Phone scams cost billions. Why isn't technology being used to stop them?

June 26 2017, by David Glance

Blocking scams should be easy. Credit: Pixabay

World-wide, credit card fraud and other scams cost the public billions of dollars. While credit card fraud is the clear leader in sheer volume of money lost, "regular scams" still result in a significant amount of money being lost each year.

Globally, credit card fraud resulted in losses of US$21.84 billion in 2015. The so-called "Nigerian scam", usually perpetrated via email, totalled US$12.7 billion in 2013. Overall losses are likely to be much larger however, as many scams go unreported.

While scams that come in over email are increasingly being picked up by spam filters, around 45% of scams in Australia (and likely other countries) are by phone and text message.

Email spam filters are using machine learning techniques to get better at identifying the wide range of scams that can arrive in inboxes. This is by far the most effective way of dealing with scams, as the average member of the public has been shown to be remarkably susceptible.

However, very little has been done about phone and text scams. This is surprising given scammers have quite brazenly stuck to using the same number or area codes over significant periods of time.

One particular scam in Australia, for example, had people claiming to be from the Australian Tax Office. One group, perhaps the same one, are now running a scam from the very same phone number where they claim to be from a motor vehicle accident company wanting to pay compensation for an accident.

This number shows up on sites like "reverseaustralia", where complaints associated with the number are recorded. However, the number is still in operation and despite there being a government agency, the Australian Competition and Consumer Commission (ACCC), tasked with dealing with scams of this type, very little is done to tackle scammers directly.

This seems hard to comprehend given it would be relatively easy for government agencies globally to provide a centralised database of numbers associated with scammers. All mobile phones have software available to check phone calls and text messages, and could look up incoming numbers against this database and warn users if there was the slightest suspicion about the caller.

A number of apps are available that actually try and do this using crowdsourced information. Truecaller and Hiya, for example, try and alert a user when someone is calling using a number associated with a reported scam. While these apps are definitely useful in protecting consumers, they are not ideal.

Government agencies like the ACCC in Australia and the Federal Trade Commision in the US receive reports of thousands of complaints from consumers with details of numbers associated with these complaints. It would be trivial for these agencies to make these numbers available to companies like Apple and Google directly to incorporate phone warnings directly into their software without the need for third parties.

The ACCC openly declares that its role is more to provide information than to enforce actual protection because of the difficulty in dealing with scammers.

Google and Apple should, however, be able to do more independently of these agencies. With the advent of machine learning techniques being used to analyse emails, it will be also possible to apply the same

technology to phone calls.

Certain techniques used by scammers are an absolute "tell" of a scam. A recent scam in the US, and spreading world wide, has involved the caller asking at some point "can you hear me" with the expectation of the victim replying "yes". This reply is then reportedly edited into a recording in which the question is changed to one asking the victim if they wanted to go ahead with the purchase of a product or service. This evidence is then used to coerce the victim to pay.

But the list of other scam types is fairly consistent, and so is identifiable by software interpreting the conversation in real time.

Governments should apply pressure on companies like Apple and Google to tackle this problem. Until then however, it is worth using one of the third party apps to ward off scams.

Provided by The Conversation

Citation: Phone scams cost billions. Why isn't technology being used to stop them? (2017, June 26) retrieved 6 May 2024 from https://phys.org/news/2017-06-scams-billions-isnt-technology.html