Read about the solutions to common Mobile Phone hacking situations

ParentShield's Security Team discusses new solutions to mobile phone security problems as old as the mobile phone itself

A Concerned Parent

ParentShield Child-Safe Network

DERBY, DERBYSHIRE, UK, March 8, 2022 /EINPresswire.com/ -- Mobile Phone Services are targeted by hackers and stalkers because they have traditionally presented an easy target. Although mobile networks have improved their processes considerably, very few phone accounts are protected by the necessary security controls to keep their users safe from hacking or identity theft.

ParentShield is designed to protect vulnerable users with a safe SIM card and is quite different from any other mobile network as a result. Here we look at the common vulnerabilities that mobile networks can suffer from.

Mobile Phones suffer from several security issues:

SIM Jacking
Number Jacking
Phone Hacking
Voicemail Hacking
Domestic Control
SIM Hijacking

SIM Hijacking, or SIMJacking is a broad term for technology or techniques for taking over the control of a SIM card by a third party. In its most technically-advanced forms, it can be performed by simply sending a specially-crafted SMS message to the phone. This can cause the SIM to perform simple tasks including sending data from the phone back to the bad guy.

> Although it may appear less abusive, it's still possible for a partner or ex-partner to move numbers onto "their network' or within their actual account with a view to escalating control or power."
>
> *Graham Tyers*

Such information can include finding the phone location, user information, call information and even perform tasks on the phone. That's pretty scary. A modern SIM card is actually a little computer in itself that can run small applications that are capable of doing a number of things – including sending and receiving messages or placing calls.

No SIMJacking on ParentShield

ParentShield's SIM cards don't support the SAT (SIM Application Toolkit) and all SMS messages – the goto method of invoking such an attack – come to ParentShield phones via our SIM firewall. An example of this can be seen in the Apple iMessage setup SMS messages that ParentShield customers can choose to see. We strip the special control characters from the SMS 'PDU' – the encoded SMS message, and allow the message to be seen as if it were a standard message.

Number Jacking

Number Jacking is the technique increasingly used to take over someone else's mobile phone number – usually with a view to obtaining OTP (One Time Passcodes) such as those sent to authorise payments or access to websites that use the phone for Two Factor Authentication (2FA).

'Owning' or in hacker speak 'pwning' someone's phone number means it's possible to access the Mose valuable and sensitive information controlled by that person. In many cases people find in a very short space of time that their bank accounts, social media accounts, and whole identity is compromised.

This can be achieved by a simple phone call to many mobile phone companies and, because they generally have very poor security processes, just pretending to be the account holder allows the attacker to close their account, and request a PAC that allows the number to be transferred to a new SIM.

Domestic Control via NumberJacking

Although it may appear less abusive than identity theft it's still possible for a partner or ex-partner to move numbers onto "their network' or within their actual account with a view to escalating control or power. Controlling someone's mobile phone – their plan, minutes, texts and data is a powerful control and even wittingly allowing this control to fall into the wrong hands can become a real problem if relationships fall apart – it's something that ParentShield sees every day.

ParentShield blocks all ‘shortcode’ SMS messages of the type used to communicate with the network so the most common variants of this attack will fail before they even start.

ParentShield users are NEVER presumed to have any authority or control in any way – so all the systems in place involve a direct communication with the parents.

While inbound number ports are possible onto the ParentShield network, they are never performed without question. The controls in place are considerably more stringent than with any other network. As a rule inbound Number Porting would only ever be performed on the instruction of a child’s social worker or a suitably-appointed welfare officer.

Phone Hacking or VoiceMail Hacking

Phone Hacking became a household name in the naughties with dozens of celebrities and espionage targets falling prey to unscrupulous, journalists in some cases, accessing voicemail messages. It has been widely practiced ever since the telephone voicemail has been in place, which is just about as long as there have been mobile phones.

Many people aren’t aware that their voicemail is stored totally unencrypted by their mobile phone company and can be accessed by simply using a simple PIN number that most mobile networks set to ‘0000’ by default. This means that anyone who wants to access your stored or current voicemail messages can do so without very much difficulty. Mobile networks have grown to have hundreds of millions of users and simply don’t have the support staff and systems to properly police SIM reset and access queries. Knowing just a little about the target – which you certainly would if it was your child’s or ex-partner’s child’s phone that you were trying to access.

No phone hacking with ParentShield

Voicemail always presumes that the person using the phone has the ability to secure and safely control their own phone and their own voicemail. So ParentShield has completely removed the VoiceMail system from its network. Obviously having no voicemail makes the process of hacking it redundant.

About ParentShield

ParentShield is the UK’s only Mobile Network designed specifically with children in mind, incorporating a wide range of tools - from call recording to keyword alerts - that allow parents to oversee their child’s phone usage without invading their privacy. It can work with any unlocked feature-phone, smartphone or smartwatch and does not require any app or parental controls to be set on the device. Its features are handled remotely, allowing for optimal convenience while kids retain their independence. The SIMs work across the UK and beyond.

Graham Tyers
Engine Mobile Ltd.
+44 1283 707057
email us here
Visit us on social media:
Facebook
Twitter
