Luxury Daily®

The News and Intelligence You Need on Luxury

SOFTWARE AND TECHNOLOGY

Mobile shoppers at risk from malicious apps and WiFi this holiday season: report

November 21, 2016

Photo courtesy of Neiman Marcus

By Danny Parisi for Mobile Commerce Daily

Ninety percent of shoppers will use their smartphones in-store this holiday season, and that puts them at particular risk for cybercrime, according to a new report from Skycure.

As mobile continues to become the primary method of digital commerce for many shoppers, the threats to their financial safety grow. This holiday season, shoppers and retailers need to be on the lookout for both malicious applications posing as retail apps and for potential WiFi hacking.

"Black Friday and Cyber Monday are a recipe for cyber-scams," said Yair Amit, CTO and co-founder of Skycure. "The first brings large groups of people using their mobile phones to one place.

"The second attracts people who might overlook security to get a better deal. Unfortunately, mobile threats exist for shoppers whether they're shopping in a store, or on a mobile device from the comfort of their own home or workplace."

Security matters

This holiday season will be one of the biggest and now, more than ever, mobile will be leading the charge for shoppers who want to make smarter decisions.

But that new power that comes from increased mobile presence in the retail world comes with a few caveats that both consumers and retailers need to be on the lookout for.

For one, mobile as a channel is still vulnerable to threats from hackers.

Skycure looked at two ways that hackers could target mobile shoppers this holiday season.

The first is through tampering with WiFi. As users continue to use their mobile devices in-store to make purchasing decisions, many of them will be looking for WiFi to connect to to save on data costs.

Hackers can take advantage of this need in two ways. They can hack into a store or mall's WiFi and gather data from

the connected devices, or they can set up their own WiFi networks, misleading customers into thinking they are safe networks set up by the retailer they are currently visiting.

Once a shopper connects to one of these networks, the hackers now have a way in to their devices and the opportunity to steal valuable data.

Skycure compiled a list of which malls around the country were the most dangerous in this regard, with the highest amount of risky WiFi networks. The top spot, a mall in Las Vegas, had 14 different WiFi networks that could put customers at risk.

Malicious apps

The other problem that mobile shoppers face is the prospect of malicious apps posing as official retail apps.

Skycure found a number of examples of apps available on mainstream app stores that posed as official apps for well-known retailers. Brands such as Amazon and Starbucks were impersonated by apps that intentionally misrepresented themselves to appear reputable.

In reality, these apps contain malicious code that can work its way into a mobile device's vulnerable areas.

One example, an app posing as an Amazon Rewards program, sent malicious code from the victim's phone to others through SMS once it had been ingrained.

While shoppers are the ones who stand the most to lose from these types of scams, the impetus falls on both customers and retailers to take measures to fight these crimes. If not, they risk losing customers' precious trust in both them and the mobile channel, shutting off an entire source of revenue and brand goodwill.