Work in Progress: Can Johnny Encrypt E-Mails on Smartphones?

Katharina Schiller and Florian Adamsky

Institute of Information Systems (iisys)
Hof University of Applied Sciences
⟨firstname⟩.⟨lastname⟩@hof-university.de

Abstract. E-mail is nearly 50 years old and is still one of the most used communication protocols nowadays. However, it has no support for End-to-end encryption (E2EE) by default, which makes it inappropriate for sending sensitive information. This is why two e-mail encryption standards have been developed— namely, Secure/Multipurpose Internet Mail Extensions (S/MIME) and OpenPGP. Previous studies found that bad usability of encryption software can lead to software that is incorrectly used or not at all. Both consequences have a fatal impact on users' security and privacy. In recent years, the number of e-mails that are read and written on mobile devices has increased drastically. In this paper, we conduct to the best of our knowledge, the first usability study of e-mail encryption apps on smartphones. We tested two mobile apps, one uses OpenPGP on Android and one uses S/MIME on iOS. In our usability study, we tested both apps with eleven participants and evaluated the usability with the System Usability Scale (SUS) and the Short Version of User Experience Questionnaire (UEQ-S). Our study shows that both apps have several usability issues which partly led to unencrypted e-mails and participants sending their passphrase instead of their public key.

1 Introduction

As a saying goes, *there is life in the old dog yet* and this is particularly true for e-mail. Numerous articles, e.g. [3, 4, 9], have predicted the end of e-mail in the last years. It has been nearly 50 years [23] since the first e-mail was sent and it is still one of the most used communication medium nowadays with over 3.9 billion [7] users worldwide. Despite the increasing usage of social media, Instant Messaging (IM), and communication tools such as Slack and Microsoft Teams—the latter ones require a valid e-mail address—the worldwide e-mail usage continues to grow. According to a forecast from the Radicati Group [7], the number of e-mail users will increase by 3 % every year.

However, there is one major change in our e-mail usage: an increasing number of e-mails are read and written on mobile devices such as smartphones and tablets. According to a report from IBM [10], 49.1 % of all e-mails worldwide are read on mobile devices. In some regions, these numbers vary, e.g. in the United Kingdom and Ireland 62.9 %, and in Europe 38.6 % are read on mobile devices.

A big problem with e-mail is the lack of End-to-end encryption (E2EE) by default. To solve this problem, the two e-mail standards, Secure/Multipurpose Internet Mail Extensions (S/MIME) and OpenPGP [6], have been developed. To encrypt e-mails with one of those standards, additional software is needed. The research community conducted various usability studies [8, 18, 19, 24] of these encryption software and concluded that the bad usability is partly responsible why e-mail encryption is rarely used. Since nearly half of all e-mails are now read and written on mobile devices, how is the usability of encryption software on mobile devices? To the best of our knowledge, this paper provides the first usability study of e-mail encryption software on mobile devices. We selected two apps, one was on iOS using S/MIME and the second on Android with OpenPGP. We conducted our study with the following Research Questions (RQs) in mind:

RQ1 Are users able to encrypt e-mails with a smartphone without critical mistakes?
RQ2 Are the apps usable according to the usability questionnaires?

Our work makes the following contributions. We *(1)* conducted a usability study with eleven participants at a German university testing two mobile e-mail encryption apps; *(2)* evaluated the usability of both apps with the Short Version of User Experience Questionnaire (UEQ-S) [20] and the System Usability Scale (SUS) [15]; *(3)* show that both apps have several usability issues which resulted in sending unencrypted e-mails and accidentally sending the passphrase instead of the public key.

2 Related Work

An early usability study of e-mail encryption was conducted by Whitten and Tygar [24] about Pretty Good Privacy (PGP) 5.0 with 12 participants. Four of them fulfilled the given sign and encryption tasks correctly, the others failed.

PGP has undergone major changes in the upcoming years, including usability issues. Eight years after their first study, Sheng et al. [22] did another research at the current at that time version of PGP 9 with even worse results. None of the participants was able to complete the tasks to verify keys and sign or encrypt an e-mail, although there have been improvements through automatic encryption.

Other approaches to the topic followed. One of them is Private Webmail (Pwm), a tool that integrates into existing webmail services and provides encryption functions as an overlay and supports automatic key management and encryption. In their study, Ruoti et al. [16] compared Pwm with a standalone tool that required manual interaction with ciphertext and discovered that for that reason users trust the standalone tool more.

In another study Ruoti et al. [17] compared two revised versions of Pwm in an A/B testing scenario regarding their level of automation to discover the impact on the understanding of encryption processes and how it helps users to avoid mistakes. Both versions received a SUS score of around 80 that is known as the highest score for secure e-mail tools at this time. The results show that automatic

encryption or manual encryption does not affect how well users understand the process.

Atwater et al. [1] checked in their study three tools on their trustworthiness, according to the level of transparency of encryption processes and the level of integration. They found that especially integrated tools can provide good usability and the majority had no preferences according to the trustworthiness, even though some of them thought standalone tools are more secure since they are an "offline" tool installed locally on their device.

Nevertheless, the existing solutions are still not widely adopted. Another research from 2015 [19] regarding one of the integrated PGP tools from the previous study shows again a poor usability by testing it with groups of participants. It shows that after decades of studies and improvement, PGP is still not user-friendly enough to be used by the masses. Ruoti et al. [18] conducted another study on three different secure e-mail tools including Pwm with pairs of acquainted participants. Their conclusions are similar to previous studies, adding that both participants acted more naturally, because they were novice and familiar with each other.

However, we did not found studies that cover e-mail encryption software on mobile devices.

3 Background

In this section, we provide a brief overview of the two encryption standards OpenPGP and S/MIME.

OpenPGP is according to the website[1] the most widely used e-mail encryption standard and is defined by the OpenPGP Working Group in RFC 4880 [6]. It is based on PGP version 5 encryption concept developed by Phil Zimmermann [13]. In OpenPGP there is no central trust entity, instead it is based on a web of trust in which participants sign keys of each other and therefore verify their identity. The public keys are often on keyservers and can easily be retrieved by other participants. Public keys also serve as a signature which also confirms the authenticity of the e-mail. The signature can be checked by comparing hash values.

S/MIME has, in comparison to OpenPGP, a central trust entity called Certification Authority (CA). One generates a public key and the CA signs the public keys and generates a certificate. The certificates are assigned to different classes and sometimes cost money. Free certificates have to be checked again after a certain period. There is no key server on which the public keys are located, so users have to request them by letting the contact send a signed e-mail. This signed e-mail contains the public key and simultaneously confirms authenticity.

[1] `https://www.openpgp.org/`

4 Study Methods

In this section, we describe our usability study method in detail.

4.1 App Selection

We intended to test OpenPGP and S/MIME on iOS and Android. To make a selection of which apps should be tested, 18 apps were investigated, 6 from the iOS AppStore, 10 from the Android PlayStore and 2 for both. According to studies [22, 24], users prefer to use their existing e-mail account. Therefore, we excluded all apps that require the creation of a new account, only offer secure communication with other users of the same app, or are not free. It turned out that none of the PGP apps for iPhone worked without errors on the test device iPhone 6s with iOS 13, and no S/MIME app on the Android device Samsung Galaxy S7 Edge.

iOS Mail App is the standard e-mail app for the iPhone and supports only S/MIME. It can be enabled in the settings menu. However, a certificate in the Public-Key Cryptography Standards (PKCS) #12 format is required. This certificate must then be installed and activated for the respective e-mail account. In preparation, we applied for the certificate, changed the format from CER to PKCS #12 format, and transferred it to the iPhone with a cable. The participants would take too long for this process and a computer is required.

FlowCrypt is a third-party app that supports OpenPGP and was selected for Android. The number of installations is according to the PlayStore over 10,000 [14]. FlowCrypt[2] is also available for GMail as a browser extension for Firefox and Chrome. At the time of the study, an app for iOS was in an early testing and evaluation phase but was not available on the app store. To use the app, the user has to login with an existing e-mail address. The app automatically generates a key pair and publishes the public key on a keyserver. After setting up a new account FlowCrypt sends a backup of the private key via e-mail, protected with the used passphrase, and a first encrypted e-mail, that informs about the app and explains basic elements.

4.2 Overview of our Usability Study

The usability tests were carried out at our university of applied sciences in Germany in January 2020. For this reason, all questionnaires, task sheets, and interviews were in German. The smartphones used for the study are an iPhone 6s with iOS 13 and a Samsung Galaxy S7 Edge with Android Version 8. We did not observe any negative influences in our study from the Operating System (OS), although the smartphones were not the latest models. We configured the devices such that only the relevant apps could be found on the start screen. The

[2] `https://flowcrypt.com/`

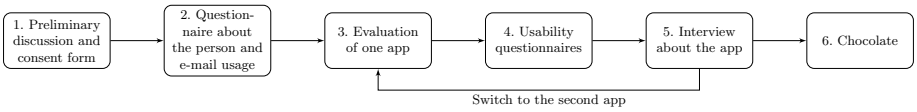


Fig. 1: Procedure model for our usability study for every participant.

participants used an prepared Gmail account for this study and did not have to enter any private data. We planned a time frame of 45 min to 60 min per attendee. An overview of the procedure model we used is presented in Figure 1.

Participants and Pre-Questionnaire. We asked in university courses for participants and contacted some others directly. Eleven volunteers participated in our study, of which seven were males and four females. The majority with seven participants was between 21–30 years old. Two participants were in the age group 31–40, and two were over 60 years old. Seven out of eleven participants work in IT, including six students. The other four participants had no former background in IT. Two of them were students of business law.

After a short introduction, the participants were told that they want to communicate with a friend John Doe about something private and therefore have to encrypt their e-mails. The participants used the e-mail address from Max Anderson. Both, the given e-mail address, including password, and the e-mail address of the contact was specified on the task sheets so that no one had to use private accounts.

Furthermore, the pre-questionnaires include questions about their smartphone usage and general questions about e-mail and encryption. The majority which includes 64 % of the participants write an e-mail with their smartphone once per month. In these e-mails, 82 % considered the content-sensitive. Surprisingly, it is important for all participants that strangers cannot read their e-mails. However, 82 % of all participants had already heard that e-mails can be encrypted, but only one of them encrypts e-mails or has done it in the past with PGP.

Usability Tests. In our usability study, we used the thinking-aloud method [11]. The tasks for both apps include subtasks for checking key management, sending encrypted e-mails, and how participants recognize encrypted e-mails because previous studies [1, 8, 19, 24] have rated these tasks as prone to problems. We decided to include the set-up processes in the usability test by giving the participants clear instructions on the required settings.

Six participants started with the iOS Mail app and five with FlowCrypt on the Android smartphone. All responses from the e-mail contact were prepared and sent by the study coordinator during the test. The usability test for the iOS Mail app first asks participants to add a new account in the settings with the given credentials and enable S/MIME in the settings menu.

After that, they should open the Mail app and read a signed e-mail from the contact, which tells them that there is a key included. At this point, they should discover and install the sender's public key, because in the next step they are prompted to send an encrypted e-mail back to the sender. If the participants skipped this task, the app shows a warning dialog that the e-mail they want to send to the contact is not encrypted. However, they could skip this warning as well and send the e-mail unencrypted. In the last subtask, the participants received a reply from the contact and they should recognize that this e-mail is encrypted.

With FlowCrypt, the participants first had to set up the app with the given e-mail address and a given passphrase. In the next step, they had to send an e-mail to the given recipient and attach their public key.

If they did this incorrectly, they received an auto-generated e-mail from FlowCrypt that gave them further instructions and helped to send the correct key to the recipient. Finally, the participants received a reply and must recognized that it is encrypted.

Usability Questionnaires. After the test, the participants immediately filled out two usability questionnaires. We decided to use the SUS [5] to compare the results with other studies [1, 16–19]. Additionally, we use the UEQ-S [21], which includes hedonic quality. Since we conducted the usability study in German, we used the translated version for SUS from the SAP User Experience Community [15] and replaced the term *system* with *app*. For UEQ-S we used the translation from the official website [20]. All answers from the questionnaires were given in the form of a Likert scale [12].

Interview. The interview finalised the usability test and the questionnaires. Both apps contained query dialogues about key management. Key management was part of a subtask, however, the question is whether the participants understood why they need to do this.

Regarding the iOS Mail App, we asked questions about the certificate and whether the participants would request one and if so, how much they would be willing to pay. Furthermore, we asked the participants what they would improve, if they would use the apps. If they did not mention the aspects we noticed during the usability test, we tried to refer to this and in most cases received explanations of things that the participants were not aware of.

5 Evaluation of the Usability Study

This section shows the results for the iOS mail app and then the results for FlowCrypt. We itemise the results by first showing the results of SUS and UEQ-S, then the observational results of the usability tests and finally the results of the interview.

5.1 Results for iOS Mail App

Usability. The average SUS score for the iOS Mail App is 42.04, which is rated between *poor* and *ok* on the Bangor's scale [2]. For better comparison, we marked this value on more a human-readable scale in Figure 3. On the acceptability scale from Figure 3, it is classified as not acceptable. Figure 2a shows the result for the UEQ-S. The chart shows the individual mean values for *Pragmatic Quality* with -0.57, *Hedonic Quality* with 0.25, and the *Overall* result -0.16. All results are classified as *bad* that can be interpreted as in the range of the 25 % worst results.

Observational Results. The first general problem we noticed was during enabling S/MIME. Nine out of the eleven participants forgot to confirm the settings for S/MIME, due to the placement of the finish button on the previous view and they switched directly to the e-mail app using the home button. The study coordinator informed the participants about this mistake, since otherwise the encryption function would not work. In general, many participants complained about the setup process. For instance, one of them said: "*To set everything up, I think I would need someone who already uses the app.*"

While all participants successfully opened the Mail app and read the received e-mail, the next problems occurred during writing an encrypted e-mail. Eight participants had difficulties finding the public key of the recipient. Two of these participants sent an unencrypted e-mail and ignored the warning dialog. One of them thought the open lock means the e-mail is encrypted. Through a hint, they found the certificate with the public key and installed it. The e-mail encryption itself takes place automatically and was no problem for the participants.

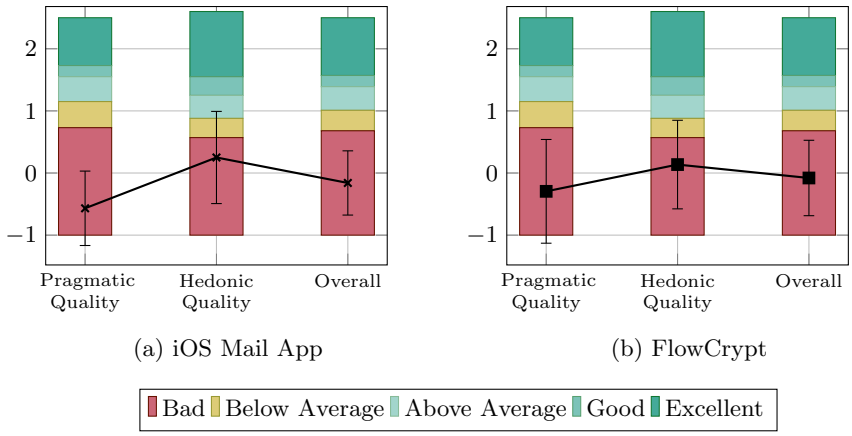
The last task asked to explain how to recognize that the e-mail is encrypted. Ten participants correctly identified the lock icon next to the sender's e-mail address as a sign for an encrypted e-mail. One of them additionally selected the e-mail address and received more information about the certificate, including the encryption status.

Interview Results. In the interview, seven participants could describe the encryption process, because they already had previous knowledge due to their employment. The other participants suspected that the installation of the certificate had something to do with the encryption process. One of them mentioned: "*I couldn't send an encrypted e-mail before I installed the certificate, so I think it's for the encryption process*". Some participants assumed the public key was a normal e-mail attachment, but it was hidden behind the sender's e-mail address. They suggested to show the certificate in a more obvious way or show a pop-up message, if an e-mail is signed and the certificate is not installed yet. All participants were sure that the certificate with the private key should not be transferred to the smartphone by sending an unencrypted email.

With eight participants, the majority would not request a certificate for private reasons. The rest could imagine doing it, if there is a reason to do so.

One of them said: "*I don't think someone is interested in my private e-mails*". Therefore, only two participants could imagine paying for a certificate.

Five participants answered yes to the question of whether they would use the app, while two did not answer, and one participant could imagine using it for business purposes only. One participant mentioned: "*The biggest problem would be to find a recipient that uses encryption as well.*"



(a) iOS Mail App (b) FlowCrypt

Fig. 2: UEQ-S results for the iOS Mail App (a) and the Android App FlowCrypt (b) with the mean values for Pragmatic Quality, Hedonic Quality, and the Overall Result. The error bars show the confidence intervals ($p = 0.05$) per scale with $N = 11$.

5.2 Results for Android App FlowCrypt

Usability. The app reached an average SUS score of 53.41. On the Bangor's scale, this is rated between *ok* and *good* and *Marginal Low* on the acceptability scale. Again, for better comparison, we marked this value on a more human-readable scale in Figure 3. The average *Overall* result of the UEQ-S is −0.08, with a *Pragmatic Quality* of −0.29 and a *Hedonic Quality* of 0.14, which can be seen in Figure 2b. All results are in the area *bad*.

Observational Results. During the setup process, we could not notice special occurrences, with the exception of a few typing errors in the passphrase that prevented the sign in. The study coordinator informed the participants if they did not notice the mistake themselves. In general, one participant described the setup as *nice and simple*. After the participants had access to the account, only one opened the information e-mail from FlowCrypt. The remaining participants ignored this e-mail or did not notice it.

For the first task, the participants had to send an encrypted e-mail with their public key attached. Seven participants performed this task correctly. One of them was still unsure, if the sent e-mail was encrypted because it was not necessary to select this as an option. Although the app shows a caption that the e-mail is encrypted, he or she did not recognize this. Out of the remaining participants, three did not find the key. One of them thought the passphrase is the public key and sent it in an encrypted e-mail to the contact. Another participant suspected the app always automatically attaches the public key to an e-mail and therefore did not attach it manually.

In all these cases, the participants received an e-mail with instructions from the app on how to proceed. All of them could follow these instructions and correctly sent the public key to the contact.

Similar to the iPhone app, the last task asks the participants to explain how they can tell whether an e-mail is encrypted. Eight participants correctly identified an encrypted e-mail based on the background or the colour scheme. One participant thought that an e-mail is only encrypted, if a key is attached and another one suspected that the word *encryption* that was in the recipient's e-mail address meant the e-mail is encrypted.

Interview Results. All seven participants working in the IT sector could describe the encryption process and understood why they needed to send the public key to the recipient. The remaining participants were unsure about it. One said: "*It's not secure to send the [public] key in the attachment.*" The question of whether they would use FlowCrypt was answered by two with yes, seven with no and one did not give an answer. One who answered with no explained: "*The app should visually look more like an e-mail app. [...] it's a mixture of e-mail app and messenger app.*" Another participant explained that he or she would only use it for business purposes but not for private ones.

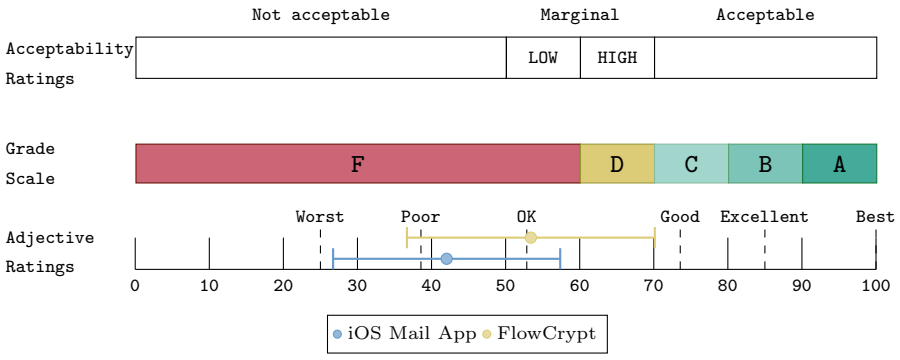


Fig. 3: The Bangor's Scale associates the SUS Scale with more human-readable scales based on [2]. The error bars show the confidence intervals ($p = 0.05$) per scale with $N = 11$.

6 Discussion and Comparison of our Results

Based on the evaluation of the usability tests, we can clarify RQ1 and RQ2 raised in Section 1. Regarding RQ1, we come to the conclusion that in our tests the participants were not able to encrypt e-mails on smartphones without critical mistakes. Most participants had difficulty sending an encrypted e-mail using the iOS Mail App. Despite a warning, some sent an unencrypted e-mail because they did not know how to proceed and could not find a solution on their own. Furthermore, participants mentioned that they would have problems to find the correct settings to activate S/MIME without help. FlowCrypt automatically encrypts e-mails, therefore less participants had difficulties with this task. The problem with this app is that the encryption process is too opaque. If users had to take care of key management, this led to a very critical mistake in one case, where the participant sent the passphrase as the public key.

Regarding RQ2, both apps are not usable according to the usability questionnaires. Even if the SUS scale for FlowCrypt is slightly over the *OK* area, the results of the UEQ-S are in the area *bad* on the benchmark chart. Apart from the usability questionnaires, more participants answered that they could imagine using the iOS Mail App for private purposes. Several participants mentioned that the setup process is too cumbersome, which could lead to a lower rate on both usability questionnaires, although the usability of the actual encryption and decryption process may be suitable.

7 Conclusion and Future Work

In this study, we analysed two e-mail encryption apps on smartphones according to the usability of their provided encryption functions, to detect if they are usable without critical mistakes. Since nearly half of all e-mails are read on mobile devices and other communication methods like messenger apps use E2EE by default, it was questionable why e-mail encryption on smartphones is not widespread. This study with eleven participants showed according to the usability questionnaires similar results as previous studies on desktop tools and indicated several usability issues. Many participants criticised a complex setup process for S/MIME and declared that they see no requirement to request a certificate for private purposes. Another problem was the participants' lack of understanding for key management, where especially S/MIME requires basic knowledge and the iOS Mail App needed manual user intervention. The results of the Android app FlowCrypt showed that too opaque handling of encryption leads to uncertainty amongst some participants because they were not sure if e-mails were encrypted.

In future work, we would like to repeat our study with more participants who better reflect the general public and have less technical background. Since the devices we used for our study were not recent ones, we would like to use current devices and use more email encryption apps, including paid apps to make more generic conclusions. We are also planning to let the participants

request certificates themselves, transfer them to the smartphone and set them up independently. Another point should be the cross-use of email encryption on mobile devices and desktop devices. We want to check whether it is possible to read encrypted e-mails and to send encrypted e-mails on all devices used, in order to prevent that users can read the same encrypted message on the smartphone but not on the computer.

Acknowledgements. We thank Zinaida Benenson for the discussion and comments that greatly improved the manuscript.

References

[1] Erinn Atwater et al. "Leading Johnny to Water: Designing for Usability and Trust". In: *Proceedings of the 11th Symposium On Usable Privacy and Security (SOUPS)*. 2015, p. 20. DOI: 10.5555/3235866.3235873.

[2] Aaron Bangor, Philip Kortum, and James Miller. "Determining What Individual SUS Scores Mean: Adding an Adjective Rating Scale". In: *Journal of Usability Studies* 4.3 (2009), p. 10.

[3] John Brandon. *It's 2018 and Email is Already Dead. Here's Who Zapped It Into Extinction*. 2018. URL: https://www.inc.com/john-brandon/its-2018-email-is-already-dead-heres-who-zapped-it-into-extinction.html (visited on 07/19/2021).

[4] John Brandon. *Why Email Will Be Obsolete by 2020*. Library Catalog: www.inc.com Section: Vision 2020. 2015. URL: https://www.inc.com/john-brandon/why-email-will-be-obsolete-by-2020.html (visited on 05/20/2020).

[5] John Brooke. *SUS – A Quick and Dirty Usability Scale*. Tech. rep. 1996, p. 7.

[6] J. Callas et al. *OpenPGP Message Format*. RFC 4880. RFC Editor, Nov. 2007. URL: http://www.rfc-editor.org/rfc/rfc4880.txt.

[7] *Email Statistics Report, 2019–2023*. Tech. rep. The Radicati Group, Inc., 2019. URL: https://www.radicati.com/wp/wp-content/uploads/2018/12/Email-Statistics-Report-2019-2023-Executive-Summary.pdf (visited on 05/20/2020).

[8] Simson L. Garfinkel. "Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express". In: *Proceedings of the 1st Symposium On Usable Privacy and Security (SOUPS)*. 2005, pp. 13–24.

[9] Todd Haselton. *Personal email is dead — but I still can't quit it*. 2018. URL: https://www.cnbc.com/2018/05/16/personal-email-is-dead--but-i-still-cant-quit-it.html (visited on 07/19/2021).

[10] IBM Watson Marketing. *Marketing Benchmark Report: Email and Mobile Metrics for Smarter Marketing*. 2018. URL: https://www.ibm.com/downloads/cas/L2VNQYQ0 (visited on 04/29/2020).

[11] Clayton Lewis. *Using the "Thinking-aloud" Method in Cognitive Interface Design*. Tech. rep. IBM Thomas J. Watson Research Center, Feb. 1982, p. 6. (Visited on 05/24/2020).

[12] Rensis Likert. “A Technique for the Measurement of Attitudes”. In: *Archives of Psychology* 22 (1932). URL: https://legacy.voteview.com/pdf/Likert_1932.pdf (visited on 05/29/2020).

[13] Hilarie Orman. *Encrypted Email: The History and Technology of Message Privacy*. SpringerBriefs in Computer Science. Springer International Publishing, 2015. ISBN: 978-3-319-21343-9. DOI: 10.1007/978-3-319-21344-6.

[14] *PlayStore: FlowCrypt: Encrypted Email with PGP*. 2018. URL: https://play.google.com/store/apps/details?id=com.flowcrypt.email (visited on 07/13/2020).

[15] Bernard Rummel. *System Usability Scale – jetzt auch auf Deutsch*. 2015. URL: https://experience.sap.com/skillup/system-usability-scale-jetzt-auch-auf-deutsch/ (visited on 05/29/2020).

[16] Scott Ruoti et al. “Confused Johnny: When Automatic Encryption Leads to Confusion and Mistakes”. In: *Proceedings of the 9th Symposium on Usable Privacy and Security (SOUPS)*. 2013. DOI: 10.1145/2501604.2501609. (Visited on 05/01/2020).

[17] Scott Ruoti et al. “Private Webmail 2.0: Simple and Easy-to-Use Secure Email”. In: *Proceedings of the 29th Annual Symposium on User Interface Software and Technology. 2016.“* Oct. 2016. DOI: 10.1145/2984511.2984580.

[18] Scott Ruoti et al. “We’re on the Same Page: A Usability Study of Secure Email Using Pairs of Novice Users”. In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI 16)*. 2016. DOI: 10.1145/2858036.2858400.

[19] Scott Ruoti et al. “Why Johnny Still, Still Can’t Encrypt: Evaluating the Usability of a Modern PGP Client”. In: (2015). arXiv: 1510.08555 [cs.CR].

[20] Martin Schrepp. *UEQ - User Experience Questionnaire*. 2018. URL: https://www.ueq-online.org/ (visited on 05/29/2020).

[21] Martin Schrepp, Andreas Hinderks, and Jörg Thomaschewski. “Design and Evaluation of a Short Version of the User Experience Questionnaire (UEQ-S)”. In: *International Journal of Interactive Multimedia and Artificial Intelligence* 4 (Jan. 2017), p. 103. DOI: 10.9781/ijimai.2017.09.001.

[22] Steve Sheng et al. “Why Johnny Still Can’t Encrypt: Evaluating the Usability of Email Encryption Software”. In: *In 2006 Symposium On Usable Privacy and Security - Poster Session*. 2006.

[23] Ray Tomlinson. *The First Email*. URL: http://openmap.bbn.com/~tomlinso/ray/firstemailframe.html (visited on 06/04/2020).

[24] Alma Whitten and J. D. Tygar. “Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0”. In: *In Proceedings of the 8th USENIX Security Symposium*. 1999.