

Implementation of LocatePC

[LocatePC](#) is an interesting piece of software that may well locate a misplaced PC when the PC is once again used while connected to the Internet. Because of the [detailed report](#) that it provides by email it is also convenient for keeping track of a PC's IP address as it moves around the corporation. Dependent upon your objective, your implementation may vary. The one which I will discuss is location of a lost or stolen PC as well as a rather simple process of preventing the misuse of a hard drive.

However, to some degree the two objectives conflict and the final choice is up to the individual user. Both solutions work with Windows Vista, XP, ME and 98. The solution for preventing the misuse of a hard drive will work with any version of any operating system on a PC whose BIOS and hard drive support it; virtually all notebook PCs manufactured since 2000 and many as far back as 1998 or earlier.

LocatePC always runs in the background as a hidden program. When your computer is connected to the Internet, LocatePC secretly sends you an email message containing information that can help identify who is using your computer and what ISP they are connected to.

If required to by law enforcement authorities, the ISP can use this email to identify which account was assigned that IP address at the time the email was sent. Usually this is enough information to identify the person who is using your stolen computer, which will hopefully lead to its recovery.

Note: LocatePC does not require or use other email software on your computer, so your computer's email software will not show any record of messages sent by LocatePC.

1. Set up LocatePC to send its messages to an address you can read without your computer -- for example, your work email, or a friend/relative's email, or a web email address. That way, you'll still be able to read LocatePC's email messages.
2. LocatePC only sends email after a user has logged on to your computer and connected to the Internet. Therefore, make sure your computer doesn't require a password at startup [if you have Windows XP, you can do this by turning on the Guest account].
3. To prevent your computer's hard drive from being bypassed (which would also bypass LocatePC): Set up your computer's BIOS to prevent booting from CD or floppy, and also set up the BIOS to require a password before allowing changes to BIOS settings.

Implementation of LocatePC

The content of the preceding box is Copyright(c) 2006-2007 by Sashazur, LLC and is the entire "About (and Usage Tips)" for *LocatePC* 1.4.9.

The following notes regarding the above "About (and Usage Tips)" tie directly to the respectively numbered paragraphs:

1. Should be absolutely adhered to. Also, you should not use your normal SMTP mail server as the transmission vehicle. More than likely, it will not work when trying to send mail via another ISP. That brings into issue which mail server should be used?
 - a. There undoubtedly many that will work. I chose [Bluebottle](#) which has been identified by *LocatePC* as a good destination for such emails. However, it also supports remote SMTP via port 587.
 - b. Why port 587 rather than 25? Commonly, ISPs block all port 25 communications that are not destined for their own SMTP server. On the other hand, port 587 is the port for messaging which normally is not blocked and Bluebottle accepts port 587 transmissions to its SMTP server.
 - c. Finally, you should not send the messages to any email address that you monitor from the email client on the PC that you are protecting. There is the risk that the thief examines the email and finds references to *LocatePC*. I use a web based email service to receive all messages from *LocatePC*.
 - d. While *LocatePC* is difficult to find and more difficult to remove, once you know that it is operating on a system it can be readily stopped once a little research has been performed and with a bit more effort it can be prevented from auto starting.
2. This advice makes sense but presents a difficulty. If followed, you should not use the hard drive password technique that I will describe later. However, I use both and will explain why.
 - a. Use of the hard drive password means that unless that password is discovered it is likely that you will never recover the PC or hard drive. Discovery of the password is unlikely unless you choose a poor one and the thief makes an effort to try to find it through trial and error.
 - b. Therefore, the question becomes, what is more important; preventing information on the hard drive being revealed or recovery of the equipment.
 - c. I choose both because, should my hard drive password be discovered by the thief I like the opportunity to have it recovered. While I have all sensitive information encrypted, it sure would feel better to recover the equipment.

Implementation of LocatePC

3. Follow to the letter. However, do not set the BIOS boot password! Setting the BIOS change password does not require the entry of a password unless trying to change entries in the BIOS. Setting the BIOS boot password will require a password before Windows is started. See 2. above in the Usage Tips and my notes as well. If you want a password prior to Windows starting, use the hard drive password as it provides far more protection.