**Theft of cellphones and IMEI**

**Cellphone Theft**

In 2008, 139.3 million smart phones were either handed over the counter in the local shops, or shipped to a buyer somewhere in the world. By the end of the fourth quarter of 2008 alone 38.1 million unites had been sold. According to Gartner, a US research firm, that's an increase of 3.7 percent if you compare it to the same quarter of 2007. Overall the increase in sales when comparing 2007 to 2008 proved to be as high as 13.9 percent.

With all these phones being handed out to customers around the world legally, it makes you wonder just how many phones are being sold illegally?

Statistically every one in five smart-phone is a fake. Crafted to look the model of any one of the most popular smart-phones.

What that means is that there's a 20 percent chance that the Nokia-phone your friend, colleague or even yourself own is actually a Nokia. In many cases the manufacturers of these copies will put a name that very much resembles the name of the real model. In some cases they will just put the original logo on the phone and sell it even still.

These kinds of phones make up for one of the major dangers in cell-phone theft and cell-phone copying. As they can easily come with malicious software installed onto them, or if they are bought with a subscription, the sim-card might be coded to apply for expensive SMS-services obviously this will be kept completely unknown to the owner of the phone untill the bill for the month arrives.

This kind of software can potentially also be installed on a regular phone. According to the metropolitan police service, there's stolen 10.000 phones on average each month[[1]](#footnote-1).

If a phone is stolen, and not reported as such, the thief, or new buyer can use the phone in your name. There's the obvious making calls, sending texts and other use of traffics and services on your bill. However you can easily set up a paid call-line, and make several calls to that line from the stolen phone and make huge profit. Furthermore, as the number and phone is adressed to the original owner, anyone with acces to the phone can go ahead and do whatever they want, and it'll be in the original owner's name.

**IMEI Theft**

If a phone is stolen, one should immediately get it locked. This can be done through submitting the IMEI number, that your phone is carrying. If your phone is stolen, and you do not get your IMEI locked, the new owner can potentially just keep buying new pre-paid cards, and do whatever he or she wants to do in your name, and you wouldn't even know about it, as there would no longer be a bill to recieve. Every phone should, in theory, carry it's own unique IMEI number. So if a theif get's a hold of a phone, and changes the billing information/address, he has succesfully stolen just the hardware of the phone and the IMEI number. The ability to use a phone completely anonymously carries great value in the crime-world. In India a group of 3 men went to stores and implanted fake (invalid) IMEI numbers in phones. The article doesnt describe what the purpose was, but one could imagine that they then kept the original (valid) IMEI numbers to themselves, or for trading purposes.

The way an IMEI number is stolen from a phone is simply by changing the IMEI shown on the phone. The location varies depending on what model it is. Then you change the IMEI inside the actual software of the phone. In India it was done using something called "The Spiderman Kit".

1. <http://www.met.police.uk/crimeprevention/phone.htm> [↑](#footnote-ref-1)