Attorney Advertising

Robinson+Cole

Data Privacy + Cybersecurity Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Now is the Busy Season for Cyber Criminals Posing as Executives to Obtain W-2s

It's the start of tax season, and many employers are sending W-2 forms to employees so they can get ready to file their tax returns. As was true over the past few years, this is not only the busy season for tax preparers, but also for cyber criminals seeking to reap millions from U.S. taxpayers by filing false tax returns to obtain a fraudulent tax refund.

Although this has been happening for years, employees still fall for this old scheme. It is such a problem that the IRS has issued multiple warnings to get the word out that this scam continues to occur and to assist companies from becoming a victim. *Read more*

Protect Yourself From Year-End Charitable Giving Scams

December is traditionally a busy month for charitable giving, as many donors are inspired by the holiday season to give generously to those in need, while others look to make year-end gifts that will qualify for a tax deduction in the current tax year.

Unfortunately, because of the increase in charitable giving, there is often an increase in charity scams during the holiday season. Donors should be wary of communications from unfamiliar organizations, including emails, texts, and phone calls, and should not provide personal or financial information without verifying the legitimacy of the request. Scammers often use popular charitable causes to solicit contributions, for example, by claiming that contributions will be used to help veterans, children, or cancer patients. The New York Attorney General recently announced the forced dissolution of one such organization, VietNow National Headquarters, which falsely claimed that contributions would be used to provide services and medical treatment to veterans. *Read more*

January 4, 2018

FEATURED AUTHORS:

Linn Foster Freedman
Carly Leinheiser
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Data Breach
Drones
Enforcement + Litigation
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

ENFORCEMENT + LITIGATION

Federal Trade Commission Approves Settlement with Lenovo Over Ad Software

The Federal Trade Commission (FTC) has approved its proposed settlement with Lenovo, Inc. over pre-installed advertising software called VisualDiscovery onto Lenovo laptops. According to the FTC, the pre-installed software "interfered with how a user's browser interacted with websites and created serious security vulnerabilities." *Read more*

DATA BREACH

Ancestry.com Server Exposes 300,000 Email Addresses and Passwords

Ancestry.com has confirmed that RootsWeb, its free website for individuals to search genealogy, recently had a security vulnerability on its server that exposed a file containing the usernames, email addresses, and passwords of 300,000 users. The compromise occurred in 2015.

According to Ancestry.com, most of the accounts that were compromised were from free trial or currently unused accounts. No financial information or Social Security information is included in the exposed file. It is informing the users whose information has been compromised.

Nonetheless, users of Ancestry.com may wish to change their passwords. *Read more*

DRONES

Surprising Predictions for the Commercial Drone Industry in 2018

2017 marked a big year for the commercial drone industry; for starters, it was the first full year of the Federal Aviation Administration's (FAA) Part 107 operating license. Now, there are over 70,000 pilots flying drones all over the skies for all sorts of purposes and applications. But since the start, the only consistent thing about the commercial drone industry has been its rapid (and radical) changes, and 2018 is sure to see even more revolution. *Read more*

Drones and the Future of Watching Sports

Some may consider drones to be annoying and noisy, but in the next few years, drones are going to become quiet, small, safe and almost effortless to fly. And because of these changes, drones will also change the way sports are covered by the media. Why? Well, drones are the perfect action cameras. Like many of the athletes they film, drones can defy physical limitations. They are more flexible and spontaneous than media camera rigs. They can film pretty much anywhere: a cliff face, over open water, or behind a dirt bike moving at 60 mph. Drones can mimic the way athletes move and with the ability to do that, drones can obtain footage beyond typical sports coverage. Drones can convey not only the image but also the feeling of the movement we are watching. *Read more*

PRIVACY TIP #120

Follow FBI Warning About Connected Toys

The Federal Bureau of Investigation (FBI) issued a warning to parents in the past about the concerns with connected toys. Many parents recently bought the newest gadgets for their kids over the holidays, without realizing the capabilities of these toys to collect, maintain, sell, and use personal information. As I chat with people about the cool gifts they gave their kids, it is worth mentioning again the risks associated with connected toys.

Toys are Internet of Things devices just like a smartphone, an alarm system or an oven. All of these computers can access, collect, maintain, sell and use the information they have access to in your home, including your child's face, voice, conversations, and location. Creepy—yes.

Prior to purchasing a smart toy for a child, understand its capabilities, whether it has a microphone, location based capabilities or a camera, what data it can collect, and what it is doing with the data. Do a little research to see if there are any complaints about the toy or the manufacturer of the toy. Check the manufacturer's privacy policy to see how they are collecting, protecting, disclosing or using your child's data. Use secure Wi-Fi to connect the toy. If you can create a password on the toy, create and use the password.

Remember that anything connected to the Internet is hackable. Make an educated choice before turning connected devices and toys on in your home. We have pointed out some examples in the past [view related post], but technology is advancing and is more sophisticated, so vigilance is warranted. After speaking with one of my friends about smart toys, she did some research and decided that it was not something she wanted her child to play with or that it be in her home at all.