Attorney Advertising

Robinson+Cole

Data Privacy + Security Insider

Leveraging Knowledge to Manage Your Data Risks

CYBERSECURITY

Forrester Cyber Predictions for 2017: Harsh Reality

Forrester recently issued its "2017 Predictions: Dynamics That Will Shape the Future in the Age of the Consumer," which among others, makes interesting predictions relating to cybersecurity risks coming up in 2017. The predictions include the CIO and the Brass Ring, Consumer Trust Is Key to Success, Scarce Talent, the Internet of Things, Artificial Intelligence, and Cloud Computing. *Read more*

ENFORCEMENT + LITIGATION

FTC Hits Telemarketer for Calling Consumers on Do Not Call List

The Federal Trade Commission (FTC) has fined the Consumer Education Group $100,000 for making millions of illegal telemarketing calls to consumers who were on the Do Not Call (DNC) Registry, including prerecorded robocalls in violation of the Telemarketing Sales Rule (TSR). The calls were made between 2013 and 2015 and were part of a campaign to generate sales leads for other companies. *Read more*

DATA PRIVACY

Broadband Providers Face New Regulations for Protection of Consumer Data

Last week, the Federal Communications Commission (FCC) released landmark protections for internet users, requiring permission from broadband subscribers before broadband providers can collect data on the subscribers' web browsing, app use, location information, or financial information. Broadband providers rely on subscriber data like this to create sophisticated, targeted advertising. Many privacy groups applaud the FCC's efforts. However, these FCC regulations have their limits. *Read more*

November 3, 2016

FEATURED AUTHORS:

Linn Foster Freedman
Kathryn M. Rattigan

FEATURED TOPICS:

Cybersecurity
Data Privacy
Drones
Enforcement + Litigation
HIPAA
Privacy Tip

VISIT + SHARE:

Insider Blog
R+C website
Twitter
Facebook
LinkedIn

HIPAA

Confusing Joint Guidance Published by OCR and FTC on HIPAA Authorization Forms

There are arguments that there is a dearth of guidance by both the Office for Civil Rights (OCR) and Federal Trade Commission (FTC), so when guidance comes out, we listen. But the most recent guidance jointly issued by the OCR and the FTC is rather confusing. The guidance, "Sharing Consumer Health Information? Look to HIPAA and the FTC Act," first asks whether your business collects and shares consumer health information. It goes on to state that "…if you share health information, it's not enough to simply consider the HIPAA regulations. You also must make sure your disclosure statements are not deceptive under the FTC Act." *Read more*

DRONES

Hackers Cause Consumer Drones to Fall from the Sky

Last week at the PacSec security conference held in Tokyo, a new device capable of fully infiltrating radio-controlled drones was unveiled by researchers. This new device exploits a vulnerability in the frequency-hopping systems in many consumer drones. The frequency-hopping systems make it easier for drones to obfuscate and protect their radio communication. Of course, this new device is not available for sale but that doesn't mean hackers may not soon find this vulnerability and begin exploiting it as well. *Read more*

PRIVACY TIP #59

Check your Privacy Settings on Your LinkedIn Account

I am watching Game 7 of the World Series, and it is the bottom of the 8th and the score is 6-6. It is very difficult to concentrate on this blog post.

So I am taking the easy way out and reminding you to check the privacy settings on your LinkedIn account.

What is the risk to a LinkedIn account? The most common is social engineering—a hacker looking to find out who your friends and family are in order to use that information for phishing schemes to attempt to find out who co-workers or acquaintances are to get their email addresses to launch a phishing scheme.

These attacks can be internal or external. A common internal attack is a fake connection request. Once a user accepts the request, the attacker gets access to all of the victim's LinkedIn activity and

connections, which is then used for social engineering for more targeted phishing or spear-phishing schemes.

External attacks occur when the hacker sends a phishing email that looks like a connection confirmation from an unknown LinkedIn user. When the user clicks on the link in the email, key logging tools are then used by the hacker to hijack the account or carry out surveillance on you and y our connections.

Here are some tips for your LinkedIn account to reduce your risk of an attack:

- If you haven't changed your password since the last LinkedIn hacking, do so now.
- Go to Privacy and Settings and go to the Profile Privacy tab. Change the setting to "Only You," which will make it more difficult for other LinkedIn users to see who you know.
- Change "Choose who can see your connections" and follow your public updates to "Your Connections."
- Go to the Communications tab and under "Who can send you invitations," the recommended setting is "Everyone," but you might want to choose "Only people who know your email address."
- Go to "Messages from members." You may wish to untick career opportunities and business deals.
- Activate "Two-Step verification" that is offered by LinkedIn under the Privacy setting.

Still tied at the top of the 9th.