

What is near-field communication (and how secure is it)?

November 6 2013, by Rob Livingstone



Near field communication isn't a new phenomenon, but it's only just now getting a real push into Australia. Credit: vernieman

Coles and the Commonwealth Bank of Australia declared last month their intention to make use of near-field communication (NFC) technology, allowing users to transfer their personal and other banking details from a smartphone to a point of sales register by simply holding their device near a reader.

So how does NFC work – and how secure is it?

In its simplest form, NFC can operate in three modes:

- In passive mode, the contact pad generates a very short-range radio frequency field which is used to read data contained in the receiving chip while passing through this radio field. Common examples include credit or payment cards, where the tiny receiving chip is inserted within the plastic card.
- In active mode, NFC-enabled devices can communicate with other NFC-enabled devices and contact points to exchange data bi-directionally. They allow users to access, for example, any data from a "tap point" such as a public transport turnstile, reading information at a museum exhibit, or a so-called smart poster. A smart poster, for the most part, takes the form of a poster or billboard in or on which readable NFC tags have been placed. These NFC tags contain information which is read by your [smartphone](#), such as the web address of the advertiser, information relating to a sales promotion, or bus timetable.
- In paired or peer-to-peer (P2P) mode, data can flow in both directions between two devices using the NFC Data Exchange Format (NDEF). Connecting devices in NFC P2P mode is in stark contrast to the cumbersome Bluetooth pairing processes. Bluetooth pairing typically involves a number of steps including identifying the target device from the list of devices within radio range of your phone, selecting that device then entering the PIN code associated with that device. This process may take anything from 30 seconds to a minute or so.

The appeal of convenience for consumers of NFC is driving smartphone providers to integrate NFC into their latest devices. With the exception of Apple, all leading smartphone manufacturers are implementing, or have already implemented, NFC technology into their devices. Nokia and BlackBerry are in various stages of developing and deploying NFC-ready [mobile devices](#), whereas Samsung smartphones are already NFC capable.

Fast on the hype, slow on the uptake

Despite the increasing use of contactless credit and [payment cards](#), expectations of a broad and rapid adoption of NFC based technologies have failed to be realised, with many deployment still in the field trial stage.



Credit: Guerrilla Futures, Jason Tester

Similarly, the road towards the digital wallet, is not paved with gold. The failure of the Google Wallet to reach market critical mass, meaning their US\$300 million investment in the Android-based solution is unlikely to yield a return.

Where Google goes, however, others are sure to follow – one such example being the Commonwealth Bank, which recently announced a NFC-capable sticker for smartphones without NFC capabilities, which turns a smartphone into a digital wallet. Time will tell whether these developments ultimately become the norm, or end up becoming a small supplement to an ever increasing range of payment methods.

The never-ending security/convenience arms race

As a consumer, how can you ensure you're never caught up in the crossfire of the never-ending war between the cybercriminals and legitimate organisations?

The answer is: you can't. Card skimming is a well-known phenomenon, and the advent of NFC takes this to a new level.

In a paper published in September in the *Journal of Engineering*, [entitled](#) "Eavesdropping near-field contactless payments: a quantitative analysis," the authors illustrated the relative ease with which NFC can be intercepted from distances of as far as a metre using easily concealable antennae and low-cost electronics.

With respect to NFC-enabled mobile devices, smartphone applications activate the NFC chip which works as a NFC reader, a point illustrated by a hacker who showed how to use an Android phone to make payments from a stranger's contactless credit card.

The Hewlett Packard 2012 cyber risk report cites the main security concern arising from a NFC chip in a payment card is the fact that the chip can always be read. When the card is in the field of a NFC reader, the information on the NFC chip can be read and stolen.

So what's at the end of the NFC rainbow?

When it comes to NFC based technologies, consumers are well advised to check where their personal liability for information security ends and that of the financial institution or related parties begins.

One thing is certain, the inherent risks in the digital world are real, and they may be something over which you have little control.

This story is published courtesy of [The Conversation](#) (under Creative Commons-Attribution/No derivatives).

Provided by The Conversation

Citation: What is near-field communication (and how secure is it)? (2013, November 6) retrieved 20 March 2024 from <https://phys.org/news/2013-11-near-field.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--