

## [Hoax emails a common type of email fraud](#)

Hoax Emails has become very common sight in the email Inbox these days since E-mail has become an essential mode of communication in the modern world. Unfortunately, that means it's also one of the most common routes for virus infection and fraud. Below are some of the most common email frauds that are committed using this method.

**Phishing Scams:** A high tech "Phishing" scam which uses pop-up or spam messages to deceive you into disclosing your personal information such as passwords, bank account or credit card numbers, Social Security numbers or anything that is confidential. The object of this hoax email scam is Identity theft. The fraudulent email is sent from the phisher that is designed to look to be sent from a reputable company. But when you click on the web link in the email it directs you to spoof site that looks like the reputable company completing the email fraud. Usually the message are asked to "update" your account information or it says that the account has been locked or hacked and ask you to click on the web link provided to correct the problem and once you do and enter your information it goes directly to the phisher that uses your information for identity theft which is used to make withdrawals from your bank along with credit cards or to request new credit cards which are quickly maxed out, etc. Recent phishing attacks have spoofed the email and websites of known companies, including Yahoo, Pfizer, Bank of America, Microsoft, and eBay, PayPal, among others.

**Work-At-Home Scams:** This scam is a hoax email that has tempting spam offers. In these message are the opportunity to make extra money along with the chance to do so also usually in the email it will say "no experience necessary." Usually the sender will say that they have "inside information," and will bait you with the lure of little or no effort easy money that can be made. Of course you are asked to pay from about \$35 to several hundred dollars to purchase the material and kits that are need and will not make you a dime. Other types of this email fraud exist that offer other types of easy money and employment however they are the same type of scam. Examples of this kind of scams will offer opportunities to stuffing envelopes, making handicrafts or medical billing from your own PC out of your home. Falling for these email fraud and paying for envelop-stuffing or handicraft material and completing the work you will be told your that poor quality of product is not worth anything. Should you sign up for the medical billing business you will be required to purchase a list of doctors. In list you will find that the doctors don't exist or are not interested in your services and never really wanted them. Similar opportunities are also sent in hoax emails as well that make similar claims.

**Credit Repair Scams:** This scam offers the promise to erase real or usually correct negative information that shows up on your credit report, in the hoax email it usually says that you can qualify for unsecured credit cards, loans and mortgages, etc. Due to the current credit problems that many people suffer from this email fraud has become a very popular scam. The offered services usually don't live up to their promise and in some cases they cause many other problems in the long run. Also they have been known to make bad suggestion such as committing fraud e.g. lying about your social security number.

**Guaranteed loans on easy terms:** Some scam hoax emails make guarantees of unsecured credit, such as home-equity loans that have no require equity in your house or credit cards no matter what your history of credit. This is another popular type of email fraud again due to people with credit problems. Usually the offered credit comes from off-shore bank. The scam email fraud is usually part of a pyramid scheme, which encourages you to earn money by signing up your family and friends to participate in the opportunity potential. After you find out the promised offers of home equity loan turns out to be list of lenders that is useless and they will turn you down since you don't meet the qualifications. The promised from the pyramid money-making and promised credit cards never come through and the schemes usually collapse.

Other common hoax emails that you will see are listed below. Usually key tipoff's will show in the subject line or in the content. Instead of your personal name they use common address such as "Dear valued customer." However it is not that hard to find a variant of your name these days. In either case it is best to beware, in either case. Free giveaways supposedly in exchange for passing on emails or bogus virus alerts or pointless petitions that lead nowhere and accomplish nothing, or false appeals to help sick children and completely fictional, warnings about companies, government policies, warnings about products or coming events.

There is no easy way to avoid these email fraud messages there is specialized software that can detect hoax emails along with phishing, though it hasn't reached maturity - it often identifies legitimate e-mail as fraud. Always treat requests for passwords or credit card numbers with suspicion. Remember, no legitimate financial institution will ask you to verify your password or sensitive data in an e-mail. The good news is that, with a little bit of foreknowledge, Hoax emails are easy to detect as email fraud. Hidden within the colorful prose of your average email often lurk telling indicators of the email's veracity.

## About the Author

[Email fraud and hoax emails](#)