Security Threats to Your Email Communications

by Eric Kangas, PhD - Internet Security Expert

Source: Excepts from The Case For Email Security, published March 31st 2015 in The LuxSci FYI Blog by Eric Kangas. Find on web: //addthis.com/bookmark.php?v=300)

EAVESDROPPING

”It is very easy for someone who has access to the computers or networks through which your information is traveling to capture this information and read it. Just like someone in the next room listening in on your phone conversation, people using computers “near” the path your email takes through the Internet can potentially read and copy your messages.”

IDENTITY THEFT

"If someone can obtain the username and password that you use to access your email servers, they can read your email and send false email messages as you."

INVASION OF PRIVACY

"If you are very concerned about your privacy, … you may also be concerned about letting your recipients know the IP address of your computer. This information may be used to tell in what city you are located or even to find out what your address is in some cases!”

MESSAGE MODIFICATION

“Anyone who has system administrator permission on any of the SMTP Servers that your message visits, can not only read your message, but they can delete or change the message before it continues on to its destination. Your recipient has no way to tell if the email message that you sent has been altered! If the message was merely deleted they wouldn’t even know it had been sent.”

FALSE MESSAGES

“It is very easy to construct messages that appear to be sent by someone else. Many viruses take advantage of this situation to propagate themselves. In general, there it is very hard to be sure that the apparent sender of a message is the true sender - the sender’s name could have been easily fabricated.”

MESSAGE REPLAY

"Just as a message can be modified, messages can be saved, modified, and re-sent later! You could receive a valid original message, but then receive subsequent faked messages that appear to be valid.”

UNPROTECTED BACKUPS

"Messages are usually stored in plain text on SMTP Servers. Thus, backups of these servers’ disks usually contains plain text copies of your messages. As backups may be kept for years and can be read by anyone with access to them, your messages could still be exposed in insecure places even after you think that all copies have been “deleted.”

REPUDIATION

"Because normal email messages can be forged, there is no way for you to prove that someone sent you a particular message. This means that even if someone DID send you a message, they can successfully deny it."