

ONLINE SCAMS: TAKING THE FUN OUT OF THE INTERNET

Pradeep Kumar Puram

Professor, CSE Department, Vivekananda Institute of Technology and Science, Bommakal,
Karimnagar, Andhra Pradesh 505001, India
pkpuram@yahoo.com

Mukesh Kaparathi

Student, CSE Department, Vivekananda Institute of Technology and Science, Bommakal,
Karimnagar, Andhra Pradesh 505001, India
mukesh.kprth@gmail.com

Aditya Krishna Haas Rayaprolu

Student, CSE Department, Vivekananda Institute of Technology and Science, Bommakal,
Karimnagar, Andhra Pradesh 505001, India
krishnaahas@in.com

Abstract

The fun of using the Internet has become sour due to the various scams taking place day in and day out, all around the world. Internet users are being trapped around every corner and their credit card information is being siphoned, all due to the presence of these online scams. This paper looks in depth into a few of these scams, and explores a solution to counter this menace.

Keywords: Security; Internet; Web.

1. Introduction

The advent of the Internet has brought some remarkable changes in the working of the world. People have embraced this technology with such enthusiasm that it is hard to imagine a world without Internet. If the invention of the radio and the television made the world a smaller place, the arrival of the Internet shrunk the world to even more minuscule dimensions. Today it is possible for an entire corporation to run its operations in a different country, and not face any problems whatsoever in its functioning. Such freedom is offered by this powerful medium known as the Internet.

However, as is the case with every other technology, the Internet can be used for harmful purposes as well. Along with the good, comes the bad. This age-old adage is very much true in the case of the Internet. The past decade has seen the rise of Internet scams, commonly known as online scams, which have made the life of the netizens very hard indeed. These *scams* occur just like in real life – an innocent person is tricked into revealing private and confidential information lured by some kind of incentive. The only difference between real life scams and Internet scams is that the speed of the scams on the Internet is much faster, and much more devastating.

Tech-savvy netizens soon realised that they could trick other users into revealing personal information like credit card numbers, and bank account logins, if they could offer those users something tempting, like a prize or a free gift. It all began as an innocent lottery scam, and soon turned into something more dangerous. Today the Internet is rife with various kinds of online scams, which have made it hard for the average netizen to have a normal browsing session. It has become a serious problem indeed with thousands of people losing their hard earned money in a matter of minutes. Such incidents take place everyday, and the situation is very grim as of today, with the future inclining towards the worse. Unless some definitive action is taken against these scams, they cannot be stopped. But then, who can control faceless criminals who hide behind their computers? This is theoretically impossible, and impractical. So where does the solution lie?

2. Types of Online Scams

There are varied kinds of online scams circulating the Internet today.[3] All attempts to stop these scams have failed in the past, and that is because the scammers are learning fast from their mistakes and are making it hard for the officials to track them down. That is why these scams are still rampant and they continue to unleash their havoc on unsuspecting netizens. The prominent kinds of online scams are listed below.

- Phishing
- Lottery Scams
- Video Scams
- Identity Theft
- Scareware

These are just a few of the most common kinds of scams presently circulating the Internet. There are still other forms of scams such as intellectual property scams, money order scams, wire transfer scams and so on, but they have begun to decrease in number because they have been controlled to some extent due to stringent security measures at banks.

3. Reason Behind Online Scams

The most common reason behind online scams is to extract financial information from the targets, which can then be used to transfer any amount of money to the scammer's personal bank account. [2]The complexity of these scams may range from a simple credit card theft to a major identity theft case. It is not always clear what the scammers' real intention behind the scams is, but their short-term intention is definitely to get a large sum of money and abscond with it as soon as they can.

The only reason behind the success of these online scams is that a lot of netizens are scared of browsing confidently on the Internet. This is true especially when they have only begun using the Internet. They seem to doubt their every move, and look for assistance at each step. When they are in this phase, they are gullible to a certain extent and they tend to do whatever they believe is true. So when they receive an email that appears to be genuine and which claims to be from their bank, they do not think twice before they click on the infected link in the email.

4. Explanation of the Common Online Scams

Due to the complexity of the online scams, it can be hard for a novice Internet user to recognise each and every scam. The large variety of scams makes it even harder for the user to stay away from the traps set in multiple websites. That is why it is necessary to have a sound knowledge about the working of such scams, so that they can be recognised and prevented, if not eradicated entirely.

4.1. Phishing

This is one of the earliest forms of scams. *Phishing* refers to the process of creating a fake webpage that looks exactly like the webpage it is mimicking. [6]This is usually a bank or credit card website. The target user is sent a cleverly disguised link through email, causing the user to believe that the email has arrived from the real bank or credit card company. When the user clicks on the link, instead of being led to the original website, the fake website shows up instead. The unsuspecting user enters his/her login credentials into the webpage, which are then sent to the scammer's harvesting page, which is usually a text file, with a script to collect the login credentials. Once the login credentials have been entered, the user is then automatically redirected to the original website, being none the wiser about the collection of the login credentials by the fake webpage. This is the basic working of a phishing scam. Over the years, it has risen in complexity and the user is literally left clueless about the whole scam. Once the scammer has the user's login credentials, he can easily modify the user's account, and

send the money to his own account. All this happens within a matter of minutes, and before the user knows it, all of his/her life savings could disappear into thin air.



Fig. 1. An example of a phishing page, mimicking the original bank webpage.

E-mails like the one shown are hard to recognise by a novice user, and thus he unwittingly falls into the trap. In spite of the bank websites warning their users to ignore such emails, there are still a lot of users who get scared of the threats issued in the emails, and they go ahead and click on the phishing link. This single scam alone has been the reason for the loss of millions of dollars all around the world.

4.2. Lottery Scams

This is another form of phishing where the damage is much more serious. Similar to the phishing scam, the user receives an email from a supposedly genuine source, claiming that the user has won a lottery conducted by a particular organisation, and to claim the prize, the user needs to reply to the email immediately with the requested details. [1] The prize mentioned is usually a large amount of money, sometimes running into millions of dollars. The user, taken aback by such a huge number, usually fails to realise that he/she had not participated in any such lottery. The promise of money generally puts rest to all logic in the user's mind, and he/she falls into the trap, in the same way as a fish falls into a fisherman's net.

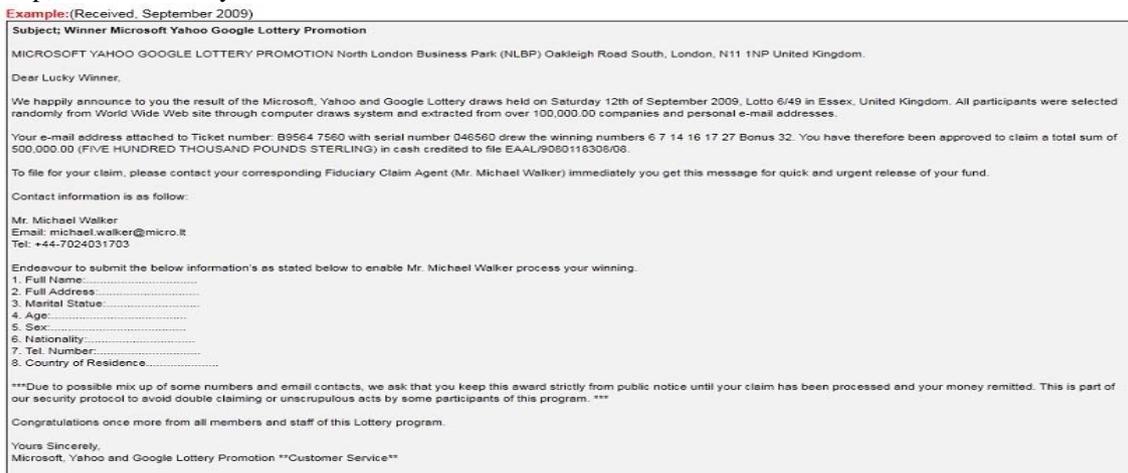


Fig. 2. An example of a lottery scam email.

In reality, there is no lottery and there is no prize waiting for the user. It is all just a hoax, intended to get the personal details of the user, and also a lump sum of money, which is extracted from the user under the guise of *processing feed*. The innocent user does not think twice before sending in any amount of money to the scammer, thinking that the prize would cover this amount as well. Sometimes the scammer asks for more information, such as copies of the user's passport, driving license and so on. This could in turn become a case of identity theft, where the scammer could use the personal information of the user for scrupulous purposes.

The only reason such scams still exist is that the scammers have become smart. They have started using the names of reputed organisations such as Google and Microsoft, to lure their targets into believing that they have won a lottery. Once the users see the names of reputed companies at the top of the mail, they tend to believe that it is a genuine email indeed. Then they go ahead and contact the scammer without thinking even for a moment that none of what the email contains makes any logical sense at all.

In these kinds of scams, the scammer plays with a person's psychological need for money, and the trick works to a large extent as well. The promise of a large amount of money is enough to make even an educated college graduate get tempted to play along. What these people do not realise is that once their money and information have been harvested, they will never hear again from these lottery organisers. There have been many complaints made to the cyber police in various countries about these lottery scams, but just as in the case of the other scams, these are hard to stop unless the users stop falling in such traps.

4.3. Video Scams

If Web 2.0 was all about blogs and news portals, the next generation of the web is all about videos. The success of YouTube is a remarkable example as to how the netizens have completely embraced videos to get the information and news that they're looking for. This rising interest in videos caught the attention of spammers, who then used it to create a whole new way of scamming people out of their money. This scam, however, is a bit more complex than it seems.

The process of video scamming involves tricking the user into viewing an infected video. Once the user tries to view the video, he is instructed to download a codec to view it. The video usually has a very catchy title that is hard to resist, so the user goes ahead and downloads the codec, determined to watch the video at any cost. However, the codec is nothing more but a piece of malware, which settles itself in the users' computer, and silently tracks all the activity that goes on. This malware could even be a key logger, which records all the strokes of the user's keyboard.



Fig. 3. An example of a fake video.

Videos such as the one shown above are hard to resist by the average netizen, and they do get a lot of clicks. [4] Like the example shown above, a lot of video scams are now being run through Facebook, which is the world's largest social networking website. Since each user on Facebook has a circle of friends, who in turn have their own circles, such video scams get successful results due to the large spread of users on the website. Although

the intent of such videos is not always apparent, the users begin to notice that their computers start behaving very strangely after they install the *codec* which the video wants.

4.4. Identity Theft

Identity theft is a kind of scam that goes hand in hand with phishing. Scammers are always after the personal information of their targets, and they use this information to take over the personal identity of the targets. This is true as far as online identities are concerned. If an Internet user is not careful, he could lose his entire online identity, in the form of user accounts, bank accounts and any other place where he has an online account. Such online identity thefts are not uncommon. They have been taking place quite a lot over the last decade, and only recently have they slowed down to a certain extent.

The process of identity theft usually involves stealing all the personal information of the target user, by means of a phishing page or any other similar mechanism. Once the user has unsuspectingly submitted his information, the scammer uses it for his own personal gain, thus stealing the identity of the user completely. Such cases can only be dealt by contacting a cyber crime expert.

4.5. Scareware

Scareware is a relatively new kind of scam that has been pestering users only recently. However, it has quickly risen to the level of a serious online scam, and something that needs to be tackled with quite seriously. Scareware, as the name indicates, is something that scares the users into parting with their money. This *something* is usually fake anti-virus software, which scares users by showing them fake reports of viruses on their computers. [7] The software is installed on the user's computer by the user himself, although unknowingly, through some infected website or other source. Once the software has been installed, it locks the system registry, and hides itself from any genuine anti-virus software running on the system. Then again, it takes complete control of the computer, without allowing the user to remove it by any means. At the same time, it keeps showing fake virus reports to the user, and prompts the user to purchase a paid version of the *anti-virus* software in order to remove the viruses. The scared user usually pays for the removal of the *viruses*, but in most cases, this only makes matters worse, since the software refuses to stay quiet., and still doesn't allow the user to regain control over the computer.



Fig. 3. An example of a scareware software.

There have been a lot of instances where people have fallen prey to scareware tactics, and have lost their hard earned money. Scareware removal usually involves the re-installation of the operating system, because in most cases the damage done is very deep, and any attempts to remove the scareware through an anti-virus solution would be useless. This is the seriousness of the scareware software once it enters the computer. The only way it can be prevented is by not allowing any new software to be installed without checking how genuine it really is.

5. Preventing Online Scams

So far, only a handful of the online scams have been described. There are still a few more variations of these scams, which regularly harass users and attempt to steal their money. Sadly, the cyber crime division in any country cannot entirely stop these scams. This is because the scammers work through a network all around the world, and the cyber laws aren't clear to trace and nab these cyber criminals. This means that it is up to the user to be careful about staying away from such scams. If the average netizen is knowledgeable enough to recognise and stay away from such scams, then they can be prevented. Although it might not be possible to bring down the whole network of scams in a single day, gradual decrease in the number of successful scams will discourage the scammers to pursue their activities.

To recognise such scams, all the user has to do is to keep an eye out for the authenticity of the emails. Lottery scams can be easily avoided because in real life there is no such lottery which gives out millions of dollars without even registering the users first. Other scams, especially video scams, can be avoided if the user thinks for a while before clicking on just about any link that is sent to him. As for emails from banks, users should realise that banks *never* send emails to their users asking for their personal information. If there is any doubt regarding this, the user can call up the bank and ask them about the authenticity of the email. This will help the users steer clear of the phishing scams.

6. The End of Online Scams?

In the near future, there appears to be no end to online scams. This is because there are thousands of people around the world who are introduced to the Internet for the first time everyday. This means that as soon as they start browsing on their own, they lie exposed to the scammers' tricks. So no matter how many people are educated about the scams, there will always be an equally large number of people who are ignorant about these scams. From the law's point of view there is not much that can be done, although there have been some attempts to curb spamming, which is a form of scamming. [5]

The true end of online scams would be on the day when every person in the world knows about the existence of the scams, and stays away from them once and for all. In practice this is not possible, so it is up to each individual Internet user to be careful about the activities they perform on the Internet, so that they will stay away from online scams of any sort.

7. Conclusions

Although it is impossible to curb all forms of online scams in the near future, it is indeed possible for the average netizen to be safe from the dangers of such scams, by *staying away from them*. This might surely appear to be a challenge, and it will take some time to recognise and educate netizens about all such scams. However, for a smooth browsing experience, it is indeed essential that the netizens first learn about these scams, so that they can then proceed to have an uninterrupted browsing experience.

References

- [1] Hoax Slayer, *Email Lottery Scams*, available at <http://www.hoax-slayer.com/email-lottery-scams.html>.
- [2] Norton 360, *Types of Online Scams and How To Fight Them Off*, available at <http://www.norton360online.com/security-center/online-scams.html>
- [3] Online Fraud Guide, *Appendix 1: Common Types of Online Fraud*, available at <http://www.onlinefraudguide.com/common-types-online-fraud-detail/>
- [4] Techie-Buzz, *The Facebook Killer - The Facebook Scam*, available at http://techie-buzz.com/scams/fox-news-video-the-facebook-killer-facebook-scam.html?utm_source=recentpost&utm_medium=web&utm_campaign=recent_post
- [5] TG Daily, *Spam Ring Shut Down By Authorities*, available at <http://www.tgdaily.com/business/39749-spam-ring-shut-down-by-authorities>
- [6] Wikipedia, *Phishing*, available at <http://en.wikipedia.org/wiki/Phishing>
- [7] Wikipedia, *Scareware*, available at <http://en.wikipedia.org/wiki/Scareware>

Pradeep Kumar Puram. He obtained his B.E. Degree from Nagpur University in 1993, and his M.Tech degree from Osmania University. He is presently working as a Professor and Head of Department for the department of CSE in Vivekananda Institute of Technology and Science, Karimnagar, India. He has an overall academic work experience of 17 years. He is also the director in the IT Division of Cerebrum Software Solutions Pvt Ltd, Hyderabad, India.

Mukesh Kaparathi. He is a final year student pursuing his undergraduate degree in CSE at Vivekananda Institute of Technology and Science, Karimnagar, India.

Aditya Krishna Haas Rayaprolu. He is currently pursuing his undergraduate degree in CSE, presently in the final year, at Vivekananda Institute of Technology and Science, Karimnagar, India.