What's Next if Your Computer is Stolen?

HE LEFT IT FOR JUST A MOMENT BUT WHEN HE CAME BACK, HIS COMPUTER WAS GONE! LAPTOP COMPUTERS ARE QUICK, EASY TARGETS. IF YOURS DISAPPEARS, YOU WANT IT BACK AND YOU ALSO WANT TO PROTECT THE IMPORTANT DATA ON THE HARD DRIVE. IT'S LIKE HAVING YOUR WALLET STOLEN BUT SIMULTANEOUSLY WORSE AND BETTER.

©Really Terrible Photographer • Creative Commons

It's worse because the computer can contain more than just some identifying information. You might have bank account information on it, complete with balances. But it's better because the data on your computer can be encrypted so that nobody else can read it and your computer might be able to tell you where it is.

Protecting the Data

FILE ENCRYPTION IS THE ONLY WAY TO BE REASONABLY CERTAIN THAT YOUR INFORMATION WON'T BE COMPROMISED IF YOUR COMPUTER IS STOLEN AND EVEN ENCRYPTION ISN'T A CERTAIN SOLUTION.

An application such as TrueCrypt can encrypt the entire hard drive and require a password at boot time. Although this is the most secure method of encryption, it precludes the use of an application that will help you retrieve your computer because the computer must be running in order to check in.

TrueCrypt can also be used to create an encrypted "drive" on the computer. This allows the computer to boot normally but protects any files you place on the protected virtual drive. During the installation, you tell TrueCrypt the name of a directory to create and how large you want the encrypted drive to be. Be sure not to use a directory that contains files; if you do, the files will be deleted.

When TrueCrypt has created the virtual drive, you can create directories on it and store files on it just as you would any other drive. The only difference is that when you reboot the computer or "dismount" the drive, it disappears. So if you simply remember to store all private data (account numbers, passwords, files from the office) on the TrueCrypt drive, those files will be protected even if someone steals the computer.

Then you can turn your attention to finding the computer and possibly even identifying the thief.

Retrieving the Computer

RECOVERING LOST COMPUTERS IS WHAT PREY-PROJECT.COM IS ALL ABOUT. IT'S A FREE APPLICATION THAT CAN TRACK YOUR COMPUTER BUT THERE'S ALSO A PAID PLAN THAT MAKES IT EVEN BETTER.

Installation is easy and I used the default option that installs in C:\Prey. A smart thief might know enough to look for this directory and destroy it but if the thief is that smart, he's probably also smart enough to look for Prey among the installed applications and remove it. Prey creates a standard entry in the Start Menu and I left that in place for the same reason.

Following installation, you need to visit the PreyProject website to configure the settings. Until you do that, your computer can't be tracked. The two reporting options are *standalone* and *Web-based*. The Web-based method allows you to monitor and control the computer from the Prey website and that's what I selected.

When you create the account on the PreyProject server, you'll be asked for your e-mail address, which is what Prey will use to communicate with you, so be sure that you get it right. Then you create a password, give the computer an identity (the default for this is the computer's name), and

specify whether the computer is a notebook or a desktop. Before the system will work, you will need to respond to the verification e-mail from PreyProject. And that's it.
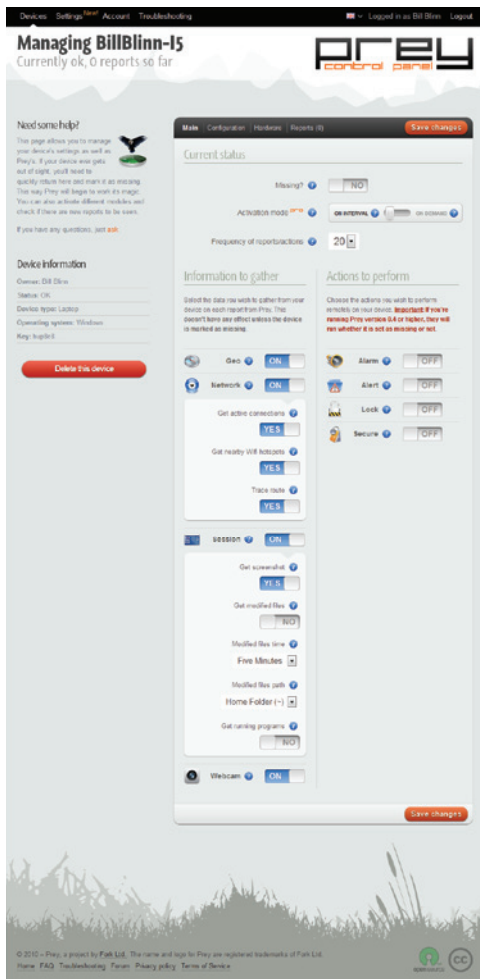

Prey uses the device's GPS, if available. If not, it will try to figure out where it is by looking at nearby Wi-Fi hotspots and triangulating.

It's Missing! Now What?

If your computer is stolen or if you just want to perform a trial run to see how Prey works, go back to the PreyProject website and mark the computer as missing. Then things start to happen.

Having marked the notebook computer as missing, I then turned it on, waited a few minutes, and (using the desktop computer) checked my e-mail. There were 2 messages from PreyProject: (1) The machine is missing and (2) Some information had arrived from the "stolen" computer.

Prey allows you to activate any built-in camera, so you might be able to take a picture of the thief using your laptop's webcam. Police like it when you're able to give them this kind of information
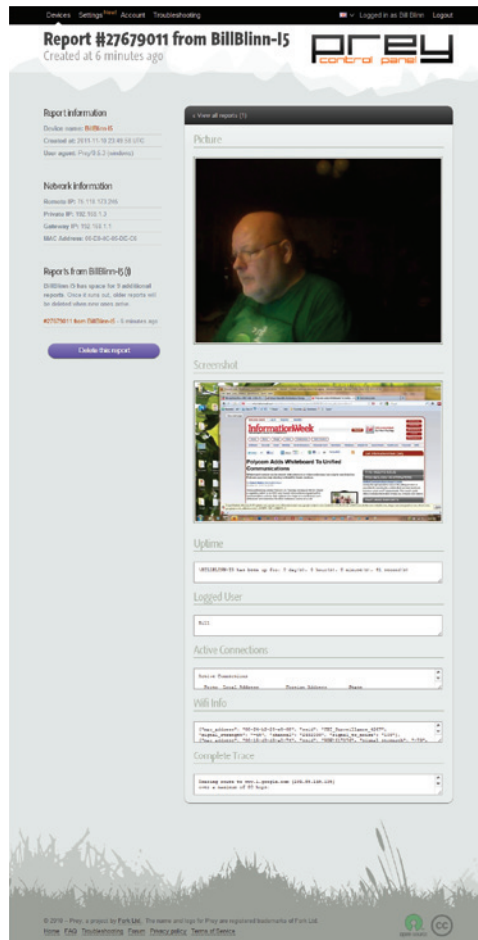
and the report had my picture from the computer's built-in camera. The report also delivered a picture of what was on the screen so you might be able to find an e-mail address or a Facebook account.

At this point, you could continue to watch as Prey tracks the thief every 20 minutes or you could become a bit more proactive. Prey can remove stored passwords used by Outlook or Thunderbird to keep the crook for using your identity in e-mail. You can also lock down your PC, which makes it unusable until your password is entered.

Or you can display a message to the thief.

In my test, Prey also ran a trace-route that might have been helpful although in this case it wasn't. It also reported the IP address of the stolen computer. The IP address would be associated with a specific Internet service provider (ISP) and the ISP would be able to provide police with the name of the customer who had that IP address at the time the report was filed.

So maybe you can recover a stolen computer and catch the thief. But even if you can't, you'll rest a little better if you know that private information on the computer is encrypted so that a thief can't use it. Ω

Today's Small Stuff

Cars, larger; everything else, smaller.

In 1968 I was working in Fort Wayne as the assistant news director. The radio station issued me a recorder that I could carry in one hand. It weighed a couple of pounds and ran for an hour or so on the batteries.

Before that, we had to take along "portable" recorders that required AC power and big reels of magnetic tape.

Today's gear for radio reporters is nothing less than phenomenal. The recorder is actually included inside the microphone.

These new devices will record for several hours using just the memory installed in them and the power provided by internal batteries.

At a time when the tools would make it possible to have the best news teams ever, there are (except for NPR) no markets for news-gathering equipment. And that's what caused me to think about a time when it was a very big thing to have a recorder that would fit in a briefcase. (Or maybe that was a very small thing.) Ω