Tips to Prevent Email Viruses and SPAM

(Revised 04/29/11)
LAUSD IT Help Desk
333 S. Beaudry Ave. 9th Floor
Phone 213.241.5200

Email Attachments: BEWARE OF ATTACHMENTS - Do not open email attachments you are not expecting. The E-mail should be deleted immediately. Emails that spread viruses come with some very deceitful messages to trick you into opening the attachment e.g. *"Your email account has been cancelled, see attachment for details"*.

Be sure to keep your District Anti-virus updated and make sure that Outlook and/or email protection is enabled.

Links in E-mails: DO NOT CLICK ON LINKS IN E-MAILS UNLESS YOU ARE EXPECTING THE E-MAIL AND YOU KNOW THE SOURCE.

Be suspicious of all emails, sometimes the virus looks like it came from an email address you recognize e.g. from admin@lausd.net. Virus attachments can have the following 'file extension': .exe, .pif. If you receive a .zip attachment and open it - make sure it does not contain a file with one of those extensions. **DO NOT OPEN ATTACHMENTS YOU HAVE NOT REQUESTED, EVEN IF THEY APPEAR TO BE FROM PEOPLE YOU KNOW.** Delete the E-mail, and then empty your Deleted Items Folder.

What is SPAM?

As it relates to LAUSD, SPAM is any kind of unwanted online communication not related your job. Some SPAM is harmless and just meant to promote a product or a cause. Others can be harmful, intent on causing damage to your computer or stealing information from you.

"Never" open attachments or click on links in E-mails where you do not know the source of the E-mail.

Some SPAM is part of an identity theft scam or another kind of fraud. Identity theft SPAM is often called a phishing scam. (pretending to be legitimate)

> Microsoft Online Safety - Fraud prevention:
> http://www.microsoft.com/protect/fraud/default.aspx
>
> Microsoft Online Safety - How to recognize phishing e-mails or links:
> http://www.microsoft.com/protect/fraud/phishing/symptoms.aspx

To protect yourself against e-mail SPAM, use e-mail software with built-in SPAM filtering. For more information, see Microsoft Online Safety - How to handle suspicious e-mail:
http://www.microsoft.com/protect/fraud/spam/email.aspx

"Spoofing an Email Address"

Unfortunately this is a common SPAM problem. Sometimes SPAMMERS find addresses to put in their SPAM and it happens they chose yours. Sending an email that appears to have come FROM someone who did not send it is known as "spoofing and email address".

Anyone with Outlook, as well as other email programs, can forge the FROM address in an email, regardless of whether they own the domain name in the address, regardless of whether they have permission to use it, and regardless of whether the domain name even exists or is valid. There is nothing that the rightful owner of a domain name can do to stop people from sending out email with an address in the FROM field that belongs to someone else.

There also is nothing that a webhost can do to stop or prevent SPAMMERS or virus mails from wrongfully claiming that your email address came FROM or was the sender of a piece of SPAM or email virus.

The most annoying part of having someone “spoofing” your email address in the FROM field of their outgoing SPAM is that no delivery and other bounce notifications will be returned to you because the undeliverable messages appear to come FROM your address.

How to Prevent SPAM

ITD Blocks 95% of all SPAM
Some email does make it through our filters. We are very aggressive with our filtering, in some cases filtering email that contains information that appears to be SPAM related.

Limit the places where you post your e-mail address
Be cautious about posting your e-mail address on public Web sites, such as newsgroups, chat rooms, bulletin boards, and so forth. When visiting public sites, you might want to use an e-mail address that is different from your main e-mail address. SPAMMERS can steal or purchase your email address for spamming purposes.

Watch out for sites that want to put you on a mail list.
When you shop online, companies sometimes add a check box that a have it selected by default. This informs the company that it is fine with you if the company to send you advertisements and give your e-mail address to other businesses (or "third parties"). Clear this check box so that your e-mail address is not shared.

Do not reply to SPAM
Never reply to an e-mail message — not even to unsubscribe from a mailing list — unless you know and trust the sender, such as when the e-mail message comes from a service, an online store, or newsletter that you have signed up with. Answering SPAM just confirms to the SPAMMER that your e-mail address is an active one.

If a company, uses e-mail messages to ask for personal information …
Do not respond by sending a message. Most legitimate companies will not ask for personal information to be sent in e-mail. Be suspicious if they do. Such a request could be a spoofed e-mail message disguised to look like a legitimate one. This tactic is known as phishing.

Do not forward chain e-mail messages
Besides increasing overall e-mail volume, by forwarding a chain e-mail message you might be furthering a hoax — or worse, a virus. Meanwhile, you lose control over who sees your e-mail address.

If you use Outlook, take advantage of the Junk E-mail Filter
Office Outlook can redirect or automatically delete SPAM by using the Junk Email Filter, which automatically evaluates incoming messages and sends those identified as SPAM to the Junk E-mail folder. See help menu – Junk E-mail for **details** or view the Microsoft online document - Overview of the Junk E-mail Filter: http://office.microsoft.com/en-us/help/HP012300281033.aspx

Who can in notify about the SPAM that I am receiving
You can forward your SPAM complaints to this government website **spam@uce.gov**.

Phishing

Lausd employees are often the target of "phishing scams" identity theft emails that are circulated to District email addresses. District employees sometimes receive emails claiming to need the employee's username and password.

DO NOT RESPOND TO ANY EMAIL ASKING YOU FOR YOUR USER ID OR EMAIL.

ITD will NEVER ask you for your password. The email is a scam attempting to gain access to your LAUSD e-mail account. This is called "phishing" and it is a common type of Internet fraud. If you think you have given out your LAUSD password to a phishing scam, immediately notify IT Help Desk at 213-241-5200.