CSO

FEATURE

Alternate keyboard apps: Too risky for your smartphone?

Ronald and Dylan Kaplan examine why alternative keyboard apps pose security risks you may not have considered

By Ronald Kaplan and Dylan Kaplan

CSO | Oct 3, 2014 9:36 AM PT

Smartphone security comes in several flavors. Most people think about who or what they email or text as the biggest privacy concern. But if you are using your smartphone for even a narrow range of its capabilities, think again.

Bank account numbers, Social Security numbers, credit card numbers and birthdates are all private information that many people repeatedly enter into their smartphones to complete transactions. What if every one of those items you entered into your smartphone were captured and retained by a third party company? Further, suppose that third party is a small startup about which you know little or nothing about.

[7 security mistakes people make with their mobile device]

[What's wrong with this picture? The NEW clean desk test]

Search tools are easily able to find patterns, like ###-##-#### for Social Security or #### #### #### #### for credit cards or just nine-digit and 16-digit numbers. This information can be automatically filtered and associated with your user id and validated by its repeated use. Who would hand over this invitation for identity theft to any old group of individuals who is smart enough to write a smartphone app? They might be creative, smart, entrepreneurial, but are they honest?

Another question you need to ask is: “are they better than Home Depot, Target and Albertsons in securing the personal data you gave them?” We know Home Depot, Target and Albertson were hacked and they have many more security professionals securing the data they capture than any small app developer. Securing such valuable data is not a simple task. The higher the value of the data, the more resources identity thieves will throw at their attacks.

At this point you are probably thinking “I’m not handing over such personal information to anyone, why would anyone do that?” Think again if you are using one of the many alternative keyboards on your smartphone. Whether the purpose of the capture is to improve accuracy or operation of their system is guise or fact doesn’t really matter.

They have your data and you trust that they are securing it from hackers and that they themselves will not use your data inappropriately or will not provide that data to anyone who knocks on their door with a court order or subpoena. Further, the developer may have only good intentions, but their code could be hacked with malicious intentions. Hacking is very unlikely for apps distributed in places like the Apple Store, but third party app stores like Cydia, used by those who jailbreak their iPhones, hacking is a real possibility. In this posting a case of an alternative keyboard app transformed into a keyboard logger is documented.

Tips for smarter smartphone use

1. Ask yourself when using these devices, "Do I care if anyone knows this?"
2. Isolate your professional life from your personal life.
3. Keep some privileged or confidential information on your devices.
4. Control the number and location of backups.
5. Don’t try to fool the professionals by hiding or deleting information.
6. Quit posting everything you do on social networking sites.

Is the data encrypted? Probably not. Certainly it could be encrypted but they often do see it as “real data,” so why encrypt. Their stated purpose for retaining your keystrokes is to analyze it for accuracy and patterns to improve the operation of their product. Often the functionality of the operation of their product depends upon the capture and analysis of your keystrokes, so if they don’t capture it many of the benefits of the alternative keyboard won’t materialize.

You should read the EULA (end user licensing agreement), but most people just click through it. The developer usually discloses that they capture and retain your data and that they won’t share it with anyone. But can you really trust those disclosures? Target, Home Depot and Albertsons made those same promises and they were not able to keep them. Besides, is that really going to protect your data from a court order?

Products that provide “swipe” keyboard functionality are certainly enticing. Who of us doesn’t want to add speed and accuracy to their data input? But as with any innovation the benefits must be weighed against the drawbacks. Do you really want someone having a copy of your every keystroke?

[12 privacy-destroying technologies that should scare you]

Before making that decision spend a week paying close attention and really thinking about all the stuff you type into your smartphone and then decide if it makes sense to give up that privacy. This is the kind of thing most of us don’t spend any time thinking about, so we have little or no idea of all the information that would be captured and retained. Remember that this is one of those many things that can’t be pulled back once it is revealed (think about email, once the send button is hit or toothpaste that has been squeezed out of the tube).

Our personal position is that there is no way we want our keystrokes stored and available to anyone but us. We fully understand that the developers can only go so far in helping us improve our efficiency without the benefit of analyzing our keystrokes. Siri, and its sister products on the Android and other platforms, capture our voice inputs and transform them into text.

They continuously analyze the accuracy of their results to refine and improve the analysis in their algorithms. This is common practice for any technology that strives, but never reaches, 100% accuracy. We would certainly enjoy taking advantage of the benefits of these innovations, but for us it’s not worth the drawbacks. We know our private information is rapidly losing its private character, but we refuse to consciously allow anything to accelerate that process.

In a previous article, published in CSO Online entitled "6 tips for smartphone privacy and security" the issue of controlling your data is addressed along with other privacy-related behaviors. However, the alternative keyboard app lies beneath the surface for those who don't have the knowledge or interest needed to understand how and where these apps derive the efficiencies that power their product. Alternative keyboard apps are just one glaring example of how protecting your privacy requires diligence.

Ronald Kaplan, MS, MBA is a partner at SICons, a management consulting and computer forensic expert witness firm in Los Angeles. He can be reached at rkaplan@sicons.com. Dylan Kaplan, BS, is a recent graduate of the Eller College of Management at the University of Arizona, specializing in Management Information Systems. While at the University of Arizona, Dylan worked at Apple Inc. providing technical support. He is currently a systems engineer living in Silicon Valley. He can be reached at dylankaplan@gmail.com.

Follow everything from CSO Online

Insider: How a good CSO confronts inevitable bad news