ATTORNEY GENERAL GEORGE JEPSEN WARNS CONSUMERS ABOUT SCAM EMAILS, OFFERS INTERNET SAFETY TIPS

We have all received e-mails containing get-rich-quick schemes, warnings of viruses, or images exploiting the latest natural disaster. These e-mails are more than just an annoyance: they may also have a malicious purpose. Besides trying to fraudulently gain access to your personal identifying information (such as Social Security numbers, checking and credit account numbers), such an unsolicited e-mail, also known as "spam," may bog down networks and clog inboxes, and malicious spam may harvest e-mail addresses, spread viruses, install spyware, or simply seek to cause fear and confusion. Past pernicious e-mails have exploited tragedies such as earthquakes, plane crashes, political instability in other countries and terrorist incidents to entice people to open attachments, forward the message to others, and send money to scam artists.

Some messages are more suspicious than others, but be especially cautious if the message has any of the characteristics listed below. These characteristics are just guidelines – not every scam e-mail has these attributes and some legitimate messages may have some of these characteristics:

- The message includes a warning to keep all communications secret or confidential ~ there's no reason why a complete stranger should ask you to keep secrets;
- There is a statement in the message urging you to forward the message;
- The message suggests bad luck for failing to perform some action;
- The message entices you financially by making promises of an award, money, or gift certificates for performing some action;
- The message offers instructions or attachments claiming to protect you from a virus that is supposedly undetected by your anti-virus software;
- The message claims it's not a hoax;
- There are multiple spelling or grammatical errors in the message, or the logic is contradictory;
- The message has already been forwarded multiple times (evident from the trail of e-mail headers in the body of the message).

What are some commonly reported e-mail scams?

Phishing Scams – Under the guise of selling goods or services, a scammer sends solicitations by e-mail seeking your personal and financial information. To appear legitimate, the scammer may even use the name, address, logo or design of a real business to fool you. Once you have given out personal information, the scammer may use it to steal your money.

Foreign Government Scam – A scammer sends an e-mail that deceives consumers into believing that he or she is a wealthy foreigner who needs help moving millions of dollars from his or her homeland, falsely promising a hefty percentage of his or her fortune as a reward for the financial assistance.

IRS, FBI, Or Other Agency Scams – Scam artists pose as officials representing the Internal Revenue Service, the Federal Bureau of Investigations, or one of several other state or federal

agencies. The lure will most often be a “tax refund” or some other monetary offer meant to establish communications with consumers. No legitimate government agency will contact you by email to offer you a refund or threaten you with arrest if you don’t cooperate by providing your personal information.

What can I do to protect myself and my organization?

- If you get an e-mail warning about a virus, call your help desk, or if you experience this at home, run your own anti-virus program.
- Do not circulate warnings or suspicious messages without first checking to verify the authenticity of the e-mail.
- Do not open an e-mail attachment unless you are absolutely sure that you know and trust the sender.
- Keep your anti-virus software up to date.
- Beware of any e-mail asking for or offering money, or seeking personal information.
- If it sounds too good to be true, it probably is!

There are some websites that offer to provide information about current scam emails, hoaxes and urban legends, including the following:

http://www.ic3.gov/default.aspx

http://www.irs.gov

http://www.fbi.gov

http://www.ftc.gov

http://www.lookstoogoodtobetrue.com

http://www.onguardonline.gov

If you've been the victim of such a scam, file a complaint with the Internet Crime Complaint Center (IC3), which is a partnership between the Federal Bureau of Investigation, the National White Collar Crime Center, and the Bureau of Justice Assistance. Information on filing a complaint with the IC3 can be found online at www.ic3.gov. You can also report the scam to the Federal Trade Commission (FTC) by calling 1.877.FTC.HELP (1.877.382.4357) or by visiting the FTC’s website at www.ftc.gov, or you can report the scam to Attorney General Jepsen at Attorney.General@ct.gov or (860) 808-5420, or file a complaint with the Department of Consumer Protection at trade.practices@ct.gov or by calling the DCP hotline at 800-842-2649.