Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

HomeKit Vulnerability: One More Reason to Accept New iOS 11.2

Apple has pushed an update to iOS 11.2 to its users. Users should consider pushing any updates that are recommended by the manufacturer, as there is usually a reason behind the update, and many times it is to fix a vulnerability. This is true with the most recent update to iOS 11.2.

A vulnerability in HomeKit was recently discovered that allows unauthorized individuals (i.e., hackers) to control IoT capabilities, such as smart locks, garage door openers, lights, thermostats and plugs through the HomeKit platform. This means that when you are able to remotely activate the security system in your residence or open and close your garage door with your smartphone, a vulnerability allows an unauthorized person to be able to do that remotely. This is an obvious concern for personal safety. *Read more*

Early Adopter—Vanguard Announces Plan to Utilize Blockchain Technology

Top mutual fund firm The Vanguard Group, Inc. unveiled a plan last week to incorporate blockchain smart contract technology into some of its indexing operations beginning early next year. Vanguard's initiative will be carried out through a partnership with the Center for Research in Security Prices (CRSP) and technology provider Symbiont and is intended to simplify Vanguard's index data sharing process. By utilizing a dedicated blockchain network created by Symbiont, Vanguard hopes to make CRSP data available to investment managers on a nearly instantaneous basis.

Vanguard's plan comes at a time when many large financial institutions are hesitant to fully commit to incorporating blockchain's untested technology into financial systems that are already subject to daily cyber threats. However, Vanguard believes that its use of blockchain will allow it to distribute sensitive and time-critical index information in a secure manner not possible under its current system, which relies on providers such as CRSP to send manual updates of fund data to investment managers throughout the day. *Read more*

December 21, 2017

FEATURED AUTHORS:

Scott M. Baird
Linn Foster Freedman
Benjamin C. Jensen
Kathryn M. Rattigan
Matthew W. Rizzini
Norman H. Roos

FEATURED TOPICS:

Cybersecurity
Drones
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

Proposed Legislation in New York Would Recognize Enforceability of BlockChain Transactions and Explore Applications of Technology

While the investment potential of cryptocurrencies, including BitCoin, has been all over the news in recent weeks, state governments have begun to explore the practical applications of blockchain, the technology underlying BitCoin. In New York, Assemblyman Clyde Vanel introduced four bills in late November related to blockchain technology. The first, Assembly Bill 8780, would amend the state technology law to allow signatures, records and contracts secured through blockchain technology to be considered valid electronic records, and signatures and further to recognize the legal validity of the use of smart contracts in commerce. This proposed legislation, recognizing legal effect to blockchain transactions and smart contracts, is similar to laws recently passed in other states, including Arizona, Nevada, and Vermont. *Read more*

Beware of New Ransomware—Spider Virus

There is no relief in sight for combating new strains of ransomware. One new ransomware, dubbed the "Spider Virus," was discovered by researchers at Netskope on December 10, 2017, and continues to attack victims to date.

To implement the Spider Virus, attackers send malicious emails containing a Microsoft Office attachment that includes macros to potential victims. If the attachment is opened and the macros are enabled, the user unknowingly downloads ransomware into the system. The ransomware encrypts the user's files, adding a "spider" extension to the files and then displays the ransom note, which tells the victim that it has been "INFECTED WITH FILE SPIDER VIRUS" in RED BOLD LETTERS with a black backdrop. *Read more*

DRONES

President Trump Reinstates the FAA Drone Registration Requirement

By signing the National Defense Authorization Act for 2018, President Donald Trump reinstated the requirement for recreational drone operators to register with the Federal Aviation Administration (FAA). The requirement was initially introduced in late 2015, but in May of this year, a D.C. Circuit Judge ruled that the FAA did not have proper authority to enforce the requirement. The Judge cited a 2012 aviation law which held that recreational drones are considered model aircraft, and that model aircraft cannot be regulated by the FAA. *Read more*

PRIVACY TIP #119

Getting the Newest Smartphone as a Gift? Take Care When Downloading Apps

'Tis the season for gift giving. Smartphones and mobile devices are a hot item during the holidays. The first thing many people do when they get a new phone or device is to start downloading apps. Since there will be a lot of downloading over the next week, here are some tips to help you detect fake apps before you download them.

Some people aren't aware that fake apps exist. They do, and if they are downloaded, they can be used by cyber criminals to take control of the device and ultimately steal your money and your personal information. A recent example is a fake version of WhatsApp, which was downloaded over one million times before it was discovered that it was fake. It was listed as Update WhatsApp Messenger. It was removed after it was reported by Reddit.

Fake apps can be very hard to detect. Here are some tips for basic app hygiene:

- Only download apps that you will actually use and that you have confirmed are legitimate. It is not a badge of coolness to download every app made
- Read the terms of use (yes, really read how the app is using your data, what it is capturing, and if it has access to your camera, microphone or location)
- Carefully review the title of the app and the description of the app. If the title, or words in the description are misspelled or the grammar is off, it could be a fake app
- Look at the app's download count. If the count is relatively low, it could be fake
- Review the permissions the app is requesting. If an app is asking for permission to access the camera, your contacts, the microphone and SMS messaging, and those permissions make no sense, it may be fake and trying to get as much access to your device as possible
- Never allow an app to obtain administrator privileges over your device
- Delete apps you no longer use

If you download a fake app, delete it as soon as you can. If it does not allow you to delete it, then wipe your phone and start over.

Finally, review the apps that you have given permission to access certain portions of your device by going into Settings, then Privacy and check each listing to see which apps have access to your contacts, calendar, photos, Bluetooth, microphone, speech recognition, camera, health, HomeKit, media, and motion & fitness. Yikes, when you think about it, that's a lot of information being given to app developers. And don't get me started on biometrics and facial recognition…

This holiday season, make educated choices about which apps you download and how much information you are allowing those apps to have access to on your phone.

Happy holidays!

© 2017 Robinson & Cole LLP. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission. This document should not be considered legal advice and does not create an attorney-client relationship between Robinson+Cole and you. Consult your attorney before acting on anything contained herein. The views expressed herein are those of the authors and not necessarily those of Robinson+Cole or any other individual attorney of Robinson+Cole. The contents of this communication may contain attorney advertising under the laws of various states. Prior results do not guarantee a similar outcome.