DEVICE MANAGEMENT

HOW TRAVELERS SECURE ELECTRONICS DURING A HOTEL STAY

By Agnes DeFranco, Ed.D., CHAE and Cristian Morosan, Ph.D.

Part I of III

This study report examines travelers' security practices for phones, tablets and laptops during hotel stays. Part I covers guests staying in U.S.-based hotels.

In today's world, one cannot escape news about cybersecurity, and the hotel community is no different. From Omni to Marriott, from IHG to Trump *(McMillian, 2016; Osborne, 2016; Pagliery, 2016; Scott, 2016)*, no one is immune. Hotels strive to provide a safe network environment for their guests. Yet, guests' behavior often influences the degree to which the network environment can be kept safe. From rogue sites to guests inadvertently opening spam e-mails, malware can then enter the hotel Internet portal and infect entire systems, compromising not just the operations of the hotel, but all activities that guests do as well. Therefore, this article is the first of a three-part comprehensive study documenting how guests view the security level of hotel network connectivity based on 24 computing behaviors and what practices guests have when staying with us. This first article was based on 1,301 guests who stayed in hotels within the United States. The second article was based on 1,017 guests who stayed in hotels outside the U.S. This second article is of importance as many of our hotels own, manage or operate properties internationally, and therefore the results have significant implications to your

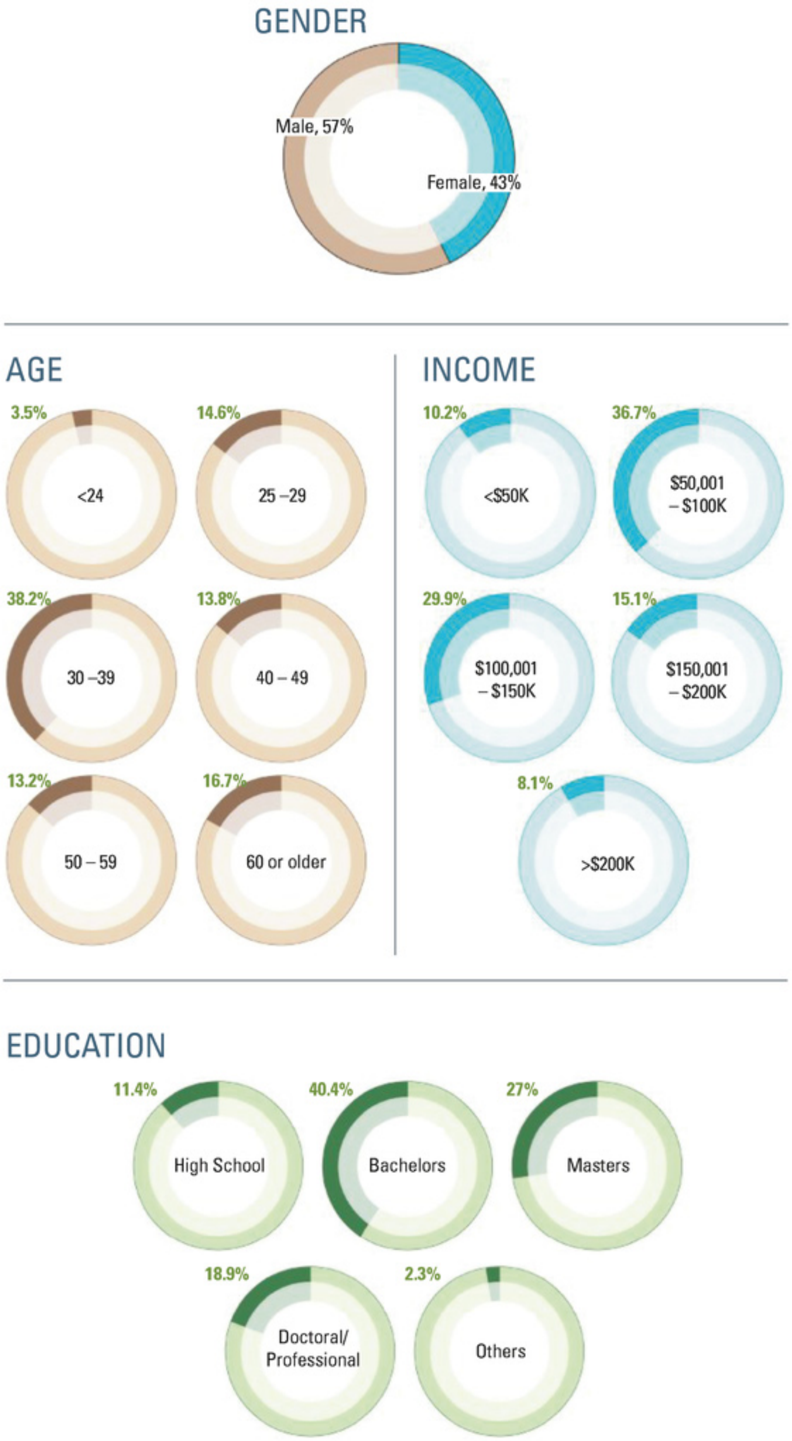
Agnes DeFranco, Ed.D., CHAE (ALDeFranco@Central.UH.EDU) is a distinguished chair and professor at the Conrad N. Hilton College of Hotel & Restaurant Management, University of Houston. She is also an HFTP Global Past President, chair of the HFTP Global Hospitality Accounting Common Practices Advisory Council and a recipient of the HFTP Paragon Award. Cristian Morosan, Ph.D. (cmorosan@uh.edu) is an associate professor at the Conrad N. Hilton College of Hotel & Restaurant Management, University of Houston. This article is partially supported by HFTP.

brand. The third article combined the 2,300+ responses to compare the results of these two groups, and also to explore if their demographics (gender, age, income and education) and their travel behavior (frequency of travel, length of stay, type of hotel and purpose of travel) would make a difference in how guests use their mobile devices in hotels. If we as hoteliers can understand our guests' mobile device behavior and preferences, we can work with our guests and other related parties (e.g., mobile device manufacturers, Internet providers, phone carriers) to mitigate cyber risks in the lodging industry.

How many devices do our guests carry with them nowadays when they travel? I was sitting at the airport, waiting for a flight to Las Vegas to attend the HFTP Annual Convention. The gentleman sitting next to me had his two phones plugged into the charging station and he was working on his laptop. The lady across from me was Facetiming on her iPad Mini tablet and when that conversation ended, she took out her phone and placed a call. Her husband, sitting next to her, pulled out his laptop after the "tablet" communication and did some work. A few minutes later, his mobile phone rang. Between these three people and me, there were 10 devices! Yes, I carried three. I needed my laptop to do work, my tablet to play some mindless games on a three-hour flight, and my phone, of course. On the flight, people were using their laptops, phones and tablets to view content over the Internet provided by the airline. Should they desire more bandwidth, for a small fee, they can be connected to the "real" Internet and send e-mails, texts and download other content. When I arrived to the hotel, as soon as I entered the room, I checked for the Wi-Fi connection.

This is 2017. Everyone, from a business person to a grandmother, has some sort of mobile device and everyone seems to need the Wi-Fi

DEMOGRAPHICS
RESPONDENT PROFILE

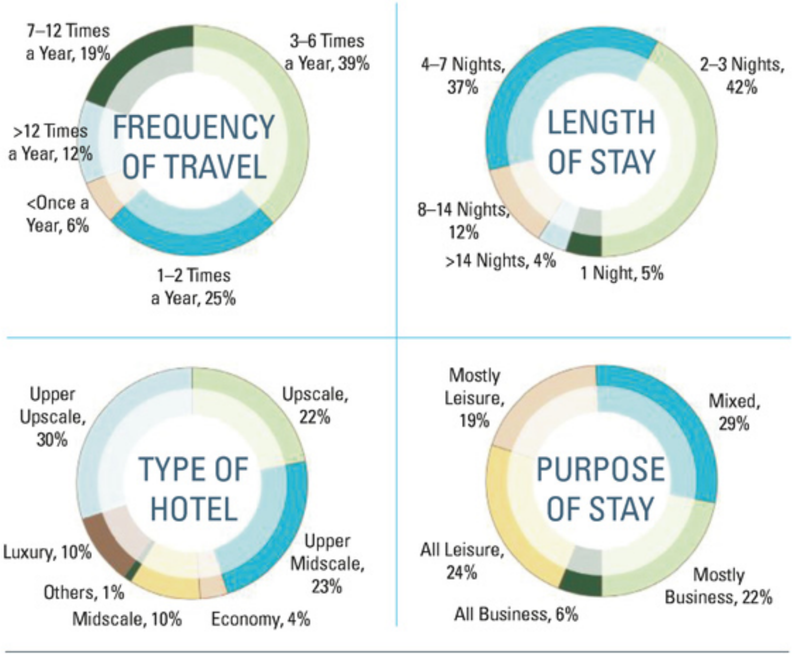


connection. As hoteliers, we understand this need, and to manage our operations, we also need reliable Internet connectivity as well. Some hotels even provide guests with a variety of levels of Internet connectivity services, from free access to a nominal fee for premium service. However, with multiple devices, multiple guests in a room, guests in our lobbies and meeting space, together with the need of the hotel itself and the staff, a reliable and secure Internet connection is a must. The cost of information and telecommunication is not small, so much so that the 11th edition of the *Uniform System of Accounts for the Lodging Industry (USALI)* now has a separate schedule for that. In addition, according to the *CBRE Hotels' Trends (2016)*, the cost of system expenses totaled 33.1 percent and Internet alone costs 4.7 percent of the entire schedule. To complicate the matter more, on the one hand guests would prefer the Internet connections to be free of charge, and on the other hand, unsavory parties are lurking in the wings, ready to hack into our systems. So, how can we keep Internet connections secure? Remember, the system is used by "people;" and in this case, many of the users are our guests who come from all parts of the world. How can we as hoteliers keep everything secure in the cyber world? Therefore, understanding our guests' usage behavior may offer us insight to help formulate our strategies to continue to afford a secure Internet environment for our guests and hotel operations.

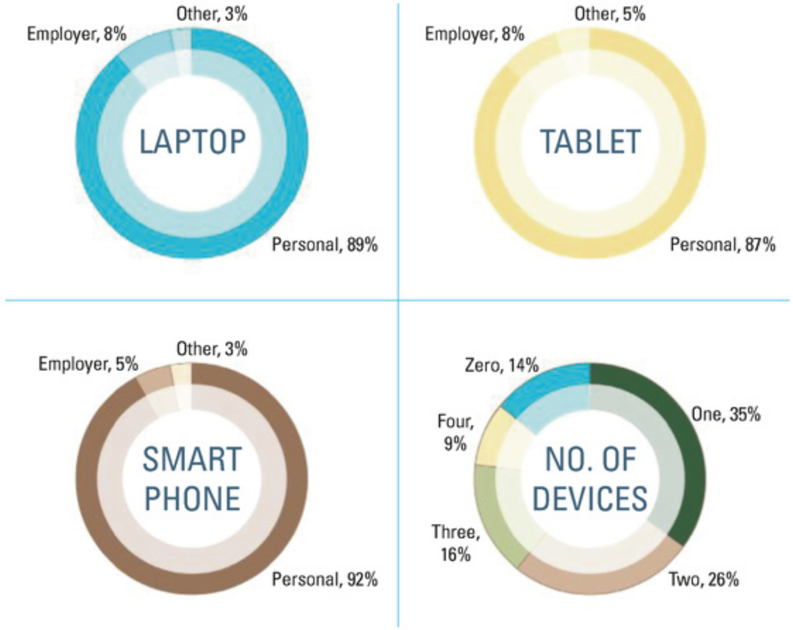
Our Guests and Their Devices

A panel survey was carried out in May 2016 and 1,301 hotel guests who traveled and stayed in hotels within the United States responded. These guests were asked to rate the risk of 24 mobile device usage behaviors ("1" being very risky to "5" being very safe) and the frequency of such behaviors ("1" being never to "5" being always).

STAY CHARACTERISTICS



DEVICES



The profile of the respondents is illustrated on page 15. Over half of our guests were male (57 percent), with the age groups of 30–39 (38.2 percent) being the most prominent. However, after this age group, the respondents were fairly evenly distributed with 13.2 to 16.7 percent across four other age groups. As for income, over 66.6 percent or roughly two-thirds were in the income brackets of $50,000 – $150,000. Over 40 percent of our guests had earned a Bachelors degree.

As for their travel patterns or stay characteristics *(see Stay Characteristics, page 16)*, 39 percent of guests traveled three to six times a year, while another 25 percent traveled one to two times a year. Seventy-nine percent of guests stayed with our hotels anywhere from two to seven nights (two–three nights at 42 percent, and four–seven nights at 37 percent). While only 10 percent stayed at our luxury properties and another 10 percent stayed at our midscale properties. The class of hotel that had most of our guests was the upper-upscale hotels at 30 percent. The upper-midscale came in second at 23 percent followed very closely in third place by the upscale hotels at 22 percent. It appeared that although 6 percent of our guests traveled strictly for business and another 22 percent were mostly for business, to balance one's busy lifestyle on the road, 29 percent of our road warriors selected "mixed" as their responses. In addition, 19 percent of the respondents traveled mostly for leisure and 24 percent traveled strictly for all leisure.

It seems that mobile devices are extensions of ourselves. As illustrated in the Device charts on page 16 the majority of the laptops (89 percent), tablets (87 percent) and smartphones (92 percent) were owned by the guests themselves, and 86 percent of our guests carried at least one device while 9 percent carried four devices. Of those, the majority of guests carried two smartphones, a tablet and a laptop.

DEVICE USAGE Safety Ratings

The panel was presented with three behavior lists for laptop, tablet and smartphone usage during hotel stays. Participants rated the behaviors from safe to risky.

LAPTOPS

Safest practices:

1) Leaving the computer in the room's safe deposit box when temporarily leaving the hotel room
2) Using antivirus protection
3) Using encryption

Riskiest practices:

1) Following hyperlinks found online
2) Leaving computer "sleeping"
3) Leaving computer on/logged in

TABLETS

Safest practices:

1) Leaving the tablet in the room's safe deposit box when temporarily leaving the hotel room
2) Connecting to secure Wi-Fi network of hotel
3) Using encryption

Riskiest practices:

1) Bringing/storing sensitive personal information on device
2) Leaving tablet "sleeping"
3) Leaving tablet on/logged in

SMARTPHONES

Safest practices:

1) Using antivirus protection
2) Using traffic encryption (VPN)
3) Using encryption

Riskiest practices:

1) Following hyperlinks found online
2) Leaving smartphone "sleeping"
3) Leaving smartphone on/logged in

Complete ratings and rankings are detailed on the following pages.

Perception versus Reality: Do Guest Practice What They Know?

The reality check came when the panel was presented with three lists of behavior on their view on laptops, tablets and smartphone usage when they stayed at our hotels. Twenty-four behaviors were listed for each device. These behaviors can be grouped into four major categories: how guests safeguard their devices (e.g., leaving the mobile device in the room's safe deposit box to shutting it down completely), how guests protect their data (e.g., encryption, bring personal information), guests' connection preference (e.g., hotel Wi-Fi, hotel wired, free connections) and guests' Internet usage (e.g., accessing resources, websites, streaming services, social media and software). The results are charted in three tables, each giving the ratings and rankings for laptops, tablets and smartphones (each with a separate table).

As illustrated in the Laptop table (page 18), our guests ranked "Leaving the computer in the room's safe deposit box when temporarily leaving the hotel room" as having the safest ranking with a 3.85 rating. This was followed very closely by "Using antivirus protection" at 3.83. The next two that received a 3.75 and 3.71 rating were "Using encryption" and "Using traffic encryption" respectively, while "Connecting to the secured Wi-Fi network of the hotel to access the Internet" was ranked fifth at a score of 3.63. Although these results might have been expected, what should also be expected then would be if one rated a behavioral item as highly safe, one should also practice that item and exhibit that behavior more

LAPTOP USAGE

Safety and Practice Ratings and Ranks

🟦 Safety Rating/Rank 🟩 Practice/Rank

🟨 Leaving computer in room's safe deposit box when out of room		Using antivirus protection		🟨 Using encryption *(file level, full disk)*		🟨 Using traffic encryption *(VPN)*	
3.85	3.26	3.83	3.64	3.75	3.27	3.71	3.23
1	11-T	2	2	3	10	4	15
Connecting to secure Wi-Fi network of hotel		Connecting to wired network connection of hotel		Accessing secure resources		Leaving computer shut down in the room	
3.63	3.72	3.60	3.29	3.59	3.26	3.57	3.44
5	1	6	9	7	11-T	8-T	5
Using bookmarks stored in device		Using e-mail clients		🟨 Accessing regular websites		Accessing popular streaming services	
3.57	3.34	3.57	3.46	3.56	3.49	3.56	3.24
8-T	8	8-T	4	11-T	3	11-T	14
Using cloud or remote desktop services for storage		🟨 Accessing social media websites		Using conferencing software		Accessing secure (https) websites	
3.56	3.16	3.55	3.35	3.51	3.14	3.50	3.25
11-T	16	14	7	15	17-T	16	13
Accepting updates from common software		Purchasing online from various vendors		Following hyperlinks provided by hotels		🟨 Connecting to free/public Wi-Fi network of hotel	
3.39	3.12	3.39	3.14	3.34	3.06	3.24	3.37
17-T	19	17-T	17-T	19	20	20	6
Bringing/storing sensitive personal information on device		Following hyperlinks found online		Leaving computer "sleeping"		Leaving computer on/logged in	
3.20	3.02	3.17	3.05	3.12	2.98	3.05	2.84
21	22	22	21	23	23	24	24

Safety Ratings — Range from 1 to 5 with 1 being very risky to 5 being very safe.

Practice — Range from 1 to 5 with 1 being never to 5 being always.

T= Tie • 🟨 Highlighted cells have at least 6 ranking differences.

often than others. As there were 24 items, six items would represent 25 percent. Therefore, any behavior that had a ranking difference of at least six ranks in its safety ranking and practice ranking are highlighted yellow in the table. There were three items that hotel guests did not rank as safe as others and yet they frequently practiced such behaviors when staying in our hotels. "Accessing regular websites" was ranked 11-tie in safety and yet, it was ranked third in practice. "Accessing social media websites" was ranked 14th in safety out of 24 items, and again, it was ranked high in practice in seventh place. Finally, coming in at 20th in safety was "Connecting to the free/public Wi-Fi (wireless) network of the hotel to access the Internet" and when it came to practice, it was ranked sixth, even one ranked higher than assessing social media websites. Since these behaviors are ranked high in frequency, hotels may want to work with their guests to ensure when they are using their laptop to access websites, social media and connecting to free/public Wi-Fi, that the guests are practicing secure Internet usage.

On the contrary, there were three items that were ranked high in their safety rankings, but were not practiced as often. It was interesting to note the top safety-ranked behavior of "leaving the laptop in the room's safe" only had a practice ranking of 11-Tie. With 75 percent of our guests staying in at least an upper midscale hotel and 62 percent at least an upscale hotel, in-room safes are available. It is possible that the inconvenience factor requiring guests to lock and unlock the safe caused guests to not practice this behavior. Similarly, our guests noted the safety in "using encryption" and also "using a virtual private network (VPN)," and ranked these two behaviors third and fourth in safety. However, regarding actual practice, "using encryption" only ranked 10th and "using VPN" was ranked 15th. These three pairs of rankings translated into areas of opportunity for hotels. The table on page 18 presents the safety and practice scores in pairs to provide a visual illustration.

Tablet Usage

A similar list of 24 behaviors were also ranked by hotel guests on their tablet usage with the exception that "Connecting to the wired network connection of the hotel to access the Internet" was replaced by "Using a phone carrier network (if available) (e.g. AT&T, Verizon) to access the Internet." The top five safest rankings were as follow: "Leaving the computer in the room's safe deposit box when temporarily leaving the hotel room," "Connecting to the secure Wi-Fi (wireless) network of the hotel to access the Internet," "Using encryption (file level, full-disk)," "Using traffic encryption (VPN) when connecting to private resources," and "Using a phone carrier network (if available) (e.g. AT&T, Verizon) to access the Internet." Thus, four of the top five rankings for tablets were identical with those of laptop usage.

The procedure used to analyze laptop usage was also employed to analyze tablet use. As illustrated in the Tablet table, five items had a difference in ranking of at least six ranks and thus were highlighted in yellow. Of the five items, three had a higher safety ranking than their practice ranking. Although hotel guests rated "encryption at the file level" as third for safety, the practice rank was low at 16-Tie. And while "using a phone carrier network" was ranked fifth for safety, the usage rank was at 11th. Similarly, "using cloud or remote desktop services for storage" has a safety ranking tied at sixth, the usage ranking was 14th. Although ranked as safe, these behaviors were not practiced as frequently, possibly due to cloud services being relatively new modes of storage, or encryption being seen as a cumbersome process that requires users to take extra steps. Most importantly, the two

TABLET USAGE

Safety and Practice Ratings and Ranks

🟦 Safety Rating/Rank 🟩 Practice/Rank

Leaving tablet in room's safe deposit box		Connecting to secure Wi-Fi network of hotel		🟨 Using encryption		Using traffic encryption *(VPN)*	
3.74	3.28	3.67	3.56	3.64	3.10	3.63	3.27
1	5-T	2	1	3	16-T	4	8
🟨 Using a phone carrier network to access Internet		Accessing regular websites		🟨 Using cloud or remote desktop services for storage		Leaving tablet shut down in the room	
3.61	3.19	3.57	3.33	3.57	3.13	3.54	3.28
5	11	6-T	3-T	6-T	14	8-T	5-T
Using bookmarks stored in device		Using e-mail clients		Accessing secure resources		Accessing popular streaming services	
3.54	3.28	3.54	3.33	3.52	3.14	3.49	3.12
8-T	5-T	8-T	3-T	11	13	12	15
Using conferencing software		Accessing social media websites		Accessing secure (https) websites		Accepting updates from common software	
3.48	3.09	3.47	3.22	3.47	3.15	3.40	3.10
13	18	14-T	10	14-T	12	16	16-T
Purchasing online from various vendors		Following hyperlinks provided by hotels		🟨 Using antivirus protection		🟨 Connecting to free/public Wi-Fi network of hotel	
3.38	3.06	3.38	3.06	3.37	3.41	3.34	3.23
17-T	19-T	17-T	19-T	19	2	20	9
Following hyperlinks found online		Bringing/storing sensitive personal information on device		Leaving tablet "sleeping"		Leaving tablet on/ logged in	
3.29	3.03	3.25	2.99	3.19	2.96	3.15	2.90
21	21	22	22	23	23	24	24

Safety Ratings — Range from 1 to 5 with 1 being very risky to 5 being very safe.
Practice — Range from 1 to 5 with 1 being never to 5 being always.
T= Tie • 🟨 Highlighted cells have at least 6 ranking differences.

SMARTPHONE USAGE

Safety and Practice Ratings and Ranks

🟦 Safety Rating/Rank 🟩 Practice/Rank

Using antivirus protection		Using traffic encryption *(VPN)*		Using encryption		Using a phone carrier network to access Internet	
3.75	3.43	3.67	3.16	3.66	3.22	3.65	3.55
1	2	2	14-T	3	8	4	1
Connecting to secure Wi-Fi (wireless) network of the hotel		Leaving smartphone in the room's safe deposit box		Using cloud or remote desktop services for storage		Accessing regular websites	
3.64	3.27	3.64	3.17	3.59	3.19	3.55	3.40
5-T	7	5-T	13	7	11	8	4
Using e-mail clients		Accessing social media websites		Using bookmarks stored in Device		Using conferencing software	
3.54	3.41	3.51	3.36	3.50	3.20	3.50	3.13
9	3	10	5	11-T	10	11-T	18
Accessing secure resources		Accessing popular streaming services		Accessing secure (HTTPS) websites		Leaving smartphone shut down in the room	
3.48	3.16	3.48	3.18	3.47	3.21	3.42	3.11
13-T	14-T	13-T	12	15	9	16	20
Accepting updates from common software		Purchasing online from various vendors		Following hyperlinks provided by hotel		Connecting to free/public Wi-Fi network of hotel	
3.41	3.15	3.37	3.10	3.34	3.12	3.32	3.28
17	16	18	21	19	19	20	6
Following hyperlinks found online		Bringing/storing sensitive personal information on device		Leaving smartphone "sleeping"		Leaving smartphone on/ logged in	
3.27	3.14	3.24	3.03	3.24	3.04	3.16	2.99
21	17	22-T	23	22-T	22	24	24

Safety Ratings — Range from 1 to 5 with 1 being very risky to 5 being very safe.

Practice — Range from 1 to 5 with 1 being never to 5 being always.

T= Tie • 🟨 Highlighted cells have at least 6 ranking differences.

items that were rated lower in safety: "using antivirus protection" (19th) and "connecting to free/public Wi-Fi" (20th) had higher usage ranking of second and ninth respectively.

Smartphones Usage

Finally, the list of 24 behaviors related to smartphone use was presented to guests. The top five behaviors that were ranked safest were: "Using antivirus protection," "Using traffic encryption (VPN) when connecting to private resources," "Using encryption (file level, full-disk)," "Using a phone carrier network (if available) (e.g. AT&T, Verizon) to access the Internet," and "Connecting to the secure Wi-Fi (wireless) network of the hotel to access the Internet."

As with tablets, five items were found to have ranking differences of at least six ranks and were highlighted in yellow in the Smartphone table. Three items had a higher safety ranking than their practice ranking. "Traffic encryption using VPN" was rated second on safety and was not used as frequently and received a 14-tied practice rank. "Leaving the smartphone in the room's safe" was ranked fifth in safety, but guests also did not practice this as often and ranked this 13th. This is more understandable as we all carry our smartphones with us anywhere we go. Finally, "using conference software" was ranked as 11-tied in safety, but only had a practice rank of 18th. On the other hand, "using e-mail clients such as Outlook or Apple Mail client with smartphones" had a safety ranking of ninth, but was used so often that it received a ranking of third; and "connecting to the free/public Wi-Fi" had a safety ranking of 20 and the practice or usage ranking was sixth.

A Game Plan for our Hotels: What's Next?

What do all these behavioral rankings of security and practice mean for our daily hotel operations? They surely offer us some detail of how guests used their mobile devices. The items that had at least a six-ranked difference in safety and practice rankings are potential areas of improvement. The insight provided by guests' responses allowed us to formulate several directions for hotels, which should improve the overall hotel practice, while enhancing guests' understanding of risk, and the actions that guests might take to reduce risk and have better hotel stay experiences. In this first part of the trilogy, five suggestions are offered for hoteliers.

1. Provide a reliable network connectivity service with sufficient bandwidth. Guests viewed connecting to the secure Wi-Fi network of the hotel to access the Internet as one of the top five most secure behaviors for all three mobile devices. It is also in the top five practice ranking for laptops and tablets. Thus, hotels need to live up to that expectation. If the connection is dropped, guests will view it as a bad stay experience. For example, many rooms at the end of the Wi-Fi range do not receive a strong enough signal, and may need to rely only on the wired connection infrastructure. Therefore, hotels need to ensure all the Wi-Fi hot spots are working and that security is ensured. In addition to maintaining network security, we also need to regularly check the security of the entire IT infrastructure of our hotels including routers and firewalls. Although these are more of the back-of-the-house and not guest-facing items, a secure IT infrastructure help fend off threats.

2. Educate consumers to engage in safe computing and access practices. This is especially important when guests use remote services. As many consumers bring with them devices mostly for the content stored on them or that they can access with them, educating consumers about using remote services (e.g., storage, computing, social communication) while staying in hotels is critical. Hotels have opportunities to educate their guests to use secure connections to access cloud-based resources, which can be done more seamlessly using the paid connectivity services of the hotel. In addition, guests are tempted to use in-room technologies to access remote resources (e.g., using smart TVs to log-in and watch content from streaming services such as Neflix). Promoting such services could result in use that would enhance the value of the entire hotel stay for guests.

3. Educate guests to use protection software and encryption for their devices and data. As storage becomes increasingly cheap, users' tend to accumulate increasing amounts of data. Whether personal or business-related, this data becomes attractive to some individuals. Such data is especially attractive as it can store credentials for a multitude of guests' accounts. Hotels have opportunities to encourage guests to use data protection steps to minimize the risk of loss.

4. Persuade consumers to connect to secure networks. While hotels have provided network connectivity options ranging from free (typically unsecure, available in the more "public" areas of properties) to paid (typically secure, sometimes offered in tiers), opportunities exist to educate consumers to use secure connections to mitigate network connectivity risk and have a better connectivity experience leading to a better overall stay. In addition, hotels can tie the secure connectivity services to other benefits that can represent attractive bundles for guests. To make these services valuable to guests, hotels could ensure that their guest-facing infrastructure is reliable and secure and that consumers can connect easily using a variety of devices. In addition, hotels can design hotel infrastructures that provide sufficient bandwidth and allow guests to enjoy securely all the behaviors that involve their mobile devices in hotels.

5. Educate consumers to use secure Internet practices after they have connected to the Internet. The IT community recognizes the critical role of the users in facilitating security breaches. Moreover, guests are likely to continue their Internet behaviors that they established as habits from their daily lives, especially given the familiarity of their devices and the bookmarked (or history-based) web content that they regularly access. Thus, it is important to recognize the role of education in guest' online practices. Basically, by emphasizing secure computing once connected, guests can reduce the likelihood of risky behaviors online, and thus reduce the likelihood of opening backdoors for people with bad intent. We can even take a step further to share Internet safety tips with guests via e-mails, videos, in-room hotel channels, brochures in rooms, or even pop-up messages on our hotels' websites.

Cyber security is a serious matter. In our second article, we will explore these ratings for guests staying in our hotels outside the United States. ■

References

- Trends in the Hotel Industry USA Edition 2016 (2016). CBRE Hotels' Americas Research. Georgia: Atlanta.
- McMillian, R. (July 8, 2016). Omni hotels warns of data breach. The Wall Street Journal. Retrieved at http://www.wsj.com/articles/omni-hotels-warns-of-data-breach-1468010853
- Osborne, C. (August 15, 2016). 20 top US hotels hit by fresh malware attacks. Retrieved from http://www.zdnet.com/article/20-top-us-hotels-hit-by-fresh-malware-attacks/
- Pagliery, J. (April 5, 2016). Trump hotels attacked by hackers – again. Retrieved from http://money.cnn.com/2016/04/05/technology/trump-hotels-hacked/
- Scott, A. (August 14, 2016). Starwood, Marriott, Hyatt, IHG hit by malware: HEI. Technology News. Retrieved from http://www.reuters.com/article/us-hotels-cyber-idUSKCN10P0ZM