Smartphone Security

Survey of U.S. consumers

Sponsored by AVG Technologies

Independently conducted by Ponemon Institute LLC

Publication Date: March 2011

Smartphone Security
Survey of U.S. Consumers
Ponemon Institute, March 2011

Part 1. Introduction

Ponemon Institute is pleased to present the findings of the *Smartphone Security Survey: A Study of U.S. Consumers* sponsored by AVG Technologies. The goal of the research is to determine consumers' perceptions about the potential privacy and security risks when using their smartphones. In addition, we wanted to learn if participants in our study care about these risks and if they take security precautions. We surveyed 734 consumers who are 18 years and older and own a smartphone.

The risks that we address in our survey concern location tracking, transmission of confidential payment without the user's knowledge or consent, diallerware (specialized malware unique to smartphones), spyware, viruses from insecure WiFi networks and others. What we learned is that most of the consumers in our study are using their smartphones without understanding that they are exposing their sensitive information to the risks listed above.

We also believe the findings of this study signal a potential security risk for organizations because so many consumers surveyed use their smartphones for both business and personal use. With business confidential information stored on these smartphones, organizations should make sure employees and contractors take appropriate precautions to secure such sensitive information. We also recommend that security policies state these precautions and ensure they are enforced.

Following are the most salient research highlights:

- Eighty-four percent use the same smartphone for both business and personal purposes. The cross over of business and personal usage means much more sensitive and confidential data is at risk and suggests that the smartphone is with them most of the time.
- Sixty-six percent admit they keep a moderate or significant amount of personal data on their smartphones. Such personal data include email address, name, contact lists, photos, videos, anniversary and personal dates, music,
- Sixty-seven percent of consumers surveyed say they are concerned about receiving marketing ads and promotions. However, less than half (44 percent) are concerned about having a virus attack on their smartphone when it is connected to an insecure Internet network.
- In addition to using it as a phone, 89 percent use their smartphone for personal email and 82 percent use it for business email. A smaller percentage of consumers use their smartphones for financial transactions including payments. In fact, 38 percent of consumers use the smartphone to make payments and 14 percent use it for banking.
- Sixty-six percent of consumers have paid at least once for an item using their smartphone. In addition, 12 percent of consumers say they have experienced a fraud attempt vis-à-vis a mobile payment scheme. Despite this fact, only six percent say they check their mobile bill or statement every month and eight percent check the statement when the bill is higher than usual.
- Fifty-eight percent of consumers say that based on how they used the smartphone for purchases, Internet browsing and location they were targeted by marketers. Accordingly, 67 percent say they are very concerned or concerned about aggressive or abusive marketing practices.

- Despite security risks, less than half of consumers use keypad locks or passwords to secure their smartphones. In addition, only 29 percent of consumers said they have considered installing an anti-virus product to protect their smartphone.
- Forty-two percent of consumers who use social networking apps say they allow smartphone versions of well-known social networking applications such as Facebook to access the same key chains, passwords and log-ins that they use of their desktops, laptops or tablet.
- Only 10 percent of consumers say they turn off Bluetooth “discoverable” status on their smartphone when not in use.

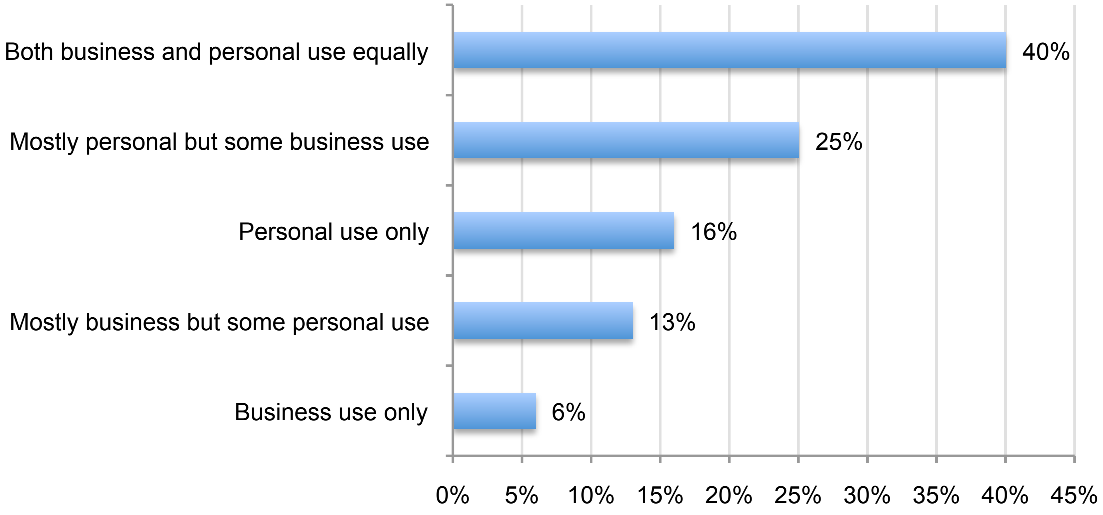
Part 2. Key Findings

In this report we have organized the findings from the study according to the following topics: Consumers' use of smartphones, consumers' awareness about the security risks that accompany their use of smartphones, scenarios that illustrate potential smartphone security risks and how consumers are or are not managing these risks.

Consumers' use of smartphones

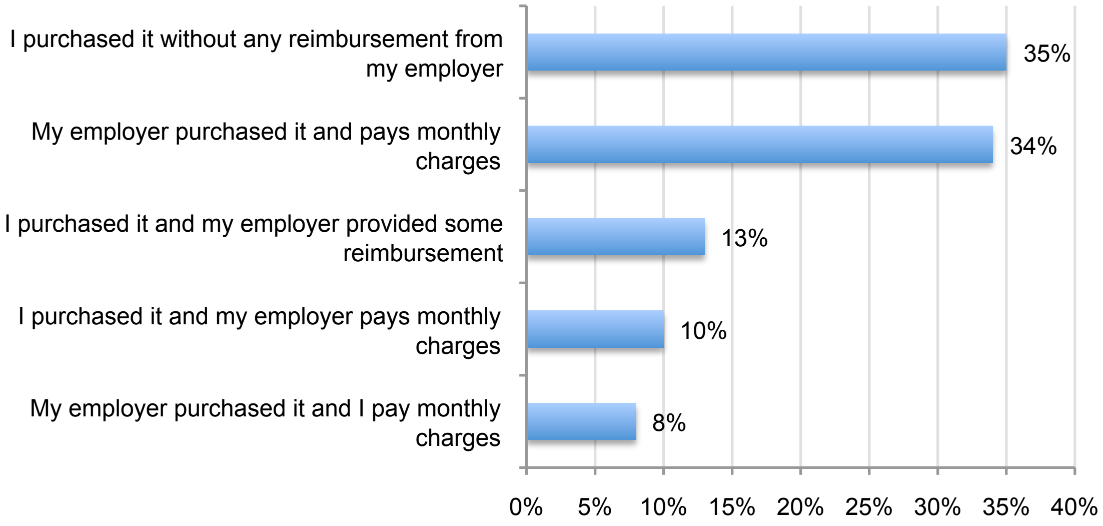
Most consumers use their smartphone for both business and personal use. Forty percent use their smartphone for business and personal use equally and 25 percent use it for personal but some business use (Bar Chart 1). Only 6 percent of consumers surveyed use their smartphone exclusively for business.

Bar Chart 1. What best describes your smartphone use?



Despite using the Smartphone for personal use, 34 percent say their employer purchased the smartphone and pays all monthly charges. As shown in Bar Chart 2, 35 percent say they purchased it without any reimbursement.

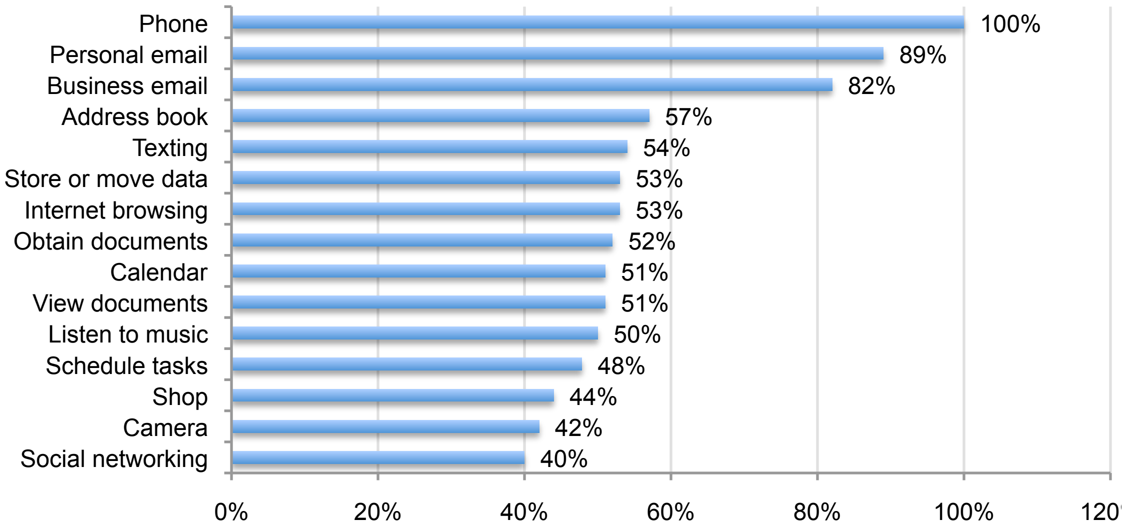
Bar Chart 2: Who purchased your smartphone and who pays the monthly service fee?



Smartphones can perform a wide range of tasks. However, the most popular use next to the phone is business and personal emailing.

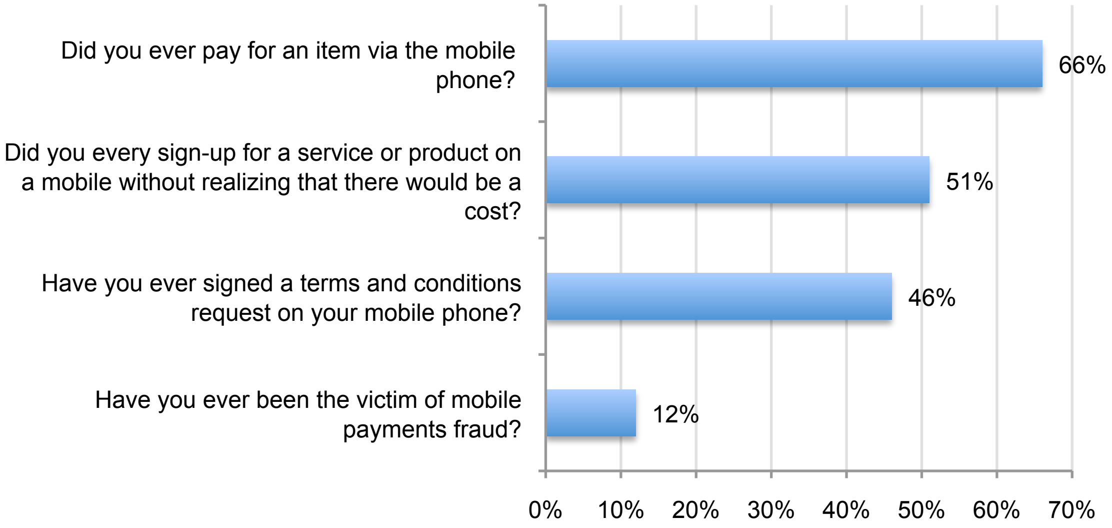
The most popular smartphone uses are checking both personal and business email, using it as an address book, texting, Internet browsing, storing or moving data, obtaining and viewing documents, as a calendar and listening to music (Bar Chart 3). Least popular are banking, travel assistance and video conferencing. (For a complete list of tasks, please see Q. 24 in the Appendix to this paper.) We suggest this finding may indicate why many in our study are not concerned about the security risks. Because consumers believe its primary use is as a phone or to email they may think (incorrectly) that there are negligible security or privacy risks.

Bar Chart 3: Tasks that consumers do on their smartphone



As reported in Bar Chart 4, 66 percent have paid for an item via their smartphone once, irregularly (once every two months) or regularly (maybe once a month). Fifty-one percent were surprised that they were charged for a service of product they signed up for.

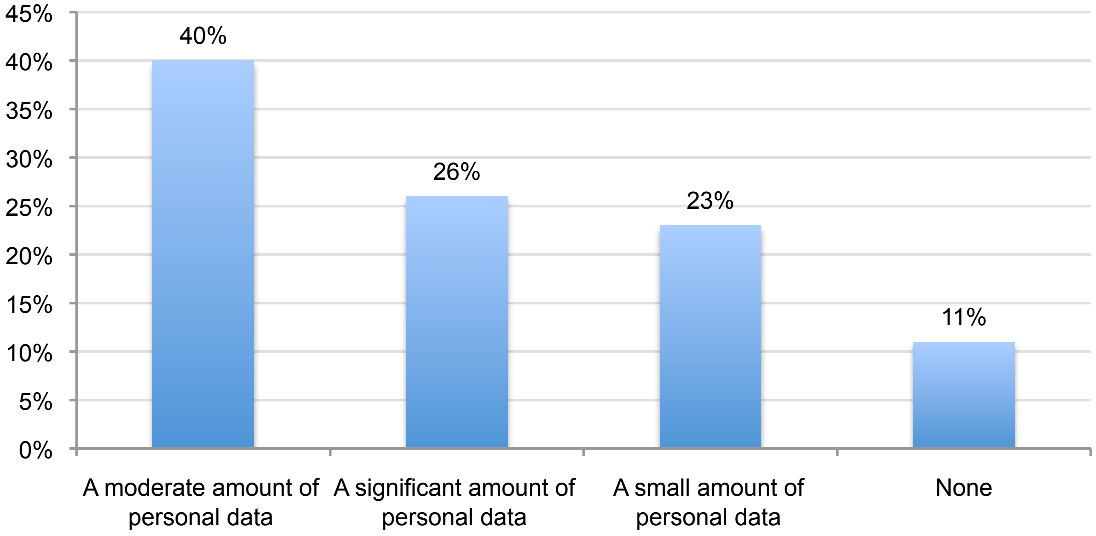
Bar Chart 4: Key questions about smartphone use
Each bar defines the percentage yes response



Consumers store confidential information on their smartphones.

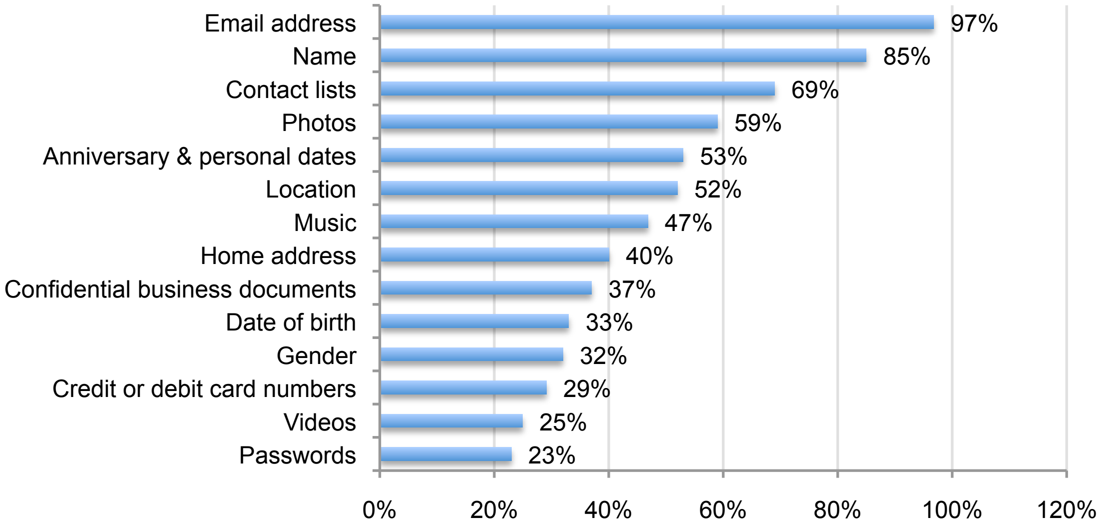
Sixty-six percent (40+26) of consumers store a moderate or a significant amount of personal data. Bar Chart 5 shows that only 11 percent say they do not store personal data on their smartphone.

Bar Chart 5: How much personal data do you store on your smartphone?



As shown in Bar Chart 6, data most often stored on smartphones include email addresses, names, contact lists, photos, anniversary and other personal dates and location. Consumers are less likely to store planned future purchases, purchase history, health data and security test questions (see Q. 23 in the Appendix for the complete list).

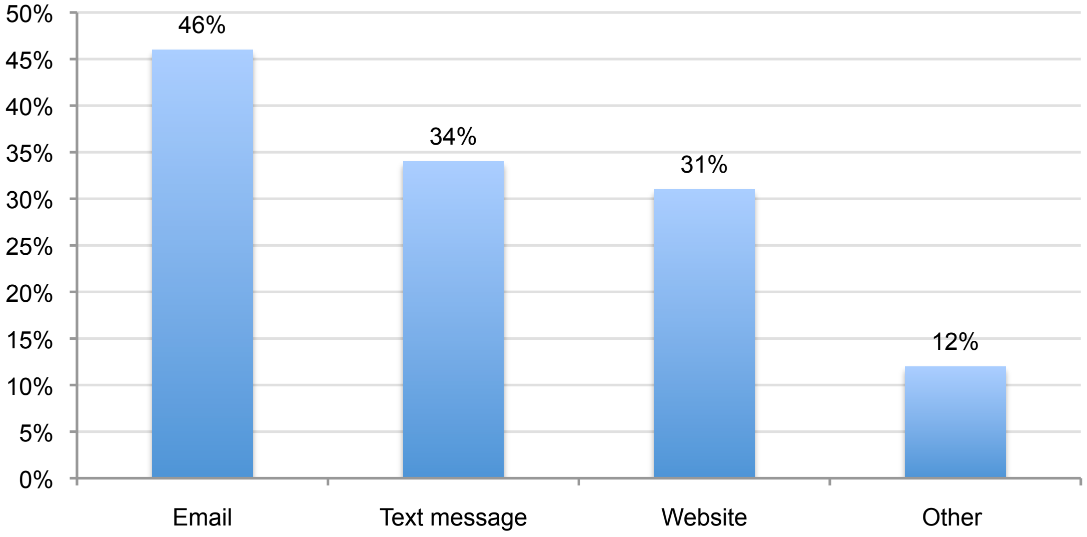
Bar Chart 6: What kinds of data do you store on your smartphone?



Many consumers surveyed have used email and text to sign up for services or products without realizing they would be charged.

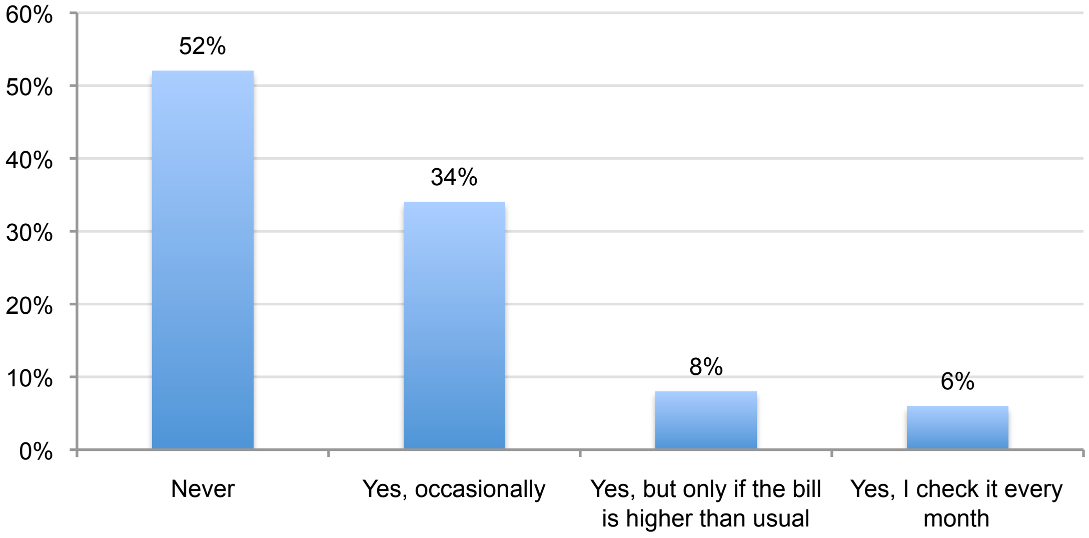
As noted previously in Bar Chart 4, 51 percent made what they thought was a free service and later found out they were charged for it. Bar Chart 7 shows most of these purchases were made by consumers using email (46 percent), text message (34 percent) and website (31 percent).

Bar Chart 7: The methods used to sign-up for services or products on your smartphone



Despite these unexpected charges, Bar Chart 8 shows consumers surveyed rarely check their bills for unusual or unidentified payments. Only six percent check their bills every month and eight percent check their bills only if it is higher than usual. Fifty-two percent never check their smartphone bills.

Bar Chart 8: Do you check your mobile bill or statement for unidentified charges?



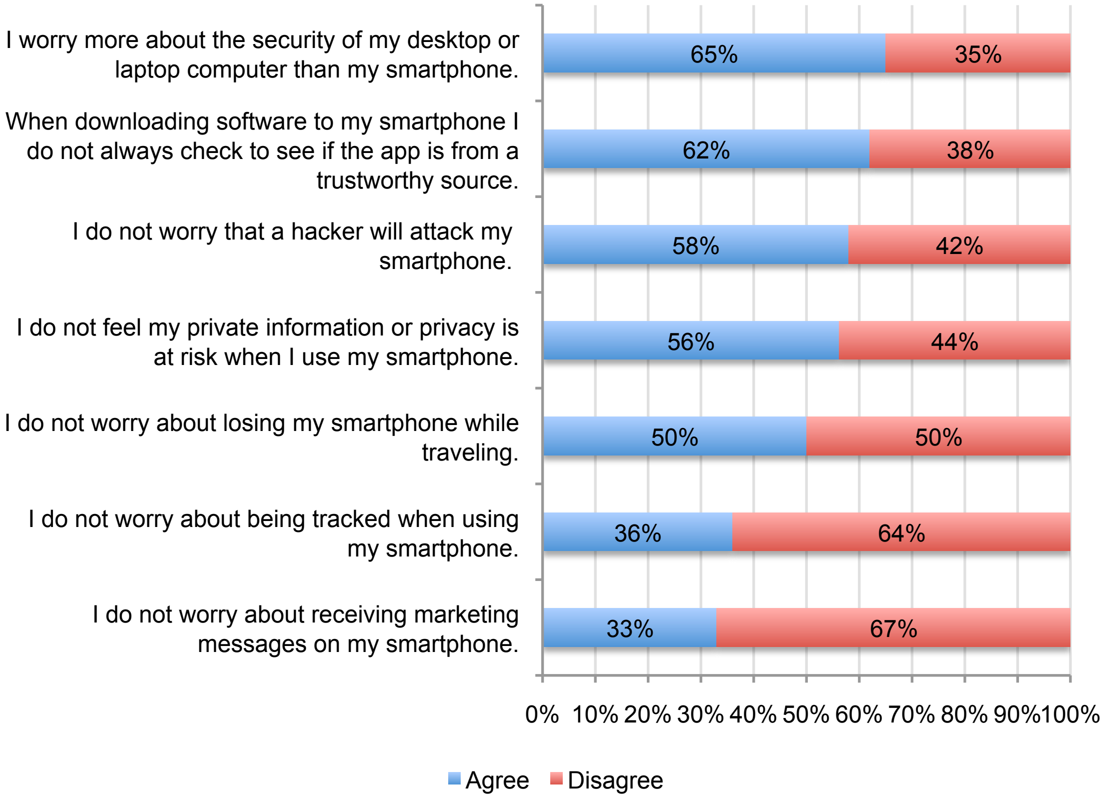
As previously noted in Bar Chart 4, the majority of consumers (78 percent) say they have not experienced any mobile payments fraud. Twelve percent say they have experienced such fraud and 10 percent are not certain.

Consumers' awareness about the security risks that accompany their use of smartphones

Marketing messages—not privacy and security risks—worry consumers.

While the majority of consumers do not feel their private information is at risk or that their smartphone will be hacked (56 percent and 58 percent, respectively), they do worry about receiving unwanted marketing messages. A shown in Bar Chart 9, consumers also worry about being tracked when using their smartphone (64 percent).

Bar Chart 9: Attributions about privacy and security risks
The agree response is a combination of strongly agree and agree.
The disagree response is the sum of unsure, disagree and strongly disagree.



They also worry more about the security of their desktop and laptop computers than the security of their smartphone. Because of these perceptions about the security of the smartphone, they are not likely to check to see if an application comes from a trustworthy source before downloading it.

Scenarios concerning smartphone risks

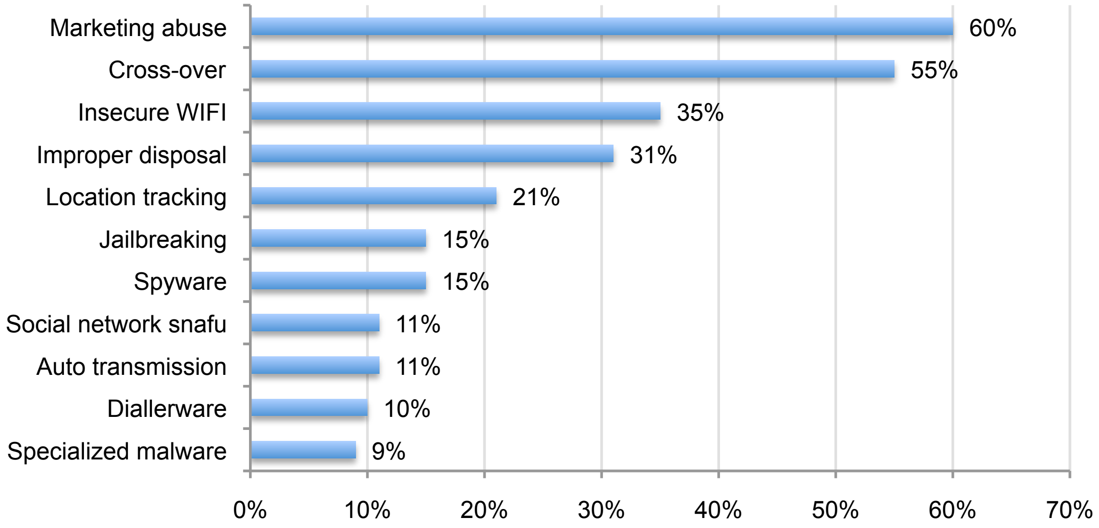
In the survey, we asked consumers to respond to eleven scenarios illustrating a range of security issues and risks. Specifically, they were asked if they are aware that what is described in the scenario could happen to them, if they are aware that they experienced what was described in the scenario and what was their level of concern. Following are the 11 scenarios:

1. Location data embedded onto image files can result in the tracking of the smartphone user.
2. Smartphone apps can transmit confidential payment information (i.e. credit card details) without the user's knowledge or consent.

3. Smartphones can be infected by specialized malware called “diallerware” that enables criminals to make use of premium services or numbers resulting in unexpected monthly charges.
4. Smartphone apps may contain spyware that allows criminals to access the private information contained on a smartphone.
5. Financial apps for smartphones can be infected with specialized malware designed to steal credit card numbers and online banking credentials.
6. If a social network app is downloaded on a smartphone, failing to log off properly could allow an imposter to post malicious details or change personal settings without the user’s knowledge.
7. A smartphone can be disposed of or transferred to another user without properly removing sensitive data, allowing an intruder to access private data on the device.
8. In many cases, people use their smartphone for both business and personal usage, thus putting confidential business information at risk (a.k.a. cross-over risk).
9. A smartphone can connect to the Internet through a local WIFI network that is insecure. This may result in a virus attack to the smartphone.
10. Smartphones contain basic security protections that can be disabled by jailbreaking, thus making the smartphone more vulnerable to spyware or malware attacks.
11. Smartphone users can be targeted by marketers based on how the phone is used for purchases, Internet browsing and location. As a result, the user may receive unwanted marketing ads and promotions their smartphone.

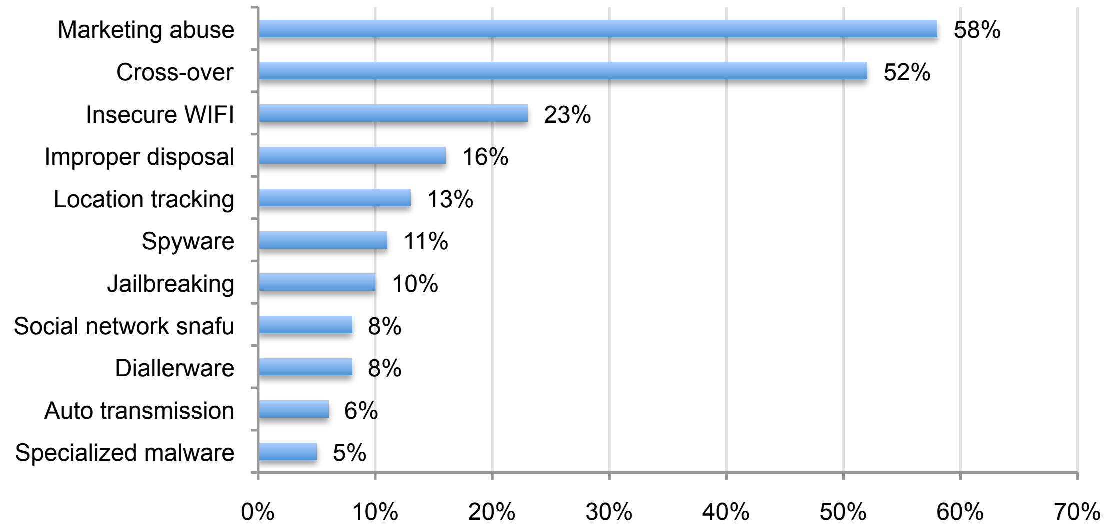
Bar Chart 10 summarizes the consumers’ level of awareness about the above-mentioned smartphone security risks. Consumers are most aware of receiving unwanted marketing messages based on their smartphone usage (60 percent). They also understand that they may be putting business confidential information at risk when using the smartphone for both personal and business use (55 percent), and that they are vulnerable to a virus when connecting to the Internet through a local WIFI network is insecure (35 percent).

Bar Chart 10: Are you aware of the following smartphone security risks?
Each bar defines the percentage yes response



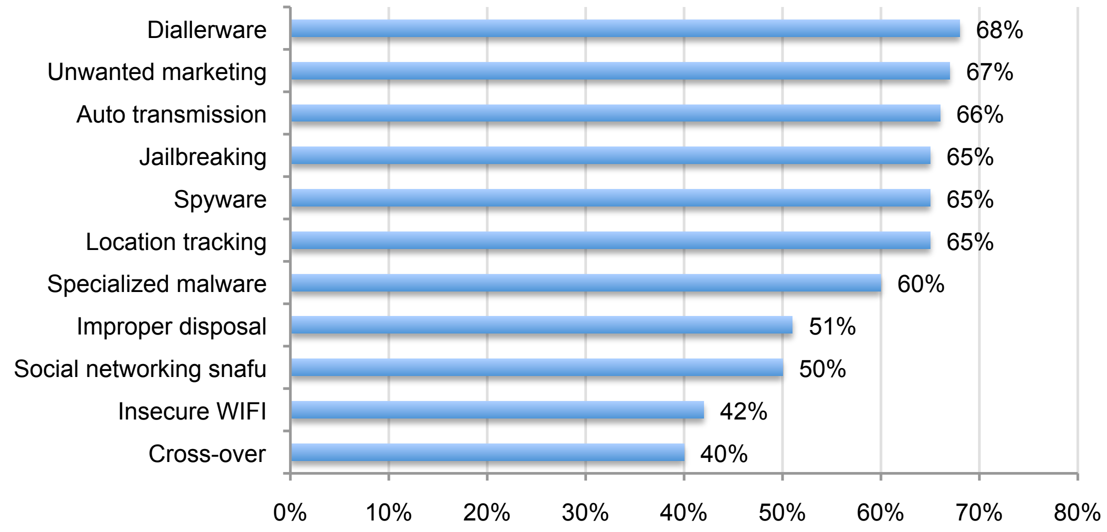
Bar Chart 11 reports consumers' actual experience with these security issues. Fifty-eight percent of consumers say they indeed have received unwanted marketing messages. In addition, 52 percent say they have experienced cross-over risk – wherein the security of business information was jeopardized because of the personal use of the smartphone.

Bar Chart 11: Have any of these situations happened to you?
Each bar defines the combined very concerned and concerned response



Bar Chart 12 summarizes consumers' level of concern about eleven smartphone security risks. Accordingly, a large percentage of these consumers say they are very concerned or concerned about each scenario happening to them, especially diallerware (68 percent), unwanted marketing (67 percent), and the auto transmission of personal data from the phone (66 percent).

Bar Chart 12: Are you concerned about of the following smartphone security risks?
Each bar defines the combined very concerned and concerned response

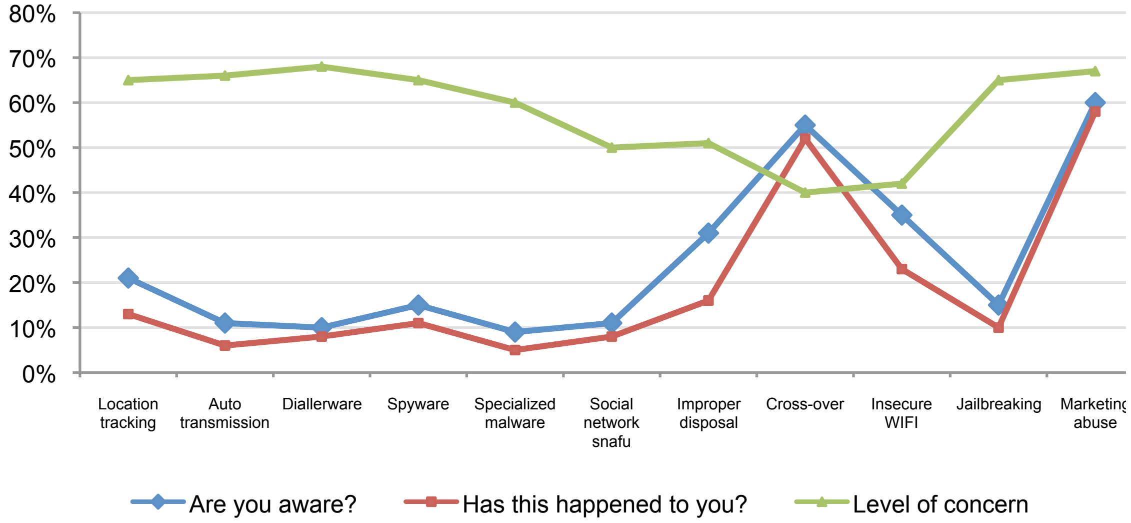


Consumers are concerned about being tracked while using their smartphones or having their security protections disabled through "jailbreaking" but generally are not aware of this risk. In contrast, only 40 percent of consumers are very concerned or concerned about cross-over and 42 percent about an insecure smartphone-to-WIFI connection.

While there is some awareness that a smartphone that is disposed of or transferred to another user without removing sensitive data could allow someone to access private data on the device, about half of consumers are not very concerned about this occurring.

In summary, consumers surveyed are least aware that the following can happen on their smartphone: the transmission of confidential payment information without their knowledge or consent, downloading a financial app for their smartphone that has specialized malware designed to steal credit card numbers and online banking credentials, "diallerware" infections that enable criminals to make use of premium services or numbers resulting in unexpected charges and spyware that allows criminals to access the private information contained on a smartphone. Those who are aware of these risks are generally very concerned about how these risks may affect their smartphone.

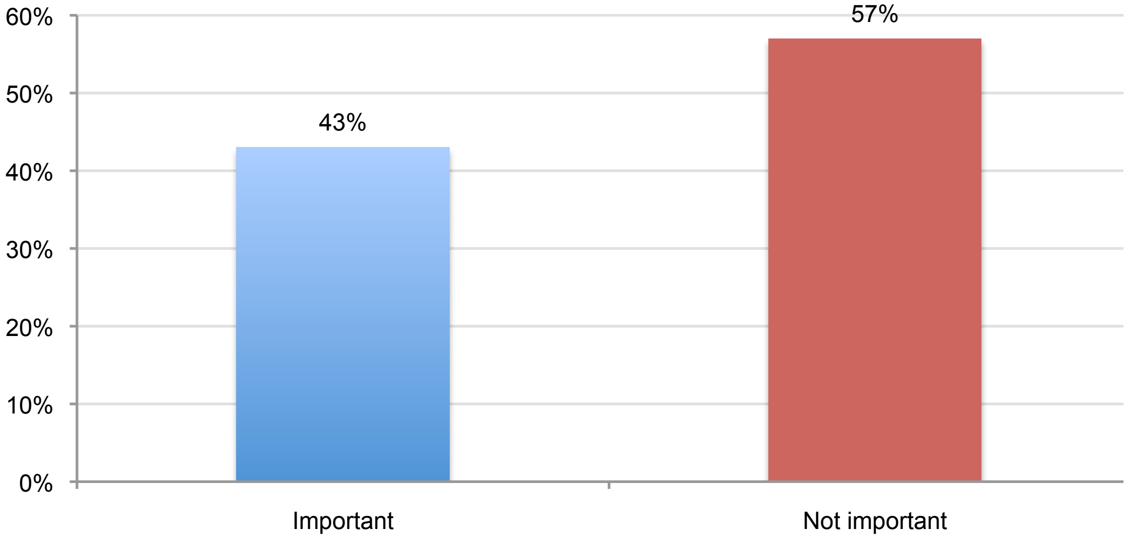
Line Graph 1: Summary of consumer responses to eleven smartphone security risks



Part 3. How consumers are managing security risks associated with smartphones Despite the confidential information on their smartphones, consumers are not taking appropriate security precautions.

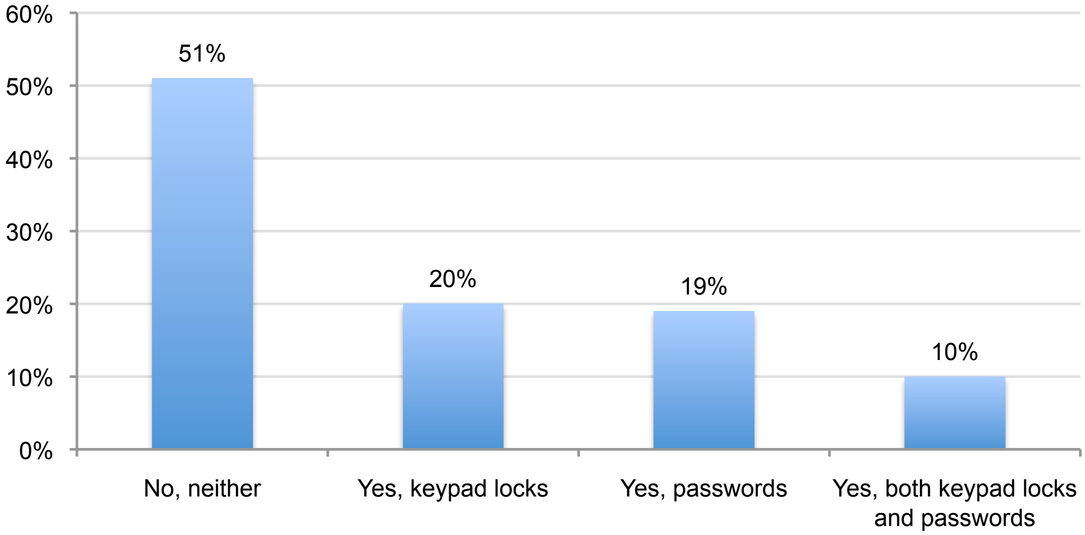
As showing in Bar Chart 13, less than half (43 percent) of consumers surveyed consider security features to be important when deciding which smartphone to purchase. It is not surprising, therefore, that they are not taking security precautions.

Bar Chart 13: How important is security as a feature on your smartphone?



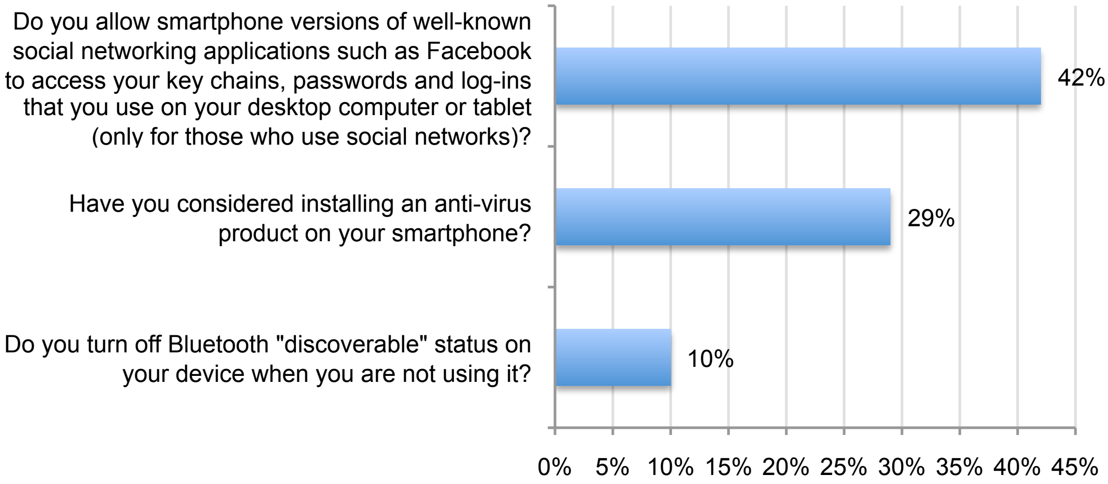
Bar Chart 14 shows 51 percent of consumers surveyed have neither keypad locks nor passwords on their smartphone. Nineteen percent have passwords and 10 percent have both keypad locks and passwords. However, when we analyzed the responses of the more experienced users the percentage dropped to 31 percent who do not use keypad locks or passwords on their smartphone.

Bar Chart 14: Do you have keypad locks or passwords on your smartphone?



Forty-two percent of consumers allow smartphone versions of well-known social networking applications such as Facebook to access their key chains, passwords and log-ins that are used on their desktop computer or tablet (see Bar Chart 15). Twenty-nine percent of consumers say they have considered installing an anti-virus product and 10 percent turn off Bluetooth "discoverable" status on their device when they are not using it. Only 10 percent set up download controls on their smartphone to protect against apps and games that may contain malware.

Bar Chart 15: Security habits of smartphone users
Each bar defines the percentage yes response



Part 4. Methods

Table 1 summarizes the sample response for this study of US consumers who own or use smartphones. Our sample frame consisted of nearly 30,000 adult-aged consumers located in the Unite States. These individuals were screened to ensure they use a smartphone for both personal and business purposes. A total of 793 responded to our web-based survey. Fifty-nine surveys failed reliability tests, resulting in a final sample of 734 consumers (2.5 percent response rate).

Table 1: Sample response	Frequency	Pct%
Sample frame	29,921	100.0%
Invitations sent	27,498	91.9%
Total returns	793	2.7%
Rejections	59	0.2%
Final sample	734	2.5%

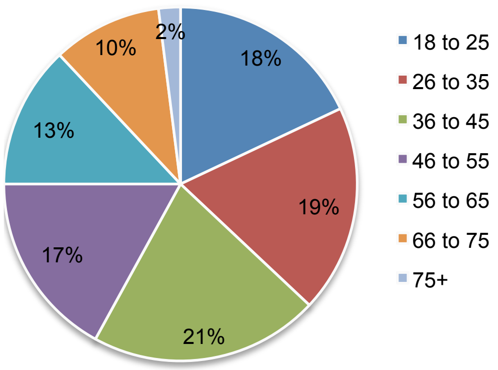
Table 2a provides the types of smartphones used by consumers. Table 2b lists the operating systems contained on these smartphones. As can be seen, the top rated smartphones are Apple's iPhone, RIM Blackberry and Google Nexus One. Accordingly, the top rated operating systems are iPhoneOS, RIM and Windows Mobile.

Table 2a. Type of smartphone	Pct%
Apple iPhone	27%
RIM Blackberry	21%
Google Nexus One	12%
Nokia N8	9%
Motorola Droid X	9%
T-Mobile G2	6%
Sprint HTC EVO 4G	6%
Palm Pre Plus	5%
Samsung Epic 4G	4%
Other	0%
Total	100%

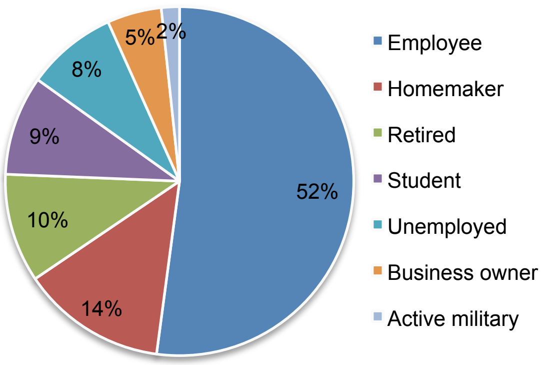
Table 2b. Operating system	Pct%
iPhoneOS	24%
RIM	19%
Windows Mobile	12%
Android	9%
Symbian OS	3%
Linux	3%
Maemo	2%
Garnet OS	2%
Bada	1%
MeeGo	1%
Other or unsure	25%
Total	100%

Pie Chart 1 reports the age range of consumers in our study. Pie chart 2 shows the employment status of consumers. The largest segment of consumers are aged 36 to 45 (21 percent), and 52 percent are employed in a full or part-time position.

Pie Chart 1: Age range

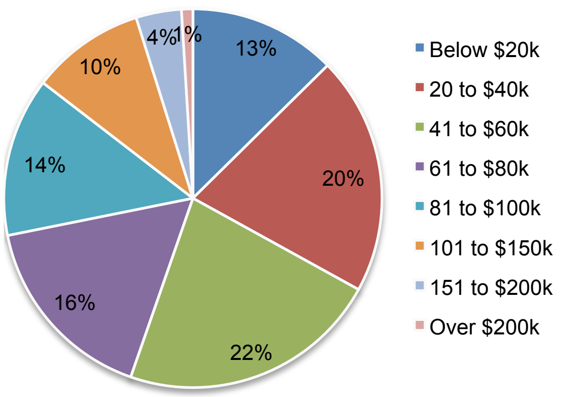


Pie Chart 2: Employment status

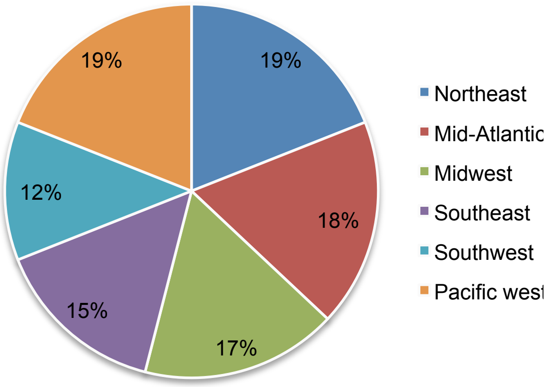


Pie Chart 3 reports the household income of consumers. Pie Chart 4 shows the location of consumers according to their region in the United States. A total of 44 states are represented in our sample. The median household income of consumers is $81,000 per year.

Pie Chart 3: Household income



Pie Chart 4: Regional location



In addition to web-based survey analysis, we conducted debriefing interviews with a random cross-section of consumers. In total 128 individuals were contacted, resulting in 66 one-to-one interviews to discuss certain questions and probe for additional insights from the consumers when appropriate.

A total of 53 percent of consumers are female, 47 percent male. Forty percent of consumers say they use their smartphone for both business and personal reasons. Only six percent say they use their smartphone solely for business (see Bar Chart 1).

Part 5. Conclusion

The key finding from this research is that consumers in our survey are unaware of the security risks associated with their smartphones. This could be attributed, in part, to the lack of information being published about smartphone security risks. We also conclude that there may be a perception that because the most popular uses are phoning and emailing they are not putting the data on their smartphones at risk.

In contrast, the security of desktop and laptop computers receives much more attention. It is not surprising, therefore, that consumers surveyed are more worried about protecting their computers from security risks. This is despite the fact these devices can contain just as much sensitive data that if lost or stolen could result in financial harm.

Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of adult-aged consumers in the United States, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that auditors who did not participate are substantially different in terms of underlying beliefs from those who completed the survey.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are information system auditors. We also acknowledge that responses from paper, interviews or telephone might result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from consumers. While certain checks and balances were incorporated into our survey evaluation process, there is always the possibility that certain consumers did not provide responses that reflect their true opinions.

Appendix: Detailed Survey Responses

Following are the survey results for a final sample of 734 adult-aged consumers located in all regions of the United States. Fieldwork concluded in February 2011.

Sample response	Frequency	Pct%
Sample frame	29,921	100.0%
Invitations sent	27,498	91.9%
Total returns	793	2.7%
Rejections	59	0.2%
Final sample	734	2.5%

Part 1. Background

Q1a. Please select the smartphone that you presently use. If you use more than one smartphone, please select the one you use most frequently.	Pct%
T-Mobile G2	6%
Apple iPhone	27%
Motorola Droid X	9%
Samsung Epic 4G	4%
RIM Blackberry	21%
Sprint HTC EVO 4G	6%
Nokia N8	9%
Google Nexus One	12%
Palm Pre Plus	5%
Other (please specify)	0%
Total	100%

Q1b. Please select the operating system your smartphone runs on.	Pct%
Symbian OS	3%
Android	9%
Linux	3%
Windows Mobile	12%
Bada	1%
MeeGo	1%
Maemo	2%
Garnet OS	2%
iPhoneOS	24%
RIM	19%
Other	0%
Unsure	25%
Total	100%

Q2. What best describes your smartphone use? Please select only one.	Pct%
Business use only	6%
Mostly business but some personal use	13%
Personal use only	16%
Mostly personal but some business use	25%
Both business and personal use equally	40%
Total	100%

Q3. Who purchased your smartphone and who pays the monthly service (usage) fee? Please select only one.	Pct%
I purchased it without any reimbursement from my employer	35%
I purchased it and my employer provided some reimbursement	13%
I purchased it and my employer pays monthly charges	10%
My employer purchased it and I pay monthly charges	8%
My employer purchased it and pays monthly charges	34%
Total	100%

Q4. Please select all the tasks that you do on your smartphone?	Pct%
Phone	100%
Personal email	89%
Business email	82%
Address book	57%
Texting	54%
Internet browsing	53%
Store or move data	53%
Obtain documents	52%
View documents	51%
Calendar	51%
Listen to music	50%
Schedule tasks	48%
Shop	44%
Camera	42%
Social networking	40%
Payments	38%
Games	34%
Maps and navigation	24%
Upload videos	24%
Location services	23%
Watch TV/films	21%
Banking	14%
Travel assistance	10%
Video conferencing	9%
Monitor health	5%

Q5. Have you ever paid for any item via your mobile phone?	Pct%
Yes, only once	11%
Yes, irregularly (maybe once every two months)	32%
Yes, regularly (maybe once a month)	23%
Never	34%
Total	100%

Q6a. Have you every signed up for a service or product on your mobile without realizing that there would be a cost?	Pct%
Yes	51%
No	49%
Total	100%

Q6b. If yes, please select the all the methods you used to sign up for the service or product.	Pct%
Text message	34%
Email	46%
Website	31%
Other	12%
Total	123%

Q7. Do you check your mobile bill or statement for unusual or unidentified payments?	Pct%
Yes, I check it every month	6%
Yes, but only if the bill is higher than usual	8%
Yes, occasionally	34%
Never	52%
Total	100%

Q8. Have you ever signed a terms and conditions request on your mobile phone?	Pct%
Yes	46%
No	21%
Unsure	33%
Total	100%

Q9. Have you ever been the victim of mobile payments fraud?	Pct%
Yes	12%
No	78%
Unsure	10%
Total	100%

Part 2. Attributions

Q10. Please rate each one of the following statements using the scale provided below each item. Strongly agree and agree shown.	Strongly agree	Agree
Q10a. I do not feel my private information or privacy is at risk when I use my smartphone.	18%	38%
Q10b. I do not worry that a hacker will attack my smartphone.	25%	33%
Q10c. I do not worry about receiving marketing messages on my smartphone.	10%	23%
Q10d. I do not worry about being tracked when using my smartphone.	11%	25%
Q10e. I do not worry about losing my smartphone while traveling.	18%	32%
Q10f. I worry more about the security of my desktop or laptop computer than my smartphone.	25%	40%
Q10g. When downloading software to my smartphone I do not always check to see if the app is from a trustworthy source.	21%	41%

Part 3. Scenarios

Q11. Sometimes location data can be embedded onto image files such as digital photos contained on your smartphone so that other people can track where you are. Were you aware that this could happen?	Pct%
Yes	21%
No	45%
Unsure	34%
Total	100%

If yes, has this happened to your smartphone?	Pct%
Yes	13%
No	28%
Unsure	59%
Total	100%

On a scale of 1 to 5, where 1 = not concerned and 5 = very concerned, how concerned are you that your location could be tracked while using your smart phone? Concerned and very concerned shown.	Very concerned	Concerned
Response	29%	36%

Q12. Smartphone apps can transmit confidential payment information such as credit card details without the user's knowledge or consent. Were you aware that this could happen?	Pct%
Yes	11%
No	53%
Unsure	36%
Total	100%

If yes, has this happened to your smartphone?	Pct%
Yes	6%
No	41%
Unsure	53%
Total	100%

On a scale of 1 to 5, where 1 = not concerned and 5 = very concerned, how concerned are you that your credit card details could be transmitted with your knowledge or consent? Concerned and very concerned shown.	Very concerned	Concerned
Response	31%	35%

Q13. Smartphones can be infected by specialized malware called "diallerware" that enable criminals to make use of premium services or numbers resulting in unexpected monthly charges. Were you aware that this could happen?	Pct%
Yes	10%
No	58%
Unsure	32%
Total	100%

If yes, has this happened to your smartphone?	Pct%
Yes	8%
No	65%
Unsure	27%
Total	100%

On a scale of 1 to 5, where 1 = not concerned and 5 = very concerned, how concerned are you that your smartphone could be infected by diallerware? Concerned and very concerned shown.	Very concerned	Concerned
Response	36%	32%

Q14. Smartphone apps may contain spyware that allows criminals to access the private information contained on a smartphone. Were you aware that this could happen?	Pct%
Yes	15%
No	53%
Unsure	32%
Total	100%

If yes, has this happened to your smartphone?	Pct%
Yes	11%
No	56%
Unsure	33%
Total	100%

On a scale of 1 to 5, where 1 = not concerned and 5 = very concerned, how concerned are you that your smartphone could be infected by spyware? Concerned and very concerned shown.	Very concerned	Concerned
Response	33%	32%

Q15. Financial apps for smartphones can be infected with specialized malware designed to steal credit card numbers and online banking credentials. Were you aware that this could happen?	Pct%
Yes	9%
No	57%
Unsure	34%
Total	100%

If yes, has this happened to your smartphone?	Pct%
Yes	5%
No	66%
Unsure	29%
Total	100%

On a scale of 1 to 5, where 1 = not concerned and 5 = very concerned, how concerned are you that your smartphone or downloaded apps could be infected by this specific type of malware? Concerned and very concerned shown.	Very concerned	Concerned
Response	32%	28%

Q16. If a social network app is downloaded on a smartphone, failing to log off properly could allow an imposter to post malicious details or change personal settings without the user’s knowledge. Were you aware that this could happen?	Pct%
Yes	11%
No	56%
Unsure	33%
Total	100%

If yes, has this happened to your smartphone?	Pct%
Yes	8%
No	55%
Unsure	37%
Total	100%

On a scale of 1 to 5, where 1 = not concerned and 5 = very concerned, how concerned are you that your failure to close the social networking app on your smartphone could allow unauthorized access and/or malicious posts your user account? Concerned and very concerned shown.	Very concerned	Concerned
Response	26%	23%

Q17. A smartphone can be disposed of or transferred to another user without properly removing sensitive data, allowing an intruder to access private data on the device. Were you aware that this could happen?	Pct%
Yes	31%
No	36%
Unsure	33%
Total	100%

If yes, has this happened to your smartphone?	Pct%
Yes	16%
No	54%
Unsure	30%
Total	100%

On a scale of 1 to 5, where 1 = not concerned and 5 = very concerned, how concerned are you that private information on the smartphone would not be removed properly before disposing of it or transferring it to another user? Concerned and very concerned shown.	Very concerned	Concerned
Response	23%	28%

Q18. In many cases, people use their smartphone for both business and personal usage, thus putting confidential business information at risk. Were you aware that this could happen?	Pct%
Yes	55%
No	28%
Unsure	17%
Total	100%

If yes, has this happened to your smartphone?	Pct%
Yes	52%
No	36%
Unsure	12%
Total	100%

On a scale of 1 to 5, where 1 = not concerned and 5 = very concerned, how concerned are you that your use of a smartphone for personal reasons could put the confidential information of your business at risk? Concerned and very concerned shown.	Very concerned	Concerned
Response	19%	21%

Q19. A smartphone can connect to the Internet through a local WIFI network that is insecure. This may result in a virus attack to the device. Were you aware that this could happen?	Pct%
Yes	35%
No	42%
Unsure	23%
Total	100%

If yes, has this happened to your smartphone?	Pct%
Yes	23%
No	45%
Unsure	32%
Total	100%

On a scale of 1 to 5, where 1 = not concerned and 5 = very concerned, how concerned are you that your smartphone when connected to an insecure Internet network may result in a virus attack? Concerned and very concerned shown.	Very concerned	Concerned
Response	22%	20%

Q20. Smartphones contain basic security protection that can be disabled by jailbreaking, thus making the smartphone more vulnerable to spyware or malware attacks. Were you aware that this could happen?	Pct%
Yes	15%
No	57%
Unsure	28%
Total	100%

If yes, has this happened to your smartphone?	Pct%
Yes	10%
No	55%
Unsure	35%
Total	100%

On a scale of 1 to 5, where 1 = not concerned and 5 = very concerned, how concerned are you that your smartphone's security settings could be disabled remotely by a third party without your knowledge or consent? Concerned and very concerned shown.	Very concerned	Concerned
Response	34%	31%

Q21. Smartphone users can be targeted by marketers based on how the phone is used for purchases, Internet browsing, and location. As result, the user may receive unwanted marketing ads and promotions. Were you aware that this could happen?	Pct%
Yes	60%
No	17%
Unsure	23%
Total	100%

If yes, has this happened to your smartphone?	Pct%
Yes	58%
No	15%
Unsure	27%
Total	100%

On a scale of 1 to 5, where 1 = not concerned and 5 = very concerned, how concerned are you that your smartphone could receive marketing ads and promotions? Concerned and very concerned shown.	Very concerned	Concerned
Response	31%	36%

Part 4. Other Questions

Q22. On average, how much personal data do you store on your smartphone?	Pct%
None (Go to Q24)	11%
Only a small amount of personal data	23%
A moderate amount of personal data	40%
A significant amount of personal data	26%
Unsure	100%

Q23. What kinds of data do you store on your smartphone?	Pct%
Email address	97%
Name	85%
Contact lists	69%
Photos	59%
Anniversary and other personal dates	53%
Location	52%
Music	47%
Home address	40%
Confidential business documents	37%
Date of birth	33%
Gender	32%
Credit or debit card numbers	29%
Videos	25%
Passwords	23%
PIN number	19%
Hobbies, sports and travel interests	15%
Ages and gender of children	13%
Names of children	13%
Alarm codes	11%
Planned future purchases	8%
Purchase history	8%
Health data	5%
Security test questions	2%

Q24. Do you use a one Gigabyte (or higher) storage device on your smartphone?	Pct%
Yes	19%
No	68%
Unsure	13%
Total	100%

Q25. What do you worry more about?	Pct%
Losing my wallet/purse	50%
Losing my smartphone	23%
I worry about both equally	27%
Total	100%

Q26. What do you worry more about?	Pct%
Losing my laptop computer	38%
Losing my smartphone	10%
I worry about both equally	19%
I don’t have a laptop computer	33%
Total	100%

Q27. Do you have keypad locks or passwords on your smartphone?	Pct%
Yes, keypad locks	20%
Yes, passwords	19%
Yes, both keypad locks and passwords	10%
No, neither	51%
Total	100%

Q28a. Do you synch your smartphone with any of the following devices?	Pct%
Laptop	44%
Desktop	38%
Another smartphone	9%
An online backup storage solution	8%
None of the above	45%
Total	144%

Q28b. How regularly do you synch your smartphone with any of the devices listed in Q28a?	Pct%
Hourly	25%
Daily	29%
Weekly	14%
Monthly	8%
Irregularly	24%
Total	100%

Q29. Do you allow smartphone versions of well-known social networking applications such as Facebook to access your key chains, passwords and log-ins that you use on your desktop computer or tablet?	Pct%	Adjusted
Yes	21%	42%
No	25%	50%
Unsure	4%	8%
I don’t use social networking apps	50%	0%
Total	100%	100%

Q30. Do you turn off Bluetooth "discoverable" status on your device when you are not using it?	Pct%	Experienced
Yes	10%	30%
No	83%	62%
Unsure	7%	8%
Total	100%	100%

Q31. Have you considered installing an anti-virus product on your smartphone?	Pct%	Experienced
Yes	29%	53%
No	71%	47%
Total	100%	100%

Q32a. Do your children have a mobile/cell smartphone?	Pct%
Yes	22%
No	33%
I don’t have children	45%
Total	100%

Q32b. If yes, do you use your children’s smartphone to keep track of them (from a security perspective)?	Pct%
Yes	41%
No	59%
Total	100%

Q32c. If yes, do you set up parental controls on the smartphone to protect your children when they access the Internet?	Pct%
Yes	21%
No	79%
Total	100%

Q33. Do you set up download controls on your smartphone to protect against apps and games that may contain malware?	Pct%
Yes	10%
No	74%
Unsure	16%
Total	100%

Q34. When deciding which smartphone to purchase, how important are its security features? Very important and important shown.	Very important	Important
Response	21%	22%

Part 5. Demographics

D1. Please check your age range.	Pct%
18 to 25	18%
26 to 35	19%
36 to 45	21%
46 to 55	17%
56 to 65	13%
66 to 75	10%
75+	2%
Total	100%

D2. What is your present employment status?	Pct%
Full-time employee	48%
Part-time employee	6%
Business owner	5%
Homemaker	13%
Retired	10%
Student	9%
Active military	2%
Unemployed	8%
Total	100%

D3. What range best defines your annual household income?	Pct%
Below $20k	13%
20 to $40k	20%
41 to $60k	22%
61 to $80k	17%
81 to $100k	14%
101 to $150k	10%
151 to $200k	4%
Over $200k	1%
Total	100%

D4. What is your highest level of education attained?	Pct%
High school	21%
Vocational	22%
University or college	45%
Post graduate	7%
Doctorate	1%
Other	4%
Total	100%

D5. Please check gender:	Pct%
Female	53%
Male	47%
Total	100%

D6. Are you head of household?	Pct%
Yes	48%
No	52%
Total	100%

D7. US Region	Pct%
Northeast	19%
Mid-Atlantic	18%
Midwest	17%
Southeast	15%
Southwest	12%
Pacific	19%
Total	100%

D8. Please rate each one of the following statements using the following five-point scale. Strongly agree and agree sown.	Strongly agree	Agree
The Internet is central to my lifestyle	25%	32%
I often give advice to others about how best to use computers and software	19%	21%
I need to ask for help if something goes wrong with my computer	22%	23%
I always try to spend as little time as possible online	16%	24%
I am often confused when I try to use the Internet to do things	23%	24%
I am really concerned about online threats	18%	35%
Only people who do risky things on the Internet are at risk to online threats	15%	28%
I don’t feel the online threat is that significant	18%	34%

Please contact us at 231.938.9900 or send an email to research@ponemon.org.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**,we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.