Vision: Shred If Insecure – Persuasive Message Design as a Lesson and Alternative to Previous Approaches to Usable Secure Email Interfaces

Jan Tolsdorf
Data and Application Security Group
TH Köln - University of Applied Sciences
Cologne, Germany
jan.tolsdorf@th-koeln.de

Luigi Lo Iacono
Data and Application Security Group
Hochschule Bonn-Rhein-Sieg
Bonn, Germany
luigi.lo_iacono@h-brs.de

***Abstract*—Despite the advances in research on usable secure email, the majority of mail user agents found in practice still violates best practices in UI design and uses ineffective and inhomogeneous design strategies to communicate and let users control the security status of an email message.**

We propose a novel interaction and design concept that we refer to as persuasive message design. Our approach is derived from heuristics and a systematic meta-study of existing HCI literature on email management, usable secure email and phishing research. Concluding on this body of knowledge we propose the design of interfaces that suppresses weak cues and instead manipulates the display of emails according to their technical security level. Persuasive message design addresses several shortcomings of current secure email user interfaces and provides a consistent user experience that can be deployed even by email providers.

***Index Terms*—usable secure email, user interface design**

1. Introduction

Email, still one of the largest text messaging systems on the internet with about 3.8 billion users, is characterised by its simplicity, efficiency and universal accessibility, but also by the lack of security: the email ecosystem is vulnerable to mass surveillance and emails are often a gateway for malicious software and targeted phishing attacks [1], [2]. While technical measures such as end-to-end (E2E) email encryption provide remedies, their widespread implementation has often failed due to poor usability of tools and support from providers [1], [3], [4]. Fortunately, providers have adopted new protocol extensions and even started to promote native support of E2E email encryption recently to guarantee users more security and privacy. However, existing user interfaces (UIs) do not sufficiently represent the cryptographic properties of email communication for ordinary users and remain ineffective when it comes to sending secure emails or protecting users from frequent hazards when receiving emails [2], [5]. In addition, cryptographic mechanisms are often available exclusively in providers proprietary mail user agents (MUAs), which means that numerous users of default MUAs from operating systems and third parties can hardly benefit from this development.

In line with the 20-year-old but still valid demand to make secure email usable [3], [5], we advocate that secure email should be considered holistic and that the results of research on E2E encrypted email and phishing provide an opportunity to develop more intuitive UI concepts that can solve existing problems and allow an easy deployment of secure email. We plead for a rethinking of the current UI design that takes into account the lessons learned from the various disciplines of HCI research on E2E email security, email phishing, email use and warning design. In particular, we emphasise the use of negative security indicators as the more natural and easily perceived alternative to current design strategies. We argue that users should not be forced to rely on symbolic and commonly misplaced security indicators and that UIs must relieve them of the mental burden of processing emails. To achieve this, we suggest the altering of the presentation and display of emails according to the actual security status in order for users to intuitively perceive its trustworthiness. We also aim to seamlessly integrate security decisions into the email composing process, as proposed by some vendors.

The rest of this work is structured as follows: First, we provide a brief overview of the research status of secure email, with a particular focus on usability. Second, we summarise and present challenges for usable secure email solutions based on related work. Third, we introduce the idea of *persuasive message design* and highlight its potential to solve existing problems. Last but not least, we conclude our ongoing work and give an outlook on the intended upcoming research activities.

2. Background

Attempts towards secure email. To address the lack of security in email communication, a number of approaches to E2E secure email solutions have been introduced early on, but their implementation failed due to usability issues [3]. In particular, the implementation of usable yet secure key management in a heterogeneous environment such as email was one of the key challenges and resulted in numerous further investigations; research aimed at reducing the complexity of key management [6]–[8] and the creation of tools that allow technical lay users an easy setup [9], [10]. The results indicate that tools can be made user-friendly with very different approaches such as using public key directories, identity based encryption or even passwords [11]. Recently, providers themselves have started to provide E2E email encryption to their users along with the necessary infrastructure, and thus variants of the above mentioned solutions are already being used,

either in closed ecosystems (e.g. Tutanota, Virtrue), in open but proprietary solutions (e.g. Google End-to-End) or in open and standardised solutions (e.g. Web Key Directory). In general, however, the usability of secure email tools was examined primarily in terms of initial setup and basic functionality, but not in terms of their daily use [5]. Their practical value, in particular with regard to the basic requirements of users to verify and guarantee the authenticity of the sender, remains questionable [12]. Providers in turn have pushed the implementation of standardised security mechanisms with particular attention to sender authentication in recent years but often independent from E2E secure email [1]. Unlike the web browsing domain, however, the use of security mechanisms by email providers has since been hidden from users who have not been able nor eager to verify connection security or sender authenticity. Yet, a rethinking has been taking place and email providers have started to display security indicators in the UI for both incoming and outgoing emails [2]. Examination of these measures has shown, however, that indicators often have a customary and inhomogeneous design between different operators and do not respect the best practices of previous research on metaphors and warning design [2]. Current choice and display of security indicators is often ineffective in protecting users from widespread attacks such as email spoofing [2], [13].

Characteristics for usable secure email. Attempts to identify characteristics that serve for the heuristic evaluation of tools have an enormous focus on key management [1], [14], [15]. Available heuristics divide into aspects of security, deployability, and usability. In the case of the latter, the features range mainly from simple set-up, effortless operation, free use, hidden or easy trust decisions, to the use of appropriate metaphors.

Our work contributes to existing literature as we summarise and complement additional features and challenges that should be considered in the evaluation and design of secure email solutions in addition to key management.

3. Challenges in the Design of Interfaces

In the following we present problems related to the design of usable secure email UIs that emerge from existing work and that we consider essential for future solutions.

3.1. Prerequisites for usable secure email tools

Security is a minor selection criterion. Investigations on the properties that are involved in users' decision making processes on choosing a communication tool found that users primarily consider the distribution and accessibility, as well as the feature set of tools, whereas security is a secondary objective [16], [17]. Especially MUAs have extensive features nowadays, making it unlikely that security features alone will induce users to change their familiar email environments or create new accounts [1], [3], [18], [19]. UI concepts should therefore work independently of tools in order to make them available to users in their existing environments.

Seamless integration into existing environments. Users prefer secure email tools that integrate seamlessly into their existing environments and do not force them to create additional accounts or abandon their workspace to perform security tasks [10], [19], [20]. Yet, integrated tools do not necessarily offer higher usability or security and their UIs often still rely on user interaction design strategies that require a deep understanding of the underlying encryption mechanisms [3], [9]. We conclude that "integrated solutions" should also make the aspects of secure email more profound and intuitive.

Usable key management. While the design of secure and usable key management remains a central research topic on usable secure email [5], users are often satisfied with solutions that can not guarantee protection from attacks by their own email providers, but involve little or no self-initiative [21]. Users generally trust their email providers to stay honest and even accept provider scans of their emails in exchange for features like free accounts, SPAM and virus detection [21], [22]. Since trust is often sufficient to ensure the security needs of the users, key directories managed by the providers might represent a possible solution for large-scale email encryption, which is why we ignore key management for the design of UIs in the following.

3.2. Challenges in controlling secure email

Ability to control the security status. Automation of key management and encryption purposes is known to enhance usability and mitigate errors [10], [20]. However, while users welcome automatic key management [21], permanently enabled and automatically processed email encryption does not meet user expectations for the purpose of secure email. While users gladly try to maintain the level of security that the sender has requested, permanent encryption is seen as paranoia [23]. Also, users do not want to burden the recipient with decrypting all incoming emails and find it stressful to turn off encryption regularly themselves. Also the practical issue of (temporarily) *unreadable email*[1] for recipients in non-cryptographic environments (e.g. mobile) requires the presence of controls over the encryption status in the sender's UI.

Prevention of fatal user errors. Previous examinations of cognitive and physical tasks that users must perform to send a secure email in widely deployed tools revealed that modern solutions require the cognitive task of opting for secure email, either (1) before composing a message (e.g. "write secure email") or (2) after composing and just before sending (e.g. toggle padlock, "send secure") [24]. Contrary to best practices, the path of least resistance is often not the most secure and tools require explicit activation of secure email. Consequently, users have been found to frequently forget to enable secure email, even if they were explicitly asked to enable encryption (10% [20], 17% [25], 25% [3] 100% [26]). Moreover, tools that do not satisfy the *integrated tool* property and operate outside the UI were found to be particularly susceptible for usability errors [26].

Avoidance of opaque security. Highly transparent and automated security lowers the perceived trustworthiness as well as the perceived security of a system and can cause application errors [20], [26]. In this regard, one coined the term *opaque security* to describe the property of a system that does not allow its users to determine whether

1. https://autocrypt.org/

security is actually turned on. Users demand feedback on the applied security mechanisms, though it is not yet solved what kind of feedback serves best. While some work proposed the visualisation of encrypted data to be helpful in conveying a system's status to users [19], [20], other researchers found that basic confirmation messages or notification dialogues are already sufficient to foster users' beliefs in a tool's security [10].

3.3. Challenges in understanding secure email

Ability to recognise the security status. The security status of a message is often ambiguous and the interpretation of digital signatures and encryption is subject to a community debate that divides on the meaning of errors and how this information can be made available to lay users[2]. Research on E2E secure email focused primarily on the usability of sending encrypted emails, but largely ignored the issue of recognising the security status of a message. A few exceptions are theoretical considerations and the claim to supply only passive feedback to not disrupt users [6], [27]. Although passive warnings violate proven best practices in usability design [28], they have made their way into implementing secure E2E email tools[3] and are used by providers to alert their users of phishing emails [2]. Numerous investigations however have confirmed passive warnings' ineffectiveness in communicating the security status of emails effectively and fail to encourage users to behave securely [2], [6], [29]. Some theoretical approaches argue for the exchange of accuracy in favour of comprehensibility, suggesting to distinguish only between unsafe, secure and corrupt messages [27].

Use of metaphors. Research has repeatedly confirmed that lay users understand basic concepts of symmetric cryptography [30]–[32], but struggle to find adequate metaphors for cryptographic signatures [33]. While metaphors are useful in explaining email security concepts to study participants, metaphors lose their meaning over time and provide little or no support to users in making security decisions under real-world conditions [33]. While research confirmed the usefulness of paper mail metaphors to distinguish between unsafe, secure and corrupt messages [34], factual tools and email operators often make use of the padlock metaphor that is known to be well understood by lay users but is criticised to be unspecific and meaningless to the email context [31], [34]. Thus, the current use of metaphors may be inappropriate to convey the security status of emails adequately.

Use of security indicators. Security indicators always face the challenge of balancing between options to highlight either the presence or absence of security. The former can be achieved by using positive security indicators to confirm that security is present, while the latter can be achieved by emphasising the absence of security with negative security indicators. In line with the discussion on the security status of a message, tools from the E2E secure email community primarily use positive security indicators using text and icons to underscore the secure status of a message[4]. Recently, however, many MUAs were found to be vulnerable to UI dressing attacks because they violated the *identifiability* principle and placed positive security indicators in email's body display area [13]. Despite the wide use of positive indicators in practice, their usefulness is highly questionable in terms of the protection they actually provide to users. Studies on online phishing have repeatedly confirmed that users often do not consciously perceive or notice the absence of such indicators and that lay users' sense of security is instead strongly influenced by the appearance of the content [28], [35], [36]. Yet, even the current use of negative security indicators by email operators in the form of text banners positioned in the body of emails that warn users against phishing emails were also found to be ineffective to protect users [2].

3.4. Challenges for a human centred design

Limited and incorrect mental models. Email users were found to have some profound misunderstandings of the underlying architecture, the message flow and the security properties [17], [22], [30]. Consequently, users are still far from understanding threat models and privacy implications that result from unsecured email transmissions, but are somehow concerned about becoming a victim to eavesdropping attacks [22]. In this regard one found that users' mental models of communication channels' security properties are biased by the physiological perception (e.g. ephemerality of the spoken word) and their very own use habits [22], [30], [31]. For example, users prefer email over mobile IM services if they have to send confidential information over the internet, probably just because email has been and is still being used for all kinds of correspondence that is associated with formal and therefore trustworthy communication [17], [30], [32]. In addition, email users have been found to perceive different levels of security for different email operators; in particular, linkages to monetary costs influence user perceptions of security, as paid or organisational email accounts have a higher reputation and are perceived to be more secure than publicly available and free accounts [30].

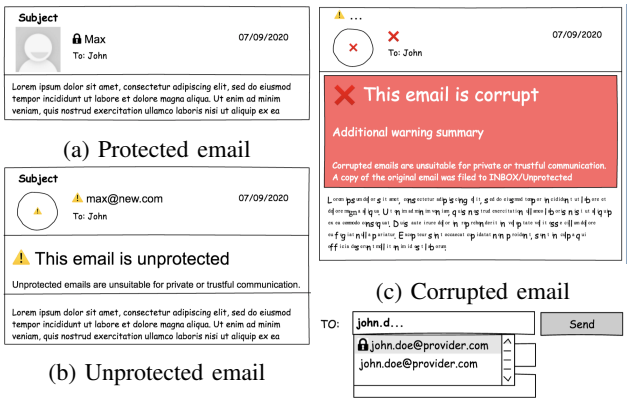
Email handling strategies and mental load. Research coined the term *email overload* [37] that describes the feeling of being overwhelmed by the constant flow of emails [38]. Concerning the latter, research in the HCI domain explored users' overall information management in search for usability improvements of existing MUA software and finally resulted in a formal description of the email workflow [39], [40]. Generally, users apply handling strategies that usually employ the minimisation of disruption to the primary (work) task. Next to other interrelated activities, the continuous handling of incoming messages, also known as *flow*, is one of the most important activities within the email workflow. It includes the action of regularly *glancing* at the inbox to decide on the priority of incoming messages and whether a context switch from the main task to the processing of emails is necessary. The glance is then followed by the *scan*, a technique used to examine messages in the inbox in greater detail. It is the result of either a context switch after performing glances or a conscious decision to terminate the primary task and process emails. Consequently, MUAs that implement secure email must supply cues that support users in their flow activity and enable them to deduce the

2. https://k9mail.app/2016/11/24/OpenPGP-Considerations-Part-I, https://dkg.fifthhorseman.net/blog/e-mail-cryptography.html

3. E.g. Gpg2win https://wiki.gnupg.org/EasyGpg2016/OutlookUi

4. https://wiki.gnupg.org/EasyGpg2016/OutlookUi

priority of incoming messages within small time intervals and little cognitive effort. Tools that restrict users from executing the flow generate a high mental load and run the risk of users getting lost in the flood of emails they receive [39]. Possible consequences are discomfort and stress, because people's email management activities are driven by anxiety to miss out on important information and the fear to lose control in the event of receiving high volumes of messages [41]. As a result, the pure handling of emails can be perceived as being time consuming and stressful, primarily springing from social norms and a pressure to quickly respond to emails or stay up-to-date. Implementation of current solutions for secure email, in particular for E2E encryption, has generally been designed to send emails securely while ignoring everyday efficiency [5]. Instead, the required level of interaction often requires enormous changes in the context, which are likely to be perceived as disruptive and not in line with the flow.



(a) Protected email

(b) Unprotected email

(c) Corrupted email

(d) Security controls integrated in the composing process

Figure 1: Persuasive Message Design

4. Future UIs for Usable Secure Email

The problems and challenges for usable secure email outlined above reflect the fact that research has already identified many problem areas, but the proposed solutions are by nature specific. Frequently, only individual partial aspects such as installation, key management, sending and decryption of received emails have been considered. We believe that the goal of making email more secure in everyday life, whether for private or professional use, could benefit from integrating the results into a holistic concept. In particular, the email handling strategies used by email users have often not been considered when designing secure email tools and conflict with fundamental aspects of email workflow or best practices in designing effective warnings. Future developments of UIs should pay particular attention to the following aspects:

- Users should not be required to switch tools for enhanced secure email UIs.
- Tools for secure email should not simply automate encryption, but offer control capabilities that integrate seamlessly into user workflows.
- UIs should not rely solely on the use of metaphors and security indicators to represent the security status of a message and in particular should complement the use of positive indicators with the use of negative indicators.
- UIs should not foster false mental models.
- UIs should enable users to still rely on heuristic processing of email because email management is complex and tedious.

We advocate combining the accumulated knowledge from phishing research with the enormous progress made in E2E secure email research to create a holistic solution, seamlessly integrating the steps of E2E security into the normal composing of messages, using semi- to fully automated key management that users consider trustworthy, and incorporating itself into the heuristic processing of emails instead of re-educating users.

4.1. Persuasive messages and intuitive UIs

E-commerce coined the term *persuasive experience* for UIs that have an appealing design, efficient functioning but also induce a feeling of privacy and security [42]. These techniques are also commonly applied in phishing attacks and have been studied in a variety of contexts for the purpose of identifying cues that make an email persuasive to its viewers [43], [44]. Users were found to rely on weak cues to determine the authenticity of an email. In particular, a professional look (e.g. logos, HTML) and the presence of legal disclaimers influences users to form a positive opinion. The subject line and assumed sender familiarity are also common properties that are used to deduce inferred utility and influences the prioritisation strategies that users apply [45]. The vulnerability of users to these cues is due to their heuristic rather than systematic processing of messages [46], [47].

We suggest the use of *persuasive email messages*, which suppress weak cues by manipulating the received emails according to their technical security level and allow users to intuitively perceive the security status. As the use of positive security indicators caused errors in the past, we propagate the use of negative security indicators instead to be used in prominent places that users use to determine the trustworthiness of an email. We provide preliminary drafts of the design in Fig. 1 that we plan to elaborate and evaluate in future user studies. Technically secure and hence *protected emails* (cf. Fig. 1a) should appear trustworthy to users by utilising cues that are known to induce trust, such as displaying the sender's full name together with positive security indicators and allow the rendering of HTML, and the use of aesthetic and legible typeface. *Unprotected emails* (i.e. ordinary email) (cf. Fig. 1b) in turn should convey a constant awareness of emails' insecurity. We suggest the display of email header fields to be adapted in order to contain technically correct information together with negative security indicators where applicable. For *corrupted emails* (e.g. failed signature verification) we envision the use of messages that convey the technically defective properties (cf. Fig. 1c) and appear most untrustworthy. Based on the demand *alter the phishing website* [28], corrupted email rendering should disrupt users from heuristic email processing, and the display of the message must prevent users from using weak cues, for example by removing the sender address as one of the strongest trusted anchor points. At the same time, however, it must meet the demand for effective management of email tasks and,

e.g., maintain the readability of the content.

In order to be able to control the security status of a message without causing additional cognitive effort, we advocate a deep integration of the decision-making process to ensure that emails are protected in the composing process of emails, for example when selecting addressees (cf. Fig. 1d). In line with community demands and research, we are striving for a simplification of possible protections statuses by allowing users to differentiate only between protected and unprotected outgoing messages.

4.2. Opportunities and possible implementations

We highlight that persuasive message design can be implemented in arbitrary ways and greatly accommodates the *good security now* principle [4], as it can be deployed independently of MUAs and operators. Our own development foresees a PGP proxy implementation that requires its users to configure their devices to use the proxy as the contacts database and email provider. The proxy injects symbols (e.g. padlock) into contact entries for email addresses with a valid PGP key. For incoming emails, a copy of the message will be manipulated according to a predefined rule set (e.g. headers, body). Similarly, operators may deploy the interaction and design concept to its user base without forcing them to change MUAs and add valuable feedback on the security of an email. The use of negative security indicators makes the solution resilient to UI dressing attacks. We envision that the manipulation of email renderings is not limited to MUAs, as users already accept that their operators apply various protection measures. Furthermore, the suppression of weak cues may impels honest senders who rely on HTML emails for customer satisfaction (e.g. advertisers) to apply protection measures that make the email system more secure and privacy friendly.

4.3. Limitations and open challenges

Our introduced approach has some limitations that require further examination. It remains one limitation that persuasive message design requires the consolidation of cryptographic techniques used in email transmission. In practical terms, its use requires a definition of what constitutes a secure email from a technical point of view, and how the use of E2E secure email tools compares to providers use of TLS and message authentication mechanisms from a users' point of view. It remains unclear how the use of different security mechanisms can be represented in an aggregated representation. Probably our approach supports only either of the above scenarios, but it is still conceivable that providers, admins or users themselves can influence the representation through appropriate configuration options.

Apart from this, the decision to permanently mark all unprotected emails with suitable cues might lead to warning fatigue as most emails are presumably still sent unprotected in reality. The permanent presence of negative security indicators may actually becomes useless over time, also because users do not experience bad consequences from handling emails that are flagged accordingly. It remains open, which restrictions of the message display users are willing to accept (e.g. suppression of images or HTML) and if they would abandon a tool or operator who enforces a persuasive message design.

5. Conclusion and Future Work

We presented prevailing challenges for the design of usable secure email UIs that go beyond the demand for a more usable key management. We suggest persuasive message design as a means to communicate security features by taking advantage of perception properties that we believe are more effective than existing solutions in meeting user demands for email. We consider our proposal to be a useful contribution to ongoing research on usable secure email by presenting a holistic and practical approach that systematically takes into account the results of previous research and best practice in order to lay the foundation for future UI design. At present, we are implementing a proof of concept of the design and interaction solution presented to empirically study and verify its effectiveness in solving the problems mentioned above.

Acknowledgement

We would like to thank the anonymous reviewers for their valuable feedback and input on our work.

References

[1] J. Clark, P. C. van Oorschot, S. Ruoti, K. Seamons, and D. Zappala, "Securing Email," *arXiv:1804.07706 [cs]*, 2018.

[2] H. Hu and G. Wang, "End-to-end measurements of email spoofing attacks," in *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD, USA: USENIX Association, 2018.

[3] A. Whitten and J. D. Tygar, "Why johnny can't encrypt: A usability evaluation of PGP 5.0," in *Proceedings of the 8th USENIX Security Symposium*. Washington, DC, USA: USENIX Association, 1999.

[4] S. L. Garfinkel, "Design principles and patterns for computer systems that are simultaneously secure and usable," 2005.

[5] S. Ruoti and K. Seamons, "Johnny's Journey Toward Usable Secure Email," *IEEE Security Privacy*, vol. 17, no. 6, pp. 72–76, 2019.

[6] S. L. Garfinkel and R. C. Miller, "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)*. Pittsburgh, Pennsylvania, USA: ACM, 2005.

[7] M. S. Melara, A. Blankstein, J. Bonneau, E. W. Felten, and M. J. Freedman, "CONIKS: Bringing Key Transparency to End Users," in *24th USENIX Security Symposium (USENIX Security 15)*. Washington, D.C., USA: USENIX Association, 2015.

[8] A. Lerner, E. Zeng, and F. Roesner, "Confidante: Usable Encrypted Email: A Case Study with Lawyers and Journalists," in *2017 IEEE European Symposium on Security and Privacy, (EuroS&P)*. Paris, France: IEEE, 2017.

[9] S. Ruoti, J. Andersen, D. Zappala, and K. Seamons, "Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client," *arXiv:1510.08555 [cs]*, 2016.

[10] E. Atwater, C. Bocovich, U. Hengartner, E. Lank, and I. Goldberg, "Leading Johnny to Water: Designing for Usability and Trust," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. Ottawa, Canada: USENIX Association, 2015.

[11] S. Ruoti, J. Andersen, T. Monson, D. Zappala, and K. Seamons, "A comparative usability study of key management in secure email," in *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. Baltimore, MD: USENIX Association, 2018.

[12] A. Reuter, K. Boudaoud, M. Winckler, A. Abdelmaksoud, and W. Lemrazzeq, "Secure Email - A Usability Study," in *Proceedings of AsiaUSEC'20, Financial Cryptography and Data Security 2020 (FC)*. Kota Kinabalu, Sabah, Malaysia: Springer, 2020.

[13] J. Müller, M. Brinkmann, D. Poddebniak, H. Böck, S. Schinzel, J. Somorovsky, and J. Schwenk, ""Johnny, you are fired!" – Spoofing OpenPGP and S/MIME Signatures in Emails," in *28th USENIX Security Symposium, USENIX Security 2019*. Santa Clara, CA, USA: USENIX Association, 2019.

[14] C. T. Moecke and M. Volkamer, "Usable Secure Email Communications - Criteria and Evaluation of Existing Approaches," in *6th International Symposium on Human Aspects of Information Security and Assurance (HAISA)*, Crete, Greece, 2012.

[15] N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, and M. Smith, "SoK: Secure Messaging," in *2015 IEEE Symposium on Security and Privacy (SP)*. San Jose, CA, USA: IEEE, 2015.

[16] R. Abu-Salma, K. Krol, S. Parkin, V. Koh, K. Kwan, J. Mahboob, Z. Traboulsi, and M. A. Sasse, "The Security Blanket of the Chat World: An Analytic Evaluation and a User Study of Telegram," in *Proceedings 2nd European Workshop on Usable Security (EuroUSEC)*. Paris, France: Internet Society, 2017.

[17] A. D. Luca, S. Das, M. Ortlieb, I. Ion, and B. Laurie, "Expert and non-expert attitudes towards (secure) instant messaging," in *Proceedings of the 12th Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO, USA: USENIX Association, 2016.

[18] A. Ferreira and R. Chilro, "What to phish in a subject?" in *Financial Cryptography and Data Security*, M. Brenner, K. Rohloff, J. Bonneau, A. Miller, P. Y. Ryan, V. Teague, A. Bracciali, M. Sala, F. Pintore, and M. Jakobsson, Eds. Springer International Publishing, 2017, pp. 597–609.

[19] S. Ruoti, J. Andersen, S. Heidbrink, M. O'Neill, E. Vaziripour, J. Wu, D. Zappala, and K. Seamons, ""We're on the Same Page": A Usability Study of Secure Email Using Pairs of Novice Users," in *Proceedings of the 2016 Conference on Human Factors in Computing Systems (CHI)*. San Jose, CA, USA: ACM, 2016.

[20] S. Ruoti, N. Kim, B. Burgon, T. van der Horst, and K. Seamons, "Confused johnny: when automatic encryption leads to confusion and mistakes," in *Proceedings of the 9th Symposium on Usable Privacy and Security (SOUPS '13)*. Newcastle, UK: ACM, 2013.

[21] W. Bai, M. Namara, Y. Qian, P. G. Kelley, M. L. Mazurek, and D. Kim, "An Inconvenient Trust: User Attitudes toward Security and Usability Tradeoffs for Key-Directory Encryption Systems," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO, USA: USENIX Association, 2016.

[22] K. Renaud, M. Volkamer, and A. Renkema-Padmos, "Why Doesn't Jane Protect Her Privacy?" in *14th International Symposium on Privacy Enhancing Technologies (PETS)*. Amsterdam, The Netherlands: Springer, 2014.

[23] S. Gaw, E. W. Felten, and P. Fernandez-Kelly, "Secrecy, flagging, and paranoia: adoption criteria in encrypted email," in *Proceedings of the Conference on Human Factors in Computing Systems (SIGCHI)*. Montréal, Québec, Canada: ACM, 2006.

[24] L. Ferreira and J. Anacleto, "Usability in Solutions of Secure Email – A Tools Review," in *Human Aspects of Information Security, Privacy and Trust (HAS '17)*. Vancouver, Canada: Springer, 2017.

[25] C. Robison, S. Ruoti, T. W. van der Horst, and K. E. Seamons, "Private Facebook Chat," in *Proceedings of the 2012 ASE/IEEE International Conference on Social Computing and 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust*, ser. SOCIALCOM-PASSAT '12. USA: IEEE Computer Society, 2012.

[26] S. Sheng, L. Broderick, and C. A. Koranda, "Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software," in *Proceedings of the 2nd Symposium On Usable Privacy and Security - Poster Session*. Pittsburgh, PA, USA: ACM, 2006.

[27] V. Roth, T. Straub, and K. Richter, "Security and usability engineering with particular attention to electronic mail," *Int. J. Hum. Comput. Stud.*, vol. 63, no. 1-2, pp. 51–73, 2005.

[28] S. Egelman, L. F. Cranor, and J. I. Hong, "You've been warned: an empirical study of the effectiveness of web browser phishing warnings," in *Proceedings of the 2008 Conference on Human Factors in Computing Systems (CHI)*. Florence, Italy: ACM, 2008.

[29] N. Stembert, A. Padmos, M. S. Bargh, S. Choenni, and F. Jansen, "A study of preventing email (spear) phishing by enabling human intelligence." in *2015 European Intelligence and Security Informatics Conference (EISIC)*. Manchester, UK: IEEE, 2015.

[30] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith, "Obstacles to the Adoption of Secure Communication Tools," in *2017 IEEE Symposium on Security and Privacy (SP)*. an Jose, CA, USA: IEEE, 2017.

[31] S. Ruoti, T. Monson, J. Wu, D. Zappala, and K. E. Seamons, "Weighing Context and Trade-offs: How Suburban Adults Selected Their Online Security Posture," in *13th Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA, USA: USENIX Association, 2017.

[32] A. Naiakshina, A. Danilova, S. Dechand, K. Krol, M. A. Sasse, and M. Smith, "Poster: Mental Models – User understanding of messaging and encryption," in *1st IEEE European Symposium on Security and Privacy*. Saarbrücken, Germany: IEEE, 2016.

[33] W. Tong, S. Gold, S. Gichohi, M. Roman, and J. Frankle, "Why king george III can encrypt," USA, 2014. [Online]. Available: http://randomwalker.info/teaching/spring-2014-privacy-technologies/king-george-iii-encrypt.pdf

[34] J. Lausch, O. Wiese, and V. Roth, "What is a secure email?" in *2nd European Workshop on Usable Security (EuroUSEC)*. Paris, France: Internet Society, 2017.

[35] M. Jakobsson and J. Ratkiewicz, "Designing ethical phishing experiments: a study of (ROT13) rOnl query features," in *Proceedings of the 15th international conference on World Wide Web*. Edinburgh, Scotland: Association for Computing Machinery, 2006.

[36] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the conference on Human Factors in computing systems (SIGCHI)*. Montréal, Québec, Canada: ACM, 2006.

[37] S. Whittaker and C. Sidner, "Email overload: Exploring personal information management of email," in *Proceedings of the Conference on Human Factors in Computing Systems (SIGCHI)*. New York, NY, USA: ACM, 1996.

[38] B. V. Hanrahan and M. A. Pérez-Quiñones, "Lost in email: Pulling users down a path of interaction," in *Proceedings of the 33rd Conference on Human Factors in Computing Systems (CHI '15)*. Seoul, Republic of Korea: ACM, 2015.

[39] G. D. Venolia, L. Dabbish, J. Cadiz, and A. Gupta, "Supporting email workflow," USA, 2001. [Online]. Available: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/tr-2001-88.pdf

[40] N. Siu, L. Iverson, and A. Tang, "Going with the flow: email awareness and task management," in *Proceedings of the 20th anniversary conference on Computer supported cooperative work (CSCW '06)*. Banff, Alberta, Canada: ACM, 2006.

[41] S. R. Barley, D. E. Meyerson, and S. Grodal, "E-mail as a source and symbol of stress," *Organization Science*, vol. 22, no. 4, pp. 887–906, 2011.

[42] H. H. Chang and S. W. Chen, "Consumer perception of interface quality, security, and loyalty in electronic commerce," *Information & Management*, vol. 46, no. 7, pp. 411 – 417, 2009.

[43] A. Karakasiliotis, S. M. Furnell, and M. Papadaki, "Assessing end-user awareness of social engineering and phishing," in *7th Australian Information Warfare and Security Conference*. Perth, Western Australia: School of Comp. and Inf. Science, 2006.

[44] K. Parsons, M. A. Butavicius, M. R. Pattinson, D. Calic, A. McCormac, and C. Jerram, "Do Users Focus on the Correct Cues to Differentiate Between Phishing and Genuine Emails?" in *Proceedings of the 27th Australasian Conference on Information Systems (ACIS)*, Adelaide, Australia, 2016.

[45] J. Wainer, L. Dabbish, and R. E. Kraut, "Should I open this email?: inbox-level cues, curiosity and attention to email," in *Proceedings of the Conference on Human Factors in Computing Systems (SIGCHI)*. Vancouver, Canada: ACM, 2011.

[46] B. Harrison, A. Vishwanath, Y. J. Ng, and R. Rao, "Examining the Impact of Presence on Individual Phishing Victimization," in *48th Hawaii International Conference on System Sciences (HICSS)*. Kauai, HI, USA: IEEE, 2015.

[47] A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. R. Rao, "Why do people get phished? testing individual differences in phishing vulnerability within an integrated, information processing model," *Decision Support Systems*, vol. 51, no. 3, pp. 576 – 586, 2011.