
**July 22, 2019**

## Protecting Your Cell Phone When a Hacker Gets Your Number

**Risk Management Question:** In haste, you mistakenly respond to a spoofed email that appears to be from a colleague before realizing you've just provided your cell phone number to a hacker. Or, you leave your cell phone in a taxi on the way to the airport, or in the pocket of the seat in front of you on the plane. *What can you do to protect yourself and the information accessible from or stored on that phone?*

**The Issues:** As we store more and more sensitive information on our mobile devices (aka cell phones) they have increasingly become a target of cyber crooks. Phone hacking methods range from traditional spear phishing and social engineering exploits to hacking into live conversations or into your voicemail, or the data stored on one's smart phone. It can also involve a SIM card swap, which is when a hacker convinces your carrier to switch your phone number over to a SIM card that they own. The hacker can then divert your incoming messages, use your phone number to make purchases in your name, trick your online accounts into changing your password for them, and send messages to others loaded with malware that appear to be from your mobile device. Unfortunately, once the bad actor has unprotected access to a phone, there is not much the victim can do. Prevention is the key, and protecting your mobile device should be your paramount concern.

**Risk Management Solutions:**
In addition to always being vigilant about responding to suspicious emails, the following security tips can prevent phone hacking:

1) Stop treating your mobile device like it's merely a cell phone. Recognize that it is a powerful mini-computer that is the gateway to your online accounts, your contacts, and in some instances, even to your employer's or Firm's network.
2) Limit the persons to whom you provide your cell phone number.
3) Never provide your cell phone number in response to an email until you have confirmed the actual identity of the person to whom you are providing it.
4) Do not leave your mobile device unattended, even momentarily, while in public places.
5) Do not allow third parties to use your mobile device out of your presence.
6) Download antivirus protection for your device.
7) Do not rely on your device's default passcode; change it.
8) Add a PIN or passcode on your wireless account.
9) Consider using two-factor authentication codes or, even better, an authentication app such Google Authenticator, Authy, or Yubikey—a physical authentication method.
10) Avoid using unprotected Bluetooth networks and turn off your Bluetooth service when you are not using it.
11) Do not allow your device to automatically connect to Wi-Fi networks. You should choose the network to join—not your device—and avoid using unsecured public Wi-Fi.
12) Use a protected app to store PIN numbers and credit cards, or better yet, do not store them on your mobile device at all.
13) Turn off the device's autocomplete feature and regularly delete your browsing history, cookies, and cache.
14) If you have an iPhone, enable "Find My iPhone."

15) If you have an Android device, consider a security app that increases its protection. There are applications available that not only provide an anti-virus solution, but also the ability to locate, lock, and remotely wipe your device if it is lost or stolen.
16) If you are a high-value target or have a sensitive account, disentangle important accounts from your cell phone number, or consider keeping those accounts on a separate device.

For a more information on protecting you device, here are a couple of helpful articles:

How to Prevent Phone Hacking and Protect Your Cell Phone (*Webroot*)

How to Protect Yourself Against a SIM Swap Attack (*Wired*)

Remember, let's be careful out there.



Steven M. Puiszis
312-704-3244
spuiszis@hinshawlaw.com


Anthony E. Davis
212-471-1100
adavis@hinshawlaw.com


Noah D. Fiedler
414-225-4805
nfiedler@hinshawlaw.com


Annmarie D'Amour
212-471-6231
adamour@hinshawlaw.com