KCS Group Europe

Super Smish Bros.

20th April 2020

Aside from phishing, hacking, vishing, ransomware, malware, social engineering, insider threats and state-sponsored espionage, a new threat is fast rising: smishing. This is where texts, instant messages and communication apps are used to scam the unwary users, through asking them to click or link or make a payment when the message purportedly comes from a trusted provider such as a bank. It is yet another front in the fraudster's war.

A smishing text could take many forms: a request for money from a friend with a 'new number', an official-looking message concerning an apparently legitimate company, an urgent alert from a bank… while the backstory may vary, the intent in all cases is the same: to con the victim into sending money, or to compromise themselves through link selection. While there are sometimes tell-tale signs (one might wonder why a bank is using a *'goog.gl'* link to their account page, or why a CEO cannot spell his own company name correctly) in general the smishes are plausible at best, and indistinguishable at worst. Indeed, in this respect they are as crafted as the sisterly phishing emails they so resemble: carefully selected victims, with an element of social engineering, targeted with a story designed to ring true and offering solution at the touch of a button.

The added danger with smishing, though, is that smartphones, more than any other device, have become extensions of our everyday lives both professional and personal. A phone will likely not only contain contact details of our networks, but access to emails, personal accounts, pictures, payment portals, and so on – a computer in the palm of our hands. Thus the loss (and the danger) is felt far more keenly, as phones are more personal (and often more valuable) than a corporate computer. And the danger of getting inside one is therefore increased as well.

Smishing has risen dramatically over the past year, in terms not only of pure textual frauds ('click this link now!') but in terms of app fraud, whereby users are tricked into using spoofed and faked apps to carry out their business (think of the damage that a fake banking app could do, for instance, if *'redirected'* towards it). In part this is down to a rise in the number of pure attempts – as more and more people, particularly in the developing world, join the smartphone church, the opportunities will increase – but also it is because of the levels of success that smishing brings. A few hundred downloads of a compromising app may not seem like much, but given the finances to which it potentially acts as a portal, suddenly a little work is needed for a lot of return – particularly if the end user does not spot anything wrong.

Obviously, there is a need for those behind the OS and apps on smartphones to drastically up their protection and scrutiny, but equally all users need to be aware of how and why smishing attacks are proving so successful: and to not voluntarily compromise themselves by not activating anything with less than 100% surety.