

Protect your Laptop

Over 600,000 laptops are stolen every year, the possibility that you can lose your laptop tomorrow is also hard to avoid. The chance of your laptop being stolen is 1 in 10. Have you ever thought about what will happen if your laptop is lost?

Have you ever thought about what would happen if your laptop was lost? Could it be sold on Ebay the next day? Will the data be removed and displayed on some websites like MySpace within a week? Will the data stored on your computer be used by a general opponent for your company? Obviously all these scripts need to be considered.

Is there a risk?

Over 600,000 laptops are stolen every year, the possibility that you can lose your laptop tomorrow is also hard to avoid. The chance of your laptop being stolen is 1 in 10. That means that about 10% of your laptop will be lost. What if you lose it or simply put it wrong?

This is a real life story for you. Last month I just got off the plane in another city, where I attended a seminar with colleagues. My friend called me, he was a successful merchant and was quite kind. When I arrived, we talked about how he had spent the last 12 hours trying to find his laptop, after he left it in the taxi in about 20 minutes. The taxi was hired by another guy with his laptop on it. When I talked to him about his risks, I asked about the obvious efforts to protect laptops, data and information before he left it in the taxi. His answer is quite similar to those of other laptops, ' *I don't have time or I think it won't happen to me* '. He called the taxi company four days later to try to find the device, and by the way I told him about some basic steps that could be taken to protect the laptop he used later.



Physical protection

First and obvious protection for your laptop is always the way to protect physics. In the case of my friend, he committed a mistake himself caused by neglecting it in the car. The initial advice that I recommend is to always keep your laptop in your pocket when you travel.

I then continued to describe devices that could be helpful in protecting physics that are often sold at markets. Some devices are as simple as buckles with bundled cables, using them laptops can be locked to the desk when you go out to have something. It is great to use at home or hotel. If you need to do even more powerful steps, you can add alarm devices if the laptop is moved, the cable is cut, . then the siren will sound loudly. This problem will discourage thieves who want to steal your computer.

Security appraisal

My friend was very worried about the 'stranger' access after he grabbed his computer, he could log in with a user account. I let him know that this is not only possible but also done quite easily. I continue to mention that there are many options that strangers can perform here, but some protections can be effective in this case.

Access is quite easy, because the stranger can install another operating system with the existing operating system, after deleting the SAM file from the original installation. When the SAM file has been deleted, the stranger can completely boot into the original installation and log in with the administrator account with a white password.

I then went on to explain that Windows Vista has a new feature to protect against this drawback, which is called BitLocker. BitLocker is a full-system encryption feature, so installing a new operating system will not be able to see the old installation files.

I also explained about previous Windows operating systems, strangers can also use the original SAM file and run it through a tool like L0phtcrack. With enough time and computing power, all passwords for local user accounts

can be found. However, newer operating systems that Microsoft has enabled SYSKEY will be protected against this attack, shown in Figure 1.



Figure 1: SYSKEY is enabled by default on newer Windows operating systems

Data protection

My friend asked me about the lost data on his computer, the nature of his concern was whether data could be read by the stranger. The computer currently contains important corporate files and other important files. And I had to tell him straight away, after he said he didn't do anything to protect the files before losing the computer. He asked a perfectly valid question, the question is how to protect the files for his new computer later.

I *first* explained that he could start with a password for the BIOS. Not only is this one way, but it is the minimum way of protecting the laptop for access to the system. There are many methods around this problem that you should implement it.

Second , I explained the difference between NTFS and FAT file systems. With NTFS, all data contained in a list of users can access the files, as shown in Figure 2.

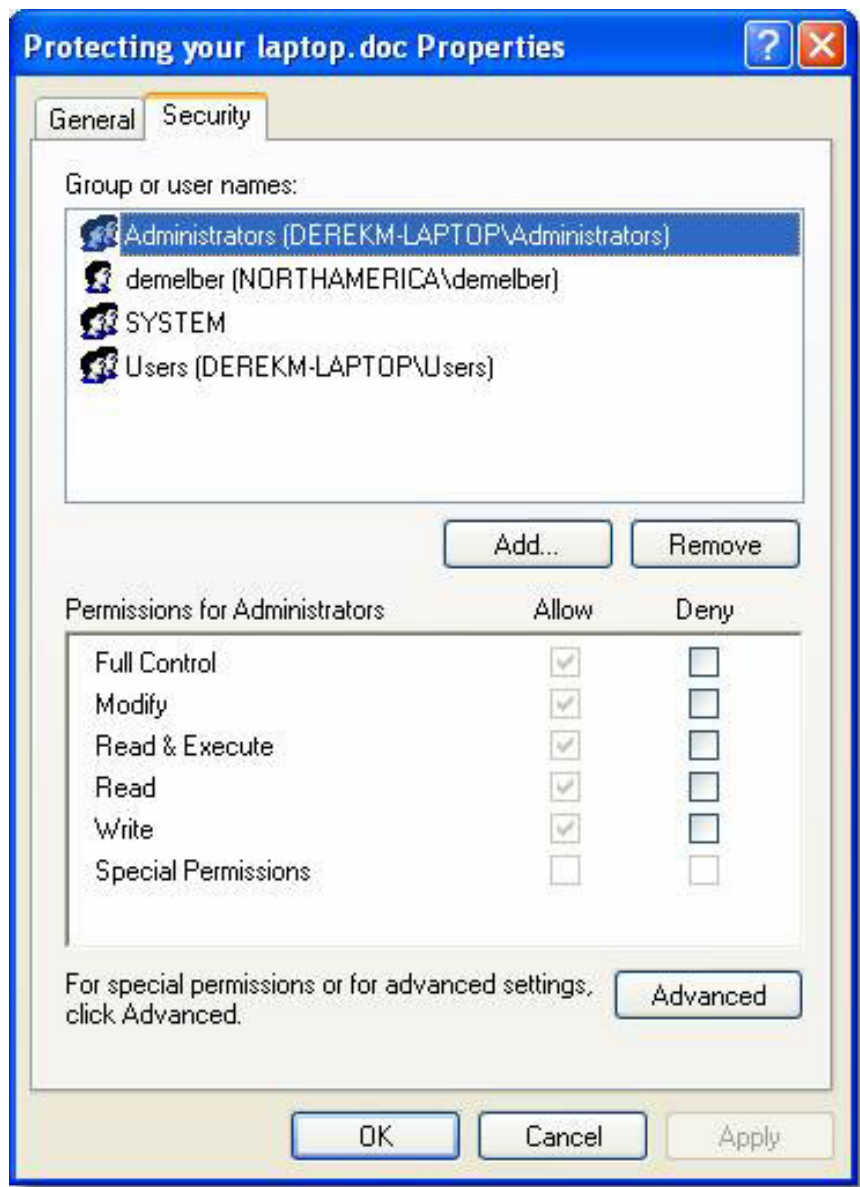


Figure 2: NTFS has an access control list (ACL) related to each file

This is not a very secure security operation for a lost laptop, but it is also a barrier to strangers trying to access files. FAT does not have permission and should not be used due to lack of security.

Third, always encrypt using the Encrypting File System (EFS). EFS was first introduced in Windows 2000 and is a method of data encryption as it was placed on the hard drive. This protection method combines with private key pair and public key with data, so if the private key is not available then the user will not be able to access the data. There are many methods around this protection issue, but they are not really easy to apply.

Fourth, I talked about another level of encryption that can be used for a third solution, which is combined with a USB drive to encrypt the storage of the private key. This encryption is much better than the built-in encryption, which is thanks to the USB key when accessing data, not just the username but the same password as the EFS option built upon.

Finally, I mentioned that all data needs to be backed up in case the laptop data is corrupted, lost or deleted. Not really a security issue but it is a data integrity issue. I can't talk about data with someone without mentioning data backup for any reason. Maybe safety has eaten into my blood.

Conclude

As I talked about how to secure my laptop with my friend, he realized that the risk of data loss and laptop is a fact. He can see clearly that the physical protection method for laptops is really necessary, which seems to be the most important aspect when he spent 4 days trying to trace it. His concern is about the access issue of strangers picking up the machine when he doesn't have a pre-preparation to protect the operating system and data. There are many options, to perform a protective action before it's too late. For you, what you should do, a sincere advice for laptop users is to follow these tips before it's too late. Good luck.

You finished reading the article "**Protect your Laptop**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.