

From: SWE IT Services [mailto:hq@swe.org]
Sent: Monday, March 08, 2004 3:29 PM
Subject: SWE Virus Protection Information

Dear SWE Member

E-mail viruses, worms and trojan horses, as well as fraudulent e-mails, are a significant concern to all of us who rely on e-mail for communication. Recent strains of viruses are becoming more sophisticated, both in terms of how they deliver their viruses, worms, etc.. and in how they disguise themselves as legitimate e-mail. To that end, please be aware of the following:

- 1) SWE will NEVER e-mail you a FILE ATTACHMENT and tell you that you must click on it to maintain, update, or activate your "account", your e-mail, etc... If you receive an e-mail that looks like it's from SWE with a message such as this and a file attachment, IT IS A VIRUS AND YOU SHOULD IMMEDIATELY DELETE THE E-MAIL WITHOUT CLICKING ON THE FILE.
- 2) Effective immediately, all e-mail sent to swe.org addresses that have .zip file attachments will be rejected and will not be delivered to the recipient. Because many new viruses are using the zip file attachment to propagate, we will no longer allow zip files through our mail system. Please send files in formats such as .doc, .xls or .pdf.
- 3) Never assume that because you know the sender, an e-mail and/or file attachment is safe from viruses. Mass mailing viruses often collect the e-mail addresses stored on an infected machine. They then create e-mail messages that claim the sender is one of the e-mail addresses they collected. These bogus e-mails look legitimate, but spread the virus.
- 4) Fraudulent e-mails, also known as spoofing, imposter, or phishing e-mails, are e-mails in which the sender address has been forged so it looks like a legitimate e-mail from a particular organization (such as SWE). These are usually designed to trick you into providing sensitive personal information that can be used for identity theft by having you reply to the e-mail or by sending you to a web site link that requests you enter information. It's sometimes hard to detect a fraudulent e-mail. That's because the e-mail address of the sender often seems genuine (such as management@swe.org). To protect yourself, be aware that SWE will never ask you to e-mail your credit card number or sensitive personal information such as your social security number. All credit card transactions with Headquarters should be done via our secure server, phone, or fax.

To further protect yourself from viruses, never attempt to open a file that looks suspicious or comes from a completely unknown sender – or even a known sender - without explanation. Be sure your computer is running a local virus scanning program and that virus definition files are regularly updated. Never open an attachment directly from an e-mail. Always save the attachment to your hard drive or the network first (depending on your organization's recommendations), then open the file from there. Virus scanning software will not always recognize an infected file as accurately when opened directly in e-mail.

If you have any questions regarding this information, please e-mail hq@swe.org or call (312) 596-5223. Thank you for your cooperation.