

Hack in the USSD



mobilesecurity.com [Sydney, NSW] USSD. No, it isn't the result of a new currency conversion site that's suffering from a stutter. USSD is the next big thing to come out of hack-land. In today's mobile world, USSD relates to Unstructured Supplementary Service Data – and is the abbreviation given to those strange codes you occasionally need to dial (or receive from your service provider) that reveal your latest balance, overage status, SMS allowance remaining, and other useful tidbits of information direct from the carrier.

Few people outside the telecommunications industry would have heard of USSD until a [story](#) broke last week about a new threat that has the potential to lead to Android devices being remotely wiped. In fact, most people probably still don't have the faintest idea what it is. So let mobilesecurity.com explain a few things – to help you understand what the concern is, but also why it's easily fixed and how you can do something to help yourself.

First off – how does this work?

Android phones (and other mobile devices) are set up to receive instructions via USSD. You may have encountered one of these already, likely when you called the support line of your mobile telecom provider, who may have asked you to type `*#06#` into the handset to reveal the [IMEI](#) number for your phone. At the time, you may have thought "that's pretty neat, I wonder what other secret codes I could enter on my phone to discover interesting information". Or you may not have thought any more about it.

Well, now is a fairly good time to start thinking a little more about it. The reason being, that users don't actually need to type *#06# into their device to reveal their IMEI number. They could just as easily visit the URL tel:*#06# from their browser. This would trigger their phone to identify itself with a message on the screen, via the phone's 'dialler' feature. So that brings us back to the earlier question: "it's pretty neat, I wonder what else I could discover by using that type of code."

It became apparent [recently](#) that a vulnerability in older versions of the Android OS allows far more than just IMEI numbers to be revealed. Specifically, devices could potentially be reset to factory settings, and SIM cards can be "killed". All this, simply by entering a USSD code or clicking on a URL in the format tel:*#xyz123 (i.e. something in the same format as *#06#). Now, that's fairly alarming in itself – imagine, you leave your phone unlocked on the office desk for 5 minutes, and the office 'joker' decides to enter that "kill" code on your device. I'd imagine you would be less than impressed.

Now let's take it one step further. Imagine you receive a fake email or SMS that appears to come from your service provider or another 'trusted' source. The SMS tells you to visit an apparently safe URL – perhaps it appears to be your carrier's customer portal. However, instead of sending you to <http://m.mymobileprovider.com>, it actually opens your browser at the URL tel:*#killSIM;resetphone.

It would be highly irresponsible to post the actual 'kill' code on this site, but you get the idea. Open that URL on your mobile device, and you could be left with a weekend restoring your apps, trying to retrieve photos and videos, and desperately trying to remember the name of the bar you were in when you met the new love of your life.

So how do you avoid this scam?

Let's face it, at the moment it's being used as a kind of joke – the bad guys here aren't taking your credit card details, they're not stealing your identity or sending a cavalcade of spam to the friends in your Contacts list. But they're inconveniencing you, and it's damned annoying.

One step on the way to avoiding all this nastiness, is to follow the same simple security precautions you've heard a million times before. I'm almost tired of saying it, but here goes, almost certainly not for the last time:

1. DO NOT click on links within emails or SMS messages on your mobile device if you have any suspicions around the origins of the message
2. DO NOT leave your phone unattended without activating the screen lock
3. DO NOT scan in QR codes willy-nilly, use a QR scanner that checks the URL before your browser opens the web page. We're not in the business of promoting specific products – but we do make exceptions for free apps that do a really basic job well. [Norton Snap](#) is a free QR reader that will verify a URL before prompting you to decide whether you want to open the page in your browser
4. Check your phone settings – ensure that your [NFC](#) reader doesn't open URLs by default, and turn off the "Service Loading" feature to avoid SMS messages being pushed to your phone via WAP, in case URLs open directly in your browser

So, those are pretty straightforward tips for avoiding nasty surprises – exactly what you’ve come to expect from mobilesecurity.com. There are also apps you can download that are specifically designed to deal with this brand-new threat. On the back of this new scare, Symantec has launched a new free app for Android, called [Norton Halt](#), which will help take care of USSD communications – just in case you forget to follow the simple rules above. Norton Halt will monitor for suspicious USSD Code requests, and then stop the dialler from executing these without the user’s permission.

This issue has only just been revealed, and it may take device manufacturers and carriers some time before they push out fixes to their customers. So, it really makes sense to consider all the options available to prevent the loss of your personal data and to keep your weekends free for other activities!

Mobilesecurity