Personal & Financial Computer Security, Online & Off

By Olen Soifer

The above picture is less of a joke than you might think. All conscienscious persons or companies, especially in any financial industry, are constantly concerned with protecting the security and confidential nature of their customer's or client's private information. However, our concern does not relieve your own responsibility to take all reasonable precautions to protect yourself, because computer, financial and online financial fraud is rampant.

Because no-one cannot constantly look over your shoulder to monitor what you do on your own to protect your own privacy, prevent identity theft, enhance your online experience, it can only be stressed that you must be especially prudent to gain your own awareness of the vulnerability of your computer and confidential information, both online and off. With this awareness, you can arm yourself with tools and techniques that will protect your PC &/or network, the information on it and the information you send and receive.

It is not suggested that you become paranoid about the possible dangers but, if you had been tracking this page since it was first written over 9 years ago, you would have watched it increase from 1 to 10+ printed pages. Part of this is because the author is continually on the lookout for new threats and solutions. Unfortunately, it is also true that threats continue to increase as "hackers" learn to exploit operating systems, browsers and software. Internet fraud is on the rise and it is estimated that as much as 80% of all emails are spam.

Be smart and keep returning to the listed tip links that are owned by people whose jobs are to keep up with the scammers. Ultimately, depending upon the value of your data and system, it is your own, sole responsibility to discover those measures needed to protect yourself, your privacy and your confidential information. As implied above, this responsibility must be a continual process, as no one-time installation of security measures can assure you of permanent protection as time passes.

Provided, below, is a list of computer-related &/or online-related actions you can take; information you should know, and links to sources of more detailed information, that will give a high measure of protection at work or at home. The volume of information is such

that you cannot be expected to take every precaution at once. But, over time, you should go through each section of this information and take every reasonable measure to protect yourself and your confidential information. Keep in mind that crooks and scammers are continually evolving and coming up with new schemes. It cannot be stressed often enough that fraudsters are more ingenious than we all might want to admit. It is your own personal responsibility to inform yourself about the newest scams.

Therefore, please be aware that, in reading this page and taking any action as a result of having reading the suggestions herein, you are acknowledging that you have read and understand the disclaimers at the bottom of this page. Because of the changing nature of computers and the online environment, and the nefarious nature of those who will do all that they can to steal confidential information, it is necessary to warn you that, as long as this document has become since it was first created, no guarantee can be made that it is complete or up-to-date at any particular time.

When possible, most of the programs mentioned in this article should be set-up to work silently, in the background, whenever your computer is on and, especially, when you are on-line. They are of little help if they are not running continually or are run only when a serious security compromise has already occurred.

1. **Install Virus protection, keep it up-to-date and keep yourself informed about new virus threats:** A virus' is a computer program that, like a biological virus, can invade other software or files and is able to generate copies of itself, and thus, spread. Most computer viruses have a destructive payload that is activated under certain conditions. Viruses need to attach themselves to another program to run, while a "worm" is a virus that can run by itself. "Trojan Horses" or "Trojans" are viruses that enter a computer hidden in a file that is voluntarily installed by a user. There are many pay and free virus protection programs. A good free program is AVG. Antivirus programs detect viruses by looking for virus names or "signatures" that are contained in a database you get when you install the AV program. It is most important that the virus database be up-to-date (set online updating to "on). Updates are available from the program's website, along with lots of other virus information. Here are a few of the major anti-virus sites: Norton Antivirus/Symantec, McAfee, AVG, Kaspersky, f-Secure. Also, click here to go to a link, below, that will help you make your Internet Explorer web browser be less vulnerable to online threats.
2. **Virus Hoaxes and other Rumors**...Be cautious about sending bulk email to friends and associates regarding virus threats or, for that matter, any rumor (a/k/a "Urban Legends") passed on to you thru someone else's bulk email forwarding. While there many viruses and scams you should protect against, there are also many virus & other hoaxes that are no threat...except for the result of, basically, false panic by Internet users. What usually happens is that a "reporter" publishes a story about a new virus threat without having verified what is actually a false rumor. Then, "helpful" people start warning against everyone they know and the warnings cascade and proliferate and the Internet slows down to a crawl. There is a big difference

between helping people you care about by warning of a genuine threat and panicking a nation based on the spread of a hoax because few people take the time to check their sources or the facts before passing on the rumor... 20 people spreading a rumor to 20 others, thru 6 generations, is 64,000,000 useless emails that waste a lot of internet bandwidth! Before perpetuating a rumor about a new virus, do you own checking at your virus protection program's website. Before spreading an "Urban Legend", read about these rumors at Snopes.com. If you have the time to spread a rumor, you should make the time to research it!

3. **Use caution when selecting an anti-spyware program:** Some of the hardest Trojans to remove are, supposedly, anti-spyware programs called Spy-Axe and Spy Falcon. These malicious programs cause popups that warn you your computer is virus infected (even if it is not...) and try to get you to buy their product. When the Trojan infects your computer, it will change your computer's registry, add files and DLL's, hijack Internet Explorer, etc. Removing them manually can be time-consuming (10 hours or more); they may require a new install of Internet Explorer and may not be removed by many genuine anti-spyware programs...we, however successfully removed it with SuperAntiSpyware.
4. **Regarding free stuff for your computer: Most of this has a hidden price** (including Trojan horses that get installed with the gift). Be cautious about downloading and installing anything that is supposedly free because they usually come hidden price. The biggest offenders are screen savers, search tool bars, automatic dialers and anti-spyware programs (see #3, above), etc. "Free Downloads" are a major source of viruses and Trojan Horses. Unfortunately, there is a big difference between actual "freeware", truly free programs, and programs that are advertised as being a "Free Download". Most free downloads are really "shareware"...these are free for awhile but, at some point, they stop working fully unless you pay for them: They may be partially "crippled" from day one, until you pay, or they may (such as many virus scanners) detect problems on your computer for free...but only fix them for a price. If you don't pay, you may also be in for endless "dunning" until you pay or delete them. Deleting them (such as Spy Axe) is sometimes virtually impossible. Again, use caution regarding free downloads. Remember the saying, "There's no such thing as a free lunch."
5. **Use a program to prevent the downloading of "phishing" or "Trojan horse" software.** Free programs such as SPYBOT and MICROSOFT ANTI-SPYWARE are quite good. SuperAntiSpyware has a free and a pay version (with more features) but the free version works quite well.
6. **PHISHING...Be very cautious if you receive an email that asks for you to confirm confidential information.** This may be a "phishing" email that is just trying to get that information for use in identity theft. For help in detecting these phony emails, read this article from the FTC and check out the Anti-Phishing Working Group. It is likely that, sooner or later, you will receive very legitimate looking emails from E-Bay, Chase Bank, Mid-America Bank, etc. asking you to confirm your account &/or password information "or your account will be deleted or deactivated..." or even an email from the IRS claiming that you are due a refund if you fill out a realistic-looking form (or can get money for taking a survey, etc). BUT, legitimate companies or governmental agencies NEVER ask you to confirm

confidential information, like that, by means of unsolicited emails. Report these emails to the appropriate authorities. If you receive a suspicious email that asks you to confirm confidential information, passwords, etc, you may want to forward it to check@phishfraud.com and they will email you back after looking the email over. Contact the appropriate company or check their genuine website for an email address to which you can forward the suspicious email (such as phishing@irs.gov). Any company that has been the subject of phishing fraud will most likely provide such an email box.

7. **ADVANCE FEE FRAUDS**...Be cautious of emails offering you a huge amount of money to help get money out of a foreign country...most notably, Nigeria, but it could be anywhere. This is just one kind of "advance fee fraud". Even if the fees are not very large, you will still, generally, end up giving out your confidential banking information. Read about the "4-1-9 fraud" here or here. Most of the time, you should be aware of ANY offer that requires you to provide confidential financial information or asks for advance fees...unless you are dealing with a government-regulated company. Advance-fee scams have cost some persons a fortune and have gotten others killed. To make themselves appear legitimate, the crooks will often create websites that appear to be legitimate banks or even government websites. You may think you have done your own "due diligence" by visiting the site and convinced yourself that it is legitimate. You may very well be wrong! You can find a list of regulators here and here is a list of phony banks & other companies used to perpetrate fraud and here are more phony banks. Again, these website constantly appearing and can look very genuine, so use extreme caution before assuming they are genuine.
8. **Unfortunately, using the "opt-out" link in much unsolicited email may make matters worse.** The opt-out option is a government requirement for unsolicited emails, but spammers often use it as a trick to have the recipients verify that their email address is "live". More often than not, the result of opting-out will be more, not less" spam because the same people who send you the unsolicited mail and get an "opt-out" back, will not be able to make money by selling your confirmed "live" email address to bulk emailers.
9. **OPT OUT!** Sign on to the Federal DO NOT CALL list if you want to minimize unsolicited calls. Go here. This is a phone, rather than a computer, issue. But, of course, the source of phone numbers is often from Internet forms. If you continue to receive calls after asking to be put on the don-not-call list, make a complaint by going back to the donotcall.gov website. The fines for soliciting people that are on the list are huge. Click **here** for an article about the "top ten" opt-out services that can minimize various unsolicited contacts. For more information, read the other articles available at the **World Privacy Forum**.
10. **Never click anywhere within a pop-up window except the "X" at the extreme upper right**...that includes avoiding the "cancel" button or some such similar button. If you use Google for searches, consider installing their free pop-up blocker on the Google Toolbar. It works as well as many pay blockers and avoids the annoying hidden software that is often downloaded unknowingly with "free" pop-up blockers.
11. **Consider using a "disposable" email address** (hotmail, etc) for online dealings that will not require future contacts or when it is possible that furnishing your email

address may result in spamming...so, if need be, you can just close that email box. There are programs to filter emails but none are perfect and you always risk filtering out at least some desirable email.

12. **E-Mail Spam**...IncrediMmail and various other email programs can be programmed to automatically sort out junk mail, but you may have to buy a "for pay" version to get the best results. It may also take some time to set up just which mail to dump and "tune it" to minimize how email the programs trash which you wanted to receive. Most of these programs that sets up a spam folder (sort of a spam recycle bin) to which the "spam" emails are directed. If you are missing important emails, they are probably in that folder. It is suggested that you do NOT set up this folder to periodically, automatically empty itself.

(See, also, scams perpetuated online, below.) In ANY of the following instances, you should delete unsolicited emails without reading them and, NEVER NOT open any attachment in an unsolicited email. To do so could cause a Trojan to be installed on your computer. In terms of specific spam, here are the worst offenders: **Confirmation Requests: (See Phishing, above)** These claim to be from a bank, Ebay, UPS or FedEx, a credit card company or other supposedly legitimate source. It could claim to be from any possible source that legitimately has your confidential information. The email may claim that the security of your account was compromised or it may claim that your account is about to be cancelled. In either case, you will be requested to verify confidential information about yourself or your account. **Foreign pharmacies**: Some of these are legitimate, some are not. Those that are not might take your money and run or steal you identity from your credit card purchase. Caution!!! Those that are legitimate will have secure order pages, and will provide reasonably fast, efficient sales and delivery of quality generic (usually) medicines. Here are two legitimate firms: Budget Medicines and OffShore Rx. We let you decide about the legality of ordering prescription medications from outside US borders. **Stock Tip Spam**: Stock spam is email that touts stock, usually penny stocks, as about to rise dramatically. They tout real companies, but their information is not to be believed. Their goal is to get stocks to rise for a little while and then they dump their own shares. One study of 37 stocks showed a drop in value after this spam came out, of 86%. The folks who put out this spam are crooks and they are breaking the law. See the Security & Exchange Commission article about "micro-cap" stocks. **Lottery and Contest Scams:** The chances of you winning the Irish Lottery or some such legitimate lottery are exactly zero if you didn't buy a ticket. The chances of winning a contest from Wal-Mart, or some such company, without having entered a legitimate contest are also zero. Wal-Mart didn't become the world's largest retailer by giving away their money at random! .**Loan Scams:** Offer great rates and terms, but all they want is your confidential information, so they can rip you off; and your application fee so they can steel even more from you. **Employment or "Friendship" Offers:** Another scams to get your upfront money (Who pays to get a job or a friend???) and your confidential information. **Knock-off watches, etc**: You can buy this crap at your local large "flea" market...and you don't risk identity theft! **Ponzi Scams:** Smaller

versions of Bernard Madoff's scam. Earlier investors are paid unrealistically high returns out of the later investors' funds. Sooner or later the gravy train derails.

13. **Consider eliminating "click and email" links to email addresses on your web pages.** There are many Internet "worms" that search the web for email addresses. The email addresses that are "harvested" by the worms are added to bulk email lists and the addressees end up bombarded with "spam". If you have your own web page, a good way to avoid this spam is to replace email contact addresses on web pages with an email form or help ticket program. Talk to your Internet provider about making this change if you are being slammed with useless spam. On blogs or other such pages, you should probably select the option that hides your email address, if that option is available.
14. **Don't open any attachment to an email unless you know who the sender is.** If you do choose to open an unknown attachment, you should have protection installed, such as ZoneAlarm (which includes email protection), or another program that scans for dangerous email attachments that can harm your system. Viruses have been sent in seemingly harmless screen savers, as "love letters", etc. In a really ominous twist, they have been sent as software purported to be protection from viruses, when in fact what was sent WAS a virus. One of the most prolific "worms" is presently spreading thru the web in an email stating it is from the FBI! Also, in the past, images and text attachments were generally considered safe to open...that is no longer the case. Finally, you should be extremely cautious if you try to play an online video and the response to your "click" is a pop-up telling you that you must first install a "codec". These are almost always some form of adware or spyware that you would be voluntarily installing!
15. **If emails you send or receive are valuable and sensitive, you can get encryption software like PGP** (Pretty Good Privacy) that uses 2 different software keys to scramble and unscramble your message. A public key that you freely distribute scrambles the message, but only your private key can unscramble it. If the people you correspond to want the same protection, they need to get the software, generate their own keys and provide you with their public key. PGP is free for private use. You can also use S/MIME (Secure Multipurpose Internet Mail Extension) that is similar to, but incompatible with, PGP. A free S/MIME toolkit is available here.
16. **Get a firewall to control who has access to your computer or network from outside the network**, via the internet, etc. ZoneAlarm is just one that is available and is free for private use. As mentioned, above, ZoneAlarm also includes email protection. See here for a bit more firewall information and tips for ZoneAlarm. If you think you may have been "hacked" (broken into from the internet), you should perform a search of your PC &/or network to see if the hacker has installed a hidden web server such as Back Orifice on it. With no firewall and BO installed, your hacker can access your machine as if he were sitting right at your keyboard...write, change, delete files; change settings, etc. Here is more information on dealing with BO type servers.
17. **Be cautious of Word and Excel documents that are sent or given to you if they contain macros**. Other programs that generate documents with macros should be suspect also. Macros can be tremendous adjuncts in documents, but can be made to

damage computers/data also. In Microsoft Word or Excel, you set the macro security level by clicking Tools, then Macro, then Security. A security level of medium is adequate for most users. It lets you choose in each document you open whether to allow the macros to run, or not. Word or Excel files you download for our site are either written by us or checked, to the best of our ability, to ensure they are safe.

18. **Ask your ISP if they try to ensure secure transmissions** through the use of SSL or other measures. Generally, in order for transmissions to be fully secure, both the initial ISP and the final recipient's ISP must use the same security measures, unless you are encrypting your documents yourself. Realize that an email or web page may go through 30 or 40 computers/routers to get to its destination.
19. **Use random passwords rather than names, addresses, phone numbers, etc.** One of the most annoying things we have to deal with is the requirement, by cautious financial services providers, that passwords be changed often. But, one of the most foolish things that many people do is to create easily guessed passwords, or passwords that are identical to their user name. A quick way to come up with a password that is random, but easy to remember, is to use the first letter of the first six to 10 words of a favorite poem, song or bible verse, etc. Such as: "Ring Around The Rosie, Pocket Full Of Posies", generates a password of **ratrpfop**. Again, the password is random but the phrase that generated it is easy to remember. (By the way, that little song isn't as happy as it sounds. It was written during, and describes, the Black Death Epidemic in Europe.) If you insist on using a password that might be easily guessed, include, at the very least, a symbol such as a "dollar sign", or something like that, to make it a bit more secure. Even if it is not required, it is best to change passwords periodically. It is also wise to NOT use the same username and password for every one of your online accounts.
20. **Don't write down passwords where others can find them and don't give your passwords out to others,** either in person, by email or on the phone unless you are sure of who you are talking to AND sure they will not abuse the information. There are a number of free programs that can store passwords, and other confidential information (addresses, account information, etc), on your computer, in such a way that a hacker (or even a person who accesses the computer in person) cannot read the information. Go to nonags.com and "search software" for "password security". (Software found on Nonags is genuine freeware.)
21. **In general, you should always guard your confidential information and give it out sparingly to others**...and that even includes lenders! Make sure the lender you are talking to is genuine...check licensing, etc...If you are not sure, don't give out the information. REMEMBER, it is not appropriate to have your social security number on a driver's license any longer. If you have an older license with the SS#, replace it.
22. **Consider paying for identity protection:** Services such as LifeLock, TrustedID, IdentityGuard and ID-Watchdog guarantee to protect &/or restore your identity, some with an up to $1,000,000 insurance policy. Other services, like Debix, carry no insurance because they insist that their protection is complete. Debix is only $24 per year. The other services listed range between $84 and $150 per year, if paid annually. (Total yearly charges will be higher if you choose to pay monthly.)

23. **Use a "re-loadable" debit card for online payments:** These can prevent recurring payments that you did not authorize OR payments for unauthorized merchandise from being charged to you. One option is Paypal. Paypal did have a recent, serious security compromise, but it will probably be corrected quickly as Ebay, who cannot afford to NOT do so, owns it. Another option is a re-loadable debit card. These can be "re-loaded" online from a normal credit card and can be left at a low balance until you need to charge something to them. Netspend is probably one of the better ones, here described by one user: "They were the only one I found that doesn't have any application fees, membership fees, minimum balance, need a checking account or have any recurring monthly fees. You pay a one-time $20 set-up fee, $1.50 to reload it and $1.00 per transaction." (If you have a vendor that continually keeps trying to collect money from Netspend after you have notified them that this was not authorized, Netspend will cancel the card and issue you another one. That is more convenient than trying to deal with a traditional credit card company to get them to reimburse you for unauthorized charges.)
24. **Use a "re-loadable" debit card for ANY payments and Be cautious of ATM machines:** A new scam involves crooks attaching devices to the front of ATM machines which steal the information from your card's magnetic stripe AND record the PIN number you enter. These attachments can appear quite genuine. You should always be suspicious of any ATM machine whose card reader sticks out beyond the rest of the machine. But, you may also want to obtain a "re-loadable" debit card to carry with you. SEE the previous article, above. The idea would be to transfer money to the card from an ATM you could trust, such as one inside a bank's lobby. Then, that is the only card you would carry. Even if you lost the card, it was stolen or if it was compromised, you could only lose the present balance and it could easily be cancelled and replaced. These cards will usually be accepted anywhere a legitimate (ie: Visa) card would be.
25. **Beware of scams perpetuated online:** Many of these could use print ads or direct mail to offer their scams and many do so along with the internet...so they are being mentioned here. Some scammers have been around for years and just "change skins" if the get caught. The Internet makes that easy. Before being roped into any moneymaking opportunity, check out what other people say about them. As your mother told you, "If it sounds to good to be true, it probably IS too good to be true!" Whether it is a "great" home business, or a HYIP ("high yield investment program"), you should always be cautious before investing money or disclosing confidential information. Go to ripoffreport or World Wide Scams to see what other people are saying about, for example, Bruce A. Berman or Carlton Sheets. For an honest critique of a whole host of "real estate gurus", go to John T. Reed's website. Be very cautious of sites, that seemingly rate moneymaking opportunities...unfortunately: Most of them are fraudulent sites owned by the very people or firm(s) they are "reviewing". You should GO HERE to read about a HYIP/Prime Bank opportunity...but READ EVERYTHING and click the links before you get too excited.
26. **If you are worried about access to sensitive data on your PC, you can store it on removable media** like floppies or CD's or install encryption in your file storage.

You may want to consider encryption software for your entire hard drive. ScramDisk is one example. You can also use PGPDisk that is free up until version 6.5.

27. **Java, JavaScript and ActiveX scripting in web documents can be used to create havoc on the machine of someone receiving the page.** If you are nervous about that, then disable Java and JavaScript. In Netscape, click Edit, Preferences, Advanced and deselect Java/JavaScript. In Internet Explorer, click Tools, Internet Options, Advanced and scroll down to Java VM. Deselect the 3 Java settings. You can also select Security in the Internet Options and raise the security level in the "slider". Bear in mind that turning off Java/ActiveX/ActiveX may disable portions of many web pages these days.
28. **Many pages use cookies to keep track of people that have been to their pages previously.** Some information about you is handed out when you return the cookie by revisiting the page. If this worries you, you can change settings in the advanced tab (see above) to refuse cookies or be asked if you will accept them. For the most part, either choice makes annoying pop-ups appear on your machine. The better choice is to get shareware, like Cookie Crusher, that lets you delete cookies, or deals with them as they are about to be handed to your PC.
29. **Consider using a true browser like Opera or FireFox which are free, or Netscape, except when the site you are accessing will not work anywhere except Internet Explorer.** Unfortunately, Internet Explorer is actually a web server that acts like a browser. It's server aspects make it subject to hacking that lets it transfer your private information to the hackers. On the other hand, removing IE, if your operating system is Windows, is probably not practical because it is firmly interwoven with the operating system. You can, however, take steps to secure your web browser by configuring those IE features that are the most vulnerable in an online environment. In an online software application you must use will only work with IE, pester the manufacturer to make the application work with other browsers.
30. **Keep your operating system and software updated with the latest security updates available from the manufacturer's websites.** For Microsoft operating systems and software, click here. Apple/Macintosh updates are available here. It is suggested that you check for updates manually, and periodically, as the automatic updating that is available can intolerably slow down your computer.
31. **Investigate spam-blocking software that can automate the process of rejecting and deleting unsolicited emails** that can clog your in-box. An email program called IncrediMail that is available in a free version and works nicely with Outlook and some other standard email programs. There are some nice graphic features that you may like, but we especially like spam/fraud blocking abilities it provides. Our initial experience with IncrediMmail is that it has not included any unwanted "Trojan Horses" or other nasty things. Cloudmark has similar spam/fraud abilities, but it features become limited after a month, unless you agree to start paying a monthly fee. Unless you enjoy being solicited to: buy replica watches; accept a mortgage with impossibly low rates; enlarge your penis, breasts (or both); or enhance your sex like with drugs (proven successful or otherwise), you may want to consider one of these products.

If your computer has been "hacked" or someone has perpetrated a computer crime against you, file a complaint with the Federal Trade Commission. You may also consider contacting your (US) state's Attorney General's Office or the Attorney General's Cyber-crime Department (or your country's equivalent) and (in the US) the Internet Crime Complaint Center or contact the FBI's National Computer Crime Squad (NCCS) at nccs@fbi.com or, by telephone, at (202) 324-9164. Here is another page of US Federal and State law enforcement agencies. The appropriate foreign agency may be obtainable from the particular country's embassy. If you suspect that your "identity has been stolen", read here about filing a Fraud Alert and ID Theft Affidavit with the three major credit repositories.

- Other agencies involved in investigating computer and internet crime include the US Secret Service, the US Postal Inspection Service and the Dept. of Homeland Security, the Internet Fraud Complaint Center and the Identity Theft Resource Center. The crimes that these organizations investigate, and attempt to educate the public about, include, among others: invasions of privacy, identity theft, industrial espionage, threats to computer networks or crimes involving 2 or more computers in different states and crimes in which a computer is a major factor in committing the crime.
- As mentioned above, while there is a lot of information here, a web page of this nature can hardly be more than a summary of information and suggestions because crooks are ingenious and new schemes appear faster than they can be listed here. Especially in regard to obtaining information regarding computer privacy issues, it is suggested that you visit the some of the above-referenced sites and the Electronic Privacy Information Center because they will be more up-to-date than this document can be. There is also a more complete list of software resources for computer privacy from the EPIC.
- **MORE About Scams:** As mentioned above there are many scams that appear on the web or in email solicitations, and it is beyond the scope of this document to describe most of them. In addition to links listed above, here some other sites that discuss, or network about, financial and online scams and frauds: FCIC, ScamPatrol, HotScams, Hoax-Slayer, ScamVictimsUnited, FraudAid, Quatloos, Scambusters, ripoffreport. and World Wide Scams.
-
- *IMPORTANT: Always be cautious of sites that purport to expose scams...but then go on to suggest that a particular "opportunity" is the "only" legitimate one they have found.* That, in itself, is probably a scam. As mentioned above, most, supposedly impartial sites, that rate moneymaking opportunities...are owned by the very people or firm they are "reviewing". Another, surprising, place to learn about frauds is YouTube.com because the submitter of a clip probably had to be quite angry after being "ripped off" to make a film about it.

- ***THIS PAGE CANNOT POSSIBLY HOPE TO BE COMPLETE OR UP-TO-DATE AT ANY TIME BECAUSE NEW SCAMS AND THREATS ARE CREATED CONSTANTLY. IT IS YOUR RESPONSIBILITY TO BE CAUTIOUS IN REGARD TO ALL OF YOUR ACTIONS. A NUMBER OF EXCELLANT LINKS HAVE BEEN PROVIDED HEREIN AND YOU MUST MAKE EVERY EFFORT TO BE EVER VIGILANT BY SURVEYING A***

VARIETY OF THOSE LINKS FREQUENTLY. IN USING ANY SUGGESTION ON THIS PAGE, YOU ARE ACKNOWLEDGING THAT YOU HAVE READ AND AGREE TO THE FOLLOWING DISCLAIMER.

Disclaimer: **Neither the author, nor the site, or host thereof, where this article was found, can guarantee that this page is fully comprehensive or up-to-date, or that the suggestions herein (or linked hereto) are safe on all, or any, systems or in all situations or any particular situation.** ***Every effort has been made to provide this page as a valuable security resource. However, as a condition of your use of this page, or any information within it, you acknowledge that you are aware that this web page includes no guarantee that it is current or all-inclusive of every possible threat or solution that exists. In addition, you agree to hold the author and website, or organization hosting this page, completely harmless in the event any loss of any kind is suffered as a result of taking any or all of the recommendations herein, or on any other page within this website or on site links within our pages. Furthermore, you acknowledge that links on this page are suggested with the best of intentions but neither the author, this site nor its host are not responsible in any way for the content of the sites or links listed herein. All sites referenced herein are listed as a public service. No copyright infringement is intended and the original authors retain all of their rights under the law.***