

9.5 Desktop Security

Reducing the Pain of a Lost or Stolen Laptop

This article is not yet done.

Imagine for a second that your laptop is stolen. What keeps you up at night? It's not the cost of the computer it's what people can do with your **data**.

But because encryption is a pain, a lot of people don't bother protecting their data. Windows user name and password is trivial to break. Here are easy steps to help you sleep better at night and also increase the chance of your laptop being returned.

Provide Contact Information

Obvious but who reading this actually has put contact information on their laptop? Vote below. Yeah me too. I got to do this right after I finish this article.

A note about a reward will also help chances of return too.

For companies who put their company name on the laptop, if you are a large organization where confidentiality is important (ie banks or government) in my opinion, putting your name on the laptop pretty much guarantees a snoop. So if you do this make sure to counter measures setup.

If you're still figuring it out, instead provide a number for a generic department that does not answer the phone with your organization's name.

Lock Your Hard Drive

Native to modern hard drives is the ability to password protect the drive at the hardware level. Once the password is set, the hard drive will not initialize without the correct password.

- Even if you move it to another computer
- You cannot even format it... it just won't initialize

Some Caveats

This is not absolute protection. If someone really wanted to, they could dismantle the drive, take out the platters and rotate the platters manually got get your data. Or if the hard drive manufacture uses more basic techniques it can be broken. However, I would say that there is a very high chance the new owner of your computer will simply toss your hard drive, put in a new one (they are so inexpensive these days) and continue along his or her merry way. That is unless you enable a BIOS boot password.

I recently had my computer die on me and ran into a gotcha. I moved my Hard drive to another IBM laptop of a different model and it would just not boot at all. To get it going, I had to set my BIOS password to be the same as my Hard drive password.

Enable a BIOS Boot Password

If you want to really turn your computer into a brick for others, put on a BIOS Boot password. These days, even shorting out the batteries does not remove the password.

If you "lock your hard drive" and "enable a boot password", and do not like the idea of having to enter two passwords, some BIOS like my IBM Lenovo X200 allow me to combine the boot password and hard drive protection password together under the same password. I enter only one password but someone else trying to dismantle my system will find both the hard drive and they motherboard useless.

With only the RAM usable the effort of reassembly for a new motherboard, there is a much higher chance of your system being returned provided you attached contact information to your laptop.

Password Protect the BIOS

Obvious, but lots of people forget this step.

Change the Boot Sequence

No point in all that effort if somebody can use a boot disk and load a custom program bypass your BIOS. Change the boot order (to boot from your C: drive first). This makes it next to impossible to get a boot virus and again frustrating to do anything with the system including installing a new operating system.

Encrypt the Drive

Also native to most new hard drives, is the ability to encrypt your data. Personally I don't go this route because it makes recovery of your data very difficult and next to impossible if you forgot your passwords.

Phone Home

...

References

<http://www.laptoptips.ca/security/hard-disk-password/> - talks about locking hard drives.

<http://www.rockbox.org/lock.html> - it is possible to unlock the drives...