Are Your Communications Secure? 3 No-Brainer Tips to Protect Your Smartphone from Hackers

Are you using an unknown wi-fi network at that coffee shop you're in? That's a no-no.

April 30, 2018 5 min read

Opinions expressed by *Entrepreneur* contributors are their own.

What would it be like if all the pictures on your phone were made public? Or, worse, if all your vital information, like your bank details, chat logs and passwords, was leaked?

Related: 6 Tips to Stop Hackers from Stealing Your Data and Your Business

Those scenarios are scary but happen every day; untold numbers get hacked no matter what their industry or sector. And, with new mobile applications coming all the time, the threat will only increase. One study revealed that out of over 8 million unique malware-installation packs for mobile devices, the majority of the packs were out there *only to steal money or personal data.*

According to Brandie Claborn, VP and chief communications officer at the security software company McAfee, the target for hackers is communication; and that, Claborn said, is our "most critical infrastructure." In fact, it's not farfetched to say that, should an attack on communications media occur, the reason would be increased hardships and

instability.

Those hardships would likely be widespread: In a University of Phoenix study, 84 percent of the U.S. adults polled said they had at least one social media account, and 86 percent were wary about sharing personal information on those accounts because, they said, they were afraid of being hacked.

Social accounts have made communication very easy; and in this regard, an enormous amount of data is exchanged daily. But the risks of people seeing their accounts compromised grows as we all become increasingly dependent on technology – especially our smartphones.

Related: Why We Need to Worry More Than Ever About Getting Hacked

Remote workers are one group particularly affected by the activities of hackers. According to a Gallup survey, these workers are probably the most engaged employees in the American workforce, particularly those spending between 60 and 80 percent of their time working at home.

The problem, however, is that, working from home, these remote workers may be less secure from cyber attacks in their online activities than their colleagues in office settings. Yet, in the course of their communications, they share a great deal of important data which is at risk of being compromised.

How do hackers get access to people’s communication media?

Hackers have a lot of tricks up their sleeves. When they gain an inroad into your social media accounts, they’ll either leak your personal information or try to make money off it. Once they “get” you, their next targets will be the friends and family on your contact list.

One of their deadliest actions is to take possession of your smartphone data. Since we hardly log out of the social accounts on our phones, hackers can gain access and rummage through our personal data.

To gain that access, hackers will send you an exact replica of the email notifications social media platforms send to your email. The email has the same branding logo and print fonts as the social media platform, so you'll hardly be able to tell the difference. When you log in, the hacker on the other end will be watching for your login details.

How do you protect yourself?

There are many methods and applications you can use to protect yourself from the destructive activities of hackers on communication devices like your smartphone. Here are three simple tips that can give you a good degree of protection:

1. Mind the apps you install. It's not a bad thing to stay updated with the latest apps, but you need to be careful where you download them from. The two most recognized app stores are Google Play and the Apple App Store. Both verify and scan apps before they add them to their product lists.

Other app sources, however, don't pass their apps through as much security, making many of those apps a safe haven for hackers.

2. Update your apps. Apps go through a series of updates. App developers are always on the lookout for bug fixes and security upgrades. To ensure that your vital information is protected from hackers, update your apps.

Usually, when there is an update to the apps on our phones, you'll get a notification of the latest update. Don't ignore it. And if by chance you disabled the notifications feature, turn it back on. Your smartphone will thank you for it.

3. Don’t tap into unknown wi-fi. Who wouldn’t be tempted with free wi-fi? But, as tempting as it may be, tapping into an unknown wi-fi network on your smartphone can create an avenue for hackers to get into your personal details.

Related: Hackers Can Use Subtitles to Infect Your Devices

What happens when you use open wi-fi is that anyone within your physical vicinity can easily snoop through your computer or phone. Due to the risks involved, it’s much safer to stay clear of unknown wi-fi altogether. You can also use a virtual private network to route your connection through a private encrypted channel that will shield the contents of your device, making sure that the information you value stays out of the wrong hands.

https://www.entrepreneur.com/article/311906