

As the Electronic Case Files system goes online throughout the nation, it, like any other software program, may become the target of hackers and virus attacks. Though we have not seen any evidence of such activity, one of the most likely scenarios for virus distribution relating to the ECF system is “email spoofing”.

Email spoofing is the act of sending an email message which appears to be from someone other than the actual sender. It is possible that a “spoofed” message could create an email message that bears a resemblance to an ECF Notice of Electronic Filing or some other official ECF communication. Such an email could contain a virus hidden in a hyperlink or attachment and bear a subject that might cause recipients to believe it to be legitimate email from the Court.

The simplest and most effective protection against email spoofing is to carefully read the address of the sender. All Notices of Electronic Filing sent from our ECF server will have a send/return address of cmecf@med.uscourts.gov. “Spoofed” messages will have a different address which may appear similar to a court address, for example cmecf@hotmail.com or liveecf@hotmail.com.

If you have any concerns about this issue or if you receive any suspicious emails relating to ECF, please contact the Clerk’s Office (207-780-3356) or the ECF Helpdesk (ecfhelp@med.uscourts.gov).