Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

NIST Publishes Updated Cybersecurity Guidance and Guidance on Passwords

The National Institute of Science and Technology (NIST) has long been a leading authority in cybersecurity—even before cybersecurity became a household name. It originally published its *Cybersecurity Framework*-intended not to be a standard, but to offer guidance—to all industries on how to begin to tackle data security.

As cyber threats expand and become more sophisticated, NIST continues to provide guidance which is helpful to the public and private sectors. NIST recently published its most recent draft cybersecurity guidance, which provides important information for companies to consider. NIST is seeking comments to the draft guidance until September 12. *Read more*

Scammers Strike Enigma Initial Coin Offering

In the latest example of security risks associated with initial coin offerings (ICOs), the blockchain startup Enigma reported on August 21 that online scammers used fake solicitations for an ICO presale to steal approximately $500,000 in ether (a virtual currency) from investors.

Enigma is a blockchain startup incubated at MIT Media Lab that is in the process of rolling out its first product, known as Catalyst. Catalyst is described as a platform providing data sets and developmental tools specifically geared for hedge funds focused on cryptocurrency markets. Enigma's funding was to be derived, in part, from a planned a token sale on September 11, 2017, with a goal of raising $20 million worth of ether. *Read more*

DRONES

UAS Components of FAA Reauthorization Bills Stalled

August 24, 2017

FEATURED AUTHORS:

Linn Foster Freedman
Benjamin C. Jensen
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Drones
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

We recently wrote about the Federal Aviation Administration (FAA) Reauthorization bills that would allow funding to the FAA to continue beyond Fall 2017. Now, it is likely that as Congressional leaders seem unlikely to reach a compromise on the FAA reauthorization bills before the end of September, a short term extension on these bills will occur. While committees in each chamber approved separate long-term reauthorization legislation in July, the unmanned aerial systems (UAS or drone) provisions may be delayed due to the lack of consensus on other manned aviation issues (e.g., air traffic control privatization and pilot training requirements). However, if the extension occurs, and the legislation does advance, these bills will address some key issues in the UAS space, including privacy protections, carriage of property, UAS traffic management, risk-based permitting, UAS defense (and counter defense), recreational drone registration, and public aircraft operations. *Read more*

The Commercial Drone Technology Evolution

The commercial drone technology ecosystem has come a LONG way in the last five years, and businesses all over the world have spent years exploring the potential of drones. Over this time, there have been at least eight distinct levels of evolution within commercial drone technology. *Read more*

PRIVACY TIP #102

How to Educate Your Employees to Use Long, Easy to Remember Passwords

I feel like I have been writing about passwords over and over and that's because I have. Despite repeatedly hearing about how important passwords are, compromised passwords continue to be an issue for organizations.

Since the National Institute of Science and Technology (NIST) recently published new guidance and is recommending the use of long, easy to remember passphrases, I thought it was an opportune time to give you some of the tips I use to educate client employees on recommended practices regarding passwords.

It is important that when an employee sits down at his or her company work station or laptop, that s/he can remember his or her password without having to refer to any written piece of paper (like a sticky note taped to the front of the workstation or inside the laptop) or check the notes on their phone. (I refer to these two examples as this is what many employees do every day so they can remember their password.) You have to get it into their brain that they have to memorize their password. It must be in their brain. I liken it to Tom Cruise in *Mission Impossible* getting his instructions and then they self-destruct. Employees in general like *Mission Impossible* movies

and laugh, but get the point. They need to come up with a password that they can memorize, self-destructs, and is not retrievable.

I am a believer in the use of long, easy to remember passphrases, which is consistent with NIST's guidance. One example I use is Myfavoritecolorispurple$ or, Myfavoritecolorisblue! This of course is not my password, but it is a clear example of a complex passphrase that is easy to remember. It has a capital letter, lower case letters and a number or symbol. My IT colleagues approve and say it is complex enough for most password requirements.

When you give your employees ideas for long, easy to remember passphrases like the ones above, tell them not to actually use the example! They need to come up with a unique phrase that they will remember when they log on to their computer. Give them subject matter ideas like hobbies, (IwishIwasasingledigithandicap/) or travel (IloveNewOrleans$) or animals or pets (Icaught5bass!) or seasons (Fall!smyfavoriteseason).

You get the drift.

The other nice thing about using passphrases is that NIST agrees they can be used for a longer period of time so employees don't get frustrated with having to change their passwords every 60 days.

So check out the new password guidance from NIST here and try to make the password education fun and engaging.