Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Pentagon Web Monitoring Data Exposed

Security researcher Chris Vickery has confirmed that web-monitoring data from the Department of Defense (DOD) was exposed through Amazon Web Services due to the way the DOD configured access by authorized users. According to Vickery, anyone with a free AWS account had access to the DOD information, which included 1.8 billion internet posts that had been scraped from publicly available sites, including information about guns, scam alert websites, and forums that contained offensive content.

Although none of the information was considered sensitive, it highlights that data is being exposed "haphazardly" according to Vickery, and "is a huge, epidemic sized problem." *Read more*

DATA BREACH

Florida Blue Breach Exposes Information of 939 Individuals

Blue Cross Blue Shield of Florida (Florida Blue) has announced that 475 applications for insurance were backed up to the cloud, on an unsecured cloud server, by an unaffiliated agent of Real Time Health Quotes, which exposed the personal information of 939 individuals.

The data that was backed up to the unsecured cloud server included Florida Blue files and copies of health, dental and life insurance applications from 2009-2014. The applications included the names, addresses, Social Security numbers, medical histories, and some banking and financial information. *Read more*

Forever 21 Latest Retailer to Suffer Credit Card Breach

Forever 21 has warned customers who used a credit card at any of its stores between March and October 2017, that their credit card may have been compromised.

November 22, 2017

FEATURED AUTHORS:

Linn Foster Freedman
Kathryn M. Rattigan
Matthew W. Rizzini

FEATURED TOPICS:

Cybersecurity
Data Breach
Drones
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

According to Forever 21, its payment card readers were not encrypting credit card information during that time and it believes there may have been unauthorized access to the credit cards. It has not indicated how many customers' cards were compromised. *Read more*

DRONES

Tethered Drone Operator's Part 107 Waiver Granted by FAA

A Columbus, Ohio based company, CivitasNow, has just become the second company ever (CNN was the first) to be granted a Part 107 waiver to fly drones over people by the Federal Aviation Administration (FAA). The FAA gave the company approval to allow its Aerotain Skye drone to operate over unsheltered people on the ground. The Aerotain Skye is a helium filled tethered drone, which, according to the agency, "resembles a tethered, floating beach ball," and "carries a camera and small motors for propulsion." Aerotain calls it the safest drone for live entertainment, with a weight of 14 lbs. and a diameter of about 7.5 feet. It looks like a very small blimp. *Read more*

Law Enforcement Forced to Learn New Skills—Criminals Turn to Drones

We know by now that there is a good chance someone is out there spray painting his drone black and taping over the lights so that he can get away with flying his drone into a prison yard to deliver contraband. But drones are also being used to spy on people, interrupt the work of emergency services, harass wild animals, and menace other aircraft. Because crime and nuisance with drones seems to be a growing trend, law enforcement has been forced to launch new forensic intelligence forces to deal solely with drone-related crimes, such as how can a criminal drone pilot be identified, when only a drone is found at the scene of a crime? Or when only fragments from a drone are found? Or when only a controller or mobile phone is found? Or when a likely pilot is suspected but no drone is in sight? *Read more*

PRIVACY TIP #115

Cyber Monday Safe Online Shopping

It is estimated that consumers will spend $4 billion online this year, including on Cyber Monday, coming up in just a few days.

With the growing increase in online shopping, particularly over the holidays, it is prime time for scheming scammers to take advantage of the unwary online shopper. Here are some things to think about while

shopping online:

- Shop directly from the store and/or brand's website instead of through a search engine. If you find something through a search engine, actually buy it through the manufacturer's or brand's direct website.
- Be wary of "deals" on Facebook and other social media sites. They can be fake or compromised Facebook accounts that ask you for credit card information or financial information and steal it. If a deal is too good to be true, it probably is a scam. Don't give your credit card or other financial information through a social media site.
- Be very cautious about Cyber Monday emails with embedded links or attachments that ask you to open them for a coupon or special deal. Any attachments or links in an email are suspect and may contain malware or ransomware. Delete them and do not open attachments or links.
- Use credit cards instead of debit cards when shopping online. A debit card gives a criminal direct access to your bank account, whereas if there is a fraudulent charge on the credit card, the bank will investigate and potentially reimburse you for some, if not all, of the fraudulent charges.
- Do not be tempted by pop-ups offering amazing deals. If you click on it, it could contain malware or ransomware. Again, if the offer is too good to be true, it is probably a scam.
- When you check out, confirm that you are on a secure connection by making sure there is a padlock icon to the left of the URL of the site and the URL should say https, which means it is a secure transmission.
- Don't shop online using public wifi. Why does anyone use public wifi anymore? It is not secure!
- Update your security software on both your computer and your mobile phone before you go shopping online.

Happy Thanksgiving and safe shopping during this holiday season!