Interdisciplinary Description of Complex Systems 16(3-A), 376-383, 2018

SMART AND SECURE?
MILLENNIALS ON MOBILE DEVICES

Peter Holicza* and Esmeralda Kadëna

Óbuda University, Doctoral School on Safety and Security Sciences
Budapest, Hungary

DOI: 10.7906/indecs.16.3.10
Regular article

Received: 17th April 2018.
Accepted: 31st August 2018.

ABSTRACT

Millennials, members of the Generation Y are constantly connected to their social circles online, they are the founders of the social media movement. These young consumers count as the largest segment of smartphone owners in most regions of the world. In fact, smartphones have become one of the most important possessions of this highly technology savvy generation. However, the advanced and widespread use of mobile devices often does not meet with the required security consciousness. People who have grown up with internet, are more likely to share personal and sensitive corporate information online by using the same device for both work and private applications, accessing free Wi-Fi networks or borrowing other devices without the appropriate protection. This work examines the crucial smartphone security risks that users face with the new technology. It aims to investigate how their practices and behaviours can pose security risks on their smartphones usage. Security practices and awareness can be improved by increasing users' knowledge. To accomplish this, education on technology is needed.

KEY WORDS

mobile device, Millennials, Generation Y, online behaviour, security

CLASSIFICATION

JEL: L63, L86, L96

*Corresponding author, η: holicza.peter@rh.uni-obuda.hu; –;
Doctoral School of Safety and Security Sciences of Obuda University, H – 1428 Budapest, Pf.:31, Hungary

INTRODUCTION: UNDERSTANDING THE MAIN USER PROFILE

It is evident that we as a society enter the digital age, physical presence and personal relations are getting less and less important. The differences in opinions between generations regarding beliefs, political views, or values, are referred to as ‘generation gap’. As the whole world is facing new challenges, in terms of changes in classical roles and established norms, which result in traditional practices being less effective and often inapplicable; it is inevitable that certain adaptations in educational system, marketing, media, security and other fields related to Generation Y are necessary. The Millennials, Digital Natives, the ‘we want it now’ – many names have been used to describe this young generation, who are characterized as technology savvy, dexterous, open to new things and able to work in team [1]. It is evident how these characteristics make this generation more critical about technical issues and impatient; and the skill of creating *instant*, but effective solutions is being more and more appreciated and desirable in all life spheres. The values and characteristics of the Y generation have been widely researched, explained and grouped [2]. In addition, researchers mapped the psychological phenomenon that is associated with this generation, the most important of which are detailed in the following list:

- **Speed:** These young people were born in an era of technological development, and the usage of information technology novelties comes naturally to them. The information resources are today much easier to reach and the search is less time consuming, instead of going to the library, one can just “Google it” and find as much relevant information within seconds, while their predecessors did not have this luxury and would not be able to gather that amount of data through their whole lifetime. The social media enables them to be informed in real-time about the latest trends, daily events and lives of their peers and opens a platform in which they can communicate and exchange information in their private and social lives.
- **Decline of personal relationships:** It is evident that online communities transformed personal relationships. Most everyday life activities are simplified and more instant, which makes the actual human contact less important. Instead of writing a letter and waiting for it to reach the recipient, or even making a call, it is enough to just send a few words and emojis on Messenger. Planning and making arrangements is also simplified as we are now able to simply log into a website or an App and check who shared their location with us-we can know who is where and with whom. Living our lives online means sharing a lot of personal information and we are often expected to do so in order of keeping up with the contemporary world, otherwise one who decides to keep their personal life offline might become non-existent to others as the live interaction loses its value.
- **Freedom and adventure:** This generation is multilingual and the internet provided such opportunities, allowing them to roam the world virtually and made it easier to do so even in reality, as the formerly known barriers are gone [3]. The advanced technology enabled us to be online everywhere nowadays and it made it possible to travel freely to almost every corner of the world, and even working from the most exotic places, that is to be what is referred to as *digital nomads* [4].
- **Uniqueness and individualism:** They try to define themselves through their appearance and to stand out from the crowd. It is easy to shape their virtual personality and image in any way that they want and present themselves to the world in a way they are comfortable with. This freedom of *choosing* the whole life, as one present to the online community, requires the increase of consciousness. Digital technology has the ability of transforming identities [5]. These platforms are well organized and enable users to control what they want others to see, which leads to only the best moments being uploaded and shown.

According to some research, it might cause significant self-esteem problems as the audience (followers) compare only these moments to their life. On the other hand, the positive or negative feedbacks on the posts raise or decrease social self-esteem and well-being of the uploaders [6].

- **Simplicity, Simplification:** They prefer the simple, fast and more concise information, which explains the spread of image sharing web pages, apps and platforms (Instagram, Flickr, Tumblr, and Snapchat) where the text content is minimal. Members of the Y generation are reading less and less and the number of people struggling with reading comprehension is growing – if a text does not fit the mobile display, it seems to be too long to read.
- **FoMO:** This completely new phenomenon, which is the FoMO (fear of missing out) defined as the anxiety that someone feels when others are engaged in a rewarding, cheerful activity, while he/she is away [7]. It has a relevant impact on the psychological state of young people and on the quality of their lives by generating a lot of negative feelings and making individuals compete on a regular basis through social media. Because of the strong impact, it is not surprising that several marketing campaigns are based on this fear, and using the following words, expressions: *do not miss it, join us* etc. and require young people to constantly be online in order of feeling like a part of a community and in track of the latest trends.

MILLENNIALS' DIGITAL BEHAVIOUR

The above-mentioned conditions count as driving force of Millennials, therefore the advanced technology plays a very important role in their daily life. According to Vocalink study, smartphone is the most preferred smart device of European Millennials [8]. Mobile devices are the gateway of personal and/or business data, both local and those delivered in the cloud. During the use of such devices, millennials lead tracks and not only with regard to themselves but also to their contacts. The owner of smartphone is considered as the partial administrator of his device because some implemented security policies and relative technological mechanisms limit his actions. But alone technology cannot address security solutions [9]. That is why there is a need to analyse human based aspects, by understanding users and creating then more effective security measures as well as supporting good security practices through engagement and collaboration [9, 10].

Boshmaf et al. analysed the users' need for protection and privacy in smartphones usage. They outlined the types of data that users want to protect and investigated users' behaviour in the protection of such of data and the results showed that users want to protect their data on smartphone but they find doing so not convenient [11]. Onwubiko and Owens showed that employer's consent with security policies and guidelines in many companies is taken for granted. Instead of this they prefer a formalistic security approach [12].

Researchers are focused on examining whether users' protective behaviours are influenced by their technical knowledge and awareness of security threats [13, 14]. Wash et al. found that users' security perceptions can be grouped according to their demographic groups and technological knowledge [13]. Their observations showed that people with lower educational levels tend to make simpler security decisions [14]. Larose et al., state that peoples' security practices are affected the most by their motivation to protect themselves against security risks [15]. Many authors showed that smartphone users' privacy concerns have focused on location tracking and sharing [16, 17]. The problems of data protection against physical risks and possibility to improve weak authentication were presented by Muslokhlove. To increase the confidence of user and safety of mobile devices, upgrading the lock screen system in support of authentication and user's accessibility and providing suitable security might be a good solution [18]. Ghosh et al. worked on user data, privacy and protection regarding semantic reasoning and user context modelling. The users' and smartphones' privacy under this framework are protected using embedded semantic policies based on the user' privacy and settings [19]. To execute the privacy policies on smartphone and to protect the data on an enterprise, Kodeswaran et al. showed a framework designed for Android platform policies [20]. The authors defined their privacy policies of acceptable information flow on mobile devices. The flow of information depends on the object involved in conforming Inter-Process Communication and its data.

USER BASED SECURITY RISKS

Mobile device users can be considered as the most effective tool that attackers have in compromising security. These devices can be victims of theft, data leakage and damage and as a result represent a significant information security risk to a Millennial. Below we present possible ways how attackers can gain access to mobile devices due to practices and users behaviours.

The malicious software (malware) industry is growing in terms of technology and structure. Malware causes breakdown of the device by entering at specific information and the damaged data/information of users becomes unusable [21]. These illegal softwares installed not directly by the user are used for all attacks that came from the outside taking advantage of the vulnerabilities in the device/system. The current platforms ask users to make the decision about accessing features such as location. These permission-granting approaches mean too much obstacles for the users. Very often most of them are ignored or not understood by users [22] and permission prompts are disruptive to the user's experience, teaching users to ignore and click through them [23]. As a consequence, users unintentionally grant applications too many permissions and become vulnerable to applications that use the permissions in malicious or questionable ways (i.e. secretly sending SMS messages or leaking location information).

Trojan or spyware, aims to seize the management and the information of the device [24]. Keyloggers are the most widely used form and are transmitted under the cover of a file that the user can unintendedly activate. The entire device in the background is under control of spywares and not noticed by the user. Worms are another type of malwares, a kind of virus, designed to spread through the network [24]. Transmitting forms (user interaction is needed) by SMS, MMS and activated by clicking on a file or opening a plug-in sent by e-mail, i.e. social engineering. Virus can penetrate into documents, send them elsewhere, distort their contents or make them unusable and make the hardware elements slow down [24]. Infected programs can be installed in other devices as well, followed by data loss, data leakage and even disruption of the conversation (for more, see *Zombie* virus) [25].

Information can also be collected and sent to someone else without permission through adware (used for advertising and promotional purposes) or cookies (supposed to offer better service to users) [24]. For iOS, the biggest threat in 2016 came from applications with very aggressive adware while Google Play saw a number of applications infected by malware [26]. Malwares are also created by some profit-oriented *teams*, like the Trojan "botnet Trojan-SMS.AndroidOS.-Opfake.a", which enabled the spread of the malware software "Backdoor.AndroidOS.Obad.a", which sends a spam containing the malware to its victim list [27]. If the mobile's operating system (OS) is out of date, it can also lead to vulnerability. Usually users don't pay attention to messages to update their mobile OS. Another issue is related to downloading from third party applications. Deficient API management is responsible for many malicious code infections. Controlled APIs have specific higher privileges to system update, file destruction, and information fetching. If attackers gain the APIs control, they could easily initiate attacks and use the privileges of the APIs [28, 29].

Other attacks (Social Engineering) [30] against users can be effective without using malicious software. *Phishing* (Password + Fishing), directs the user to a false (imitation) website in order to steal private information (credentials, credit card information, user name or password) [31]. Secure Sockets Layer (SSL)/Transport Layer Security (TLS) encryption is a protocol that assures users and provides data security when implemented correctly. Today it is used in many applications such as internet banking. If the code is left uncontrolled, the settings can be changed unwillingly and the information which was supposed to be safe and transmitted can be stolen through the communication path [32].

All smartphones have camera and touchscreen which can also lead to potential attacks. Users go to third party applications and if the source application is a problem, users are at risk of installing malicious programs. As a result, they can steal personal information or gain root access to their device [33, 34].

Considering the case of stolen or lost device, everyone can easily gain access to it if the screen is not locked, and encryption is an essential measure when it comes to security. With data like bank card information, passwords, sensitive data (messages, photos, videos, etc.), encrypting the data on smartphone keeps most personal information secure. A good defence practice against hackers can be the use of a strong password (a long one, mixed chars numbers and letters: owners' method) [35]. The longer the password, the stronger the encryption key.

CONCLUSION

The Millennials' digital habits have a lot of risk factors, such as the *internet at any price* mentality: internet access from any kind of free Wi-Fi networks, the lack of security measures and general unconsciousness about potential online threats.

Malicious softwares, Trojan or spyware, viruses, outdated operating systems, downloading from *third-party app*, unlocked touchscreen were identified. Hackers can easily manipulate this generation through Social Engineering tricks. Millennials rarely consider privacy and security of their smartphones, however, the increasing amount of sensitive data pose security challenges to users. In order to prevent data and information leakage is very important to increase the security awareness of people. Technology alone cannot address and solve security problems as they are not just a matter of technological factors, but human factor is involved as well. More attention should be paid to human behaviour, general attitude and misconceptions with regards to smartphone security. There is a need for education on technology in order of creating more effective security measures.

ACKNOWLEDGEMENT

Present article has been supported through the New National Excellence Program of the Ministry of Human Capacities of Hungary.

REFERENCES

[1] Jami, L.J.: *Who are Millennials? And what they want from libraries, bookstores and librarians.*
World Class Learning and Literacy through School Libraries. International Association of School Librarianship, Berkeley, 2008,

[2] Noble, S.M.; Haytko, D.L. and Phillips, J.: *What drives college-age Generation Y consumers?*
Journal of Business Research **62**(6), 617-628, 2009,
http://dx.doi.org/10.1016/j.jbusres.2008.01.020,

[3] Lazányi, K.: *What is the Role of Higher Educational Institutions in Managing their Students' Competencies?*
Science Journal of Business and Management **3**(1-1), 46-52, 2015,
http://dx.doi.org/10.11648/j.sjbm.s.2015030101.18,

[4] Prensky, M.: *Digital Natives, Digital Immigrants Part 1.*
On the Horizon **9**(5), 1-6, 2001,
http://dx.doi.org/10.1108/10748120110424816,

[5] Perillo, S.: *Reaching Generation Y: To be or not to be relevant.*
Australian Anglican Schools Network, Melbourne, 2007,

[6] Bolton, R.N., et al.: *Understanding Generation Y and their use of social media: a review and research agenda.*
Journal of Service Management **24**(3), 245-267, 2013,
http://dx.doi.org/10.1108/09564231311326987,

[7] Przybylski, A.K.; Murayama, K.; DeHaan, C.R.; and Gladwell, V.: *Motivational, emotional, and behavioral correlates of fear of missing out.*
Computers in Human Behavior **29**(4), 1841-1848, 2013,
http://dx.doi.org/10.1016/j.chb.2013.02.014,

[8] Vocalink*: The Millennials Influence – Europe*.
https://www.ipsos.com/sites/default/files/2017-05/vocalink-the-millennial-influence-europe.pdf,
accessed 20th March 2018,

[9] Furnell, S. and Clarke, N.: *Power to the people? The evolving recognition.*
Computers and Security **31**(8), 983-988, 2012,
http://dx.doi.org/10.1016/j.cose.2012.08.004,

[10] Colwill, C.: *Human factors in information security: The insider threat who can you trust these days?*
Information Security Technical Report **14**(4), 186-196, 2009,
http://dx.doi.org/10.1016/j.istr.2010.04.004,

[11] Muslukhov, I.; Boshmaf, Y.; Kuo, C.; Lester, J. and Beznosov, K.: *Understanding Users' Requirements for Data Protection in Smartphones*.
In: Kementsietsidis, A. and Vaz Salles, M.A., eds.: *Proceedings of the 2012 IEEE 28th International Conference on Data Engineering Workshops*. IEEE, Arlington, pp.228-235, 2012,
http://dx.doi.org/10.1109/ICDEW.2012.83,

[12] Onwubiko, C. and Owens, T.J., eds.: *Situational Awareness in Computer Network Defence: Principles, Methods and Applications.*
IGI Global, Hershey, 2012,
http://dx.doi.org/10.4018/978-1-4666-0104-8,

[13] Wash, R. and Rader, E.: *Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users*.
In: Faith Cranor, L.; Biddle, R. and Consolvo, S., eds.: *Proceedings of the Eleventh Symposium On Usable Privacy and Security SOUPS 2015*. USENIX Association, Ottawa, pp.309-325, 2015,

[14] Aytes, K. and Conolly, T.: *A Research Model for Investigating Human Behavior Related to Computer Security*.
In: Americas Conference on Information Systems 2003 Proceedings. Association for Information Systems, No. 260, 2003,

[15] Larose, R.; Rifon, N. and Lee, D.:*Keeping our network safe: a model of online protection behaviour.*
Behaviour and Information Technology **27**(5), 445-454, 2008,
http://dx.doi.org/10.1080/01449290600879344,

[16] Kelley, P.G.; Benisch, M.; Cranor, L.F and Sadeh, N.: *When are users comfortable sharing locations with advertisers?*
In: Tan, D.; Fitzpatrick, G.; Gutwin, C.; Begole, B. and Kellogg, W.A., eds.: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Vancouver, pp.2449-2452, 2011,
http://dx.doi.org/10.1145/1978942.1979299,

[17] Consolvo, S., et al.: *Location Disclosure to Social Relations: Why, When, & What People Want to Share.*
In: Kellogg, W.; Zhai, S.; van der Veer, G. and Gale, C., eds.: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Portland, pp.81-90, 2005,
http://dx.doi.org/10.1145/1054972.1054985,

[18] Muslukhov, I.: *Survey: Data Protection in Smartphones Against Physical Threats*.
Term project paper on Mobile Security and Privacy. University of British Columbia, Canada, 2012,

[19] Ghosh, D.; Joshi, A.; Finin, T. and Jagtap, P.: *Privacy Control in Smart Phones Using Semantically Rich Reasoning and Context Modeling.*
In: Dietrich S., et al., eds.: *Proceedings of the 2012 IEEE Symposium on Security and Privacy Workshops*. IEEE, San Francisco, pp.82-85, 2012,
http://dx.doi.org/10.1109/SPW.2012.27,

[20] Kodeswaran, P., et al.: *Securing Enterprise Data on Smartphones Using Run Time Information Flow Control*.
In: Aberer, K.; Joshi, A. and Mukherjea, S., eds.: *Proceedings of the 2012 IEEE 13th International Conference on Mobile Data Management*. IEEE, Bengaluru, pp.300-305, 2012,
http://dx.doi.org/10.1109/MDM.2012.50,

[21] Porter Felt, A.; Finifter, M.; Chin, E.; Hanna, S. and Wagner, D.: *A survey of mobile malware in the wild.*
In: Jiang, X.; Bhattacharya, A.; Dasgupta, P. and Enck, W., eds.: Proceedings of the 1st ACM *Workshop on Security and Privacy in Smartphones and Mobile Devices*. ACM, Chicago, pp.3-14, 2011,
http://dx.doi.org/10.1145/2046614.2046618,

[22] Porter Felt, A., et al.: *Android Permissions: User Attention, Comprehension, and Behavior*.
In: Faith Cranor, L., ed.: *Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, Washington, No.3, 2012,
http://dx.doi.org/10.1145/2335356.2335360,

[23] Motiee, S.; Hawkey, K. and Beznosov, K.: *Do Windows users follow the principle of least privilege?: Investigating user account control practices*.
In: Faith Cranor, L., ed.: *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM, Redmond, No.1, 2010,
http://dx.doi.org/10.1145/1837110.1837112,

[24] Bidgoli, H.: *Volume III: Threats, Vulnerabilities, Prevention, Detection and Management*.
Handbook of Information Security. John Wiley & Sons, New Jersey, 2006,

[25] Gao, C. and Liu, J.: *Modeling and restraining mobile virus propagation.*
IEEE Transactions on Mobile Computing **12**(3), 529-541, 2013,
http://dx.doi.org/10.1109/TMC.2012.29,

[26] McAfee: *Mobile Threat Report 2016*.
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2016.pdf, accessed 20th March 2018,

[27] Unuchek, R. and Chebyshev, V.: *Mobile Malware Evolution: 2013.*
https://securelist.com/mobile-malware-evolution-2013/58335, accessed 20th March 2018,

[28] Prodanovic, R. and Simic, D.: *Survey of Wireless Security.*
Journal of Computing and Information Technology **15**(3), 237-255, 2007,
http://dx.doi.org/10.2498/cit.1000877,

[29] Kataria, A.; Anjali, T. and Venkat, R.: *Quantifying Smartphone Vulnerabilities.*
In: Dutta, M.K.; Rai, J.K. and Padey, S., eds.: *Proceedings of the 2014 International Conference on Signal Processing and Integrated Networks*. IEEE, Noida, pp.645-649, 2014,
http://dx.doi.org/10.1109/SPIN.2014.6777033,

[30] Symantec: *2016 Internet Security Threat Report.*
https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf, accessed 20th March 2018,

[31] Anderson, R.J.: *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2nd ed.
Wiley Publishing Inc., Indiana, 2008,

[32] Hubbard, J.; Weimer, K. and Chen, Y.: *Study of SSL Proxy attacks on Android and iOS mobile applications.*
In: *Proceedings of the 2014 IEEE 11th Consumer Communications and Networking Conference*. IEEE, Las Vegas, 2014,
http://dx.doi.org/10.1109/CCNC.2014.6866553,

[33] Pore, A. and Bartere, M.: *A Review on Camera Based Attacks*.
International Journal of Computer Science and Technology **6**(1-1), 88-92, 2015,

[34] Bartere, M. and Pore, A.: *Preventions and Features of Camera Based Attacks on Smart Phones*.
International Journal of Emerging Trends and Technology in Computer Science **4**(4), 9-12, 2015,

[35] Keszthelyi, A. and Kadëna, E.: *Misunderstanding how Passwords Work*.
Volume of Management, Enterprise and Benchmarking in the 21st century III. Óbuda University, Keleti Faculty of Business and Management, Budapest, 2016.