The 2014 Top Ten Internet Scams

1) **Nigerian 419 scam**

You receive an email from a person of either a wealthy family or in a position of responsibility. It is a desperate cry for help in getting a very large sum of money out of the country. A common variation is a woman in Africa who claimed that her husband had died, and that she wanted to leave millions of dollars of his estate to a good church.

In every variation, the scammer is promising obscenely large payments for small unskilled tasks. This scam, like most scams, is too good to be true. Yet people still fall for this money transfer con game.

They will use your emotions and willingness to help against you. They will promise you a large cut of their business or family fortune. All you are asked to do is cover the endless "legal" and other "fees" that must be paid to the people that can release the money.

The more you are willing to pay, the more they will try to drain your wallet. You will never see any of the promised money, because there isn't any. The scam has been used with fax and traditional mail, and is now used with the Internet. This scam is not new; its dates back to 1920s when it was known as the Spanish Prisoner's scam. The number "419" refers to the article of the Nigerian Criminal Code dealing with fraud.

2) **"Make Money Fast" chain emails**

This is a remake of the classic pyramid scheme. You get an email with a list of names, you are asked to send some small amount, say ten dollars by mail to the person whose name is at the top of the list, add your own name to the bottom, then remove the top name on the list and forward the updated list to a number of other people.

The author of this scam letter painstakingly explains that, if more and more people join this chain, when it's your turn to receive the money, you might even become a millionaire! These extraordinary returns are promised on the original investment. You are not investing much but the promise of a great return is a great lure. As with the previously circulating snail-mail version of this chain, the email edition is just as illegal. This is often called a Ponzi scheme after Charles Ponzi, who used this technique in the 1920s.

3) **Advance fees paid for a guaranteed loan or credit card**

You get an offer about applying for a "pre-approved" loan or a credit card that charges an up-front fee, ask yourself: "why would a bank do that?" These scams are obvious to people who take time to scrutinize the offer. Reputable credit card companies do charge an annual fee but it is applied to the balance of the card, never at the sign-up. Consider that these people do not know you or your credit situation, yet they are willing to offer massive credit limits.

4) **Lottery scams**

You are notified that you have won the lottery, often in a far country. You have visions of all of the wonderful things that you can do with the money. The visions of a dream home, fabulous vacation, or other expensive goodies you could now afford with ease, could make you forget that you have never ever entered this lottery in the first place.

This scam will usually come in the form of a conventional email message. It will inform you that you won millions of dollars and congratulate you repeatedly. All you have to do is to pay a "small" processing fee and the lottery winnings are yours.

5) **Items for sale overpayment scam**

This one involves an item you might have listed for sale such as a car, truck or some other expensive item. The scammer finds your ad and sends you an email offering to pay much more than your asking price. The reason for overpayment is supposedly related to the international fees to ship the car overseas. In return, you are to send him the car and the cash for the difference.

The money order you receive looks real so you deposit it into your account. In a couple of days (or the time it takes to clear) your bank informs you the money order was fake and demands you return the money immediately.

6) **Employment search overpayment scam**

You have posted your resume, with at least some personal data accessible by potential employers, on a legitimate employment site. You receive a job offer to become a "financial representative" of an overseas company you have never even heard of before. The reason they want to hire you is that this company has problems accepting money from US customers and they need you to handle those payments. You will be paid typically a 5 to 15 percent commission per transaction. When you apply, you are told to provide your personal data including bank account information, so you can “get paid”. Instead, you will experience some, or all, of the following:

7) **Disaster relief scams**

Tsunami, and Katrina have in common? Real disasters happen such as Tsunamis in Japan, 9/11, and Katrina. Tragic events where people are killed, survivors lose their loved ones, and everything they own. In times like these, good people pull together to help the survivors in any way they can, including online donations. Scammers set up fake charity websites and steal the money donated to the victims of disasters.

If your request for donation came via email, there is a chance of it being a phishing attempt. Do not click on the link in the email and volunteer your bank account or credit card information. Your best bet is to contact the recognized charitable organization directly by phone or their website.

8) **Travel scams**

These scams are most active during the summer months. You receive an email with the offer to get amazingly low fares to some exotic destination but you must book it today or the offer expires that evening. If you call, you’ll find out the travel is free but the hotel rates are highly overpriced.

Some can offer you rock-bottom prices but hide certain high fees until you “sign on the dotted line”. Others, in order to give you the “free” something, will make you sit through a timeshare pitch at the destination. Still others can just take your money and deliver nothing.

Also, getting your refund, should you decide to cancel, is usually a lost cause, often called a nightmare or mission-impossible.

Your best strategy is to book your trip in person, through a reputable travel agency or proven legitimate online service like Travelocity or Expedia.

9) **"Turn Your Computer Into a Money-Making Machine!"**

Although not a full blown scam, this scheme works as follows: You send someone money for instructions on where to go and what to download and install on your computer to turn it into a money-making machine… for spammers.

At sign-up, you get a unique ID and you have to give them your PayPal account information for the "big money" deposits you'll "soon" be receiving. The program that you are supposed to run, sometimes 24/7, opens multiple ad windows, repeatedly, thus generating per-click revenue for spammers.
These constant applications take over your computer and kill your performance.

10) **Phishing emails and phony web pages**

This is the most widespread Internet and email scam today. It is the modern day "sting" con game. "Phishing" is where digital thieves lure you into divulging your password info through convincing emails and web pages. These phishing emails and web pages resemble legitimate credit authorities like Citibank, eBay, or PayPal. They frighten or entice you into visiting a phony web page and entering your ID and password. Commonly, the guise is an urgent need to "confirm your identity". They will even offer you a story of how your account has been attacked by hackers to lure you into entering your confidential information.
The email message will require you to click on a link. But instead of leading you to the real login https: site, the link will secretly redirect you to a fake website. You then innocently enter your ID and password. This information is intercepted by the scammers, who later access your account and fleece you for several hundred dollars.

These scams are not new. They have evolved to take advantage of advances in technology. You remember when your mail box was stuffed with unwanted solicitations. Now, through the wonders of internet and email it less expensive and easier to distribute so it is your email mailbox that gets stuffed.