Mobile fraud: it's on the rise and what you can do about it

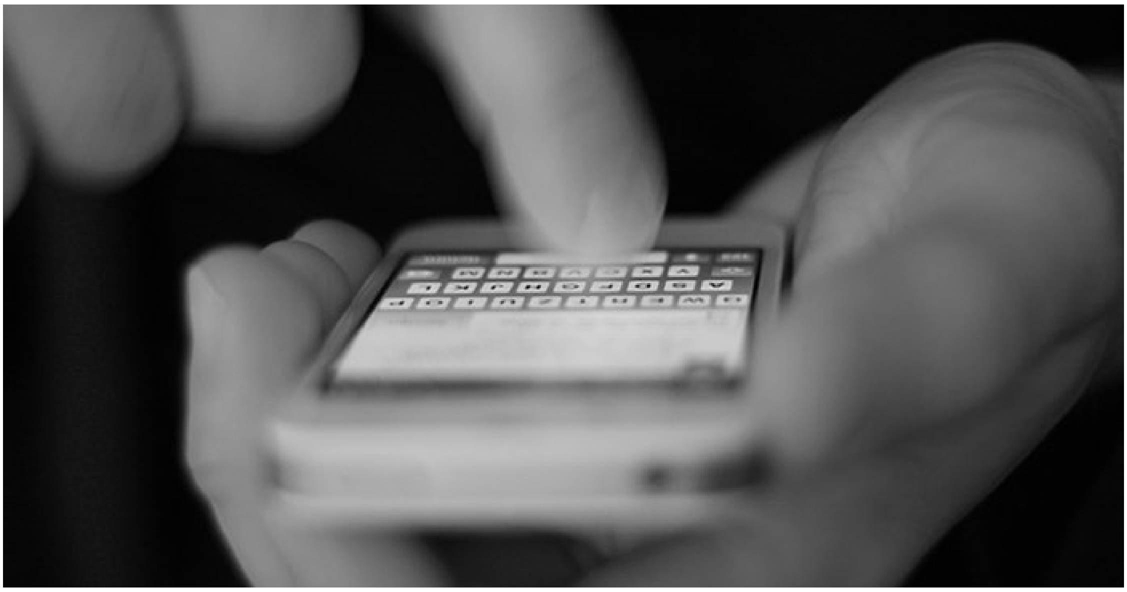
By Chad Fichardt

23 Jul 2015

Think that you are safe? Believe that your mobile device is secure and your transactions completely protected? You'd be wrong...

Fraud has never been more profitable or ubiquitous

In February 2014, RiskIQ unveiled research that showed how malicious mobile apps in Google Play had spiked nearly 400%. That's a staggering 388% increase from 2011 to 2013. In 2015, new research found that there were thousands of unauthorised apps and app stores that referenced high-level brands and that 17% of these were already blacklisted as they had failed a virus scan or linked users to a known source of malware. There are hundreds of thousands of apps and mobile services claiming to offer secure shopping portals or games or entertainment, and a significant percentage of these are actually designed to steal credit card information, banking details and hard-earned cash.



relexahotels via pixabay.com

The Kount book *Nowhere to hide: uncover mobile fraud before it's too late* also pulls out some startling statistics - the most important of these being volume. There are nearly 10 billion mobile devices on the planet today, more than there are televisions and, perhaps even more concerning, more than there are people who own a toothbrush. While oral hygiene is a possible new worry, what these numbers are actually highlighting is how the market is packed full of rich pickings for the criminal element. Fraud has never been more profitable or ubiquitous - geographical location and language are no barriers to entry when it comes to hacking a mobile device and accessing a person's finances.

Primary points of purchase

Alongside the widespread adoption of the mobile device is the rapid growth of mobile commerce or mCommerce. According to Kount, mobile transactions are projected to reach nearly three-quarters of a trillion dollars in 2017. However, it should be up to the user who gets their cash, so how can they protect themselves and be aware of the dangers that lurk unseen on their mobile screens?

The five primary points of purchase for mobile devices are: at the point of sale, as a point of sale, mobile payment platforms, direct carrier billing and closed/open-loop mobile payments. Mobile commerce needs highly specialised fraud prevention to overcome the risks - lost and stolen devices, easy account takeover and creation, loopholes in existing systems that are perceived as trusted, 'click-'n-collect' capabilities move swifter than the systems that prevent theft, and pre-paid mobile devices are cheap tools for fraud.

Invest in protection

Users need to place protections onto their mobile devices to prevent them from being easily accessed. According to Mel Gischen, marketing manager at electronic payment provider, PayU, "Not having a backup or a remote wipe system or placing password protection on a device means that the user may as well walk up to the nearest person on the street and hand them their credit card, login details and a shopping list."

Invest in a good backup solution that is recommended by a reliable source and use it regularly. The same applies to encryption; it's worth adding on an additional layer of protection by using encryption software on all mobile devices as this will instantly slam up a barrier against a quick hack.

Then ensure that remote wiping is activated - most modern devices allow for this and delete all sensitive information the moment the device goes missing. Other options for protecting, and possibly even retrieving, the mobile phone are GPS tracking through services such as 'Find my Phone' and Lock Screen Contact Info where people can instantly see a name and an alternative number and use that data to return the smartphone if it was lost, not stolen.

Gischen adds, "It is vital to check for credible and trusted websites and third-party security providers, especially when making payments on your phone. As a rule, treat this exactly the same as you would when buying online from your laptop or desktop."

Finally, avoid being caught in the first place. Don't sing for joy and enter private information when receiving a text that announces a big prize win, don't fall for a fake charity request, don't provide bank details to anyone unless it is part of a registered transaction and always ensure that apps downloaded from the various app stores are secure, virus-free and valid.

ABOUT THE AUTHOR

Chad Fichardt, senior PR account director at Media Web