SmartTV, Smartphones and Fill-in-the-Blank Employees

Peter Silva, 2012-12-09

Right off the bat, I know the title sounds like it's all connected but they are only slightly related so I'll give you the option of dropping out now. Still here? Cool. I've been traveling over the last couple weeks and stories catch my eye along the way that I probably would've written about but didn't. Until now. Besides it's always fun to roll up a few stories in one to get back on track.

TV's are becoming cutting edge multimedia devices that reside on your living room wall. You can stream movies, browse the web, check weather, plug in USBs for slideshows/video, play games, home network along with simply catching the latest episode of your favorite program. This article from usatoday.com talks about many of the internet enabled TVs and their capabilities. For instance, some TVs are now including dual-core processors to make web browsing more enjoyable since many TVs don't have the processing power to load web pages quickly, or at least what we're used to on our computers. Also coming out are TVs with screen resolutions four times greater than full HD screens – these are the 4K sets. These new 4K sets apparently has dampened any lingering 3D enthusiasm, which seems waning anyway. In addition to TVs, other appliances are getting smart, so they say. There are new refrigerators, air conditioners, washers, and dryers which are all app-controlled. Users can turn them on and off from anywhere. I know there are mobile 'apps' but it would be a easy transition to start calling our appliances, apps also. Close enough. How's the clothes cleaning app working? Is the food cooling app running? I've mentioned many times that while all this is very cool stuff, we still need to remember that these devices are connected to the internet and subject to the same threats as all our other connected devices. It's only a matter of time when a hacker takes down all the 'smart' refrigerators on the East Coast. I also think that TVs, cars and any other connected device could be considered BYOD in the near future. Why wouldn't a mobile employee want secure VDI access from his car's Ent/GPS display? Why couldn't someone check their corporate email from the TV during commercials?

Smartphones, as most of you are aware, are changing our lives. Duh. There is an interesting series over on cnn.com called*, "Our Mobile Society," about how smartphones and tablets have changed the way we live.* The first two articles, How smartphones make us superhuman and On second thought: Maybe smartphones make us 'SuperStupid'? cover both sides of the societal dilemma. In 2011, there were 6 Billion mobile phone subscriptions worldwide servicing the 7 Billion people who live on this planet, according to the International Telecommunication Union. These connected devices have made trivia, trivial and we can keep in constant contact with everyone along with people driving, texting and generally not paying attention to anything around them while interacting with their appendage. Pew also released a survey indicating that 54% of cell phone consumers who use mobile apps have decided not to install an app after learning how much personal information they'd have to share; and 30% of that group has uninstalled an app for privacy reasons. We are so concerned about our privacy that we're now dumping apps that ask for too much info. I know there is a 'We all have one & use it everyday day but don't look, ok' joke somewhere in there.

To Educate or Not Educate. I have no idea why I only saw this recently but back in July, there was a lively discussion about whether security awareness training for employees was money well spent. I've often written about the importance of ongoing training. In Why you shouldn't train employees for security awareness, Dave Aitel argues that even with all that training, employees still click malicious links anyway. Instead of wasting money on employee training, organizations should bolster up their system's defenses to protect employees from themselves. Boris Sverdlik of Jaded Security posted a rebuttal saying that employees are and should be accountable for what happens in the environment and no amount of controls can protect against people spilling secrets during a social engineering probe. In a rebuttal to both, Iftach Ian Amit, from Security Art says they are both right and wrong at the same time. He states, '*Trying to solve infosec issues through technological means is a guaranteed recipe for failure. No one, no technology, or software can account for every threat scenario possible, and this is exactly why we layer our defenses. And layering shouldn't just be done from a network or software perspective – security layers also include access control, monitoring, tracking, analysis, and yes – human awareness. Without the human factor you are doomed*.' His position is that when it comes to 'Information Security,' we focus too much on the 'information' part and less on the holistic meaning of 'security.' His suggestion is to look at your organization as an attacker would and invest in areas that are vulnerable. That's your basic risk analysis and risk mitigation.

We are in a fun time for technology, enjoy and use wisely.

ps

References

- Smart TVs offer web browsing, instant video streaming
- Poll: Cellphone users dump apps to save privacy, lose their phones anyway
- Forget 3D. Your dream TV should be 4K
- How smartphones make us superhuman
- On second thought: Maybe smartphones make us 'SuperStupid'?
- Technology Can Only Do So Much
- Unplug Everything!
- Why you shouldn't train employees for security awareness
- You Shouldn't train employees for Security Awareness – REBUTTAL
- Why Training Users in Enterprise Security May Not Be Effective
- Security Awareness and Security Context – Aitel and Krypt3ia are both wrong?

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc. Corporate Headquarters info@f5.com	F5 Networks Asia-Pacific apacinfo@f5.com	F5 Networks Ltd. Europe/Middle-East/Africa emeainfo@f5.com	F5 Networks Japan K.K. f5j-info@f5.com