Scammers will set up fake charity websites and steal your money donated to victims of disaster. If you request for a donation to come via e-mail, there is a very likely chance of it being a phishing attempt. Do not provide unknown individuals with personal information, credit cards or bank account information.

#8 Travel Scams

Travel scams are the most attractive during the summer months. You [receive an e-mail for amazingly low [fare to an exotic destination, but book it right now, because the offer expires in 24 hours. If you call you'll find out the travel may be free, but the hotel is overpriced. Often times, you may be contacted via telephone to attend a "short" presentation in order to collect your "free trip." These presentations are hard sell and involve joining a club, or becoming a "travel representative" to the tune of thousands of dollars with little or no benefit to you, learning after the fact the "free trip" has so many disclaimers it is useless. Remember you should be provided a three day cancellation if you are attending a presentation at a hotel when you enter into the agreement.

#9 E-Mail Pyramid Scheme

The classic pyramid scheme: you receive an e-mail with a list of names and you are asked to send $5.00-$10.00 by mail to the person who name appears at the top of the list, add your name to the bottom, and forward the updated list to a number of other people. Keep in mind the list, add your name to the bottom, and forward the updated list to a number of other people. Keep in mind the list of names is more than likely being manipulated to keep the creator of the list on top permanently. Please remember this is the same as sending this through the US mail, it is fraud.

#10 Turn Your Computer Into a Money Making Machine

Although not a full blown scam, this scheme requires you to send 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.
The risk to your computer and identity are multiple from this scam.

WHO TO CONTACT

Johnson County District Attorney's
Consumer Protection Division
913-715-3003
http://da.jocogov.org

Internet Fraud Watch
http://www.fraud.org/

INTERNET FRAUD

From The
Office of the District Attorney
Tenth Judicial District

Stephen M. Howe
District Attorney

Johnson County, Kansas
CONSUMER PROTECTION

TOP 10 INTERNET SCAMS

#1 Nigerian Scam a/k/a 419

Most of you have received this e-mail it is a desperate cry for help to get a large sum of money out of the county. This scam, like all scams, is too good to be true. This scam is not new, its variant dates back to the 1920's when it was called 'The Spanish Prisoner' con.

#2 Advanced fees/guaranteed loans

If you are thinking of applying for a credit card that requires an upfront fee ask yourself "why would a bank require this fee?" Reputable credit card companies sometimes charge an annual fee, but the fee is applied to your balance, never at the time you sign up.

#3 Lottery Scams

Most of us dream of "hitting the jackpot" quitting our jobs and retiring. Chances are you will receive at least one intriguing e-mail from an unknown individual saying you've won a huge amount of money. The catch: before you collect you must pay a processing fee or taxes on this windfall. DO NOT FALL FOR THIS SCAM!

#4 Phishing E-mails

This is becoming one of the most wide spread internet and e-mail scams today. "Phishing" is where digital thieves lure you into divulging your password through very convincing e-mails and web pages. The e-mail appears to be legitimate, such as Visa, Citibank, PayPal where they frighten you to visit a phony web page requesting you enter your ID and password. Often times the e-mail will talk about how your account has been attacked by hackers or is at security risk to convince you to enter confidential information. Once you click on the provided link it will redirect you to a fake website. This information is intercepted by the scammers allowing them to access your account. If ever in doubt – contact your financial institute directly via telephone or in person.

#5 Items for Sale or the (Overpayment Scam)

This scam involves an item you may have for sale, such as an expensive car, truck or jewelry. The scammer finds your ad and sends you an e-mail offering to pay much more than the listed price. The reason for over-payment is supposedly related to shipping fees, transportation costs. In return the scammer wants you to send the item and the cash of what was left from the overpayment. The money order or check you receive will look real, but after the hold period the bank will inform you that the form of payment was fake and debit your account. In many documented cases the money order may genuinely be real, but was stolen and never authorized by the bank.

#6 Employment Search

You post your resume with some personal data on a legitimate employment site. You receive a job offer to become a "financial representative" of an overseas company you have never heard of. The reason they wish to hire you is that their company has problems accepting money from US customers and they need a representative to handle these transactions. You will be paid 5 to 15 percent per every account you handle. If you apply and are "hired" you will need to provide the scammer with your personal data such as bank account information, social security number, date of birth, etc., but instead of getting paid you may experience anything from ID Theft, money stolen from your account, receipting of fake checks or money orders, and sending funds that are not valid to "your employer." Never provide personal information or bank account information to unknown individuals.

#7 Disaster Relief Scams

What do 9/11; Katrina, Tsunami and Earthquake Reliefs efforts have in common? These are all disasters or tragic events that impact so many. In times like these, good people come together to help survivors in any way they can, including online donations.