeted on a specific victim based upon a context of the victim collected in advance.

- **Authority scams:** In *Authority scams*, scammers pretend to be employees at banks (*Bank scams*), government agencies or international organizations (*government/organization scams*). The scammers abusively use the names of renowned organizations (e.g., FBI and IMF) to gain trust of victims. In bank scams, scammers offers pre-loaded ATM cards or charity funds to victims,

Table 2.2 Scam email taxonomy

Type	Category	Subcategory	Manual tagging	SVM classification
Non-targeted	Authority	Bank	99 (5.0 %)	18,680 (8.6 %)
		Government, organization	78 (3.9 %)	
		Total	177 (8.9 %)	
	Loan		55 (2.8 %)	6,428 (3.0 %)
	Lottery		215 (10.8 %)	24,132 (11.1 %)
	Money transfer	Charity, dying person	105 (5.3 %)	93,271 (42.8 %)
		Business, commodity	185 (9.3 %)	
		Next of kin	367 (18.4 %)	
		Widow, orphan, refugee	118 (5.9 %)	
		Etc.	47 (2.4 %)	
		Total	822 (41.1 %)	
Targeted	Business email compromise		54 (2.7 %)	5,295 (2.4 %)
	Rental		43 (2.2 %)	7,228 (3.3 %)
	Romance		203 (10.2 %)	20,960 (9.6 %)
Both targeted and non-targeted	Employment		71 (3.6 %)	10,191 (4.7 %)
	Sales		11 (0.6 %)	(Merged with business)
	Phishing		71 (3.6 %)	9,368 (4.3 %)
Misc.	Others		165 (8.3 %)	22,192 (10.2 %)
	Invalid emails		113 (5.7 %)	
	Total		278 (13.9 %)	
Total				2000
				217,745

The ten most prevalent scam categories (excluding *Others* and *Invalid emails*), and the numbers (and percentage) of emails in our compendium belonging to each category based on manual tagging and an SVM classification

requiring a fee in advance. Similarly, scammers in government/organization scams notify their victims that they are able to receive charity funds and require a fee for the process. Sometimes these types of scams involve threats (e.g., unsolicited money related to an illegal business in the victim's account) or malware propagation (e.g., attachment containing virus or worms [4]). *Authority* scam emails mostly look like official emails from the organizations, and the processes explained in the emails also seem official.

- **Loan scams:** Scammers in *Loan scams* make a fake loan offer to victims at an attractive interest rate. But scammers ask for upfront fees for further loan service processing through money transfer companies such as Western Union or MoneyGram. Once a victim transfers the fee, scammers stop communicating with the victim.

- **Lottery scams:** *Lottery scams* bring the unexpected but happy news that the victim's email address has been entered into a lottery and has won the prize.¹ Scammers usually require a fee in advance for transferring a sum of prize money. This is one of the most typical and prevalent forms of non-targeted scams.
- **Money transfer scams:** Scammers in *Money Transfer scams* usually have funds in African countries and want to transfer the funds to victims' countries for several purposes. Scammers in *Charity/Dying Person scams* usually have an inheritance of several million in US dollars and ask victims to help move the money to a charitable fund in the victims' countries. *Business/commodity* scammers are looking for a business partner who will help them invest their money or sell their commodity in the victims' countries. The *Next of kin scam* is one of the most prevalent forms of fraud. Scammers in this category usually claim to be bankers or attorneys who have access to abandoned accounts of a client who has passed away. They propose putting the victim's name as a next of kin so that the victim can inherit the money. *Widow/orphan/refugee* scammers typically claim that they are in unstable countries suffering from internal wars or dictators. They have an inheritance from a parent or husband who has passed away recently and want to transfer the money out of their countries for safety. The *Etc.* subcategory includes scam emails that were not classified. In all cases, victims are promised a certain percentage of the transferred funds in return for helping the scammers, but the victims are also required to pay an upfront fee for the money transfer process.

2.2.2 Targeted Scams

In targeted scams, scammers may have obtained information about their potential victims, e.g., the fact that the victim is looking for an apartment on Craigslist or is selling an old iPhone on eBay. Since the scammers are able to exploit this knowledge, conversations in targeted scams are more natural and plausible.

- **Business email compromise scams:** *Business Email Compromise (BEC) scams* generally target specific companies that have dealings with foreign businesses. In this scam category, scammers can be sellers who present a product catalog with attractively priced goods or services, and sometimes they can be buyers who request a product list from victim businesses. Since scammers are "foreign" businesses, payments are usually done via wire transfer or other electronic payments. Seller scammers prefer these payment methods since they are easy to perform but hard to reverse. Likewise, buyer scammers also prefer them since it is relatively easy to fabricate fake payment notifications to victims.

¹Oddly, to scammers, it is not *people* who are entered in lotteries, but *email addresses*. Correspondingly, email addresses, not their owners, are the winners of the lotteries.

- **Rental scams:** *Rental scams* may either target users who post listings on classified advertisements websites seeking a rental, or may post a fake rental listing by themselves to lure the victims. A common methodology of these scammers is to attract victims with low-priced rentals and then ask for an upfront fee for the first month rent and security deposit. The scammers often copy an actual rent listing and repost that with a much lower rent. They may ask the victims to inspect the house first, but usually a victim is not allowed to enter the house since the supposed home owner (scammer) is away for a good purpose (e.g., mission trip to African countries). Hence it may be hard for the victim to figure out if the rental listing is legitimate or not.
- **Romance scams:** *Romance scams* are slightly different from other types of scams in that scammers have to build a relationship with a victim over a relatively long time. Once the scammer successfully establishes a relationship with the victim, he may request money for various reasons, e.g., to purchase a airline ticket. Since the initial phase of a *Romance* scam is just “normal” conversation, it is relatively hard to determine whether it is scam. Please see Chap.10 for an in-depth study on *Romance* scams.

2.2.3 Scams that Are Both Non-targeted and Targeted

Certain types of scams fit both the non-targeted and targeted categories.

- **Employment scams:** *Employment* scams can be both non-targeted and targeted: non-targeted *Employment* scams, like spam, are sent to unspecified email addresses, and targeted *Employment* scams start with job listing on classified advertisements websites. One typical form of *Employment* scam starts with an attractive job offer from a company located outside of the victim’s home country. Then the victim is usually required to provide an upfront fee for documentation process, e.g., visa application.
- **Phishing scams:** The general goal of *Phishing scams* is either to steal victim’s private credentials (e.g., password or social security number) or to cause the victim to install malware by spoofing famous companies that hold the victim’s money or account information (e.g., banks or PayPal). The key trick in this type of scam is links embedded inside emails that lead the victim to the scammer’s own websites.
- **Sales scams:** In *Sales scams*, scammers can be either the seller or the buyer. The seller scammer posts a fraudulent ad on classified advertisements websites, and the buyer scammer responds to the victim’s legitimate advertisement and makes a fake payment, e.g., a fake PayPal payment notification or a bogus check. One typical example of the *Sales* scam is the used car sales scam where a scammer posts a fraudulent ad selling a non-existent car on a classified advertisements website.

2.2.4 Miscellaneous Scams

In some cases, it is hard to classify a scam email into one of the scam categories listed in Table 2.2. Those scam emails are classified as *Miscellaneous* scams and not used in further analysis.

- **Others:** Scam emails that do not belong to any of the scam categories described above are classified as *Others* scams. Those are usually various scam categories with relatively low prevalence.
- **Invalid emails:** Some scam emails collected from scam reporting websites are not in valid form (e.g., no email content). These emails are classified as *Invalid emails*.

2.3 Scam Classification

Because the original source datasets do not provide a uniform, consistent email classification, we have classified each of the emails in our scam email dataset into the email scam categories described in the previous section.

The first step of scam classification is to establish the ground truth for the classification. Two thousand scam email samples randomly selected from our dataset were inspected manually and tagged on the scam categories listed in Table 2.2. The result of manual tagging is also shown in Table 2.2. The manual tagging result shows that about 41 % of all scam email samples are *Money transfer* scams. The second and third largest categories are *Lottery scams* and *Romance scams*, which account for about 11 and 10 % of scam email samples respectively. Both scam categories are also well-known, typical types of email scams.

A support vector machine (SVM) [2] classifier was implemented using the Python *scikit-learn* library [6] and was trained and evaluated using our 2,000 manually tagged scam email samples. Common English stop words (e.g., “a”, “any”, “am” and so on) and other non-alphabetical characters. (e.g., “:”, “.” and so on) were removed to eliminate meaningless terms from the feature space. Numerical characters and the dollar character “\$” were retained since these are obviously meaningful. Term frequency–inverse document frequency (TF–IDF) [5] features were extracted from each sample and 80 % of the sample was randomly selected as the *training set* and 20 % as the *test set*. Then SVM classifier was trained based on the training set and its performance was evaluated using the test set. Evaluation of the SVM classifier was repeated ten times using different training and test sets, and the evaluation results are presented in terms of *precision/recall* and *ROC curves* in Fig. 2.1. To improve classification accuracy, scam emails were classified to the category level only. Additionally, *Business Email Compromise* scams and *Sales* scams were merged due to the similarity of email contents in such scams. The *Miscellaneous* scam category was not included in the SVM classifier evaluation since it accounts for a small number of various scam types.

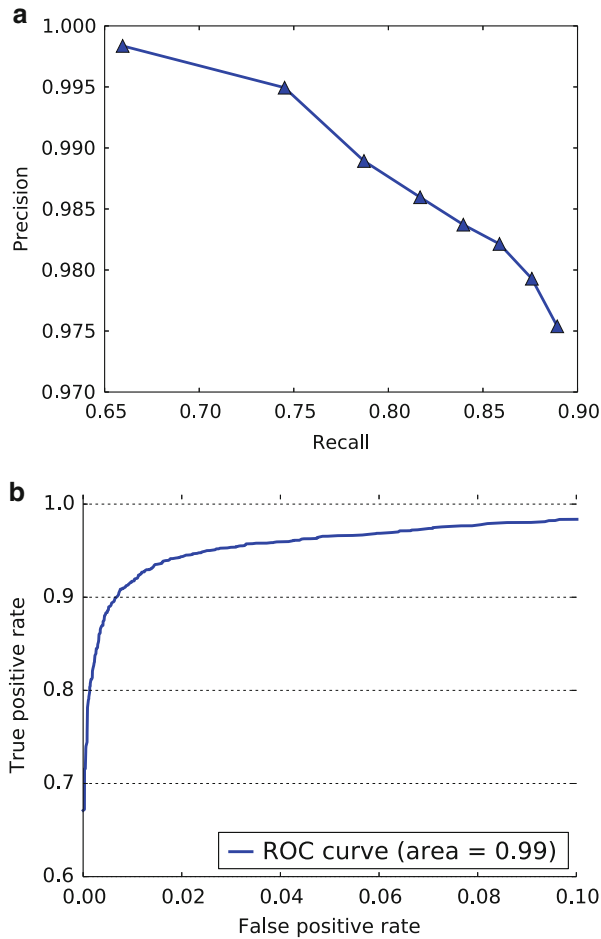


Fig. 2.1 Precision/recall and receiver operating characteristic (ROC) curves of the SVM classifier. For ten major scam categories, the SVM classifier shows over 97 % precision with over 65 % recall, and the area under the ROC curve (AUC) is 0.99. All performance metrics are cross-validated averages measured using 2,000 samples divided randomly into training and test sets of size 80 and 20 %, averaged over ten repeats. (a) Precision/recall curve. (b) ROC curve

In Fig. 2.1a, the SVM classifier shows precision of higher than 97 % with at least 65 % recall for all scam categories. According to the receiver operating characteristic curve in Fig. 2.1b, the SVM classifier shows over 90 % true positive rate with lower than 1 % false positive rate. Although our SVM classifier may not show the minimal false positives and false negatives, it does demonstrate a sufficient performance to show overall trends in scams.

The remaining scam email dataset was classified using the SVM classifier trained on all of the manually-tagged emails. The overall classification result is presented in Table 2.2 in the rightmost column. *Money transfer* scam accounts for the largest portion of scam emails in both results, 41 % in manual tagging and 43 % in SVM classification. Within the *Money transfer* scam category, a typical Nigerian scam called *Next of kin* forms 18 %, and *Widow, orphan, refugee* scams make up about 6 % of all scam emails. The second largest scam category (other than Miscellaneous) is the *Lottery* scam according to both manual tagging and SVM tagging, accounting for about 11 % of all scam emails in our compendium. Similar agreement is seen in all scam categories between manual tagging and SVM classification results in Table 2.2. This observation strongly supports the preciseness and effectiveness of our SVM classifier.

2.4 Scam Trends

We can use our scam email taxonomy and the FBI/IC3 annual reports to examine long-term trends. Our analysis focuses on the scam email dataset and long-term trends for the years 2006–2014 inclusive.

First, let's take a look at the trends in scams in terms of the number of complaints made to the FBI/IC3. The annual number of scam complaints reported to the FBI/IC3 is presented in Fig. 2.2. On average, the number of scam complaints reported to the FBI/IC3 has increased by about 3 % each year between 2006 and 2014.

Now the analysis of our scam email dataset is presented. Figure 2.3 shows the overall trends in terms of the percentage of scam emails reported to four scam reporting websites. Later in this section, further analysis of the long-term trends of each scam category is described in detail.

2.4.1 Targeted vs. Non-Targeted Scams

Let's now consider the trend in how scam emails are targeted. Figure 2.4 shows the numbers of emails we classified as Targeted or Non-Targeted, respectively, in our compendium for the years 2006–2014. Scam categories belonging to “Both targeted and non-targeted” scams were excluded from the analysis to minimize confusion that may result from the ambiguous nature of the mixed scam categories. The analysis clearly shows that non-targeted scams have continuously decreased over the last 9 years while targeted scams have moved in the opposite direction.

In 2006, non-targeted scams accounted for the majority of scam emails (about 96 %) while targeted scams corresponded to a very limited percentage (about 1 %). In 2014, on the other hand, the percentage of non-targeted scams decreased drastically to 31 %, while targeted scams increased steeply to 48 %. This result

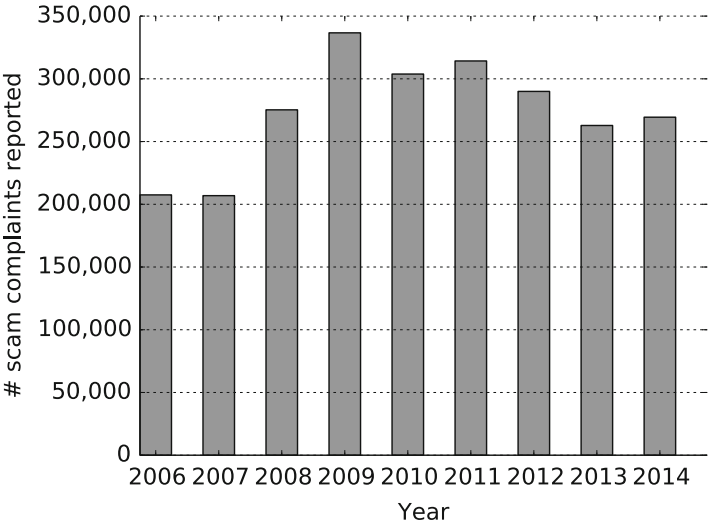


Fig. 2.2 Number of scam complaints reported to the FBI/IC3 [3]. The number of scam complaints has increased on average by about 3 % each year

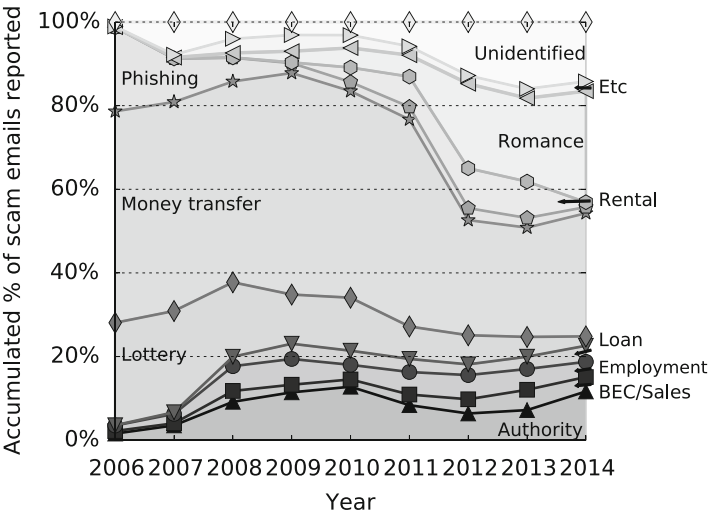


Fig. 2.3 Fraction of scam emails reported to scam reporting websites

implies that scammers’ fraud methodology has improved, from simple spam-like scams (e.g., *Lottery* and *Money transfer* scams) to more personalized and plausible scams aided information about specific victims (e.g., *Business email compromise*, *Romance* and *Sales* scams).

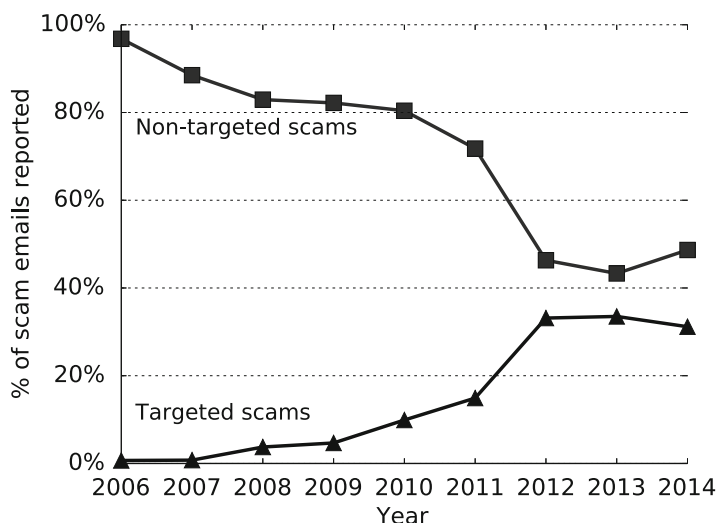


Fig. 2.4 Targeted vs. non-targeted scams. Targeted scams increase continuously from 1 % in 2006 to 31 % in 2014, but non-targeted scams decrease from 96 % in 2006 to 48 % in 2014

2.4.2 Scams on the Rise

Now let us present scam categories that have increased over the years. The overall trends in scam shown in Fig. 2.3 were inspected thoroughly and three scam categories showing a marked increase over the 9 year period were identified: *Authority*, *BEC/Sales* and *Romance* scams. Then we compared our findings with the FBI/IC3 annual reports [3] to cross-check them. Figure 2.5a and Table 2.3 shows the analysis of scam categories on the rise and the corresponding results from the FBI/IC3 annual reports, respectively.

Authority scams show a gradual increase from about 2 % in 2006 to about 13 % in 2010 and 12 % in 2014. Although it is hard to match our analysis to the reports due to different scam categorizations, we are able to find from the FBI/IC3 reports that *FBI scam* (a type of *Authority* scams) is included as one of the most frequently reported scams from 2009 to 2014. Even though the *FBI scam* in the FBI/IC3 reports does not cover all kinds of *Authority* scams, it still partially supports our analysis.

A similar trend is also observed for *Romance* scams. Romance scams show a rapid increase from less than 1 % in 2006 to 20 % in 2012. According to the FBI/IC3 reports, the Romance scam also has been prevalent from 2011 and is included in the most frequently reported scams.

BEC/Sales scams also increase continuously over the 9 years, from about 1 % in 2006 to about 3 % in 2014, both as a fraction of the entire volume of self-reported scam emails. Although neither *BEC* or *Sales* scams were identified as one of the most frequently reported scams in the FBI/IC3 annual reports, *BEC* scam is now considered an emerging scam category. According to the 2014 FBI/IC3

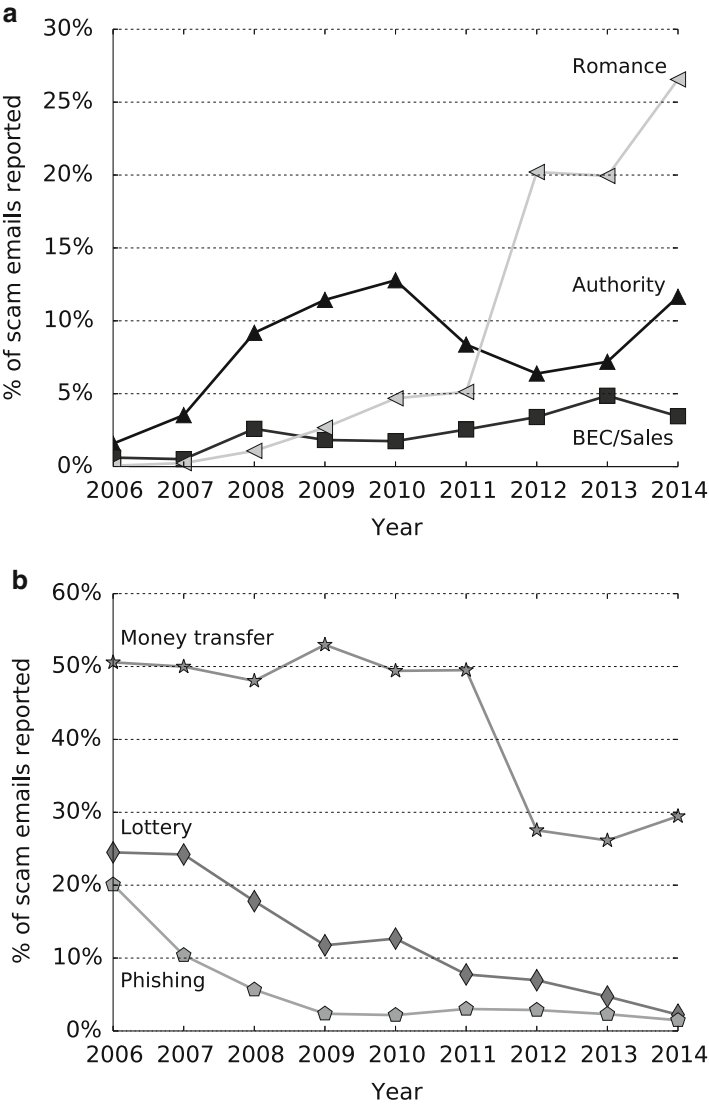


Fig. 2.5 Trends in scams. Fraction of all emails classified into scam categories on the rise (*panel a*) and in decline (*panel b*). (**a**) Scams on the rise. (**b**) Scams in decline

annual report, the *Business Email Compromise* (BEC) scam was first reported in 2010 and has evolved into more sophisticated and various forms since 2013. Since January 2015, the FBI has seen a 270 % increase in identified victims and exposed loss, with reported losses exceeding \$2.3 billion in losses between late 2013 and early 2016. It should be understood that the entire scam problem is likely to be under-reported, though, since most victims recognize that there is likely to

Table 2.3 Most frequently reported scams in the FBI/IC3 annual reports [3]

Category	Years								
	2006	2007	2008	2009	2010	2011	2012	2013	2014
FBI scams	↓	↓	↓	↑	↑	↑	↑	↑	↑
Romance scams	↓	↓	↓	↓	↓	↑	↑	↑	↑
Real estate scams	↓	↓	↓	↓	↓	↓	↑	↑	↑
Identity theft	↑	↑	↑	↑	↑	↓	↓	↓	↓
Investment & Nigerian letter scams	↑	↑	↑	↓	↓	↓	↓	↓	↓

FBI and *Romance* scams are more frequently reported in recent years. On the other hand, *Identity theft*, *Investment* and *Nigerian letter* scams are less frequently reported in recent years

be no recourse. Simply speaking, insurance companies do not protect users and organizations against being scammed, and it is understood that law enforcement fights an uphill battle. Many victims simply decide to move on.

2.4.3 Scams in Decline

From the analysis of scam trends, three scam categories in decline are observed: *Lottery*, *Money transfer* and *Phishing* scams. Figure 2.5b shows the fraction of those three scam categories each year from 2006 to 2014. As before, we looked for corresponding scam categories in the FBI/IC3 reports and show the result in Table 2.3.

The *Money transfer* scam is the most frequently observed scam in our dataset, but it was not possible to find an exactly matching category in the FBI/IC3 reports. However the statistics of *Investment* and *Nigerian letter* scams, which are directly related to *Money transfer* scams, are found from the FBI/IC3 reports. Combining both investment and Nigerian letter scams, they are included in the most frequently reported scams until 2008 and are not included afterwards. Hence it is reasonable to argue that the statistics of the FBI/IC3 reports support our observation that *Money transfer* and *Phishing* scams are getting less frequent in recent years.

Phishing and *Lottery* scams, additional typical non-targeted scams, have also decreased continuously from 20 and 24 % in 2006 to 3 % for both in 2014. Even though it was not possible to find an exact match, the statistics of *Identity theft*, which is a close match to *Phishing* scam, was found in the FBI/IC3 reports. As shown in Table 2.3, identity theft was one of the most frequently reported scams until 2010 and was not included afterwards.

References

1. M. Beals, M. DeLiema, M. Deevy, Framework for a taxonomy of fraud. http://fraudresearchcenter.org/wp-content/uploads/2015/07/FFRC_Taxonomy_FullReport_7-22-15.pdf (2015)
2. C. Cortes, V. Vapnik, Support-vector networks. *Mach. Learn.* **20**(3), 273–297 (1995)
3. Federal Bureau of Investigation, Internet Crime Complaint Center (IC3) annual reports. <https://www.ic3.gov/media/annualreports.aspx>
4. M. Jakobsson, Z. Ramzan, *Crimeware: Understanding New Attacks and Defenses*, 1st edn. (Addison-Wesley Professional, Indianapolis, 2008)
5. K.S. Jones, A statistical interpretation of term specificity and its application in retrieval. *J. Doc.* **28**(1), 11–21 (1972)
6. F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, E. Duchesnay, Scikit-learn: machine learning in Python. *J. Mach. Learn. Res.* **12**, 2825–2830 (2011)

Understanding Social Engineering Based Scams

Jakobsson, M. (Ed.)

2016, XVI, 130 p. 51 illus., 18 illus. in color., Hardcover

ISBN: 978-1-4939-6455-0