

# What is a Secure Email?

Joscha Lausch  
Freie Universität Berlin  
joscha.lausch@fu-berlin.de

Oliver Wiese  
Freie Universität Berlin  
oliver.wiese@fu-berlin.de

Volker Roth  
Freie Universität Berlin  
volker.roth@fu-berlin.de

**Abstract**—While security indicators for web browsers have been and still are an active research area, comparable indicators for secure email have received relatively little attention. However, similar questions emerge, for example, how users interpret existing indicators and whether there exist other indicators that are potentially more effective. In our paper, we review existing indicators used in the context of email encryption. Based thereof, we identify and study promising candidates and compare them using a survey instrument with 164 participants. Based on the results, postcards, mail envelopes and a torn envelope warrant further investigation. They offered an intuitive access and consistent interpretation on par with the dominant padlock metaphor.

## I. INTRODUCTION

Security research is directed at making the Internet a safe place for most if not all users. However, determining ahead of time whether a given Internet communication is safe and secure is often impossible. In many cases, context is needed to make that determination. Security indicators are meant to alert users to situations in which they should pay attention to the security state of their communication. Often, indicators are designed to convey additional information meant to make it easy and efficient for users to decide how to behave in any such situation.

Designing security indicators “the right way” is an active area of research. For example, Felt et al. [13] recently presented their work on security indicators for browsers, which led to the design of new security indicators for Google Chrome. The new indicator consisted of a green lock with the textual label “secure.” A discussion ensued among the presenters and the audience about what “secure” means in the context of a website. It may refer to the guarantees of confidentiality, reliability and integrity usually associated with a TLS connection [8], a view often taken by developers. On the other hand, users may interpret “secure” to mean the absence of harmful features in a website, for example, the absence of malware or phishing attempts. Obviously, here is a tension between the security indicator design and these two interpretations because a secure connection is certainly necessary to warrant a “secure” label but it may not be sufficient, given users’ expectations.

Our current research interest is the question how we can design email applications for smartphones with end-to-end encryption in a fashion that is easy to use. The question what “secure” meant in the context of a website resounded in our own research on how to communicate to a user what the security state of an email is. What do people think when asked what a secure email is, and how shall indicators for secure email be designed? Towards a better understanding of these questions, we:

- 1) Investigated the indicators currently in use on a variety of platforms and matched them with the technical properties of secure email.
- 2) Selected indicator designs which seemed to have merit and conducted a comparative study of them using a survey instrument and four dimensions of interpretation.
- 3) Collected and summarized the data and looked for significant differences between the indicators based on four dimensions. One dimension was the concept “secure” in its abstract form without reference to a particular property that makes “secure” secure. The other three dimensions consisted of properties that describe the far ends of confidentiality, integrity and authenticity in an intuitive fashion, that is, they are interpretable without knowing the formal definition of these properties in a technical security context.

We found that three indicators, a postcard, a mail envelope and a torn mail envelope that shows bits of the contained letter (briefly, the letter metaphor) worked well. The letter metaphor had consistent support by intuition compared to alternatives such as a padlock. The survey results suggest that participants’ interpretation of the letter metaphor was as sound and consistent as their interpretation of the padlock metaphor, and had advantages when signaling error conditions.

However, our study must be considered preliminary because our sample of the user population is skewed towards privacy-aware and tech-savvy users, it is clearly not representative of the population at large. Nevertheless, the letter metaphor showed promise, which is why we chose it for our ongoing research on easy-to-use end-to-end encryption for email on smartphones.

In what follows, we first tease apart some relevant properties associated with secure email, how they may be combined in practice and what signaling requirements result. Subsequently, we discuss related work. Next, we summarize the results of our investigation of email security indicators in use, followed by a rationale why we chose the letter metaphor and why it has intuitive appeal, followed by a description of our study and its results, followed by our statistical analysis of

participants’ responses, followed by a discussion of limitations and interpretation of results and our conclusions.

## II. INGREDIENTS OF SECURE EMAIL

Email clients (mail user agents) connect to a mail transfer agent via HTTP, IMAP, POP or SMTP. Any of these protocols may be tunneled through an encryption layer such as TLS [9]. The endpoints should authenticate themselves. User agents typically use a certificate or key fingerprint to authenticate the server. Servers require a password to authenticate users. Since web browsers are generic tools, they make the security state of connections explicit to the user. Hence, users are confronted with potentially multiple and seemingly inconsistent indicators when they use a browser to access a web mail service that also supports end-to-end encryption (for example, when the connection is “secure” but the email is not). Traditional user agents typically hide that state and merely report a working or failing connection to the mail transfer agent. We focus on mobile mail user agents and assume that the connections to mail transfer agents is pass or fail. In other words, we only deal with the security state of sent and received email.

Secure email can have four properties: **Unprotected:** Email bears no indication of cryptographic processing. **Confidentiality:** The contents of email are encrypted. **Integrity:** The contents of email is received as sent. This can be achieved by means of message authentication codes or digital signatures. **Authenticity:** The receiver can be convinced that the email was sent by someone holding a specific private key. This can be achieved by means of key agreement and message authentication codes or by means of digital signatures. **Non-repudiation:** The receiver can convince a third party that a given email has been sent by the holder of a specific private key. This can be achieved by means of digital signatures.

Non-repudiation implies authenticity and authenticity implies integrity. The reverse is not true. For example, an email body protected by means of a hybrid public/secret key encryption scheme with key encapsulation and a message authentication code may offer integrity but no authenticity because anyone could have created that email body (the public key of the receiver is involved but not the private key of the sender). A hybrid scheme with key agreement and message authentication code offers authenticity to the receiver but not necessarily non-repudiation because the sender’s and the receiver’s keys must be combined to derive the necessary key material. The two most popular message syntax standards for end-to-end encrypted email, S/MIME [31] and PGP [14], use signatures in lieu of message authentication codes in order to provide email authenticity and integrity.<sup>1</sup> Depending on the implementation, disabling signatures may leave users with confidentiality but limited integrity, which is counter-intuitive to users, and has confused even the designers of cryptographic protocols at times [1].

Most mail user agents with S/MIME or PGP support digital signatures explicitly. We believe this overshoots the target and complicates the user interface. What is called for most of the time is email integrity and authenticity but not non-repudiation. The former is a property of the email (received as sent) and

---

<sup>1</sup>PGP does support a so-called *modification detection code* that provides some integrity but is weaker than a message authentication code.

the latter are properties of who sent it. In our paper, we focus on the former property. We defer the issues around signaling authenticity and linking the sender to an identity to subsequent work because this requires more extensive analysis. This leads to three primary states we wish to signal to the user: (i) the email was sent in the clear; (ii) the email was uncorrupted and encrypted for the recipient; and (iii) the email is corrupted or broken. In case (iii) we do not care about whether a signature did not verify correctly or an encryption padding was invalid. Neither should happen in the absence of attacks if reliable transport is used for email, which we assume from the outset (in practice, there are cases in which mail transfer agents reformat email in a way that breaks cryptographic verification but this should be fixed by other means before cryptographic processing takes place).

## III. RELATED WORK

In what follows, we review existing literature on the study and design of security indicators. We cover security indicators in the context of web browsers and secure email.

### A. Webbrowser

In one of the first studies on browser security indicators, Friedman et al. [15] interviewed 24 participants. About half of them were able to identify a *https* connection on screenshots of web browsers. Friedman et al. argued that security indicators, much like keys or padlocks, can support the “idea of a ‘place’ that can be made secure” and less the concept of transport security [15]. Whalen and Inkpen studied how participants surf the web by means of an eye tracker [32]. They reported that 11 of 16 participants used security indicators (a padlock, in their study) to check whether a connection was secure or not. In their experimental setup, participants connected to a local website instead of a bank’s genuine website. All but one participant regarded the fake website authentic. Whalen and Inkpen noted that small icons can be confusing, security indicators should be interactive and users pay little attention to certificates when checking a website’s security.

Schechter et al. [25] performed a laboratory study in which participants connected to genuine banking websites via a concealed proxy using their genuine credentials. The proxy modified all connections so that they used *http* instead of *https*. Still, all of their participants entered their credentials in order to log into their accounts. Participants disregarded any present security indicators or their absence in making their decision.

Felt et al. [13] conducted online surveys on different security indicator designs. They tested four positive security indicators (security property is present) and four negative indicators (insecurity property is present), see also Figure 1. They found out that users confused transport security and content security, for example, the presence of malware or phishing.

Other researchers investigated security indicators in the context of phishing as well [5], [7], [27]. Browser warnings and dialogues were also studied extensively [2], [6], [10], [12], [20], [28], [29]. Amrutkar et al. [3] investigated security indicators on mobile devices and concluded that designing effective indicators is even more challenging on these devices because of the smaller displays and platform diversity.

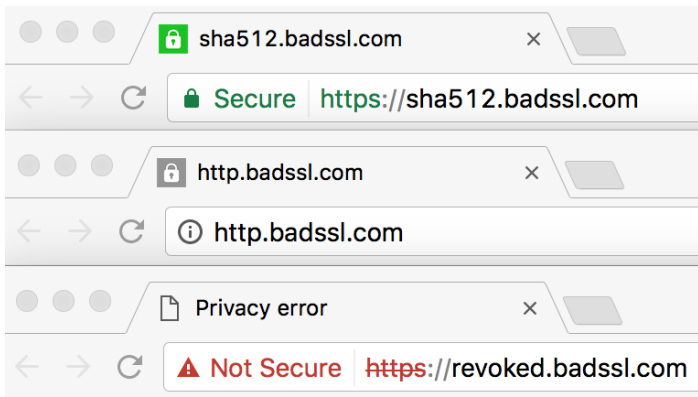


Fig. 1. Google Chromes security indicators: A circle for an unencrypted connection, a padlock for encrypted connection, a triangle for corrupted connection.

### B. Secure Email

Whitten and Tygar conducted a cognitive walkthrough and a laboratory study on the usability of PGP 5.0. They remarked that the metaphor of keys can be confusing since a classical padlock can be opened and closed with the same key whereas public-key encryption requires two keys. Furthermore, they regarded the studied program too complex [33]. Many researchers investigated key exchange and key management [4], [16], [17], [22] but did not look at indicators specifically.

Ruoti et al. [23], [24] reduced the management overhead of encryption by proposing a system based on identity-based encryption [26] (IBE). In an IBE encryption scheme, public keys can be arbitrary strings, for example, email addresses. Private keys are computed from a public key and a set of secret domain parameters. This eliminates the need to distribute and authenticate public keys at the expense of privacy because a central entity must keep the domain parameters in order to be able to generate fresh private keys for new participants as needed. This enabled Ruoti et al. to keep their indicators simple. They used a green label that states whether or not an email was encrypted.

Few different metaphors for email encryption are proposed in the literature. Roth et al. [22] proposed postcards and mail envelopes in order to signify two different email encryption policies. Tong et al. [30] proposed medieval metaphors for email encryption, for example, locks and chests. Bai et al. [4] used a key and padlock metaphor to symbolize secret and public keys in their user studies.

Fahl et al. [11] proposed a tool to encrypt private facebook messages. Their security indicators were text messages such as “This is an unencrypted message!” and green boxes drawn around encrypted messages. In a user study of Garfinkel and Miller, the background color of a message (green, yellow, grey, red) indicated different levels of security [17]. In summary, security indicators seem to have been studied well in the context of web browsers but significantly less so in the context of secure email.

## IV. INDICATORS IN THE WILD

Support for secure email is widely available on all platforms. More recently, messenger applications with encryp-

tion support are becoming popular. In order to determine which types of security indicators are in use we surveyed 8 applications on a variety of platforms. On the desktop, we looked at the security indicators of Apple Mail, Mailvelope,<sup>2</sup> Outlook and Thunderbird. On Android we inspected K9<sup>3</sup> in combination with OpenKeyChain.<sup>4</sup> On iOS we inspected the default iOS Mail application, Mynigma<sup>5</sup> and Tutanota.<sup>6</sup> Tutanota and Mynigma do not support S/MIME or PGP. Instead the developers implemented protocols of their own based on AES and RSA. Apple Mail, default iOS Mail, Outlook and Thunderbird support S/MIME by default. K9 and Mailvelope support PGP. Enigmail is a PGP extension for Thunderbird. Thunderbird uses similar security indicators for PGP and S/MIME. All applications on all platforms, except Tutanota and Mynigma, have separate indicators for encryption and digital signatures. All applications used a padlock as an indicator for an encrypted message. Thunderbird is somewhat inconsistent in its approach. When composing email, a key icon indicates the encryption state whereas a padlock is used when reading received email. Some apps, for example, Tutanota, Mynigma and K9, use colors as an additional indicator. The American National Standards Institute (ANSI) Z535.1-2006 defines safety colors for use in work areas and when labeling equipment. Therein orange indicates a warning and red indicates danger [18], as opposed to no risk. A green padlock usually indicates an encrypted message. In K9, the padlock is green only if the corresponding key is verified and is orange otherwise. A grey crossed-out padlock indicates that encryption is disabled. Arguably, if we focus on confidentiality then encryption is always at least as good or better than no encryption. From that perspective it seems more appropriate to use orange or even red for unencrypted email. This is what Mynigma does, it labels unencrypted email with red indicators. Apple Mail, Thunderbird, Outlook and iOS Mail do not provide security indicators for unencrypted and unsigned messages.

While security indicators for encryption are very similar across applications (largely padlocks), different security indicators exist for signed and unsigned email. Apple Mail and iOS Mail label signed email with a checkmark within a seal. Thunderbird uses a letter (mail envelope) with a seal instead (when reading email) and a pen (when composing). K9 uses a mixture of indicators, namely, a padlock with or without a cross, a crossed-out padlock, the colors green, orange and red, and three dots next to the padlock that can be solid or unfilled. These indicators are used to signal a variety of states comprised of the fact whether or not encryption is used, whether signatures are used, whether signatures can be verified, and whether signers are trustworthy according to some metric. The choice of colors and dots in combination appears to be inspired by the Threema<sup>7</sup> messenger, which uses three dots as indicators. One red and two grey dots indicate the lowest degree of trustworthiness (not verified), followed by two orange dots and one grey one (verified by Threema), followed by three green dots (verified by the user).

<sup>2</sup><https://www.mailvelope.com/en>

<sup>3</sup><https://k9mail.github.io/>

<sup>4</sup><https://www.openkeychain.org/>

<sup>5</sup><https://mynigma.org/en/>

<sup>6</sup><https://tutanota.com/>

<sup>7</sup><https://threema.ch/en>



Fig. 2. K9s security indicators: A crossed-out padlock for unencrypted email (in composing screen), a padlock for encrypted and signed email depending on verification degree of the signature, a padlock with a cross inside for corrupted email. The graphics are taken from their git-repository: [github.com/k9mail/k-9/tree/master/images/drawables-pgp/docs](https://github.com/k9mail/k-9/tree/master/images/drawables-pgp/docs)

In summary, mail user agents (MUA) uniformly indicate encrypted emails with padlocks but use varying colors. Not all MUAs support digitally signed email. When signed email is supported, MUAs use a variety of symbols. This complicates consistent signaling of the security state of an email in a multi-device world.

## V. OUR INDICATORS

Our investigation of email security indicators in the wild turned up mixed results. Most developers seem to agree on the padlock metaphor for encryption but have different views when it comes to digital signatures. The situation becomes increasingly confusing if one mixes the two mechanisms. The K9 approach is perhaps an indicator of that. Telling the user exactly what went wrong when something went wrong becomes very complicated and perhaps should not even be the goal. We would rather avoid this complication. If the signature is broken then this is treated as if any integrity protection was broken (for example, an encryption padding turns out bad). If everything is correct then the information obtained from the signature is used to indicate our degree of trust in who the sender is (which is outside our current scope). In this paper, we focus on the signaling of the encryption and integrity state. This leaves us with three states we must signal to the user, (i) unencrypted, (ii) properly encrypted and integrity protected and (iii) broken (see also Section II).

The padlock is not quite perfect in this case. While its interpretation appears well established for the presence (closed) or absence (unlocked) of encryption, developers disagree somewhat about what to do in the case of an email whose encryption (or signature) is corrupted. A closed padlock with a cross appears to be a contender for an emerging convention but there is no intuitive explanation what a padlock with a cross is supposed to mean because there is no practical analogy. This leaves us with a somewhat unsatisfying situation. Therefore, we decided to pursue a different metaphor instead that is more suited to convey the three states in an intuitive fashion. In 2005, Roth et al. [22] proposed a postcard and mail envelope (briefly, letter) metaphor to symbolize different mail encryption policies. We decided to augment this metaphor with a torn mail envelope (briefly, torn letter), which indicates intuitively, or so we think, that the letter’s confidentiality may have been compromised – a direct consequence of the fact that the envelope’s integrity has been compromised. In order to validate our intuition, we conducted a survey study (see Section VI) with the goal to compare the letter metaphor with the padlock metaphor and the seal metaphor. Our hypothesis was that the letter metaphor would fare better than the padlock metaphor and the seal metaphor in the case of encryption.

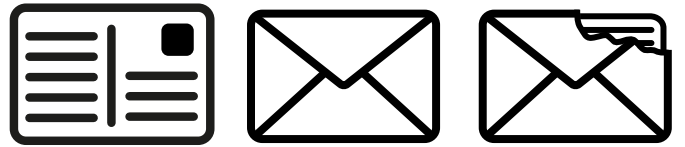


Fig. 3. Our security indicators: A postcard for unencrypted or unsigned email (state i), a letter for encrypted and signed email (state ii), a torn letter for corrupted email (state iii).

## VI. STUDY

We were interested to learn how well users would understand the postcard and letter indicators and how users would interpret them. Towards this end, we conducted a comparative study based on a survey instrument. Since our development target is iOS, we used security indicator icons for comparison that generalize well and are comparable to indicators of a typical iOS application, that is, iOS Mail. We borrowed the padlock icons from ModernPGP<sup>8</sup> and designed all other icons ourselves in order to maintain a consistent style. Table II shows the final designs.

### A. Method

Our survey was web-based and hosted on Google Forms. Invitations were distributed via email and Twitter. Our Twitter message only mentioned that the study was about email security. The email invitation additionally mentioned the security indicator and email usage aspects of our study. We offered no incentives for participation. A crowdsourcing platform like *Amazon Mechanical Turk* was not used amongst other reasons because our main target population is in Germany, where platforms like that are not widely used. The survey was divided into four sections. In the first section, we asked questions about participants’ general expectations towards secure email, whether they used modern crypto messengers such as *Signal*, *WhatsApp*, *Threema*, *Jabber with OTR* or others, and whether they were familiar with basic encryption properties and whether they have a key pair for email encryption.

Depending on their responses, we asked participants either why they do not use email encryption or with how many contacts they communicate in encrypted form. In the second section, participants were asked to rank all offered security indicators on a Likert scale along several dimensions. This was the main focus of our study and we report further detail on these questions in Section VI-B. In the third section, we used questions to assess participants’ understanding of the inherent properties of encryption and digital signatures. The survey concluded with questions about email usage and demographics in section four. Overall, participants answered up to 27 questions of which 4 were optional. The survey is in the appendix.

### B. Questions

The padlock icon is perhaps the icon that is used most often to indicate encrypted email in a MUA. A seal icon is used often to indicate the presence or absence of a digital signature. We were interested to learn what users actually associate with these

<sup>8</sup><https://github.com/ModernPGP/icons>

	Respondents
Male	66.5 %
Female	31.7 %
Other	1.8 %
In Education	58.5 %
Middle school	0.6 %
A-Level equiv.	30.5 %
Apprenticeship	3 %
Bachelor degree	25.6 %
Masters degree	36.6 %
PhD	3.7 %
Age 18–24	26.2 %
Age 25–34	39.6 %
Age 35–44	10.4 %
Age 45–54	8.5 %
Age 55–64	11 %
Age 65 or over	4.3 %

TABLE I. DEMOGRAPHICS OF THE 164 PARTICIPANTS

icons and the letter icons we posed. Towards this end, we chose four dimensions. One abstract security dimension and three dimensions that convey the different aspects of confidentiality, authenticity and integrity in a fashion that is intuitive and easy to understand even without knowing how these terms are formally defined. The four dimensions are:

insecure	↔	secure
unconcealed	↔	confidential
manipulable	↔	not manipulable
suspicious	↔	trustworthy

Participants rated all icons along these four dimensions on a 5-point Likert scale. In order to account for the absence of a strong association between the offered dimensions and icons we allowed participants to indicate a *no association* condition. This helped avoiding the typical effect that undecided participants tend to select the neutral position on a Likert scale if they cannot relate to the question. This modification of the Likert scale is particularly useful in our case because not all dimensions apply to all icons (by expectation) even though participants should be able to indicate whichever association they have. It is noteworthy that all icons were presented on one page, but participants had to scroll to see them since there is no overview. With common display resolutions the participants should see only one icon at a time.

### C. Demographics

We recruited most of our 164 participants via a mailing list internal to the computer science department of the Freie Universität Berlin. The list is subscribed predominantly by students and researchers. We recruited additional participants not necessarily affiliated with the university by means of email and Twitter. The median age of our sample is 29 years. Since the language of the survey was German it is safe to assume that our participants speak German. 70.7 % of our participants stated that they have an IT background and almost two thirds have an academic degree. Our respondents stated a high regard for privacy. 82.9 % said that privacy is very important or important to them. 23.2 % indicated that they work in a field where they come into contact with privileged information which requires special protection, for

example, doctors, lawyers and journalists. Table I summarizes the demographics of our respondents. Because of the high levels of IT expertise and concern for privacy among the participants we consider our sample to be fairly knowledgeable with regard to the concepts of encryption and digital signatures.

### D. Results

1) *Expectations towards Secure Email*: The features participants expected most of secure email were confidentiality, authenticity and integrity, as opposed to receipts for received email or the property that attachments are harmless. 96.3 % answered that only the sender and the receiver should be able to read an email's contents. 94.5 % answered that the receiver should be certain that the email actually came from the alleged sender. 86.6 % answered that an email should be received as it was sent. 51.8 % answered that a secure email ought to reach its recipient.

By comparison, only about half of our respondents (43.9 %) answered that a secure email should imply that attachments and links are harmless, that is, free of malware. Only 9.8 % answered that the sender gets an acknowledgment of receipt. Four participants posted expectations of their own to the list. One wrote that a secure email must be easy to use. Another expects that secure email reaches its recipient in under 5 minutes. The third one expects that links and attachments cannot be changed, in addition to the immutability of the email's contents. Yet another wrote that the meta-data should not disclose any information from the content.

2) *Use of Encrypted Communication*: In this section, we summarize the answers to the questions we asked in regard to participants' use of encrypted communication. 40.9 % of our participants responded that they have a key-pair for email encryption. This result is perhaps due to the high fraction of computer scientists in our sample. 72.2 % of those without a key-pair would like to encrypt their emails and only 15.5 % do not want to encrypt their emails at all. Twelve participants did not want to decide for or against and chose to answer in free-form using a text field we provided for that purpose. Five participants said that they do not know enough about the topic to make up their mind, or were not able to assess the risk of one choice over the other. Two participants answered that they preferred that encrypting their email was not necessary. One participant would like to encrypt email if only it was easier. One participant stated that the email-clients should offer that functionality by default. Yet another participant felt that the benefits of encrypting email do not outweigh the added complication.

The majority of participants (52.6 %) who do not have encryption keys gave as a reason that they always wanted to look into it but never got around doing so. 30.9 % said that it was too complicated for them and 22.7 % thought no one else would use email encryption. 11.3 % believed that they are not a target and as many participants responded that they do not need it. Two respondents said email encryption is too complicated for their communication partners and another two participants said that they simply did not think about email encryption before. One participant stated that she never heard of email encryption before. Another participant stated that he is not using it anymore because he lost his public key.



One respondent said he does not need encryption because he does not exchange sensitive information via email. Another respondent stated that she believes her web-interface to maybe encrypt email for her.

The majority (89.6%) of the 67 respondents with email encryption keys use PGP and 31.3% use S/MIME. 20.9% use both standards. The groups of communication partners who are using encrypted email to communicate with each other are relatively small. 47.8% have 2–3 contacts with encryption keys, 26.9% communicate encrypted with 4–10 contacts and 10.4% have more than 10. 14.9% have only one person with whom they use encryption.

In our sample, more than twice as many people (82.9%) use encrypted messaging with Signal, Threema or OTR as use encrypted email. By far the most common application is WhatsApp (61.6%). Threema is used by 26.5% of our sample and Signal by 21.3%. Close up with 19.5% is Jabber with OTR. 32.9% use other encrypted communication channels.

Despite the high percentage of crypto messenger users in our sample, email is still used widely and actively. 42.7% use email more than 5 times a day, and 37.2% use email multiple times a day. 11% use it about once a day and 6.7% every 2–3 days. 2.4% check their email only once a week and nobody fewer than that. 70.7% have between 2 and 5 email accounts and 17.7% have even more than that. Only 11.6% have just one email account.

3) *Understanding of Encryption Properties:* Most of our respondents (68.9%) think they know the difference between encryption and digital signatures. 19.5% stated that they do not know the difference and 11.6% were not sure. We compared these statements with the answers participants gave to our questions in regard to the properties of encrypted and digitally signed email. Since different implementations of email encryption protocols have different properties, we concentrated on basic functions. For example, PGP offers message authenticity as an optional feature. Therefore, we counted participants' answers as correct if they answered that encryption offers confidentiality and not authenticity, and if they answered that digital signatures offer authenticity and integrity but not confidentiality. Based on this scoring, only 38.4% of our sample knew the correct properties. Across all answers on the properties of encryption, 94.5% knew that encryption offers confidentiality, 51.2% stated that it offers integrity and 23.1% stated that encryption offers authenticity. If we ignore answers on the integrity of encryption then 73.2% gave the correct response for encryption. 87.8% knew that a digitally signed email offers authenticity, 57.9% stated that it offers integrity and 7.3% stated that digital signatures offer confidentiality. In total, 47% of the respondents were able to correctly identify the properties of digital signatures.

4) *Associations to Security Indicators:* Figure 4 shows how strongly our participants associate security indicators (see Figure 3) with the dimension insecure ↔ secure. It is striking how well established the closed padlock is in the context of security. Only 2.4% see no association between the symbol and security and 90.9% give it a score of 5 (secure) or 4. The letter gets a mixed response. 14.6% do not associate it with security, 36% tend to *secure*, 23.2% tend to *insecure* and 14.6% see it as neutral. Seals were least associated with

	secure	confidential	not manipulable	trustworthy
	1	1	2	3
	3	4	3	4
	1	1	1	1
	5	5	5	5
	1	1	1	2
	4	3	4	4
	1	2	2	1

TABLE II. MEDIANS OF THE ASSOCIATIONS OF THE SECURITY INDICATORS ON THE SCALE 1–5 WHERE 5 IS THE PROPERTY IN THE HEADER

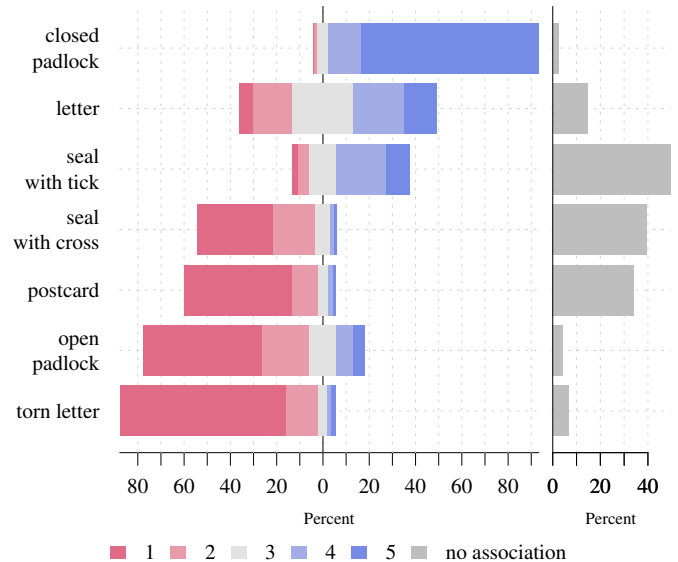


Fig. 4. Security indicator ratings between *insecure* (1) and *secure* (5)

security (seal with cross 49.4%, seal with tick mark 39.6%). The postcard was not associated with security either (34.1%). On the other hand, 88% of those who did associate it with this dimension did so on the *insecure* side. Another interesting observation is that 20 people (12.2%) associated the open padlock with security (a score of 4-5) and 19 (11.6%) chose the neutral position (a score of 3). The difference to the torn letter is surprisingly large. Even though 4 more participants had no association, 86% associated the torn letter with insecurity (a score of 1-2) compared to 71.9% in the case of the open padlock.

We move on to the results for the confidentiality dimension,

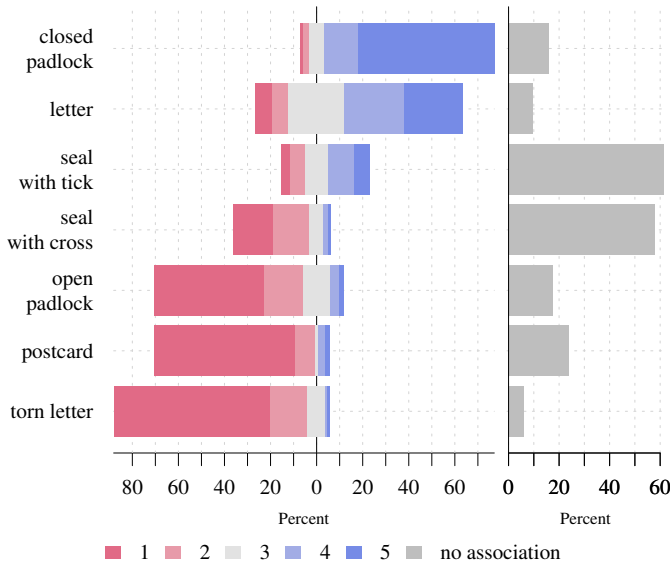


Fig. 5. Security indicator ratings between **unconcealed** (1) and **confidential** (5)

shown in Figure 5. The number of respondents who answered *no association* in the case of seals is noteworthy. At about 60% this is the highest number of *no association* responses on all four measured dimensions. Indeed, seals are not typically used to indicate properties related to confidentiality and many participants seem to have internalized this. The number of people who answered *no association* in the case of a closed padlock icon (15.9%) is notably higher than in the case of the general security dimension (the difference is 13.5%). This is worth noting because most MUAs use this icon to indicate confidentiality. The results hint that the security-related associations of the padlock might be of a more general nature. Still, the padlock evokes the strongest response with regard to confidentiality, followed by the letter icon. The open padlock and the postcard score similarly in regard to the confidentiality dimension, but a few more participants associate the postcard with *unconcealed*.

Figure 6 indicates that our sample is quite undecided about whether a letter is manipulable or not. 25% tend to *manipulable* (score 1–2), 31.7% tend to the neutral position and 26.2% tend to *not manipulable* (score 4–5). Once again, the seals are the icons with the highest rate of *no association*.

On the dimension suspicious ↔ trustworthy (Fig. 7) there is a remarkably large gap between the torn letter and the next two contenders, the seal with the cross and the open padlock. The torn letter also has the fewest *no association* responses by a margin of 8.1%.

We also looked at differences in associations to the icons between participants who have a key and those who do not have a key. The only remarkable difference we found was with the letter on the security dimension. As table III shows, more participants without a key saw the letter as more secure than those with a key. In regard to the lock icon our participants showed similar tendencies as in participants with a key seem to think things are less secure. 83.5% of those without a key saw the lock as secure (5) whereas only 67.2% of the key

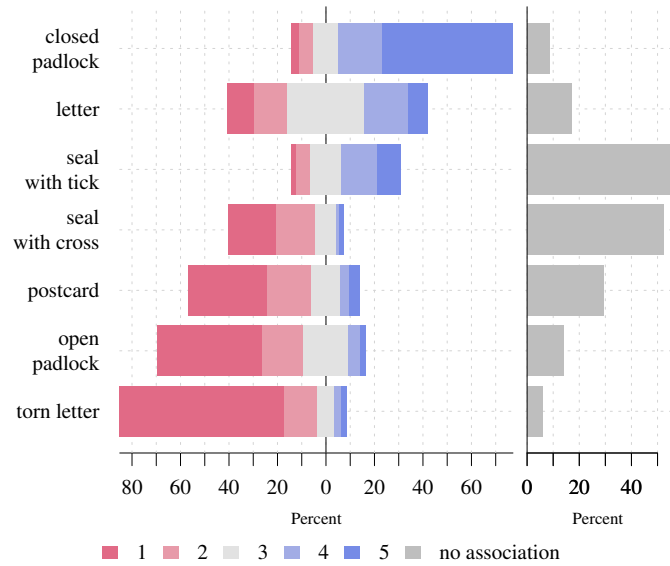


Fig. 6. Security indicator ratings between **manipulable** (1) and **not manipulable** (5)

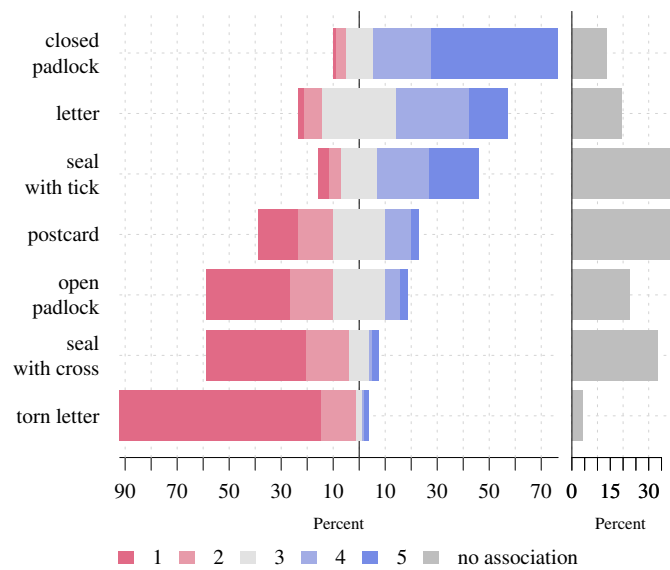


Fig. 7. Security indicator ratings between **suspicious** (1) and **trustworthy** (5)

holders thought the same. There were proportionally more participants with keys who ranked the lock icon as neutral (3) or rather secure (4). The seal icons are better known by participants with an encryption key. They also saw them more strongly associated in the directions they are commonly used in.

In order to look more closely at the general perception of a letter versus a postcard, we asked our participants whether they trust the contents of a letter more than the contents of a postcard. Three quarters (75%) of our sample answered affirmatively and the others disagreed. However, when asked whether they would pay an invoice printed on a postcard, only 11.6% said they would.

Rating	have a key [n=67]	have no key [n=97]
letter icon on security dimension		
4 or 5	22.4 %	45.4 %
3	28.4 %	24.7 %
1 or 2	34.3 %	15.5 %
no association	14.9 %	14.4 %
lock icon on security dimension		
4 or 5	86.6 %	93.8 %
3	9 %	2.1 %
1 or 2	0 %	3.1 %
no association	4.5 %	1 %
seal with tick icon on trust dimension		
4 or 5	46.3 %	34 %
3	10.4 %	16.5 %
1 or 2	10.4 %	7.2 %
no association	32.8 %	42.3 %
seal with cross icon on trust dimension		
4 or 5	1.5 %	5.2 %
3	4.5 %	10.3 %
1 or 2	67.2 %	46.4 %
no association	26.9 %	38.1 %

TABLE III. RATINGS OF DIFFERENT ICONS ON THE SECURITY AND TRUST DIMENSIONS GROUPED BY PARTICIPANTS WHO HAVE A KEY FOR EMAIL ENCRYPTION OR NOT

### E. Statistical Analysis

The dataset on security indicator associations we collected and described in Section VI-D4 is paired and on an ordinal scale. We performed a pair-wise comparison of the studied indicators using the non-parametric Wilcoxon rank sum test separately for all dimensions. For each dimension we performed 42 pairwise and sided tests with an alpha error of  $\alpha = 0.05$  and used Bonferroni correction to adjust our significance level. In each test we removed participants who responded with *no association* in any of two compared symbols. This is necessary because the *no association* response is outside the Likert scale, that is, not ordinal.

Tables IV, V, VI and VII show the resulting  $p$ -values for each individual dimension. For each row and column we tested whether the indicator in the row is ranked lower on the dimension than the indicator in the column. Statistically significant results are marked with an asterisk. Along each dimension, the padlock rated the most positive symbol and the torn letter was rated the most negative symbol.

### F. Limitations

In a sample of 200 000 individuals taken from 20 industrialized countries [21], only 5.4 % were classified as having an experience level that is comparable to 66.5 % of the sample in our study. 70.7 % of our participants stated that they have an IT background and almost two thirds have an academic degree. The sample we studied is clearly skewed towards tech-savvy individuals, most likely because we recruited most of them via a mailing list internal to the computer science department of the Freie Universität Berlin. Since our solicitations for participation in the survey included references to security indicators and email, it is likely that our sample suffered from a self-selection bias as well. The high number (82.9 %) of participants who said that privacy is very important or important to them supports that hypothesis. Also, the number of participants who reported that they work with sensitive data is fairly high (23.2 %). Overall, this indicates that our sample

is not representative of the general population. Clearly, further research and experimentation is necessary in order to verify whether the results we obtained in our study are reproducible in more general samples of the population.

## VII. DISCUSSION & CONCLUSIONS

The seal metaphor conspicuously evoked the largest number of *no association* responses on all dimensions. Furthermore, somewhat to our surprise, the seal with a tick mark was rated significantly less trustworthy than a closed padlock. One possible explanation might be that seals are a historic relic and are not in practical use any longer in the context of mail. Their use in modern contexts is largely limited to indicating the integrity of food containers and signaling adherence to dubious standards for product quality. This may have watered down associations of authenticity and value that wax seals on letters once enjoyed. Another possible explanation might be that users simply have challenges recognizing and correctly interpreting seal indicators in the context of electronic communication. Yet another explanation might be that many users view the closed padlock as a strong overarching security indicator – stronger than the specific indicator for the trustworthiness dimension. Either reason diminishes the value of seals as indicators.

Among the encryption indicators, the letter icon scored second place along all dimensions, following the closed padlock, which consistently scored first place. The seal with tick scored higher than the letter icon in the security and manipulability dimensions. However, the former are typically used in the context of signatures. By comparison, the letter icon received more diverse ratings. This is especially obvious in the *manipulable* dimension. We wonder whether German history may have played a role and the possibility that many participants might have grown up in East Germany (in the GDR). In the GDR, letters were routinely steamed open by the “Staatssicherheit” [19]. Examples such as this indicate limitations of the letter metaphor. However, padlocks are routinely opened in practice as well. Hence, it remains open for investigation why letters are rated, for example, less trustworthy than padlocks. One possible explanation is that padlocks are already well-established as security indicators in browsers and the associations carry over to the email context.

On the other hand, the torn letter icon scored remarkably well. Participants consistently ranked it last on all dimensions, and it scored the least number of *no association* responses. This renders the torn letter icon particularly useful for indicating error conditions. This is valuable in the context of email encryption because users must be particularly attentive when decryption errors occur. This is similar to the approach of Felt et al. [13] who emphasized the relevance of error cases as well, albeit in the context of web browsers [13, Fig. 4].

The postcard and the torn letter differed significantly only in the dimensions *manipulable* and *trustworthy* even though postcards offer no confidentiality in practice. This is actually consistent with what one might expect in practice given a letter that shows marks of manipulation, such as a torn-off edge. Hence, the torn letter appears quite useful to indicate a security incident as opposed to a random error.

Even though we did not use color in our study, most security indicators were ranked as expected. This suggests





							
		< 0.001*	0.732	< 0.001*	< 0.001*	< 0.001*	0.073
	1		1	< 0.001*	1	0.041*	1
	0.272	< 0.001*		< 0.001*	< 0.001*	< 0.001*	< 0.001*
	1	1	1		1	1	1
	0.999	< 0.001*	1	< 0.001*		< 0.001*	0.942
	1	0.96	1	< 0.001*	1		1
	0.93	< 0.001*	0.999	< 0.001*	0.059	< 0.001*	

TABLE IV. P-VALUES OF WILCOXON RANK SUM TEST. FOR EACH CELL WE TESTED WHETHER THE SYMBOL OF THE CORRESPONDING ROW IS CONSIDERED LESS SECURE THAN THE SYMBOL OF THE CORRESPONDING COLUMN. \* INDICATES STATISTICAL SIGNIFICANCE ( $p < 0.05$ )

that colors may not be necessary to discriminate between different states, besides being of dubious usefulness for color-blind individuals. We did not focus on authenticity in the course of this study. However, we found that users expect confidentiality, integrity and authenticity.

In summary, the letter metaphor showed merit compared to commonly used metaphors such as the padlock one and warrant further investigation. We suspect that the letter metaphor derives its benefits from the close relationship that paper mail and electronic mail enjoy with regard to users' mental model.

#### ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their helpful comments. The first and second author were funded by the Bundesministerium für Bildung und Forschung (Federal Ministry of Education and Research, Germany) under grant number 16KIS0360K (Enzevalos).

#### REFERENCES

- [1] M. Abadi and R. Needham, "Prudent engineering practice for cryptographic protocols," *IEEE Trans. Softw. Eng.*, vol. 22, no. 1, pp. 6–15, Jan. 1996. [Online]. Available: <http://dx.doi.org/10.1109/32.481513>
- [2] D. Akhawe and A. P. Felt, "Alice in Warningland: A Large-scale Field Study of Browser Security Warning Effectiveness," in *Proceedings of the 22Nd USENIX Conference on Security*, ser. SEC'13. Berkeley, CA, USA: USENIX Association, 2013, pp. 257–272.
- [3] C. Amrutkar, P. Traynor, and P. C. van Oorschot, "Measuring SSL Indicators on Mobile Browsers: Extended Life, or End of the Road?" in *Proceedings of the 15th International Conference on Information Security*, ser. ISC'12. Berlin, Heidelberg: Springer-Verlag, 2012, pp. 86–103.
- [4] 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*, ser. SOUPS '16. Denver, CO: USENIX Association, 2016, pp. 113–130.
- [5] R. Biddle, P. C. van Oorschot, A. S. Patrick, J. Sobey, and T. Whalen, "Browser Interfaces and Extended Validation SSL Certificates: An Empirical Study," in *Proceedings of the 2009 ACM Workshop on Cloud Computing Security*, ser. CCSW '09. New York, NY, USA: ACM, 2009, pp. 19–30.
- [6] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter, "Your Attention Please: Designing Security-decision UIs to Make Genuine Risks Harder to Ignore," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*, ser. SOUPS '13. New York, NY, USA: ACM, 2013, pp. 6:1–6:12.
- [7] R. Dhamija, J. D. Tygar, and M. Hearst, "Why Phishing Works," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '06. New York, NY, USA: ACM, 2006, pp. 581–590.
- [8] T. Dierks, "The transport layer security (TLS) protocol version 1.2," *IETF*, 2008.
- [9] —, "The Transport Layer Security (TLS) Protocol Version 1.2," RFC 5246, Aug. 2008.
- [10] S. Egelman, L. F. Cranor, and J. Hong, "You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '08. New York, NY, USA: ACM, 2008, pp. 1065–1074.
- [11] S. Fahl, M. Harbach, T. Muders, M. Smith, and U. Sander, "Helping Johnny 2.0 to Encrypt His Facebook Conversations," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ser. SOUPS '12. New York, NY, USA: ACM, 2012, pp. 11:1–11:17.
- [12] A. P. Felt, A. Ainslie, R. W. Reeder, S. Consolvo, S. Thyagaraja, A. Bettes, H. Harris, and J. Grimes, "Improving SSL Warnings: Comprehension and Adherence," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ser. CHI '15. New York, NY, USA: ACM, 2015, pp. 2893–2902.
- [13] A. P. Felt, R. W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M. E. Acer, E. Morant, and S. Consolvo, "Rethinking Connection Security Indicators," in *Twelfth Symposium on Usable Privacy and Security*, ser. SOUPS '16. Denver, CO: USENIX Association, 2016, pp. 1–14.
- [14] H. Finney, L. Donnerhacke, J. Callas, R. L. Thayer, and D. Shaw, "OpenPGP Message Format," RFC 4880, Nov. 2007.
- [15] B. Friedman, D. Hurley, D. C. Howe, E. Felten, and H. Nissenbaum, "Users' Conceptions of Web Security: A Comparative Study," in *CHI '02 Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA '02. New York, NY, USA: ACM, 2002, pp. 746–747.
- [16] S. L. Garfinkel, "Email-Based Identification and Authentication: An Alternative to PKI?" *IEEE Security and Privacy*, vol. 1, no. 6, pp. 20–26, Nov. 2003.
- [17] 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 2005 Symposium on Usable Privacy and Security*, ser. SOUPS '05. New York, NY, USA: ACM, 2005, pp. 13–24.
- [18] A. N. S. Institute, "ANSI Z535.1-2006: Safety Colour Code," Rosslyn, Virginia, 2007.
- [19] H. Labrenz-Weiß, *Abteilung M (MfS-Handbuch)*. Berlin: Federal Commissioner for the Records of the State Security Service of the former German Democratic Republic, 2005. [Online]. Available: [http://www.bstu.bund.de/DE/Wissen/Publikationen/Publikationen/handbuch\\_abt\\_m\\_labrenz-weiss.pdf?\\_\\_blob=publicationFile](http://www.bstu.bund.de/DE/Wissen/Publikationen/Publikationen/handbuch_abt_m_labrenz-weiss.pdf?__blob=publicationFile)
- [20] M.-E. Maurer, A. De Luca, and S. Kempe, "Using Data Type Based Security Alert Dialogs to Raise Online Security Awareness," in *Proceedings of the Seventh Symposium on Usable Privacy and Security*, ser. SOUPS '11. New York, NY, USA: ACM, 2011, pp. 2:1–2:13.

- [21] OECD, *Skills matter: Further results from the survey of adult skills*, 2016. [Online]. Available: [https://www.oecd.org/skills/piaac/Skills\\_Matter\\_Further\\_Results\\_from\\_the\\_Survey\\_of\\_Adult\\_Skills.pdf](https://www.oecd.org/skills/piaac/Skills_Matter_Further_Results_from_the_Survey_of_Adult_Skills.pdf)
- [22] 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, Jul. 2005.
- [23] 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 CHI Conference on Human Factors in Computing Systems*, ser. CHI '16. New York, NY, USA: ACM, 2016, pp. 4298–4308.
- [24] S. Ruoti, J. Andersen, T. Hendershot, D. Zappala, and K. Seamons, "Private Webmail 2.0: Simple and Easy-to-Use Secure Email," in *Proceedings of the 29th Annual Symposium on User Interface Software and Technology*, ser. UIST '16. New York, NY, USA: ACM, 2016, pp. 461–472.
- [25] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer, "The Emperor's New Security Indicators," in *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, ser. SP '07. Washington, DC, USA: IEEE Computer Society, 2007, pp. 51–65.
- [26] A. Shamir, "Identity-based Cryptosystems and Signature Schemes," in *Proceedings of CRYPTO 84 on Advances in Cryptology*. New York, NY, USA: Springer-Verlag New York, Inc., 1985, pp. 47–53.
- [27] J. Sobey, R. Biddle, P. C. Oorschot, and A. S. Patrick, "Exploring User Reactions to New Browser Cues for Extended Validation Certificates," in *Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security*, ser. ESORICS '08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 411–427.
- [28] A. Sotirakopoulos, K. Hawkey, and K. Beznosov, "On the Challenges in Usable Security Lab Studies: Lessons Learned from Replicating a Study on SSL Warnings," in *Proceedings of the Seventh Symposium on Usable Privacy and Security*, ser. SOUPS '11. New York, NY, USA: ACM, 2011, pp. 3:1–3:18.
- [29] J. Sunshine, S. Egelman, H. Almuhammedi, N. Atri, and L. F. Cranor, "Crying Wolf: An Empirical Study of SSL Warning Effectiveness," in *Proceedings of the 18th Conference on USENIX Security Symposium*, ser. SSYM'09. Berkeley, CA, USA: USENIX Association, 2009, pp. 399–416.
- [30] W. Tong, S. Gold, S. Gichohi, M. Roman, and J. Frankle, "Why King George III Can Encrypt," <http://randomwalker.info/teaching/spring-2014-privacy-technologies/king-george-iii-encrypt.pdf>, accessed: 2017-03-15.
- [31] S. Turner and B. C. Ramsdell, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification," RFC 5751, Jan. 2010.
- [32] T. Whalen and K. M. Inkpen, "Gathering Evidence: Use of Visual Security Cues in Web Browsers," in *Proceedings of Graphics Interface 2005*, ser. GI '05. School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada: Canadian Human-Computer Communications Society, 2005, pp. 137–144.
- [33] A. Whitten and J. D. Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, ser. SSYM'99. Berkeley, CA, USA: USENIX Association, 1999, pp. 14–14.

APPENDIX  
STATISTICAL ANALYSIS





							
		< 0.001*	0.058	< 0.001*	< 0.001*	< 0.001*	0.004*
	1		1	< 0.001*	1	0.882	1
	0.944	< 0.001*		< 0.001*	< 0.001*	< 0.001*	< 0.001*
	1	1	1		1	1	1
	1	< 0.001*	1	< 0.001*		< 0.001*	0.093
	1	0.121	1	< 0.001*	1		1
	0.997	< 0.001*	1	< 0.001*	0.91	< 0.001*	

TABLE V. P-VALUES OF WILCOXON RANK SUM TEST. FOR EACH CELL WE TESTED WHETHER THE SYMBOL OF THE CORRESPONDING ROW IS CONSIDERED LESS CONFIDENTIAL THAN THE SYMBOL OF THE CORRESPONDING COLUMN. \* INDICATES STATISTICAL SIGNIFICANCE ( $p < 0.05$ )















							
		< 0.001*	1	< 0.001*	0.518	< 0.001*	0.606
	1		1	< 0.001*	1	0.009*	1
	< 0.001*	< 0.001*		< 0.001*	< 0.001*	< 0.001*	< 0.001*
	1	1	1		1	1	1
	0.485	< 0.001*	1	< 0.001*		< 0.001*	0.515
	1	0.991	1	< 0.001*	1		1
	0.402	< 0.001*	0.999	< 0.001*	0.49	< 0.001*	

TABLE VI. P-VALUES OF WILCOXON RANK SUM TEST. FOR EACH CELL WE TESTED WHETHER THE SYMBOL OF THE CORRESPONDING ROW IS CONSIDERED EASIER TO MANIPULATE THAN THE SYMBOL OF THE CORRESPONDING COLUMN. \* INDICATES STATISTICAL SIGNIFICANCE ( $p < 0.05$ )















							
		< 0.001*	1	< 0.001*	0.99	< 0.001*	1
	1		1	< 0.001*	1	0.368	1
	< 0.001*	< 0.001*		< 0.001*	< 0.001*	< 0.001*	< 0.001*
	1	1	1		1	1	1
	0.01*	< 0.001*	1	< 0.001*		< 0.001*	0.994
	1	0.635	1	< 0.001*	1		1
	< 0.001*	< 0.001*	1	< 0.001*	0.006*	< 0.001*	

TABLE VII. P-VALUES OF WILCOXON RANK SUM TEST. FOR EACH CELL WE TESTED WHETHER THE SYMBOL OF THE CORRESPONDING ROW IS CONSIDERED LESS TRUSTWORTHY THAN THE SYMBOL OF THE CORRESPONDING COLUMN. \* INDICATES STATISTICAL SIGNIFICANCE ( $p < 0.05$ )

APPENDIX  
ONLINE SURVEY

## E-Mail Sicherheit

Vielen Dank für Ihre Teilnahme an dieser kurzen, anonymen Umfrage zur E-Mail Sicherheit!

**\*Required**

**Nutzen Sie sichere Kommunikationskanäle wie Signal, OTR etc.?**  
(Mehrfachnennung möglich)

- Signal
- WhatsApp
- Threema
- Jabber mit OTR
- Andere

**Was erwarten Sie von einer sicheren E-Mail? \***  
(Mehrfachnennung möglich)

- Nur Absender und Empfänger können die E-Mail lesen.
- Der Inhalt der E-Mail erreicht den Empfänger so, wie der Absender ihn gesendet hat.
- Der Empfänger kann sicher sein, dass die E-Mail vom Absender stammt.
- Die E-Mail erreicht den Empfänger.
- Der Absender erhält eine Empfangsbestätigung.
- Die Anhänge und Links der E-Mail sind ungefährlich. (z.B. Virenfrei)
- Other: \_\_\_\_\_

**Kennen Sie den Unterschied zwischen Verschlüsselung und digitaler Signatur? \***

- Ja
- Nein
- Nicht sicher

**Haben Sie ein Schlüsselpaar für die Verschlüsselung von E-Mails? \***

- Ja
- Nein

**NEXT**

Never submit passwords through Google Forms.

Fig. 8. First page of the survey.

## E-Mail Sicherheit

\*Required

### E-Mail Sicherheit

**Warum nutzen Sie keine E-Mail-Verschlüsselung? \***  
(Mehrfachnennung möglich)

- Brauche ich nicht
- Zu kompliziert
- Nutzt sonst auch keiner
- Für mich interessiert sich eh niemand
- Wollte ich mich schon ewig mit beschäftigen, bin ich aber noch nicht zu gekommen
- Other: \_\_\_\_\_

**Würden Sie Ihre E-Mails gerne verschlüsseln? \***

- Ja
- Nein
- Other: \_\_\_\_\_

BACK NEXT

Never submit passwords through Google Forms.

## E-Mail Sicherheit

\*Required

### E-Mail Sicherheit

**Welche E-Mail Verschlüsselungsverfahren nutzen Sie? \***  
(Mehrfachnennung möglich)

- PGP
- S/MIME
- Other: \_\_\_\_\_

**Mit wie vielen Ihrer Kontakte nutzen Sie E-Mail-Verschlüsselung? \***

- 1
- 2 - 3
- 4 - 10
- mehr als 10

BACK NEXT

Never submit passwords through Google Forms.

Fig. 9. Second pages of the survey. Participant has no email encryption key (left). Participant has an email encryption key (right).


## E-Mail Sicherheit

**\*Required**

### Symbole


Im Folgenden sehen Sie eine Reihe von Symbolen. Bitte geben Sie auf der Skala von 1 bis 5 an, mit welchem der vorgegeben Wörter Sie das Symbol eher verbinden. Wenn keines der beiden Wörter auf das Symbol zutrifft, wählen Sie bitte "Keine Assoziation".

**Was assoziieren Sie mit Symbol 1? \***



	1	2	3	4	5	Keine Assoziation
unsicher (1) - sicher (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
unverborgen (1) - vertraulich (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
manipulierbar (1) - nicht manipulierbar (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
suspekt (1) - vertrauenswürdig (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Was assoziieren Sie mit Symbol 2? \***



	1	2	3	4	5	Keine Assoziation
unsicher (1) - sicher (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
unverborgen (1) - vertraulich (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
manipulierbar (1) - nicht manipulierbar (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
suspekt (1) - vertrauenswürdig (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Was assoziieren Sie mit Symbol 3? \*



	1	2	3	4	5	Keine Assoziation
unsicher (1) - sicher (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
unverborgen (1) - vertraulich (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
manipulierbar (1) - nicht manipulierbar (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
suspekt (1) - vertrauenswürdig (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Was assoziieren Sie mit Symbol 4? \*



	1	2	3	4	5	Keine Assoziation
unsicher (1) - sicher (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
unverborgen (1) - vertraulich (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
manipulierbar (1) - nicht manipulierbar (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
suspekt (1) - vertrauenswürdig (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Was assoziieren Sie mit Symbol 5? \*




	1	2	3	4	5	Keine Assoziation
unsicher (1) - sicher (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
unverborgen (1) - vertraulich (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
manipulierbar (1) - nicht manipulierbar (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
suspekt (1) - vertrauenswürdig (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Fig. 10. First (left) and second part (right) of the third page of the survey.




Was assoziieren Sie mit Symbol 6? \*



	1	2	3	4	5	Keine Assoziation
unsicher (1) - sicher (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
unverborgen (1) - vertraulich (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
manipulierbar (1) - nicht manipulierbar (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
suspekt (1) - vertrauenswürdig (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Was assoziieren Sie mit Symbol 7? \*



	1	2	3	4	5	Keine Assoziation
unsicher (1) - sicher (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
unverborgen (1) - vertraulich (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
manipulierbar (1) - nicht manipulierbar (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
suspekt (1) - vertrauenswürdig (5)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

BACK NEXT

Never submit passwords through Google Forms.

## E-Mail Sicherheit

\*Required

### Allgemeine Fragen

Wenn Sie die Antwort nicht wissen, können Sie die Felder frei lassen.

Vertrauen Sie dem Inhalt eines Briefes eher als dem Inhalt einer Postkarte? \*

Ja  
 Nein

Würden Sie eine auf eine Postkarte gedruckte Rechnung bezahlen? \*

Ja  
 Nein

Eine verschlüsselte E-Mail ermöglicht es...  
(Mehrfachnennung möglich)

Gewissheit über die Identität des Absenders zu haben  
 Informationen nicht für Dritte einsehbar zu übermitteln  
 Gewissheit zu haben, dass der Inhalt der E-Mail nicht verändert wurde

Eine digital signierte E-Mail ermöglicht es...  
(Mehrfachnennung möglich)

Gewissheit über die Identität des Absenders zu haben  
 Informationen nicht für Dritte einsehbar zu übermitteln  
 Gewissheit zu haben, dass der Inhalt der E-Mail nicht verändert wurde

BACK NEXT

Never submit passwords through Google Forms.

Fig. 11. Third part of the third page of the survey (left) and the fourth page (right).

# E-Mail Sicherheit

\*Required

## Abschließende Fragen

Wie häufig nutzen Sie E-Mail? \*

- Mehr als 5 mal am Tag
- Mehrmals am Tag
- Einmal am Tag
- Alle zwei bis drei Tage
- Einmal pro Woche
- Noch seltener

Wie viele E-Mail-Accounts haben Sie? \*

- 1
- 2-5
- >5

Wie schätzen Sie Ihre Computererfahrung ein? \*

- |          |                       |                       |                       |                       |                       |         |
|----------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|---------|
|          | 1                     | 2                     | 3                     | 4                     | 5                     |         |
| Anfänger | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | Experte |

Wie wichtig ist Ihnen Ihre Privatsphäre? \*

- |       |                       |                       |                       |                       |                       |      |
|-------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|------|
|       | 1                     | 2                     | 3                     | 4                     | 5                     |      |
| wenig | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | sehr |

Haben Sie einen IT-Hintergrund?

- Ja
- Nein

In welchem Jahr sind Sie geboren? \*

Your answer \_\_\_\_\_

Geschlecht \*

- Weiblich
- Männlich
- Other: \_\_\_\_\_

Was ist Ihr höchster Bildungsabschluss? \*

- Mittelstufe oder vergleichbar
- Abitur oder vergleichbar
- Ausbildung oder vergleichbar
- Bachelor oder vergleichbar
- Master, Diplom oder vergleichbar
- Promotion

Befinden Sie sich noch in der Ausbildung? \*

- Ja
- Nein

Arbeiten Sie in einem Tätigkeitsfeld mit besonders schützenswerten Daten? (Ärztin, Anwältin, Journalistin etc.)

- Ja
- Nein

BACK

SUBMIT

Never submit passwords through Google Forms.

Fig. 12. First part (left) and second part (right) of the fifth page of the survey.