E-Mail Safety Tips

SLOCOE uses several systems to help mitigate viruses, malware and spam. However, since no system is 100% infallible, viruses, malware and spam can and will get through. Please review the following information to help protect your email and computer.

If you suspect that you have been infected by a virus or malware please contact Tech Services immediately.

Questionable Attachments and Links

NEVER open an attachment unless you know what it is and who sent it. If you have any doubts, contact the sender by telephone or separate e-mail to ask if they sent it. It would be better to delete a legitimate message and have to have it sent again, than to open a malicious attachment and suffer the consequences of having your computer infected with a virus.

Likewise, NEVER click on images or links to Web sites if you are suspicious of them for any reason. This includes links in e-mail messages and links on Web pages. Some links that may look harmless are designed to redirect you to a site with undesirable content or to a site that will transmit a virus to your computer (or both). Using a bit of caution while reading e-mail and browsing the Internet can be quite helpful in avoiding virus problems.

Do's and Don'ts

- **DON'T** open attachments that you are not expecting, regardless of who they come from.
- **DON'T** reply to suspicious messages or forward them to friends.
- **DO** verify that the apparent sender actually sent the original e-mail if you doubt the validity of a message. Call the sender or send an e-mail by creating a **NEW** message. Do **NOT** reply to the original message.
- **DON"T** forward the email to Tech Services. Call or send a separate email to Tech Services about the suspicious email.

Spammers like to steal passwords for services like online banking, eBay, or e-mail accounts so they can send more spam messages. **Legitimate e-mails will NEVER ask for your username or password and very rarely contain attachments**. When in doubt about changes to your online services open a new browser window and log into your account to check for yourself.

- **DO** be particularly cautious when you receive e-mail about services and Web sites that you use.
- **DON'T** click on links or copy Web addresses from within messages.

Staying informed and knowing how to identify harmful messages is the easiest way to protect yourself and keep your computer virus-free.

Tech Services Emails

Occasionally, Tech Services receives reports from users who receive e-mail messages claiming to be from "Tech Services", the "Support Team", “System Administrator”, or a similar source. These e-mails make a variety of claims attempting to trick the user into replying to the message or opening infected attachments included in the message. The exact wording varies, but the text usually claims that your account has been deactivated or that you recently changed your settings, password, or contact e-mail and need to verify them. **These messages were NOT sent by Tech Services** and are no different from the dozens of spam messages that most people receive every day.

Remember:

Regardless of who a message claims to be from, it is always necessary to use common sense and caution when checking your e-mail. It is also essential to maintain current anti-virus protection and do regular operating system updates. Spammers have become increasingly more sophisticated and use many tricks to fool people and defeat mail filters. Harmful messages may include text taken from legitimate e-mails regarding procedures, contact information or virus scanning, so the messages appear genuine. Spam messages often include deceptive links that redirect you to malicious Web sites and may "spoof" or fake the "from" address of the e-mail so it appears to come from your friends, work, or school. **You** are your best defense against viruses and it is your responsibility to be well-informed and cautious.