# Report on

# WiFi Adoption and Security Survey 2012

# Hong Kong

Version 1.0

June 2012

This report can be downloaded from:

http://www.safewifi.hk

**Organizer**



Hong Kong Wireless Technology Industry Association

(WTIA)

香港無線科技商會

http://www.hkwtia.org

**Sponsor**



Office of the Communications Authority

(OFCA)

通訊事務管理辦公室

http://www.ofca.gov.hk

# Report on

# Wi-Fi Adoption and Security Survey 2012

# Hong Kong

Prepared by:

Dr. Ge Zhan,Tung Wah College

Prof. Jerome Yen, Tung Wah College and HKUST

Under Advisory by:

Mr. Ken Fong

Immediate Past Chairman and Honorary Chairman (Life),
Hong Kong Wireless Technology Industry Association (WTIA)

June 2012

# Introduction

The adoption of Wireless Local Area Networks (WLANs) (IEEE 802.11), or Wi-Fi, has been continuously widening and deepening in recent years. Similarly, the services that can be delivered over the Wi-Fi network also have been growing exponentially. Substantial efforts have been made by the Hong Kong SAR Government through the Digital 21 Initiative since 2008 to turn Hong Kong into a wireless city. By May of 2012, Wi-Fi facilities have been installed at around 400 premises in all the 18 districts of Hong Kong SAR. As the usage of Wi-Fi might cause safety related problems, such as leaking of personal information or insufficient protection of the transmission of financial transaction, significant amount of efforts have also been made in education and promotion of the technologies of Wi-Fi security. Such promotion or education has been made either through government-sponsored campaigns or through TV and Radio programs since 2008. However, the current usage of Wi-Fi and the problems that the Wi-Fi users encountered has not been investigated and reported recently.

Unanswered, but important, questions include how, where and why do people use Wi-Fi in Hong Kong SAR? Do they have sufficient knowledge in using such Wi-Fi Network? Do they have sufficient support when they encountered problems? Have people learnt about the security related knowledge, such as, where to download and how to install security systems so that they can use Wi-Fi safely? For the users from different locations, with different

education background, and at different age groups, do they have similar pattern in their Wi-Fi usage and knowledge about the Wi-Fi security. We particularly focus on the questions that can help Hong Kong SAR government to adjust or fine-tune their strategies in promotion or education of Wi-Fi network.  Such questions include, for example, is it easy to find access point to the Wi-Fi network? Is the network stable? Etc.

A self-administered survey was conducted in first half of 2012 as a first step towards answering these questions. It has been found in prior research that the dominant group of Wi-Fi users was younger population (Horrigan, 2008). However, such survey was conducted mainly with subjects from other countries. Therefore, their findings might not reflect the situation in Hong Kong. In order to provide broader coverage, the samples contained in this survey consisted of college students, both undergrad and graduate, who studying at various local universities as well as employees that cover education and business sectors.

Questionnaire data were collected from 283 respondents and 276 were found eligible to support the study.

## Current Use of Wi-Fi for Internet Access

The Wi-Fi Alliance defines Wi-Fi as "wireless local area network (WLAN) products" that allow an electronic device to exchange data with the use of radio waves. Devices, such as a personal computer, video game console, Smartphone, tablet and digital audio player, can connect to internet via a Wi-Fi access point.

Survey respondents were asked to select the time length of their use of Wi-Fi (Figure 1). Over half (51 percent) of respondents indicate that they have used it for more than two years. One-fifth (26 percent) have one- to two-year experience. Thirteen (13) percent of respondents indicate they had 6-12 months experience. Few report that they have used Wi-Fi for less than six months (8 percent), and very few indicate that they have never used it (1 percent).

A considerable amount of respondents use WiFi intensively in their recent access to internet (Figure 2). Half of WiFi users use it more than four hours on daily basis. About one-third (30 percent) use WiFi less than ten hours a week. Another 17 percent of respodents state "unless necessary, otherwise, I would not use it". Again, only 2 percent express "never use it".

# Figure 1. Experience of Using Wi-Fi
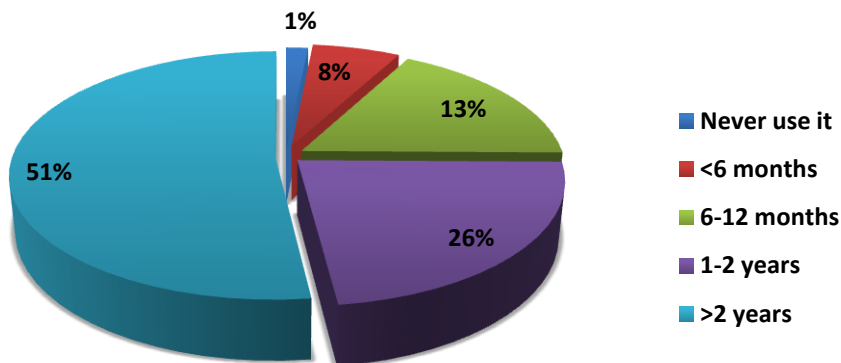


# Figure 2. Pattern of Recent Wi-Fi Usage
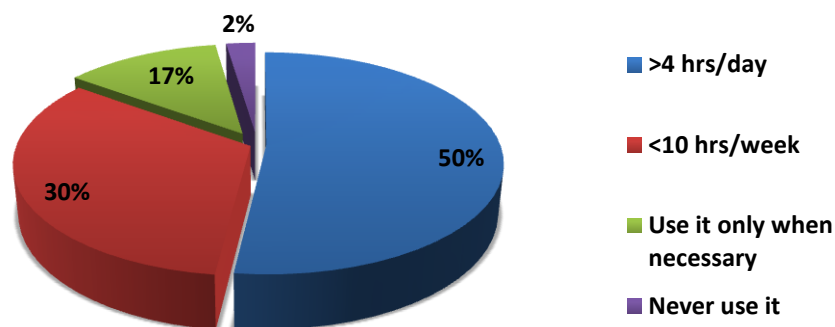


Wi-Fi users get access to internet at a variety of places, but the most common access point is "home", where 229 respondents, or 83 percent out of 276 valid responses, connect to internet via Wi-Fi at home (Table 1). Free public Wi-Fi services, although aggressively promoted and developed by government since 2008, has not been widely used so far (85 responses or 31 percent). In general, male users are more likely to use Wi-Fi than female. Particularly, the proportion of male users (63 percent) using Wi-Fi at office is much higher than that of female users (49 percent). The use of Wi-Fi at business districts also shows a difference between male (47 percent) and female (44 percent).

Many young people (aged 15-25) use Wi-Fi at home (88 percent), campus (69 percent) and free GovWiFi access points (41 percent). They are less likely to use it at business districts (36 percent) and office (24 percent). Older people (46+) have less use of free GovWiFi (13 percent). Unsurprisingly majority of them do use Wi-Fi at home (79 percent) and office (79 percent).
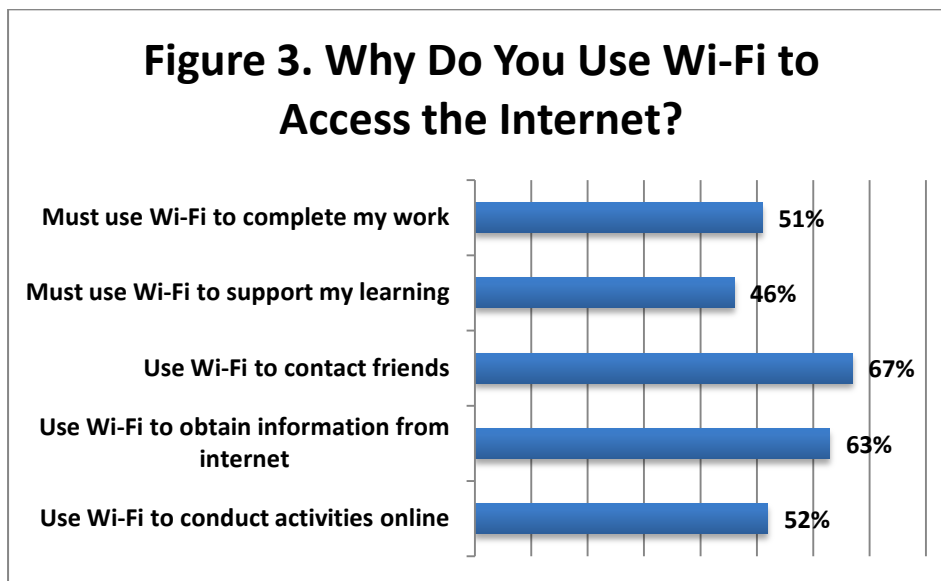
| Table 1. Demographic Profiles by Place | | | | | | |
|---|---|---|---|---|---|---|
| | **Home** | **Campus** | **Office** | **Business Districts** | **Free GovWiFi** | **Total** |
| **Gender** | | | | | | |
| Male | 85% | 41% | 63% | 47% | 29% | 93 |
| Female | 83% | 42% | 49% | 44% | 31% | 172 |
| **Age** | | | | | | |
| 15-25 | 88% | 69% | 24% | 36% | 41% | 102 |
| 26-35 | 86% | 39% | 65% | 50% | 27% | 66 |
| 36-45 | 73% | 16% | 76% | 55% | 29% | 51 |
| 46+ | 79% | 13% | 79% | 45% | 13% | 47 |
| **Education** | | | | | | |
| Secondary school | 79% | 5% | 79% | 43% | 16% | 63 |
| Associate degree | 84% | 57% | 34% | 40% | 41% | 98 |
| Bachelor degree | 83% | 42% | 58% | 50% | 25% | 72 |
| Master+ | 91% | 66% | 53% | 53% | 41% | 32 |
| **Region** | | | | | | |
| Hong Kong Island | 73% | 33% | 60% | 44% | 31% | 52 |
| Kowloon | 83% | 39% | 45% | 49% | 30% | 76 |
| New Territories | 87% | 46% | 57% | 43% | 29% | 132 |
| Remote Islands | 100% | 40% | 40% | 40% | 80% | 5 |
| Total | 229 | 114 | 148 | 122 | 85 | *276* |

By looking at the different Wi-Fi access points across education levels, we found that as people who have higher level of education, their use of Wi-Fi in general increases. This is particularly true for using Wi-Fi at home and in business districts. There is a slight drop in usage of free GovWiFi for those with a bachelor's degree, from 41 percent in comparison to 25 percent, but it increases up to 41 percent for Masters.

In terms of the geographic distribution of Wi-Fi usage in Hong Kong, we found that respondents from more sub-urban regions, such as the new territories, are more likely to use Wi-Fi at home (87 percent) and campus (46 percent) in comparison to Hong Kong islands (73

and 33 percent respectively), and Kowloon (83 and 39 percent respectively). Home (100 percent) and free GovWiFi (80 percent) are more important for Wi-Fi users from remote islands. For the use of Wi-Fi at office, the proportion is higher in Hong Kong Island (60 percent), while Kowloon dominates in business districts usage at 49 percent.

As presented in Figure 3, there are two main reasons of using Wi-Fi to access to the Internet, which are contacting friends (67 percent) and obtaining information from Internet (63 percent). Half of the respondents use Wi-Fi to conduct activities online and complete their work. Also worth of mentioning is that 46 percent of respondents indicate that Wi-Fi is a must to supporting my learning.

## Figure 3. Why Do You Use Wi-Fi to Access the Internet?

| | |
|---|---|
| Must use Wi-Fi to complete my work | 51% |
| Must use Wi-Fi to support my learning | 46% |
| Use Wi-Fi to contact friends | 67% |
| Use Wi-Fi to obtain information from internet | 63% |
| Use Wi-Fi to conduct activities online | 52% |

We witness great variance in the activities that conducted by respondents with Wi-Fi network (Figure 4). Above 70 percent of respondents use Wi-Fi to search and download information as well as check and answer e-mails, while financial transactions and investment activities account for 32 percent and 21 percent respectively. Furthermore, 39 percent of respondents use Wi-Fi network for entertainmental activities such as playing on-line games. 30 percent of respondents do on-line purchasing via Wi-Fi.
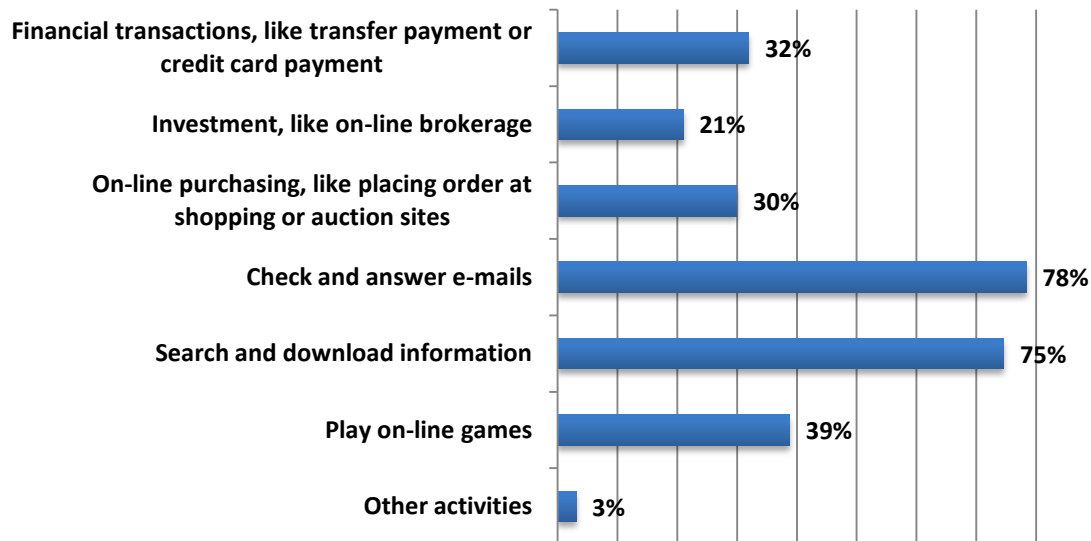
## Figure 4. Activities Conducted Through Wi-Fi Network

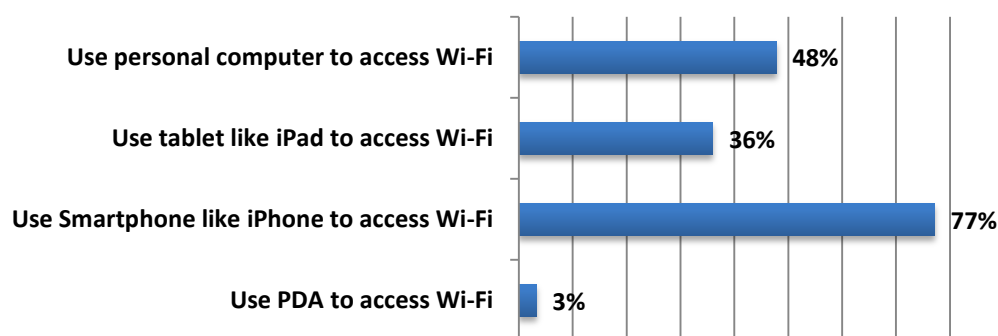| Activity | Percentage |
|---|---|
| Financial transactions, like transfer payment or credit card payment | 32% |
| Investment, like on-line brokerage | 21% |
| On-line purchasing, like placing order at shopping or auction sites | 30% |
| Check and answer e-mails | 78% |
| Search and download information | 75% |
| Play on-line games | 39% |
| Other activities | 3% |

Figure 5 presents how people access Wi-Fi. Smartphone, such as the iPhone, has become an overwhelming device to access Wi-Fi that account up to 77 percent. About half of respondents use personal computers to access to Wi-Fi, while using Tablet such as the iPad accounts for 36 percent. Few respondents (3 percent) choose PDA to access Wi-Fi.

## Figure 5. How Do You Access Wi-Fi?

| Access method | Percentage |
|---|---|
| Use personal computer to access Wi-Fi | 48% |
| Use tablet like iPad to access Wi-Fi | 36% |
| Use Smartphone like iPhone to access Wi-Fi | 77% |
| Use PDA to access Wi-Fi | 3% |

The booming of Smartphone market is evident in our findings (Figure 6) that 96 percent of respondents are Smartphone users. iOS Smartphone in our survey is the market leader that account for 40 percent of the market. This is followed by Android Smartphone which is used by 38 percent of respondents. Of the Smartphone users, 55 percent have shared their Smartphone as Wi-Fi Hotspots or Wi-Fi tethering (Figure 7). Among the Smartphones who share their phones as the hotpots, half of them are iOS Smartphones, followed by Android that account for 37 percent.
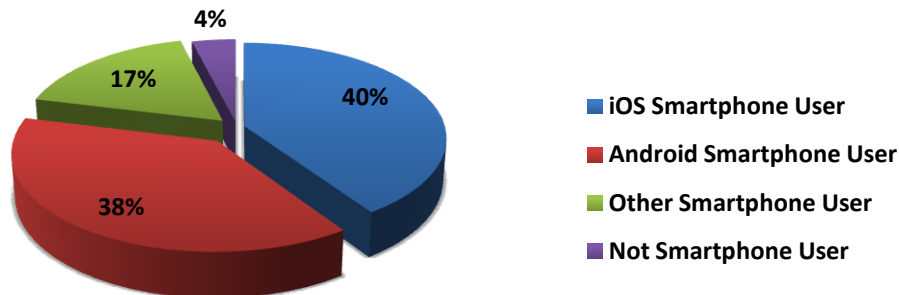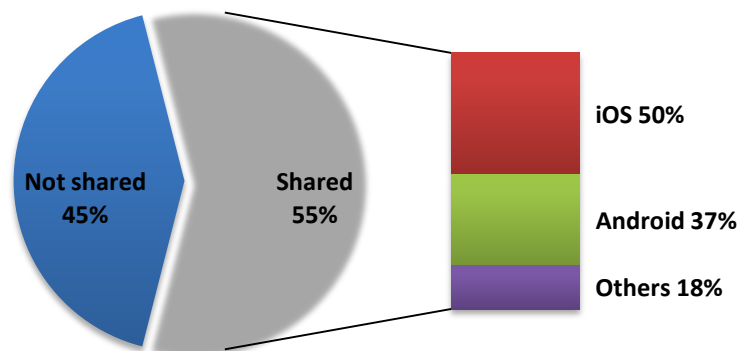
## Figure 6. Are You a Smartphone User?



- iOS Smartphone User
- Android Smartphone User
- Other Smartphone User
- Not Smartphone User

4%
17%
40%
38%

## Figure 7. Smartphone Shared as Wi-Fi Hotspots



Not shared 45%

Shared 55%

iOS 50%

Android 37%

Others 18%

Figure 8 and 9 present the comments or suggestions by our respondents to the government and commercial service providers. At first glance, over 70 percent of citizens complain about inadequate Wi-Fi access points provided by both the government and commercial service providers. About 50 percent of respondents are unsatisfied with the stability of service quality and bandwidth provided by government, and over one third of respondents are unsatisfied with the stability and bandwidth provided by commercial providers. Another big concern to Wi-Fi users is inadequate transparency of the service provided by commercial sector, commented by 32 percent of respondents.

**Figure 8. Comments or Suggestions Regarding the Free Wi-Fi Services Provided by Government**

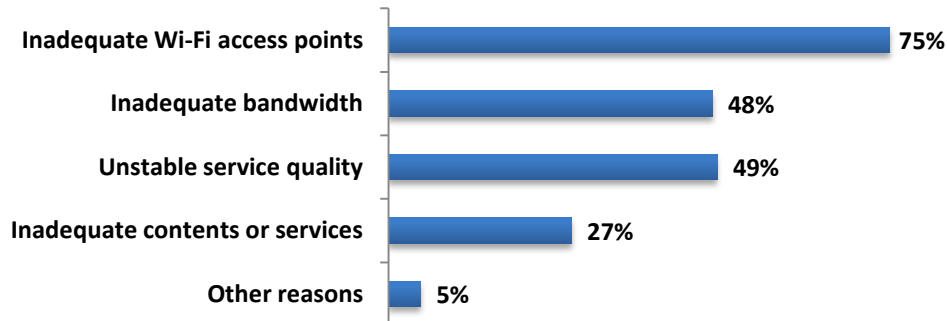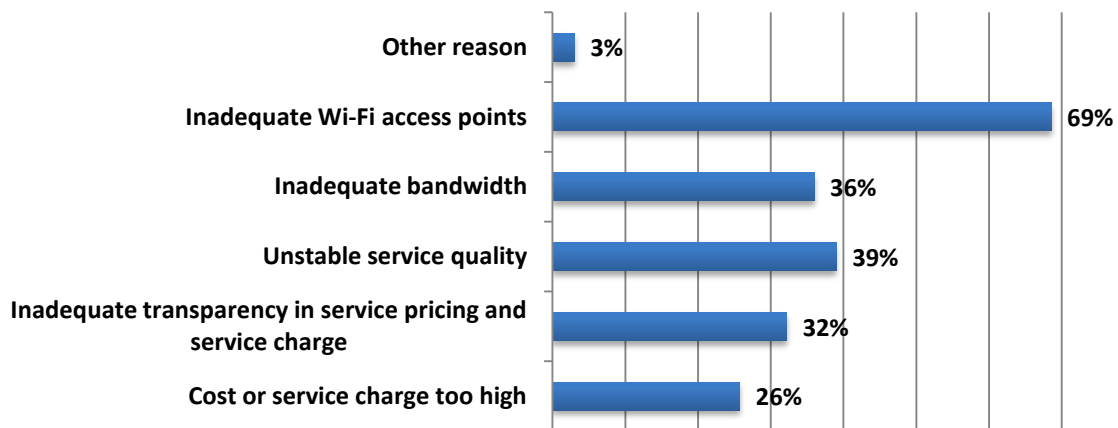| Category | Percentage |
|---|---|
| Inadequate Wi-Fi access points | 75% |
| Inadequate bandwidth | 48% |
| Unstable service quality | 49% |
| Inadequate contents or services | 27% |
| Other reasons | 5% |

**Figure 9. Comments or Suggestions Regarding the Wi-Fi Public Hotspots Provided by Commercial Service Providers**

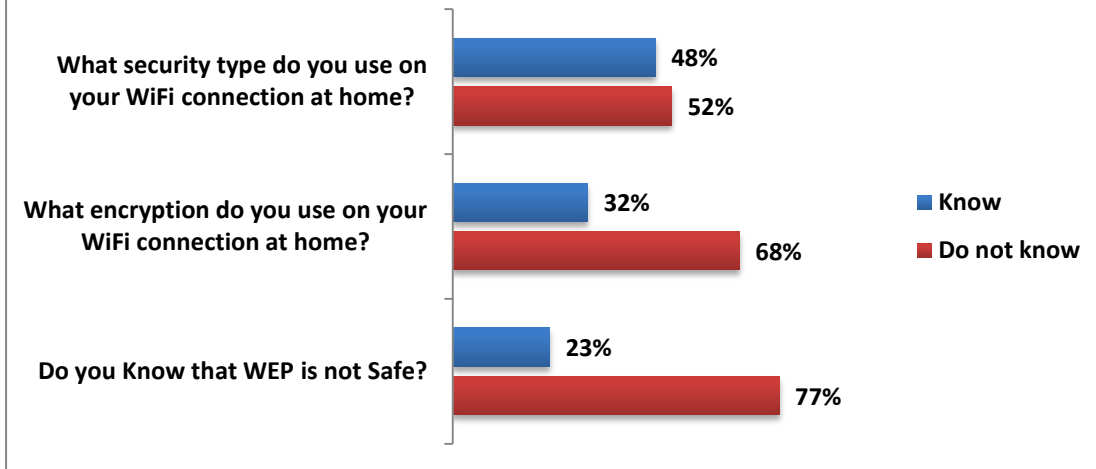| Category | Percentage |
|---|---|
| Other reason | 3% |
| Inadequate Wi-Fi access points | 69% |
| Inadequate bandwidth | 36% |
| Unstable service quality | 39% |
| Inadequate transparency in service pricing and service charge | 32% |
| Cost or service charge too high | 26% |

## Security of Using Wi-Fi for Internet Access

Wi-Fi security concerns the prevention of unauthorized access to computers via wireless networks. Currently the most common types of security are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and WPA2. WPA and WPA2 are more advanced encryption standard than WEP. WPA2, for example, uses an encryption device to encrypt the network with a 256 bit key, which significantly improves security with the longer key length.

The implementation of the protocol in WPA2 has made Wi-Fi network safer than before. Nevertheless, established studies reveal that Wi-Fi is still exposed to serious threats and attacks from many sources (Gold 2010; Haque, Amola and Singh, 2012; Trimintzios and Georgiou, 2010). To our surprise, the respondents surveyed on average have a relatively positive perception of Wi-Fi security (Figure 10). They (58 percent ) believe in the statement "Using Wi-Fi to access to Internet would not disclose my personal privacy, for example, the location where I am". They (53 percent) feel that the security measure provided by Wi-Fi is adequate, and 50 percent indicated that using Wi-Fi to access to Internet is safe.

### Figure 10. Perception of Wi-Fi Security

| | |
|---|---|
| Using WiFi is safe | 50% |
| The security measure provided by WiFi is adequate | 53% |
| Using WiFi would not disclose my personal privacy such as location | 58% |
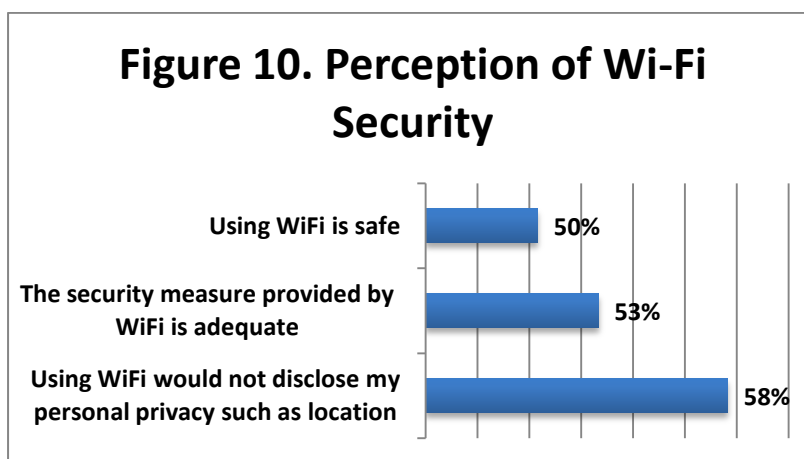
Do people have sufficient awareness and knowledge of Wi-Fi security? Interestingly, many people choose "I don't know" to security-related questions (Figure 11). For example, 52 percent of respondents do not know how to answer the question "what security type do you use on your Wi-Fi connection at home?", and about 80 percent do not know whether WEP is safe or not. Majority people unfamiliar with the security type, let alone the encryption technologies used in the security software (68 percent). It strongly signifies that although people are familiar with the concept, purpose and use of Wi-Fi, they are not have sufficient knowledgeable about security technologies which are critical in protecting their safe usage of Wi-Fi network.

## Figure 11. Security Knowledge Rate

What security type do you use on your WiFi connection at home?
- Know: 48%
- Do not know: 52%

What encryption do you use on your WiFi connection at home?
- Know: 32%
- Do not know: 68%

Do you Know that WEP is not Safe?
- Know: 23%
- Do not know: 77%

Legend:
- Know (blue)
- Do not know (red)

The proportion of people surveyed who are aware of using open Wi-Fi is as low as 8 percent (Figure 12). Similarly, 10 percent of users use shared connections for security. WPA Personal (60 percent) is the most common standard that people use on their wireless network, and it seemed that WPA2 has not been fully transitioned (29 percent). Unsurprisingly, WPA and WPA2 Enterprise are less common in use (2 and 3 percent respectively). The dominance of the WPA 2 enterprise over the WPA enterprise explains the security needs of business which are keeping updated to the latest standard for security, leaving WPA enterprise completely unused.

## Figure 12. Security Type at Home

- Open: 8%
- Shared: 10%
- WPA Personal: 60%
- WPA Enterprise: 2%
- WPA2 Personal: 29%
- WPA2 Enterprise: 3%
- 802.11X: 3%
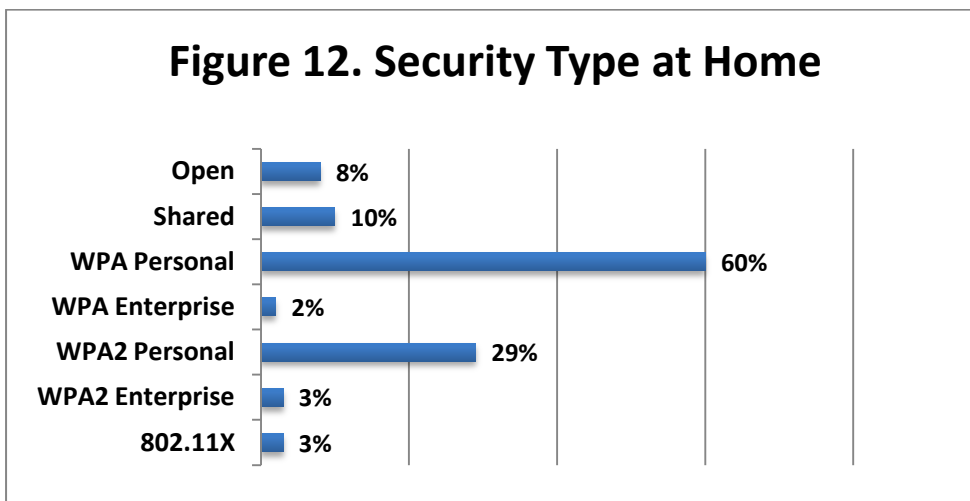
The proportion of respondents reporting "Do not know the importance of security settings at home" is surprisingly low at around 25 percent (Figure 13). The number of people who do not know how to setup Wi-Fi security settings on the router and the device accounts for over one third. Also noteworthy is that about one fourth of respondents do not think that it is necessary to turn on the Wi-Fi security setting.

## Figure 13. If You Do Not Enable the Wi-Fi Security Setting at Home, What Is the Reason?

| | |
|---|---|
| Do not know importance | 25% |
| Do not know how to setup Wi-Fi security settings | 40% |
| Do not know how to setup Wi-Fi security setting on the device | 34% |
| Don't have right to decide the Wi-Fi security settings | 14% |
| I don't think it's necessary to turn on the Wi-Fi security setting | 23% |
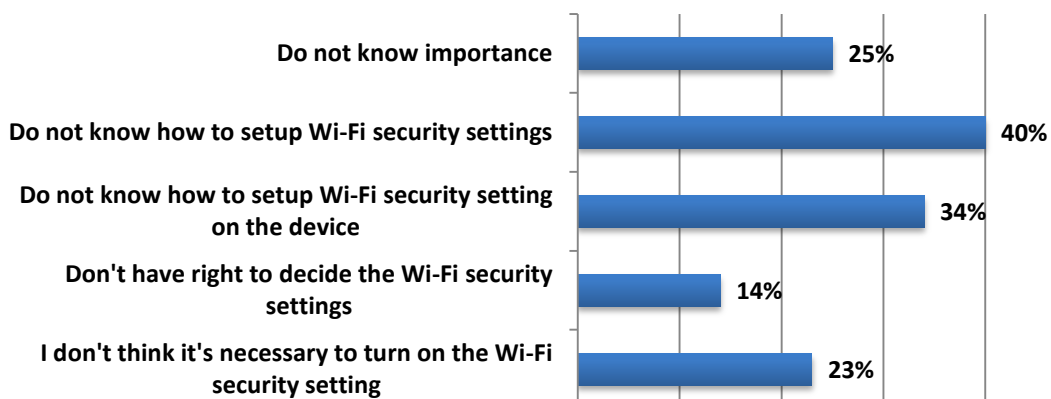
The findings on the encryption at home (Figure 14) again reflect the lack of understanding or awareness about technical specifications. 76 percent of respondents indicate the adoption of WEP at home. However, the use of open and shared settings which involve WEP encryption has been confirmed by only 18 percent of respondents (see Figure 12). A much smaller proportion of people are aware of their usage of TKIP (18 percent) and AES (11 percent).

Why do people prefer WEP? Possible answers are listed and ranked in Figure 15. People use it mostly because they are not aware of other security technologies, confirmed by 55 percent of respondents. The second biggest reason is "I do not have time to change it" (18 percent). People claim that their routers and devices on the customer end do not support more secure technologies account for 12 and 6 percent respectively. Another 17 percent of respondents cannot change the setting of router because it was done by suppliers.
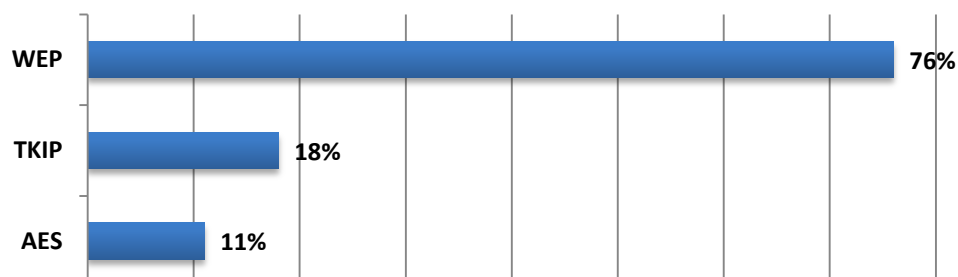
## Figure 14. Encryption at Home

| | |
|---|---|
| WEP | 76% |
| TKIP | 18% |
| AES | 11% |

## Figure 15. Why Would You Use WEP Encryption Technologies?

I do not know other secure technologies — 55%

I do not have time to change it — 18%

The router does not support more secure technologies — 12%

The device on the customer end do not support more secure technologies — 6%

The setting of the router was done by supplier, I could not change the setting — 17%
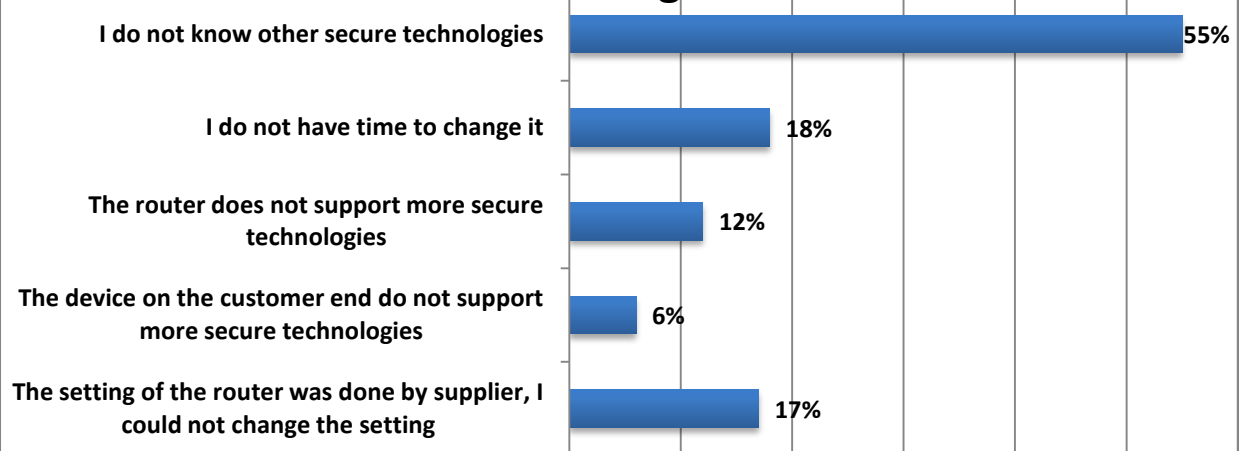
## Use of Free Public Wi-Fi Services Provided by Government

How do people use free public Wi-Fi services provided by government? We find that among users of free GovWiFi, 62 percent of them have used Wi-Fi for longer than two years (Figure 16). There is a moderate amount of those with experience of less than two years, less than one year, and less than six months (19, 17, and 2 percent respectively). In terms of pattern of recent Wi-Fi usage, a majority of users of free GovWiFi use Wi-Fi more than four hours daily, 27 percent use Wi-Fi less than 10 hours per week, and 11 percent use it only when necessary.

## Figure 16. Use of Free GovWiFi and Wi-Fi Experience
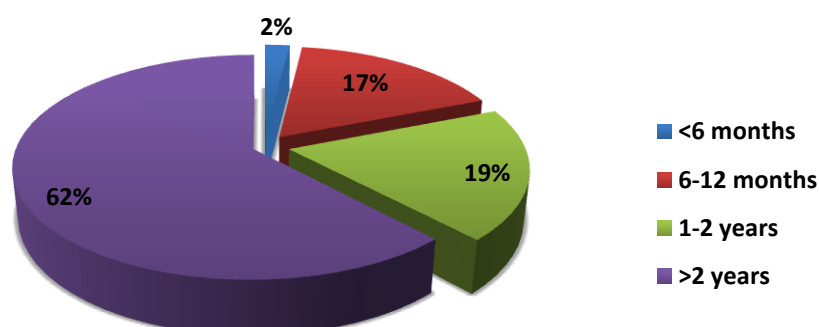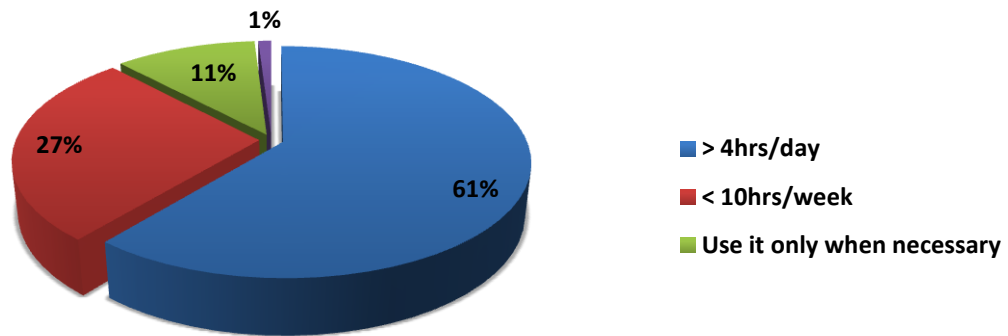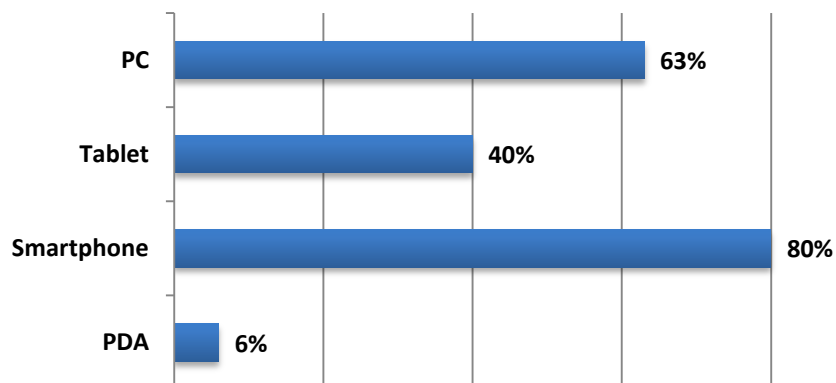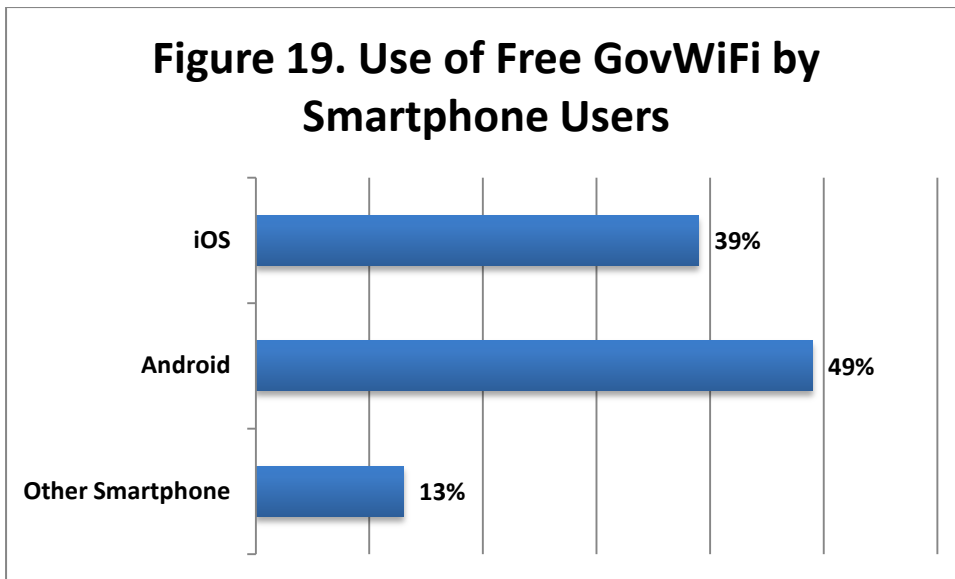
2%
17%
19%
62%

- <6 months
- 6-12 months
- 1-2 years
- >2 years

**Figure 17. Use of Free GovWiFi and Pattern of Recent Wi-Fi Usage**

- > 4hrs/day
- < 10hrs/week
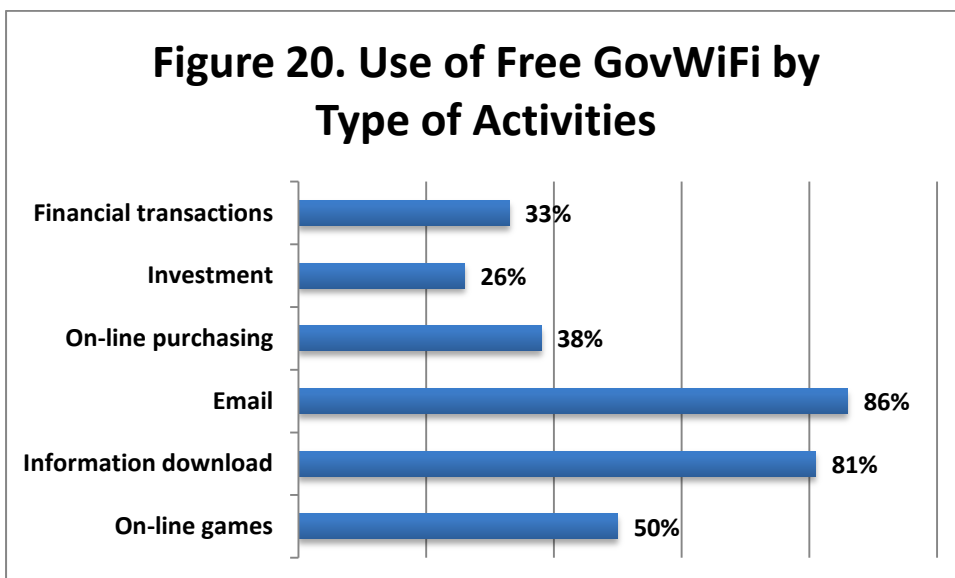- Use it only when necessary

1%
11%
27%
61%

Most people use Smartphone (80 percent) and personal computers (63 percent) to access free GovWiFi (Figure 18). Tablets have been fairly common among the users of free GovWiFi, where 40 percent of them now use this device. Legacy devices such as PDAs have low usage at 6 percent. Since Smartphone is the most popular device for connecting to free GovWiFi, its use by types of Smartphone is reported in Figure 19, in which Android users (49 percent) are 10 percent higher than that of iOS users (39 percent), and other Smartphone users account for 13 percent.

**Figure 18. Use of Free GovWiFi by Types of Device**

| Device | Percentage |
|--------|-----------|
| PC | 63% |
| Tablet | 40% |
| Smartphone | 80% |
| PDA | 6% |

## Figure 19. Use of Free GovWiFi by Smartphone Users

iOS — 39%

Android — 49%

Other Smartphone — 13%

What activities tend to be conducted with free GovWiFi? Email and information download are the most dominant, which account for 86 and 81 percent of users of free GovWiFi respectively (Figure 20). On-line games are more common than on-line purchasing at 50 percent vs. 38 percent. Financial transactions and investment activities are less likely to be conducted over free GovWiFi with 33 and 26 percent respectively.

## Figure 20. Use of Free GovWiFi by Type of Activities

Financial transactions — 33%

Investment — 26%

On-line purchasing — 38%

Email — 86%

Information download — 81%

On-line games — 50%

## Current Encryption Knowledge and Practice at Home

Is knowledge of encryption technology influenced or affected by their gender, age, education or residence? A demographic analysis is conducted in order to provide possible answers to such questions. Analysis results are presented in Figure 21. There is a strong contrast between the male and female in terms of knowledge of encryption at home (Figure 21a), where 76 percent of females do not know what their encryption is and 56 percent of males are aware of the encryption they use. There is also a correlation between those of different ages and

encryption awareness at home (Figure 21b). Those aged at 26-35 (41 percent) and above 56 (50 percent) tend to know their encryption at home.

There is a very strong correlation between the knowledge of encryption and education levels (Figure 21c) that 86 percent of people with secondary school education during form 1-3 are not aware of the encryption at home, but the unawareness is much lower (56 percent) for those with Master or Doctoral degrees, regardless of the fields that they study. This makes a strong case that education in general can improve the awareness of wireless security.

**Figure 21. Demographical Analysis of Encryption Knowledge: Do People Know the Type of Encryption Used at Home?**



(a)



(b)



(c)



(d)
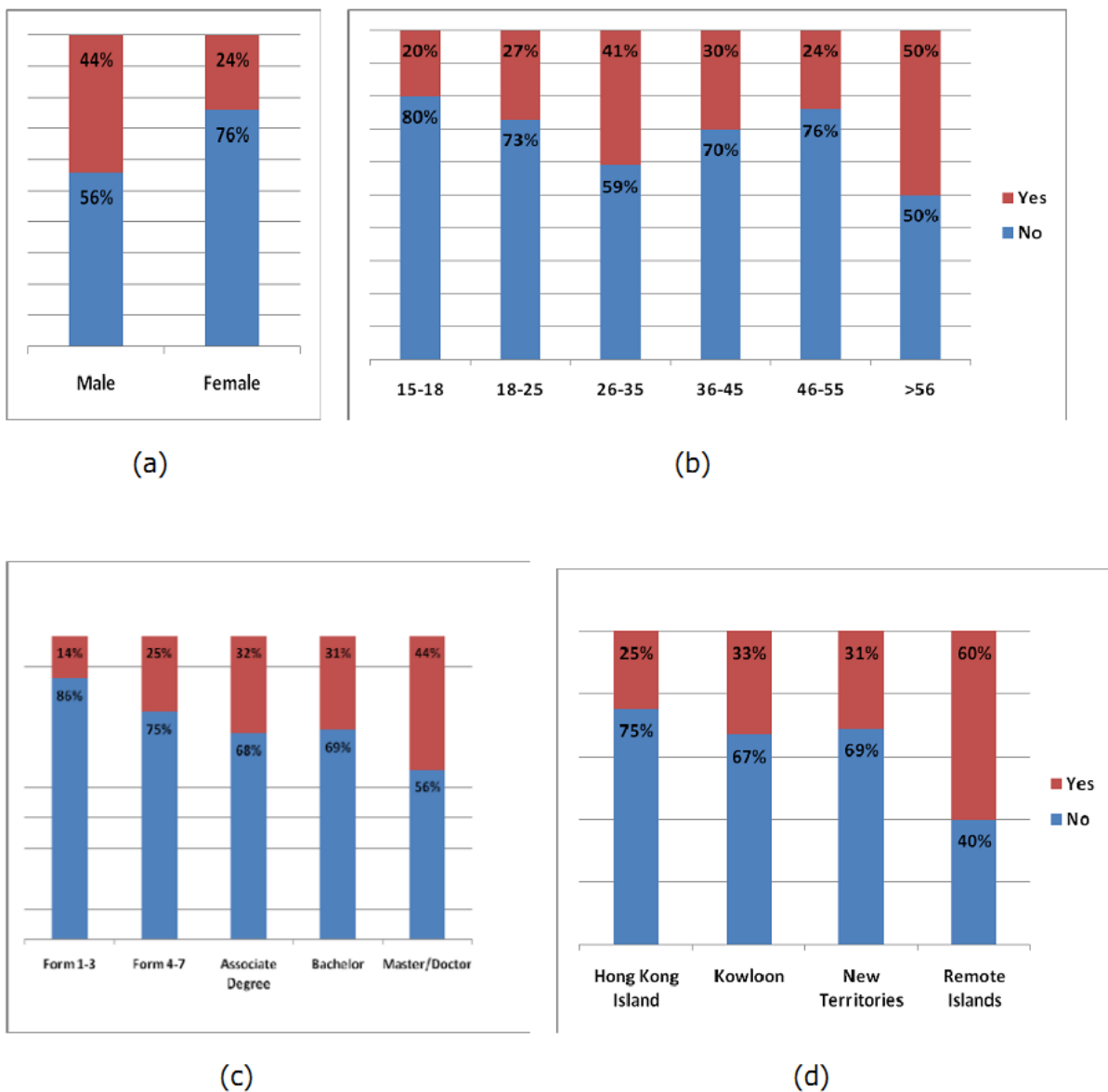
Interestingly, 75 percent of Hong Kong Island residents do not know the type of encryption at home (Figure 21d). The rate of unawareness is 67 and 69 percent respectively for those living

16

in Kowloon and the New Territories. For people living in remote Islands, the proportion is much smaller. Only 40 percent do not know their encryption at home.

Among the people who are aware of the type of encryption used, including WEP, TKIP and AES, 78 and 73 percent of the male and female use WEP at home (Figure 22a). More advanced types of encryption such as TKIP and AES are less adopted so far. Figure 22b reflects a strong trend of using safer encryption by older people. As shown in Figure 22c, a greater proportion of people with secondary school (43 percent) and post graduate education (36 percent) use TKIP or AES, while these techniques are adopted by less than 20 percent of people with associate and bachelor degree.

## Figure 22. What Type of Encryption Do People Use at home?



(a)

(b)

(c)

(d)
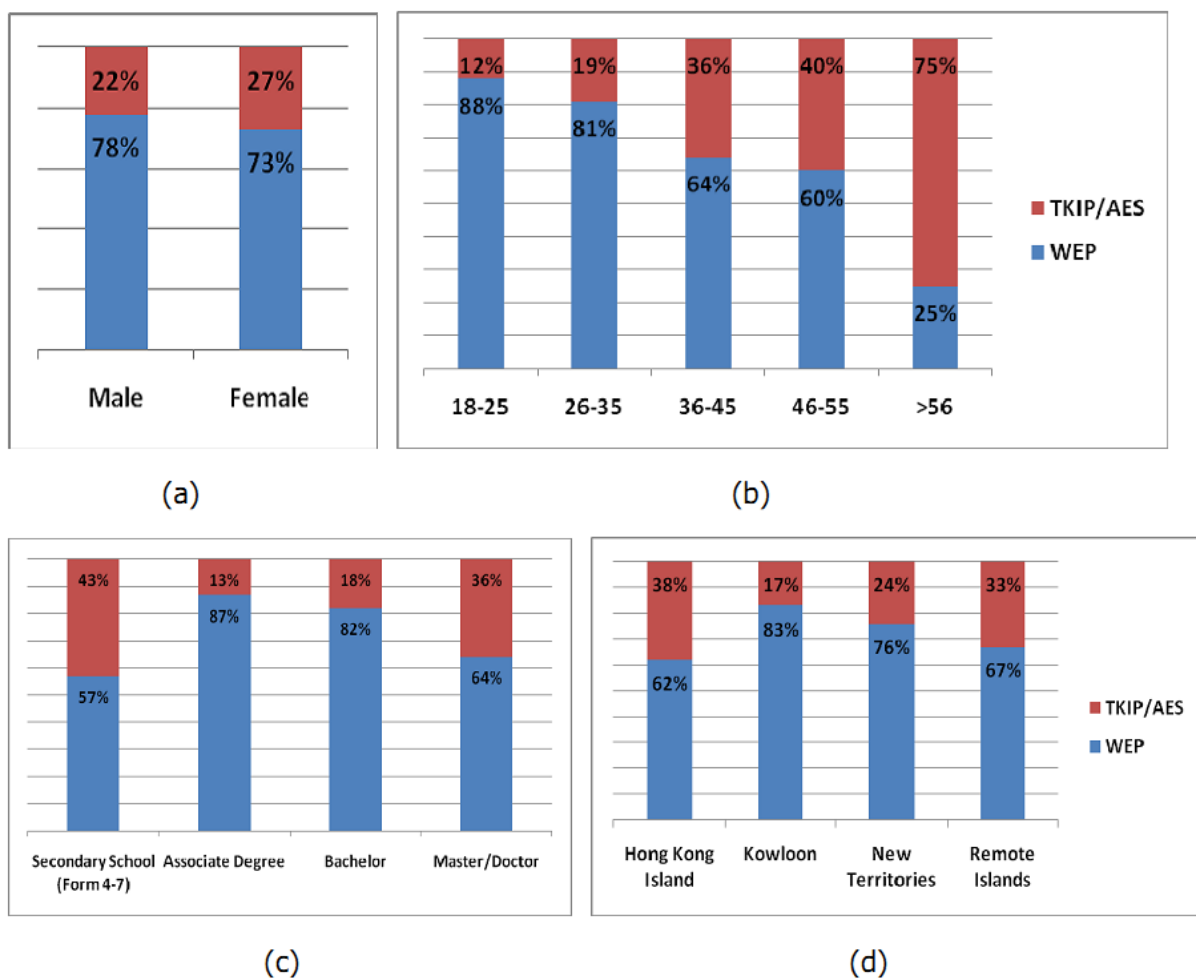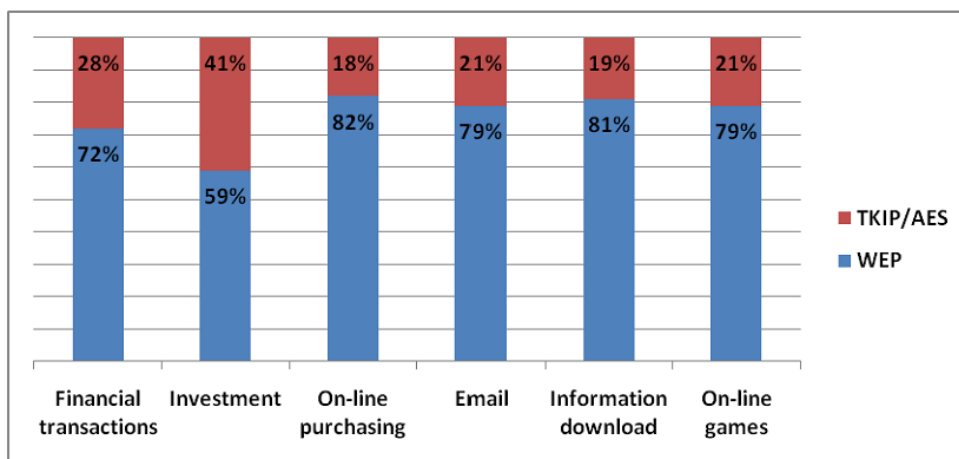
(e)

Although Hong Kong Island residents lack encryption knowledge compared with the other three districts (see Figure 21d), they have better chance to use safer encryption with 38 percent of them using TKIP or AES (Figure 22d). This is probably because they receive higher quality internet service without knowing the details about the encryption technologies they use. Remote islands also have greater use of safer encryption, where one third of residents use TKIP or AES at home.

Figure 22e presents the distribution of encryption types by on-line activities. At home, most people are confident in conducting all types of activities. Over 50 percent of people use WEP, the less safe encryption. Particularly, WEP is used by 80 percent of people who do on-line purchasing, download information, send or receive email, and play on-line games. Among those conducting investment activities, a smaller proportion (59 percent) use WEP. We will summarize the findings we have in the Conclusion section.

## Conclusion

The continuous efforts from Hong Kong SAR Government in recent years on promoting and facilitating the use of Wi-Fi have made it possible for people to use Wi-Fi easily either at home or in other places. Free public Wi-Fi services provided by Hong Kong SAR Government have been used by a significant proportion of people that account for 31 percent of respondents of this survey. Nevertheless, more access points and more stable service quality are needed as commented by the respondents. We see a greater need of new access points in New Territories as a smaller proportion of people from this region have a chance to use Wi-Fi in these free premises. People living in Hong Kong Island have safer encryption set up at home, but most of them are not aware of the type of encryption they used. A greater proportion of people from Kowloon, New Territories and Remote Islands still use WEP at home, which is unsafe. Efforts and resources should be allocated to upgrade their encryption standard or promote related knowledge and skills.

The research findings reveal a strong trend that about 80 percent of people currently use Wi-Fi at home with Smartphones. However, many of them are lacking necessary security knowledge to prevent them from potential on-line threats and attacks. For example, more than half of people surveyed do not know what type of security used in their Wi-Fi connection. Among the other half, who do know the type of security used, over one third of them do not know how to setup Wi-Fi security settings on the router and the device. Some of

them cannot distinguish between security setting and encryption. The lack of security knowledge in the population could be attributed to the fact that insufficient public education on Wi-Fi security was provided and the misunderstanding that setting up Wi-Fi security settings is difficult or time consuming. In addition in order to build more access points and also to encourage people to use them, government should provide more public education/training programs on Wi-Fi security and provide practical guidelines to the citizens in the future.

The lack of security knowledge and support would not only create on-line threats or harms to individual residents, but also block the economic development, for example, the financial market development. Therefore it may decrease the competitiveness of Hong Kong as the financial hub in Asia region. Among all the possible activities that can be conducted with Wi-Fi connection, the three least frequently conducted activities are financial transactions, investment and on-line purchasing. People without proper Wi-Fi security knowledge and ability to adjust such settings may feel unsafe or uncertain to conduct these activities outside their home or outside their office where they have cable internet.
As a result, business activities are confined in limited space, and the benefits of internet or wireless communication, such as, Wi-Fi, in growing economy are not fully exploited. To build Hong Kong into a wireless city and develop Hong Kong SAR's core competitiveness, government and citizens should play active roles in supporting Wi-Fi security teaching and learning by providing more resources.

**References:**
Gold, Steve (2010), "Why WPA Standards Won't Protect Your Network," *Infosecurity*, 7 (1), 28–31.
Haque, Md. Alimul, Yashi Amola, and N.K. Singh (2012), "Threat Analysis and Guidelines for Secure WiFi and WiMAX Network," *World Applied Programming*, 2 (2), 110-115.
Horrigan, John B. (2008), "Home Broadband Adoption 2008," *Pew Internet & American Life Project Survey*, Retrieved June 26, 2012, from http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Broadband_2008.pdf
Trimintzios, Panagiotis and George Georgiou (2010), "WiFi and WiMAX Secure Deployments," *Journal of Computer Systems, Networks, and Communications*, 2010, 8.