future internet

MDPI

Article

Managing Access to Confidential Documents: A Case Study of an Email Security Tool

Elham Al Qahtani [1], Yousra Javed [2,*], Sarah Tabassum [3], Lipsarani Sahoo [3] and Mohamed Shehab [3]

[1] Department of Software Engineering, University of Jeddah, Makkah 23445, Saudi Arabia; eaalqahtani@uj.edu.sa
[2] School of Information Technology, Illinois State University, Normal, IL 61761, USA
[3] Department of Software Information Systems, University of North Carolina, Charlotte, NC 28223, USA; stabass2@uncc.edu (S.T.); lsahoo1@uncc.edu (L.S.); mshehab@uncc.edu (M.S.)
* Correspondence: yjaved@ilstu.edu

Abstract: User adoption and usage of end-to-end encryption tools is an ongoing research topic. A subset of such tools allows users to encrypt confidential emails, as well as manage their access control using features such as the expiration time, disabling forwarding, persistent protection, and watermarking. Previous studies have suggested that protective attitudes and behaviors could improve the adoption of new security technologies. Therefore, we conducted a user study on 19 participants to understand their perceptions of an email security tool and how they use it to manage access control to confidential information such as medical, tax, and employee information if sent via email. Our results showed that the participants' first impression upon receiving an end-to-end encrypted email was that it looked suspicious, especially when received from an unknown person. After the participants were informed about the importance of the investigated tool, they were comfortable sharing medical, tax, and employee information via this tool. Regarding access control management of the three types of confidential information, the expiration time and disabling forwarding were most useful for the participants in preventing unauthorized and continued access. While the participants did not understand how the persistent protection feature worked, many still chose to use it, assuming it provided some extra layer of protection to confidential information and prevented unauthorized access. Watermarking was the least useful feature for the participants, as many were unsure of its usage. Our participants were concerned about data leaks from recipients' devices if they set a longer expiration date, such as a year. We provide the practical implications of our findings.

Keywords: access control; confidential emails; email security tool; end-to-end encryption; user study

Citation: Al Qahtani, E.; Javed, Y.; Tabassum, S.; Sahoo, L.; Shehab, M. Managing Access to Confidential Documents: A Case Study of an Email Security Tool. *Future Internet* **2023**, *15*, 356. https://doi.org/10.3390/fi15110356

Academic Editor: Claude Chaudet

Received: 17 September 2023
Revised: 14 October 2023
Accepted: 19 October 2023
Published: 28 October 2023

1. Introduction

Sharing of confidential information via email and text has become an ingrained aspect of day-to-day life due to the ease of access and availability of high-speed internet, computers, and smartphones. A recent survey demonstrated that 70% of emails contain sensitive information [1]. However, although standard email, by default, is not end-to-end encrypted with tools such as PGP and S/MIME, people still use it to share their personal information without any extra protections. This was shown by a recent study that analyzed 81 million sent email messages and found that only about 0.06% of them were encrypted [2]. People are more concerned about data leaks from recipients' devices rather than data during transit [3,4].

The adoption rate of end-to-end encryption and access control tools remains low. Although the usability and perceptions of several end-to-end secure messaging apps and email encryption tools have been investigated [5–11], user attitudes and concerns regarding the email encryption platforms that additionally provide built-in access control have not been investigated.

Our study seeks to understand user perceptions of an email security tool and how they use it to manage access control to their confidential information. The existing literature on email encryption tools mostly focuses on studying usability for performing encryption. They did not investigate access control (i.e., how users would use the tools' security features to manage access control to various types of sensitive content sent via email). We chose Virtru [12] over other secure email tools (such as Private Webmail (Pwm), ProtonMail, PGP (Mailvelope), Gmail Confidential Mode (GCM), and Tutanota) due to its usability and user preference [10,13], as well as fine-grained security features such as automatic key management, integration with users' existing Gmail accounts, allowing non-Virtru recipients to read encrypted email without Virtru being installed, and having built-in access controls that can help Gmail users control their emails after they are sent. Our study targets first-time Virtru users, since we were interested in first impressions and the likelihood of adopting this tool for sharing and receiving sensitive content via email. Additionally, we focus on the most common sensitive forms and documents users send via email, as shown by one Al Qahtani et al. [10]. Therefore, we investigate user perceptions of Virtru and how they use its security features to manage access control to three types of confidential information, namely medical, tax, and employee personal information, if sent via email. More specifically, our research questions are the following:

- RQ1: What are users' first impressions when receiving an end-to-end encrypted email using an email security tool?
- RQ2: How comfortable are users with sharing various types of confidential information (medical, tax, and employee) using an email security tool?
- RQ3: How do users use an email security tool's additional features to manage access control to their confidential information?

To answer these research questions, we conducted an interview-based user study on 19 participants. Our results showed that the participants' first impression upon receiving an encrypted email was that, due to the tool's interface, it looked suspicious, especially when received from an unknown person. However, after they were informed about the benefits of using the tool, they were comfortable sharing medical, tax, and employee information forms via the tool. Regarding managing access control to the three types of confidential email information, the expiration time and disabling forwarding were the most useful features for the participants for preventing unauthorized and continued access, and the only reason for not using them was to prevent unforeseen accessibility issues for the recipient. While the participants did not understand how the persistent protection feature worked, many still chose to use it, assuming it provided some extra layer of protection to prevent unauthorized access to all three types of confidential information. Watermarking was the least useful feature for the participants, irrespective of the type of confidential information in the email, as many were unsure of its usage. Our participants were more concerned about data leaks from recipients' devices (for instance, if their email account were to be compromised) if they set a longer expiration date (such as a year). Our findings provide practical implications that could help users share confidential information via end-to-end encryption tools.

2. Background

2.1. Virtru

Virtru is an end-to-end encryption platform that encrypts Gmail messages, attachments, and files stored on Google Drive, including Google Docs, Google Sheets, and Google Slides [12]. Virtru's simple Chrome extension keeps emails and files secure in Google Workspace, preventing Google and unauthorized parties from accessing information. Recipients can read a Virtru encrypted email without Virtru installed. Virtru uses a secure reader platform that allows users to access it right in their web browser by clicking on the Unlock Message button in their Virtru secure email. Upon verifying that they are an authorized recipient of that email or file, they can read and reply to the secure email directly from their browser.

In addition to encrypting messages and attachments, the security options of Virtru (see Figure 1) allow users to perform the following tasks:

- Add persistent file protection (PFP) to the encrypted file: This feature restricts access to only authorized users, even if it is shared or downloaded. New (unauthorized) users are allowed to request access to a file, and they will be forced to authenticate in their web browser prior to seeing the secure file in Virtru's Secure Reader. If someone requests access to a file that a user owns, then the recipient will receive an email notification from Virtru. Unauthorized users will not be granted access.
- Set an expiration date for an encrypted email or file: Users can restrict access after a particular point in time. If a recipient tries to access the content after its expiration, then they will receive a prompt indicating their access has expired. Expiration can also be managed after an email has been sent.
- Disable forwarding: This ensures that the recipients can access the encrypted content but will stop any additional users from gaining access to the message. If the original recipient sends the email to a new party, then the new user will not be added as an authorized user and will not be able to unlock the message.
- Add watermarking to a secure file: Recipients will only have access to content inside the Secure Reader, and their email addresses will be watermarked across the document. This feature prevents the recipient from downloading the file and keeping a local copy.
- Revoke (or reauthorize) access: Virtru even allows the sender to revoke access to specific recipients granularly at any time. If recipient access is revoked, then users will receive a prompt indicating their access has been removed.

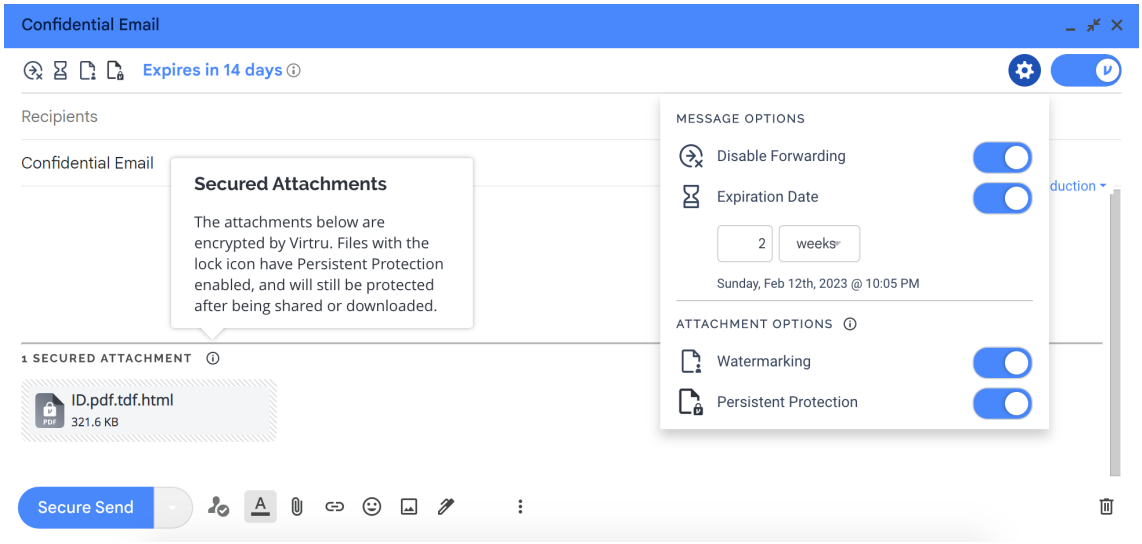


Figure 1. Virtru's email composition window along with its message security options.

Various universities and companies in the US utilize Virtru [14,15], allowing them to add an extra layer of security to their email messages. While Virtru works for a few email providers, it does not work with all web applications [16]. Furthermore, Virtru's private keys are associated with each device, and thus they cannot be used across devices. It also relies on a centralized server to verify that users own their respective email addresses and deliver private keys [17]. However, it uses a distributed architecture for unique symmetric key generation for each email [18]. By keeping content and encryption keys separate, only authorized parties are able to access unencrypted content, making it impossible for Virtru to decrypt user content [18]. In this way, data are kept private, even from Google or unauthorized parties. Although Virtru provides email transmission security, it does not protect against email accounts becoming compromised [19]. Therefore, Virtru offers secure encryption alternatives to portal-based encryption technologies. With these technologies, data can be encrypted, but this necessitates the use of separate systems by the recipient and

the user [20]. This set-up may grant vendors access to their data, potentially introducing the risk of data breaches.

2.2. Comparison of Popular Email Security Tools

This section contrasts 6 popular email security tools, namely Private WebMail (Pwm), Tutanota, PGP (Mailvelope), ProtonMail, Gmail Confidential Mode (GCM), and Virtru. These tools can either be integrated with the major email service providers (Gmail, Outlook, Yahoo, etc.) or need a separate website or tool from where the encrypted email should be composed, sent, and received. Most of these tools provide end-to-end email encryption or other forms of access control. Virtru provides both integration with email service providers and end-to-end encryption, as well as additional forms of access control such as setting an email expiration date and time. Table 1 summarizes this comparison.

Table 1. Comparison of popular existing email security tools.

Email Security Tool	Integration with Email Service Provider	Security Features	Threats
Private WebMail (Pwm) [21]	Yes, with Gmail via a browser extension	Automatic key management, end-to-end encryption	(1) An attacker that compromises the extension software (2) A malicious email service provider that impersonates the user or uses social engineering to obtain sensitive data
Tutanota [22]	No, needs a separate website	Key pair generation, end-to-end encryption, digital signature	(1) A malicious email service provider that provides software to access the user's data or to have their secure email account password guessed or stolen
PGP (Mailvelope) [23]	Yes, with many providers via a browser extension	Key pair generation, end-to-end encryption, digital signature	(1) An attacker who gains access to the user's email account could attempt to convince the user's contacts to encrypt messages with the attacker's public key instead of the user's true public key
ProtonMail [24]	Yes, with many providers	Key pair generation, end-to-end encryption, digital signature	(1) An attacker that compromises the software (2) A malicious email service provider that impersonates the user or uses social engineering to obtain sensitive data
Gmail Confidential Mode (GCM) [25]	Yes, with Gmail	Email expiration time, revoke access, disable forwarding, recipient authentication	(1) Lack of end-to-end encryption (2) Screenshots and screen recording to save a copy of the document
Virtru [12]	Yes, with Gmail via a browser extension	Automatic key management, end-to-end encryption, email expiration time, revoke access, recipient authentication, persistent file protection, disable forwarding, watermarking	(1) An attacker that compromises the extension software (2) A malicious email service provider that impersonates the user or uses social engineering to obtain sensitive data (3) Screenshots and screen recording to save a copy of the document

3. Related Work

This section describes the literature most relevant to our work.

3.1. Sharing Confidential Information

Users often need to share sensitive pieces of information, such as their social security number (SSN) and medical history, with trusted entities or possibly unknown recipients. Even though secure communication mediums are available, when privacy and security are considered minor factors, information will be shared without a formal security process [7,26]. To investigate sensitive data-sharing practices, Dell [27] commissioned a global survey of 2608 professionals handling sensitive data at companies. The survey results showed that 72% of employees were willing to share sensitive, confidential, or regulated company information without proper data security protocols in place. Also, Warford et al. [3] explored users' experiences with sending sensitive information via standard (unencrypted) email, which was the most common transmission method users used when they sent their sensitive documents, such as their financial information, health information,

and information related to their children. Users could share sensitive health information on social media (Facebook), which can negatively affect users' privacy [28,29].

Recently, users have been using end-to-end encrypted messaging applications (e.g., Whatsapp or Signal) to communicate privately. However, many users believe that SMS is more secure than WhatsApp and that they are not targeted by government and special service surveillance [30]. Users' decisions are affected more by peer influence than secure messaging apps' security features [26]. Similarly, even though WhatsApp users were informed that their messages were end-to-end encrypted, the participants noticed it but failed to understand the implications correctly. In our study, we wanted to understand how users perceive sending and receiving an end-to-end encrypted email via Virtru.

3.2. Adoption of Encryption Tools

Despite existing efforts toward raising user awareness about the security and privacy of their information and disseminating knowledge of how to utilize security and privacy tools, the adoption of encryption tools remains low. Taking this issue into account, Das et al. and Luca et al. [26,31] investigated the social processes influencing people's decisions to adopt a new security tool or practice. They found that social processes played a significant role in adopting new security tools and were effective at boosting security sensitivity. Two studies evaluated the differences in motivations for (not) following computer security practices [32] and smartphone security measures [33] based on the rational decision model. They found there were differences in users' perceptions regarding the benefits, risks, and costs associated with their decisions.

In other studies [6,34], researchers explored the reasons why secure email tools are not widely used by users. Several barriers have been identified within the workplace that prevent the adoption of encrypted email [6]. As a result of technical issues, usability issues, and social considerations, the participants did not consider using them frequently. In another study [35], the researchers found that average users were more likely to adopt secure email tools (e.g., Virtru) when integrated with webmail, such as Gmail. Ruoti et al. [13] evaluated three secure email systems, with Virtru being one of them. As a result of users' interactions with Virtru, fewer mistakes were made, and its perceived usability score was higher. We add to the existing literature by understanding the use perceptions of end-to-end encrypted email and how people use Virtru's security features to manage access control to their medical, tax, and employee information if sent via email.

3.3. Mental Models of Encryption

The cybersecurity research community has endorsed using secure communication methods to protect confidential information. Abu-Salma et al. [7] explored users' knowledge, experience, and perception of different communication tools. They found that many participants did not understand the fundamental concept of end-to-end encryption, which decreased their motivation to adopt secure tools. They identified several inaccurate mental models that underpinned participants' reasoning and decision making. Gaw et al. [6] conducted a study by interviewing a sample of users from an activist organization whose tasks required secrecy. The participants had different levels of technical sophistication and involvement with confidential information. They explored users' decisions about whether and when to encrypt emails and hypothesized that the organization's employees would have a strong motivation to encrypt emails. They found that the participants perceived only "paranoid people" or "people up to no good" would use encryption. Furthermore, a group of researchers [36] identified four mental models of encryption as a problem that illustrated how users perceived encryption.

Whitten and Tygar [37] found that non-adoption of secure encryption tools is due to usability issues, such as users having great difficulty using email encryption software. On the contrary, Renaud et al. [34] found that the non-adoption of secure encryption tools might not be entirely due to usability issues. Their results showed several fundamental issues, such as misaligned incentives, incomplete threat models, and insufficient

understanding of encryption. They also mentioned that just expanding the availability and usability of encryption functionality will not be enough to increase the adoption of end-to-end encryption. They suggested that creating comprehensive end user mental models related to email protection could increase adoption. Krombholz et al. [38] explored users' mental models of the "HTTPS" protocol. They found that end users often mistake encryption for authentication, significantly undervalue the security advantages of HTTPS, and neglect security indicators. Recently, users began using Gmail's Confidential Mode (GCM) to share confidential emails, believing it encrypts them [10]. While GCM does not encrypt email content, it does ensure confidentiality by using built-in access controls. We designed a video message to highlight the importance of using end-to-end encrypted email before our participants explored Virtru's security features.

4. Methodology

We first reviewed existing email security tools. However, we only focused on tools that are integrated with Gmail's web interface. For instance, Tutanota is another email security tool [22] that uses a separate website, and it is not integrated with Gmail's web interface. The service provider (Virtru) does not access unencrypted user content or decrypt it, and it has built-in access controls that can help Gmail users control access to their emails after they are sent. While Virtru provides security for email transmission and storage, it does not prevent attackers from compromising email accounts. In this study, we aim to understand how users perceive receiving end-to-end encrypted emails for the first time. In addition, we want to know how they respond to scenarios where sensitive information is sent via an encrypted email (e.g., when a user revokes an access message for a specific action) as well as how they manage access to the confidential information after it has been sent.

4.1. Recruitment

We recruited participants from the university via social media platforms. All interested participants completed a screening survey to determine their eligibility by ensuring they used Gmail accounts frequently, sent emails containing confidential information before, were at least 18 years old, had the ability to install the email security tool's extension on their computers, and had never used encryption tools via email. The eligible participants who agreed to participate were asked to read the consent form and participate in the interview via an online meeting. The participants who completed the study each received a USD 10 Amazon gift card. Our institutional review board approved the study (Protocol #). The average study duration was approximately 50 min.

4.2. Demographics

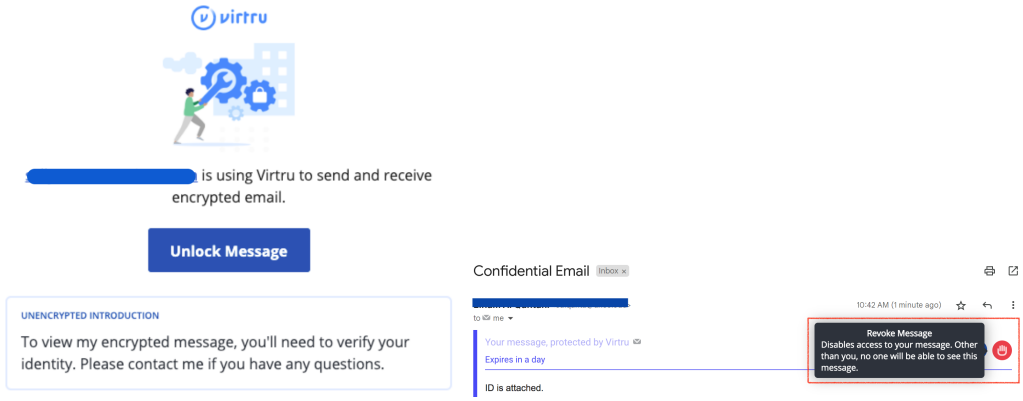
We interviewed 19 participants. Each participant was asked a set of demographic questions, such as age, gender, employment status, experience working in or studying computer-related fields, and the highest level of education completed. The majority of our participants (52.6%) were aged 20–29 years, 4 (21%) were aged 18–19 years, 2 (10.5%) were aged 30–39 years, 2 (10.5%) were aged 40–49 years, and 1 was aged above 50 years. Similarly, our participants were mostly female (N = 11, 57.9%), whereas eight participants were male (42.1%). Additionally, 57.9% of our participants were students, 26.3% were both employees and students, but a few of them (15.8%) were employed full time. Additionally, the majority of our participants did not have any experience working in or studying computer-related fields, and only wight of them had experience in these fields. Regarding the highest level of education achieved, nine of the participants had completed college or an associate's degree, seven had completed high school or some equivalent, and three had completed a master's degree.

4.3. Study Design

We conducted online interviews with 19 participants. Each participant was reminded of the importance of the consent form at the beginning of the interview. Once the par-

ticipants reconfirmed their interest in participating in our study, we began recording the interview sessions. Zoom's recording feature was used to record the audio and video. The participants were first asked a set of questions on how they perceived the security and privacy of Gmail. After that, we asked the participants to perform three tasks.

In the first task, we aimed to explore the participants' first impressions of receiving a secured email as shown in Figure 2a. We told the participants that we would send an email to their email address (without saying anything related to this investigated email security tool). Since these participants were receiving an encrypted email for the first time, we asked them to state their impression after opening this email, their rating of how easy they thought it was for them to understand the text in that email, and their rating of how familiar they were with the concept of "encrypted email" as described in the email.



(**a**) (**b**)

Figure 2. Email security tool (Virtru's) sender and recipient window after email is sent. (**a**) Recipient window. (**b**) Sender window showing revoke access option.

In the second task, we wanted to make sure that the participants were able to compose an email using the email security tool and explore its security features. Thus, the participants were first asked to watch a video that included security- and privacy-related information about this email security tool, the importance of using it, and a demo on adding the email security extension to their Google Chrome browser. The video transcript is available in Appendix B. Then, we asked them to think aloud while composing an email with this email security tool and explore its security features.

In the third task, the participants were provided with three hypothetical scenarios to understand how users manage the access control using the tool's security features in the encrypted email and how they rated their satisfaction and concern once they shared their confidential information via standard email and encrypted email. To perform this task, the participants were first asked to download three sensitive documents and forms (employee information form, medical history form, and W-9 (tax) form) on their personal devices. These forms were filled with fake information as an example. We asked the participants to imagine that the information in all these forms, including sensitive information such as social security numbers, belonged to them and that there was no need to change these forms. The three scenarios are described below:

- For the employee information form, we included employee information such as employee IDs and contact information. The given scenario was between the participants and the human resource department (HR). We asked them to imagine that they were newly hired by a company, and they were asked to email their employee information form to HR a week before they joined the company so HR could review it anytime during this week.
- For the medical history form, we included information about a person's health history (e.g., unhealthy habits and the patient's medical history). The given scenario was between the participants and a doctor's office. We asked them to imagine visiting a

new doctor for the first time, and the new doctor's office needed their medical history form before they went to their appointment, which was three days later.

- For the W-9 form, we included information about a person's tax information (e.g., account number, taxpayer identification number, and employer identification). The email was between the participants and a certified public accountant. We asked them to imagine that they had hired a certified public accountant (CPA) to prepare their taxes, and their W-9 form was shared with a certified public accountant (CPA) for 24 h.

All participants were asked to demonstrate how to change the the security settings based on the given scenario and think aloud while performing this task. After that, they were asked to review the email they sent and discuss what made them (not) choose the expiration date, disabling forwarding, watermarking, and persistence protection. We used the randomizer function to change the scenario order for all participants since there were three scenarios. Lastly, the participants answered a set of demographic questions. The interview questions, scenarios, and instructions are listed in Appendix A.

4.4. Analysis

We collected both quantitative and qualitative data. For the quantitative data, we used the Wilcoxon signed-ranks test to analyze the ordinal data for users' satisfaction and concerns regarding using standard email and an end-to-end encryption email. The Wilcoxon signed-ranks test is a nonparametric statistical hypothesis test [39]. Since, the sample size in our study was small, and the data were not normally distributed, we used this test over the Student's t-test. We used Statistical Package for the Social Sciences (SPSS) for quantitative analysis. For the qualitative data, we utilized an inductive approach. The data were first coded independently by two researchers in Microsoft Excel to avoid any bias and to capture all possible codes. The coding criteria used were as follows. We looked for patterns in the data to develop themes that could explain the patterns in our data. These patterns were then categorized into themes. We then discussed, refined, and updated the two sets of coded data to resolve any disagreements. Therefore, the Cohen's Kappa (inter-rater agreement) test was not conducted [40].

5. Results

5.1. Opinions about Encrypted Emails

Before answering our first research question and exploring the security features of end-to-end encrypted email, we wanted first to evaluate our participants' understanding of the encryption concept. We asked the participants several questions, such as (1) rate familiarity with the term "encryption" on a scale from 1 to 4 (1 = I have never heard of this, 2 = I have heard of this, but I do not know what it is, 3 = I know what this is, but I do not know how it works, and 4 = I know generally how this works), (2) describe what encryption means, (3) explain whether there is anyone besides the recipient who can read the email content, and (4) explain whether Google gives the government direct access to their email if requested.

We found that a majority of the participants (52.6%, N = 10) knew what encryption was, but they did not know how it works, whereas a few participants (N = 3) generally knew how encryption works. However, several participants (26.3%, N = 5) still did not know what encryption was, but they had heard of it.

With regard to explaining what encryption means, we found that the most pronounced description was information protection (12/19). For instance, one of the participants (P6) said, *"I believe encryption is just like protecting your information, so that I'd assume like hackers and other people, and like spam bots can't get access to it beyond that, or like how it actually works and stuff."* The next frequent phrase was scrambling messages (7/19). In the words of P10: *"Encryption is scrambling, or like scrambling the data in such a way, so that any third party cannot understand what's talking in between the original parties."* Other phrases used by the participants were data encoding and decoding (4/19), data encapsulation (1/19), communication safety (2/19), prevent unauthorized access (2/19), uses codes and keys

(5/19), security system (1/19), uses numbers and blockchain (1/19), web security and privacy (1/19), and uses password (1/19). Table 2 summarizes the themes emerging from the participants' responses about what encryption means.

Table 2. Participant opinions about what encryption means.

Encryption Meaning	No. of Participants
Information Protection	12/19
Scrambling Messages	7/19
Data Encoding and Decoding	4/19
Communication Safety	2/19
Prevent Unauthorized Access	2/19
Uses Codes	2/19
Uses Keys	3/19
Security System	1/19
Uses Numbers and Blockchain	1/19
Web Security and Privacy	1/19
Uses Password	1/19
Data Encapsulation	1/19

Additionally, when asked whether the participants thought there was anyone besides the recipient who could access the content of their email, we found that only two participants did not know if a third party could access and read their emails. Most participants (N = 8, 42.1%) did not think anyone could read and access the content of their emails. For example, there were the following two comments: *"I don't think anybody reads my email because I think Gmail as an end-to-end encryption model*, and *"because Gmail has protected the email so only the person who I'm sending it to can see it."* The remaining participants (N = 9, 47.4%) believed that there was someone or some third party who could access and read their emails. They stated that hackers (3/19), Gmail or Google employees (6/19), university employees (2/19, with a comment shown below), third parties (2/19), the government (1/19), and police (1/19) could access their emails, aside from the intended recipients.

Participant P14 commented, *"I would say if I'm using something like my school email, they definitely probably can keep tabs on that make sure I'm not doing anything sketchy with my personal email. I don't know of anybody in particular, but I'm sure at some point in time, someone has been able to access my account and read them."*

Table 3 summarizes the themes of the participants' opinions on who could access their emails aside from the intended recipients.

Table 3. Participant opinions about who can access their emails aside from the recipients.

Entities with Access to the Email	No. of Participants
None	7/19
Hackers	3/19
Gmail employees with access	3/19
Google employees with access	3/19
University employees with access	2/19
Third parties	2/19
Anyone with CC	1/19
Government	1/19
Police	1/19

Regarding Google giving the government direct access to the participant's emails if requested, we found that the majority of the participants (N = 10, 52.6%) believed that Google gives the government access to their emails when requested, 31.6% of the participants (N = 6) did not think so, and 15.8% did not know whether Google gives the

government direct access to their emails. We found that 11 out of 19 participants mentioned that Google needs valid reasons to give the government direct access to their emails. Many participants shared that investigating crime-related cases (8/19) and having a warrant (5/19) can allow the government access to case-related emails. For example, one of the participants (P7) commented, *"If they have a warrant, and they do have like evidence that if there were a crime being committed, then I believe they would be able to give the access."* The other circumstances mentioned by the participants for Google to give the government direct access to their emails were being required by law enforcement (2/19), depends on the requester (1/19), and needs user permission (1/19).

Summary. The majority of our participants demonstrated awareness of encryption technology but did not understand how it works. Some participants thought that no one besides the recipient could read or access the emails. However, the majority of the participants believed that Google gives the government direct access to their emails when requested, especially if the email is related to a criminal case or law enforcement has a warrant to investigate it.

5.2. First Impressions of an Encrypted Email

To answer the question of *what users' first impressions are when receiving an encrypted email using an email security tool*, we asked the participants to explore the encrypted email since they did not have any previous experience with sending and receiving encrypted emails. Virtru allows non-Virtru recipients to read an encrypted email without installing it and access the email content via Secure Reader. Therefore, the participants could perform this task without installing the email security tool. Figure 2a shows a similar email presented to the participants. The participants were asked what their impression was when they saw this email. They were also asked how they would respond if they received this email from an entity they did not know and why as well as how they would respond if they received this email from an entity they knew. Additionally, they were asked how easy or difficult they think it would be for them to understand the content in this email and how familiar they were with the concept of "encrypted email" as described in this email.

Regarding the themes of participants' reactions when they first saw an end-to-end encrypted email, two perspectives were categorized when looking at the findings. Some participants had negative impressions when they first saw this encrypted email, such as it looking suspicious (7/19), seeming like spam/phishing email (4/19), or having a confusing interface (1/19). Those who had a positive impression said that it needed verification which felt safe (5/19), had encrypted email content (2/19), seemed more secure and serious (4/19), and had a friendly interface (1/19), as shown in Table 4.

Table 4. Participants' first impressions about emails encrypted using Virtru.

First Impression	# Participants
Looks suspicious	7/19
Needs verification	5/19
Seems like spam or phishing email	4/19
Encrypted message	2/19
Seems more secure	4/19
Confusing interface	1/19
Similar to regular email	1/19
User-friendly interface	1/19

When asked how they would respond if they received such an email from an entity they did not know, the majority of the participants mentioned they would not open it (8/19). For instance, one of the participants (P17) commented, *"If I have received an email from an unknown person, I wouldn't open it."* Four participants stated that they would delete the email, two participants would mark it as spam, and one participant mentioned blocking

the email address. Other responses were read it (3/19), verify the sender's email address (2/19), check links (1/19), analyze (1/19), and reply (1/19).

In contrast, when we asked how the participants would respond if they received this email from an entity they knew, we found that 7 out of 19 participants would open it. One participant (P1) said, *"Well, I wouldn't hesitate. I just clicked the Unlock Message button, and I just proceeded to go along with what was happening"*, and four participants mentioned that they would contact the sender before opening. For instance, (P3) commented, *"Just ask the sender if this was meant to be sent to me or if it was sent in error"*, and only one participant mentioned that they would feel safe when receiving this kind of email from a known entity.

Moreover, we found that most of our participants (N = 18, 94.8%) stated that it was (somewhat or very) easy for them to understand the text in this email, while 52.6% of the participants were moderately familiar with the concept of encrypted email as described in this email (Figure 2a). A few participants (N = 4, 21.1%) were not at all familiar with the concept of "encrypted email" described in this email, whereas another four participants were slightly familiar with this concept.

Summary. For a majority of the participants, the first impression of an encrypted email was that it looked suspicious, and if they received any email like this from an unknown person, they would not open it. However, if the sender were a known entity, then most of the participants stated that they would open the emails after confirming with the entity first. The content of this email was easy to understand, and about half of the participants were familiar with the concept of encrypted email depicted by the tool.

5.3. Sharing Confidential Information

We wanted our participants to explore the security options that the email security tool offers and to be able to compose an email with it easily before evaluating their interactions with the encrypted email when sharing their sensitive information. We first asked them to watch a video (see Appendix B for the video transcript) that included security- and privacy-related information about the investigated email security tool (Virtru), the importance of using it, and a demonstration of adding its extension to their Google Chrome browser. After performing this task, the participants added the email security extension to their Google Chrome browser. Then, they were asked to compose an email using this extension and think aloud while performing this task. All participants performed this task without any difficulties. After the participants sent their emails, they received a notification informing them they had successfully sent their first encrypted email with this email security tool.

To answer the research question, (*"How comfortable are users with sharing various types of confidential information using this email security tool, namely medical, tax, and employee?"*) the participants were provided with three hypothetical scenarios to understand (1) how they utilized security features to manage the access control for the encrypted email and (2) how they rated their satisfaction and concern once they shared their confidential information via standard email and encrypted email. First, the participants downloaded three documents (employee information form, medical history form, and W-9 form) on their personal devices. These forms had been filled out with artificial information as an example based on the given scenario. Therefore, we asked the participants to imagine that the information in these forms, such as the social security number (SSN), belonged to them. The order in which the three scenarios were presented to the participants was randomized.

5.3.1. Scenario 1: Employee Information Form with Human Resources

In this scenario, we first asked the participants to review the employee information form, state whether they considered it to include sensitive information, and rate this form's information sensitivity. All participants stated that they considered this employee information form to include sensitive information. They provided many examples of included sensitive information, such as an employee ID, SSN, and contact information. We found that 21.1% of the participants rated this form's information sensitivity as "moderately sensitive", and 78.9% rated it as "very sensitive".

After providing the hypothetical scenario, all participants performed this task by sending their forms to the HR's email address. Then, the participants rated their satisfaction with sharing their SSNs in the employee information form using their regular or standard email and secured email. Also, they were asked to rate their concerns regarding sharing their SSNs in the employee information form with HR using their regular or standard email and secured email.

The Wilcoxon signed-ranks test showed that the participants' satisfaction with sharing SSNs in the employee information form via secured email was rated higher by the participants compared with sharing via standard email ($Z = -3.6$, $p < 0.001$ (Table 5)). Therefore, we found that all participants (100%) rated their satisfaction as moderately or very satisfied if they shared their SSNs with HR using secure email compared with standard email (26.4% rated it as moderately or very satisfied). Also, the test indicated that the users were more concerned if they shared their SSNs with HR via regular or standard email than secured email ($Z = -3.8$, $p < 0.001$ (Table 5)). Furthermore, 63.2% of the participants were not at all concerned if they shared their SSNs with HR using secure email compared with standard email (47.4% rated themselves as "very concerned").

Table 5. Participants' ratings of satisfaction and concerns about sharing confidential information via standard email and end-to-end encrypted email.

	Sharing via Standard Email (Mean)	**Sharing via Email Security Tool (Mean)**	**Z Score**	***p* Value**
Users' Satisfaction: Employee form	Mean = 1.8	Mean = 3.7	$Z = -3.6$	$p < 0.001$
Users' Satisfaction: W-9 Form	Mean = 1.4	Mean = 3.7	$Z = -3.9$	$p < 0.001$
Users' Satisfaction: Medical Form	Mean = 1.6	Mean = 3.7	$Z = -3.8$	$p < 0.001$
Users' Concerns: Employee Form	Mean = 3.2	Mean = 1.4	$Z = -3.8$	$p < 0.001$
Users' Concerns: W-9 Form	Mean = 3.2	Mean = 1.3	$Z = -3.7$	$p < 0.001$
Users' Concerns: Medical Form	Mean = 3.4	Mean = 1.3	$Z = -3.9$	$p < 0.001$

5.3.2. Scenario 2: W-9 Tax Form with a Certified Public Accountant

In this scenario, we first asked the participants to review the W-9 form, state whether they considered it to include sensitive information, and rate this form's information sensitivity. All participants stated that they considered this employee information form to include sensitive information, such as SSNs and account numbers. We found that 94.7% of the participants rated this form's information as "very sensitive".

Following the hypothetical scenario, the participants were asked to email this form to the CPA's email address. After that, the participants rated their satisfaction with sharing their SSNs in the W-9 form with the CPA using their regular or standard email and secured email. Also, they were asked to rate their concerns about sharing their SSNs in the W-9 form with the CPA using their regular or standard email and secured email.

We used the Wilcoxon signed-ranks test to compare participants' satisfaction with sharing sensitive information via standard email and secure email. The test indicated that the participants' satisfaction with sharing SSNs in the W-9 form via secured email was rated higher than sharing SSNs in this form via standard email ($Z = -3.9$, $p < 0.001$ (Table 5)). Therefore, we found that all the participants rated their satisfaction as moderately or very satisfied when sharing their SSNs with the CPA using secure email compared with standard email. We also conducted another Wilcoxon signed-ranks test and found that the participants were more concerned if they shared their SSNs with the CPA via regular or standard email compared with secured email ($Z = -3.7$, $p < 0.001$ (Table 5)). Therefore, we found that 68.4% of the participants were "not at all concerned" if they shared their SSNs with the CPA using secure email compared with standard email.

5.3.3. Scenario 3: Medical Health Form with a Doctor's Office

For the third scenario, we first asked the participants to review the medical history form, state whether they considered it to include sensitive information, and rate this form's information sensitivity. All participants stated that this form included sensitive information (e.g., medical history, health habits, and SSNs). We found that 78.9% of the participants rated this form's information sensitivity as "very sensitive".

After providing the hypothetical scenario, the participants were asked to email this form to a doctor's office. The participants rated their comfort with sharing their SSNs in the medical history form with the doctor's office using their regular or standard email and secured email. Also, they were asked to rate their concerns about sharing their SSNs in the medical history form with the doctor's office using their regular or standard email and secured email.

We performed the Wilcoxon signed-ranks test, which indicated that the participants' comfort with sharing SSNs in the medical history form via secured email was rated higher compared with sharing it via standard email ($Z = -3.8$, $p < 0.001$ (Table 5)). All participants rated their satisfaction as moderately or very satisfied if they shared their SSNs with the doctor's office using secure email compared with standard email. Also, the test indicated that the users were more concerned if they shared their SSNs with the doctor's office via regular or standard email than secured email ($Z = -3.9$, $p < 0.001$ (Table 5)). We found that 73.7% of the participants were "not at all concerned" if they shared their SSNs with the doctor's office using secure email compared with standard email (52.6% said they were "very concerned").

Summary. The participants were comfortable with sharing their confidential information via an encrypted email. Our results showed that the participants were more satisfied when they shared their medical, tax, and employee information forms via secure email compared with their regular email. However, they expressed that they would be more concerned if they shared these confidential forms via regular email instead of an encrypted email.

5.4. Security Settings

To answer the research question, (*"How do users use the email security tool's additional features to manage access control to their confidential information?"*) the participants were asked to open secured emails that they sent earlier and to review what security options (e.g., set an expiration time, enable disable forwarding, add watermarking, or add persistent protection) they enabled based on the given scenarios, as shown in Table 6. They were also asked to provide their reasons for selecting or not selecting security features.

Table 6. Percentage of participants who did or did not select security options for each sensitive content type.

Content Type	Security Features	Selected	Not Selected
Employee	Expiration Time	68.4%	31.6%
	Disable Forwarding	68.4%	31.6%
	Watermarking	36.8%	63.2%
	Persistent Protection	84.2%	15.8%
W-9	Expiration Time	84.2%	15.8%
	Disable Forwarding	89.5%	10.5%
	Watermarking	57.9%	42.1%
	Persistent Protection	94.7%	5.3%
Medical	Expiration Time	89.5%	10.5%
	Disable Forwarding	63.2%	36.8%
	Watermarking	31.6%	68.4%
	Persistent Protection	84.2%	15.8%

5.4.1. Expiration Time

Selected:

For the employee form, 14 out of 19 participants stated that they would select the expiration time feature. When we asked why they would select this option, 13 participants stated that it would be sufficient access time for the scenario. Only one participant mentioned that he would choose this option to avoid access afterward. For the W-9 form, 13 participants mentioned selecting an expiration time to remove continued access. Only one participant would select this because of the urgency of document access. For the medical form, 16 participants selected this feature to allow access for limited time.

Participant P7 commented: *"I would like it to disappear since it is a 9 W form that I'm sending. Once it has been looked at by the accountant. I would like it not to still be in the email. So that my people aren't able to access it after those 24 h, and it's not just sitting there because, you know, people don't always usually go back and delete all their emails. So it just kind of sits there. So, having this expire in a day, would be like really convenient."*

Not Selected:

Five of our participants did not select the expiration time option for the employee form, and they would do so because the company may need future access. One participant mentioned avoiding a bad impression, and another participant shared that it was not important to him. For the W-9 form, three participants chose not to select the expiration time to allow future access. Also, one participant mentioned that it was not needed for that document. However, for the medical form, only two participants stated that this feature was not needed.

Participant P6 commented: *"Because even though they said it would last for a week. I don't know how fast or how slow HR works, and so I don't want to set a bad impression by sending them something, and then, once they get around accessing it, they find that it's already expired and gone."*

5.4.2. Disable Forwarding

Selected:

The majority of the participants selected the disable forwarding option to prevent unauthorized access and resharing. This reason was most prominent for the employee form (13/19, with a comment shown below), the W-9 form (16/19), and the medical form (9/19).

Participant P6 commented: *"because, as my public accountant, they should be the ones handling my information. If they're sending my personal information to others, there's something wrong with them, and I need to hire somebody else."*

Not Selected:

The main reason for not selecting this option for the employee form was to enable sharing access, as stated by four participants. For the W-9 form, one participant mentioned they trusted the recipient, and another one mentioned allowing resharing as the reason for not selecting this option. For the medical form, their reasons were to allow sharing with other departments (5/19) and having **other protections in place** (1/19). Moreover, some participants thought this feature was not needed for the following documents: the employee form (1/19), W-9 form (1/19), and medical form (3/19).

Participant P10 commented: *"Because I thought that the doctors might need the information, to share it with the other person (in the same department) Other like responsible persons so that they can actually get their insights on my history."*

5.4.3. Watermarking

Selected:

The most common reason for selecting the watermarking feature was the extra layer of protection, as stated by three participants for the employee form, two participants for the W-9 form, and five participants for the medical form (a comment is shown below). Other reasons for selecting this option for an employee form were curiosity, document

protection from unauthorized access, and prevention of document copying. For the W-9 form, participants selected this option to protect personal information (3/19), ensure data integrity (2/19), and prevent copying (1/19). For the medical form, one participant stated distinguishing between the original document and its copy as the reason for using this feature.

Participant P18 commented: *"I think watermarking just adds another layer of protection in case someone wants to download the file and send it to a third party on a different email... So, for instance, if I get an email back saying, Hey, we need you to take the watermarking off, for whatever reason, then I would resend it and take it off."*

Not Selected:

The main reason for not selecting the watermarking option was that the participants were unsure of the usage, since three participants for the employee form, six participants for the W-9 form, and three participants for the medical form mentioned this. Many participants shared that they thought this option was not needed for these documents: the employee form (10/19), W-9 form (4/19), and medical form (9/19). Additionally, people did not select this to avoid a bad impression about access (1/19), because the document was already secure (1/19), and it being inappropriate to use this feature (1/19) for the employee form. For example, participant P5 commented, *"Since this is going on the company file, I figured that was inappropriate the situation because they can just maybe do that themselves, or you know I trust them to not need to have this on."*

5.4.4. Persistent Protection

Selected:

The two major reasons for choosing the persistent protection feature were the extra layer of security (employee form: 6/19, W-9 form: 9/19, and medical form: 9/19) and to prevent unauthorized access (employee form: 7/19, W-9 form: 8/19, and medical form: 9/19). Additionally, one participant mentioned preventing misuse of personal information in the employee form. For the medical form, four people stated they were preventing resharing. For example, participant P9 commented, *"So I want that document to be secured, even if someone downloads it or takes it out of the system, or even offline. But then tries to forward it later; all of that is tied. So I know that that they won't be able to pass that information along digitally without it being corrupted."*

Not Selected:

The majority of the participants who did not select the persistent protection option said that they thought this option was not needed. One participant stated this reason for each of the three forms. For the employee form, one participant was not sure of the usage. Also, another participant wanted to prevent accessibility or usability issues by not using the persistent protection feature (e.g., this comment was mentioned by P12: *"Don't want to make it hard to circulate within the company."*)

5.5. Expectations from the Recipient's Side

After the participants shared their documents based on the given scenarios, they were asked whether they thought the emails they sent could be misused if they set a longer expiration date, such as a year. According to the scenarios, the employee information form needed to be accessed by HR during one week, the medical history form needed to be accessed by the doctor's office for three days, and the W-9 needed to be accessed by a CPA for 24 h.

We found that the majority of our participants agreed that their encrypted emails could be misused by the same entities if they set a longer access time. The participants provided their reasons for the possibility that their emails could be misused, since there was no trust in the entities' attitudes that allowed them to misuse their information (12/19). For example, participant P17 commented, *"I think there's always the possibility that the information could be*

misused, because of the fact that it's being sent to a human. You could also have someone who was in that position who was not an honest and trustworthy person, and because they would have access to my social security number, there is a possibility that they could misuse that."

Also, the participants were concerned about entities taking screenshots or copies of their information (3/19). For example, participant P8 commented, *"I believe that if I set the expiration date for a year, it gives them enough time to copy the entire document, and they won't even need the document at all. They have a hard copy for themselves to manipulate."*

Additionally, a few participants discussed the possibility that someone could hack the entities' email accounts and access their information if they set a long access time (3/19). For instance, participant P16 commented, *"If you set it for like a year, that gives more time for people to, I guess, hack into either [their] Gmail or the other way is, they could exceed the information when they're not supposed to, and then use it against you."*

On the other hand, we found that four participants did not think the email could be misused even if they set a longer expiration date. The prominent reason was that the email was secure due to encryption (e.g., the comment shown below), and the attachment features were enabled, such as persistent protection and watermarking.

Participant P1 commented, *"Because these emails are actually encrypted and not just sent out, it'd be a lot harder for them to be accessed by third-parties or anyone I didn't intend for it to be sent to. It'll be hard for them to access it. Each email had documentation; I made sure to secure that. So I feel like even after or during a year, it'd be hard for them to be viewed."*

We also asked the participants how they would handle the situation where they accidentally sent an email to the wrong person and they realized it afterward. In this task, the participants demonstrated how they would change the security setting using one of the emails they sent.

Half of our participants (N = 9) initially suggested changing the security settings. The expiration time on their email content was changed to one minute. In addition, many of them mentioned revoking email access after that.

Participant P8 commented, *"I would change the security setting...change the expiration date to a minute, so that immediately, the email, after a few minutes, gets deleted from the site... Along with these settings, I would first select this red route. It is revoked."*

Nine other participants pointed out the Revoke Access button on the top of the email window, as shown in Figure 2b, which disables access to the email content and attachments. For example, participant P19 said, *"Before Virtru... Google doesn't allow me to undo it after 30 s or something, but I can delete the email sent accidentally just by using revoke the message. That's a great advantage of using Virtru cause without that; the email once sent, we cannot do anything."*

6. Discussion

Perceptions of the encryption concept. End-to-end encryption is still rarely used by non-expert users, even in target groups such as journalists [41]. In our study, most participants professed awareness of encryption technology, but they did not understand how it works (Section 5.1). However, many users still believed that no one could access their email through Google or a third party. Misconceptions were still present. For instance, P10 commented, *"Because I think it's TLS encrypted, and I think it's end-to-end encrypted. Anyone in between, like any person that's staying in the middle, I think, he or she won't be able to extract the information."* The user might have a misunderstanding between point-to-point encryption and end-to-end encryption because Virtru hides the underlying encryption process. The majority of our participants showed their general understanding of the encryption objective, whereas a few participants used technical words to describe the encryption concept, which suggests that they have partially correct mental models of end-to-end encryption. Therefore, the lack of our participants' understanding of the encryption process is still a problem, which confirms the findings of previous studies [30,36,42]. Educating users about how encryption works with an accurate model is a challenging task. The researchers in [36] recommended aligning communication efforts and designs with the functional models of encryption that users already possess.

Interaction with encrypted emails. Before providing our participants with details about the security tool, most of them had negative impressions when they first saw this encrypted email by stating that it seemed suspicious or like a spam or phishing email, particularly if it came from an unknown entity, whereas those who had a positive impression felt safe since it seemed secure, required users to verify themselves before unlocking the encrypted message, and had a friendly interface. Even though Virtru has good usability [13], improving the usability of encryption is not enough. There is a need to improve risk communication that can be delivered to users about encryption. Our participants were introduced to the importance of utilizing end-to-end encrypted email (via video) to help them understand the benefits of using encrypted emails. When the participants composed an encrypted email for the first time, no one faced any difficulties after watching the video. They were comfortable using security features (e.g., setting an expiration time and disabling forwarding). We also found strong evidence that our participants were more satisfied when they shared their medical, tax, and employee personal information via end-to-end encrypted email (secure email) rather than regular email. Also, they were more concerned about sharing their sensitive information via regular email without using secure email. These findings confirm prior work [43–45] by providing evidence of the effectiveness of video-based risk communication on users' risk perceptions and actual behavior in the security context.

Expectations from the recipient. Previous research [46] has shown that users are most concerned about controlling their emails' permanence (ephemerality), which limits their ability to control how their sensitive information would be used. Our participants found the expiration date feature in the encrypted email useful, along with other security features, to limit access to their medical, tax, and employee information to a specific period. However, when we asked them whether they thought the emails they sent could be misused if they set a longer expiration date, such as a year, our participants did not trust the recipients' attitudes as they could take screenshots of their information, or the recipients' email accounts could be hacked. Overall, they were more concerned about data leaks from recipients' devices rather than from the sender's account, which confirms existing findings [3].

7. Limitations and Future Work

Our work is not without limitations. Firstly, we were unable to recruit a more diverse sample despite advertising the study on a university mailing-list, social media, Craigslist, and through flyers. However, a majority of the interested individuals who ended up completing the study were students. Therefore, our results may be considered exploratory and cannot be generalized for all users. Including non-university participants, such as less tech-savvy users or employees who frequently share work-related sensitive information, would enhance the study by ensuring a more diverse sample.

We asked simple questions to evaluate our participants' understanding of encrypted emails, such as whether someone could access their email content. Further research is needed to ask detailed and less technical questions to measure users' understanding between point-to-point and end-to-end encryption using secure communication tools. Additionally, we targeted first-time users, since we were interested in first impressions and the likelihood of its adoption for sharing and receiving sensitive content via email. A follow-up study is needed to compare the findings in this study with those of existing Virtru users.

Virtru provides more controls to track the emails in the control center after they have been sent (e.g., checking if the email is accessed or shared by the recipients, providing validation reports, and listing all authorized recipients who access the email). It would be interesting to investigate what happens beyond such tracking, such as with the following questions:

- Do users review their confidential emails to check if they have been accessed by recipients?

- Are users concerned about their emails if they stay in the recipient's email inbox based on the set expiration date?
- What are the users' expectations of the email deletion concept (e.g., the undo feature vs. revoking access at any time)?

A future study can be conducted to evaluate the effectiveness of risk communication notifications added to Gmail's web interface via a browser extension once Gmail users share sensitive data or confidential attachments.

Aside from end-to-end encryption of email data, our participants were comfortable managing its access control using the expiration date and disabled forwarding features. However, some participants were confused about the attachment features (watermarking and persistent protection). A future study is needed to evaluate the impact of risk communication by presenting scenarios highlighting the importance of using the attachment features tailored to specific populations, such as a scenario showing how students watermark authorized recipients' names on their academic papers or school projects when sharing with other students to prevent recipients from leaking their sensitive data.

8. Conclusions

The end-to-end encrypted email adoption rate is still low, and many users struggle to make use of these tools due to usability issues, lack of understanding, and misconceptions. We conducted a study on 19 participants to understand user perceptions of an end-to-end encryption platform and how they used it to manage access control (expiration times, disabling forwarding, persistent protection, and watermarking) to confidential information, such as medical, tax, and employee information sent via email. Our results show that the tool's emails were perceived as suspicious, especially when they came from unknown senders. After the participants learned about the tool's features and how it works, they were comfortable sharing medical, tax, and employee information with it. The expiration time and disable forwarding features were most useful for preventing unauthorized access and continued access to the three content types. Many participants chose to use persistent protection even though they did not understand how it worked, believing it would provide an additional layer of security and prevent unauthorized access. Watermarking was the least useful feature for the participants, as many were unsure of its usage. Our participants were concerned about data leaks from recipients' devices if they set longer expiration dates. Furthermore, our findings provide practical implications that could help users to share confidential information via end-to-end encrypted communication media.

Author Contributions: Conceptualization, E.A.Q. and Y.J.; methodology, E.A.Q.; investigation and formal analysis, E.A.Q., S.T., Y.J.; resources, E.A.Q., M.S.; data curation, E.A.Q., S.T., L.S., Y.J.; writing—original draft preparation, E.A.Q., Y.J., S.T., L.S.; writing—review and editing, E.A.Q., Y.J.; visualization, E.A.Q. and Y.J.; supervision, M.S.; project administration, E.A.Q. and Y.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding. The APC was funded by Illinois State University.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Interview Questions

- How would you rate your familiarity with the encryption concept on a scale from 1 to 4 (1: I've never heard of this, 2: I've heard of this but I don't know what it is, 3: I know what this is but I don't know how it works, 4: I know generally how this works)
  In your own words, could you describe what encryption means?
- When you send an email to an entity using Gmail, do you think there's anyone besides the person who can read and access the content of your email?
  (YES) Who do you think reads your email?

(No) Why do you not think no one reads your email?
(I do not know) Could you please elaborate?

- Do you think that Google gives the government direct access to your email if it is requested?
  Why do you think that?
- How did you know about our study?

Task 1

(Researcher's Script) *I will send you an email for the first task and then ask you a few questions about this task. Could you please send me your email address in the Zooms' Chat so I can send you an email?*

Ok, when you open the email that I sent, please share your screen and check the email for a few seconds.

- What is your impression when you see this email?
  How would you respond if you received this email from an entity you do not know? Why?
  How would you respond if you received this email from an entity you know? Why?
- Please rate how easy or difficult you think it would be for you to understand the text in this email on a scale from 1 to 4 (1: Very difficult, 2: Somewhat difficult, 3: Somewhat easy, 4: Very easy)
- Please rate how familiar you are with the concept of "encrypted email" as described in this email on a scale from 1 to 4? (1: Not at all familiar, 2: Slightly familiar, 3: Moderately familiar, 4: Very familiar)

(Researcher's Script) *You can stop sharing your screen!*

Task 2

(Researcher's Script) *I will provide you with two links in the Zoom chat. The first link is for the video and the second one is for the slides. Please first click on the first link and watch the video that introduces Virtru. After you watch the video, you can click on the second link for the slides to easily follow the steps of setting up Virtru.*

- Please compose an email using Virtru and explore its security features for two minutes. No need to send it to anyone. Make sure to think aloud while performing this task.

Task 3

(Researcher's Script) *Now, I will share a link to Google Drive in the chat box, and you need to download three documents from Google Drive on your device that you can easily access to perform the following tasks. These documents are the Employee information form, W-9 form, and Health record information form. Please let me know if you have completed downloading.*

Now, in the following task, you will be asked to compose an email with Virtru and attach one of these documents. I will send the email address in the Chatbox (email address), imagining that this email could belong to Human Resources Department, Doctor's office, or a certified public accountant based on the given scenario.

- Do you have any questions so far before moving to the next task?

1. **First Scenario**
   (Researcher's Script) *Now, please open the document titled "Employee Information Form" and take a moment to read this form. Let me know when you have completed the reading. Please imagine that all information in this form, including sensitive information such as the social security number, belongs to you. No need to fill out this form because it is just an example.*
   - Do you consider this form to include sensitive information?
     (Yes) Why do you think it includes sensitive information?
     (No) Why do you think it does not contain sensitive information?
   - Please rate this document's information sensitivity (Not at all sensitive, Slightly sensitive, Moderately sensitive, Very sensitive)

- How satisfied are you when you share your SSN in the Employee Information Form with the Human Resources Department using your regular/standard email without Virtru? (Not at all Satisfied, Slightly Satisfied, Moderately Satisfied, Very Satisfied)
- How concerned or unconcerned would you be if you shared your SSN with the HRD via your regular/standard email without Virtru? (Not at all concerned, Slightly concerned, Moderately concerned, Very concerned)
- How satisfied are you when you share your SSN in the Employee Information Form with the HRD using a secure email such as Virtru? (Not at all Satisfied, Slightly Satisfied, Moderately Satisfied, Very Satisfied)
- How concerned or unconcerned would you be if you shared your SSN with the HRD via Virtru? (Not at all concerned, Slightly concerned, Moderately concerned, Very concerned)

Scenario (Researcher's Script) *Imagine that you are newly hired by a company, and you were asked to email your "Employee Information Form" to the Human Recourses Department a week before your joining the company, so they can review it anytime during this week. When you compose an email and attach the form, please demonstrate how to change the security settings based on this scenario and think aloud while performing this task. After that, you can email your form to the HRD using the email address that we shared with you.*
Now, let's review the email you sent to HRD; please go to the sent email/sent folder and open it. Make sure to share your screen after you open this email.

- Expiration time feature
  (Expiration time selected) Why did you choose a week as an expiration date in this email
  (Expiration time not selected) Why did you not choose a week as an expiration date?
- Disable forwarding feature
  (Disable forwarding selected) Why did you disable forwarding in this email?
  (Disable forwarding not selected) Why did you not disable forwarding in this email?
- Watermarking feature
  (Watermarking selected) Why did you add watermarking to the attached document in this email?
  (Watermarking not selected) Why did you not add watermarking to the attached document in this email?
- Persistent Protection feature
  (Persistent Protection selected) Why did you add persistent protection to the attached document in this email?
  (Persistent Protection not selected) Why did you not add persistent protection to the attached document in this email?

(Researcher's Script) *You can stop sharing your screen!*

2. **Second Scenario** (Note: we asked participants the same questions in the first scenario, and we asked them to attach the W-9 Form based on this given scenario.)
   Scenario (Researcher's Script) *Imagine that you have hired a Certified Public Accountant (CPA) to prepare your taxes. Your W-9 form was shared with a Certified Public Accountant (CPA) for 24 h. When you compose an email and attach the form, please demonstrate how to change the security settings based on this scenario and think aloud while performing this task. After that, you can email your form to a Certified Public Accountant (CPA) using the email address that we shared with you.*
   Now, let's review the email you sent to a Certified Public Accountant (CPA); please go to the sent email/sent folder and open it. Make sure to share your screen after you open this email.
   (Note: we asked participants the same questions in the first scenario.)
3. **Third Scenario** (Note: we asked participants the same questions in the first scenario, and we asked them to attach a Medical History Form based on this given scenario.)

Scenario (Researcher' Script) *Imagine visiting a new doctor for the first time. The new doctor's office needs your medical history form before you come to your appointment, which is three days later. You decided to email this form. When you compose an email and attach the form, please demonstrate how to change the security settings based on this scenario and think aloud while performing this task. After that, you can email your form to the Doctor's office using the email address that we shared with you.*
Now, let's review the email you sent to the Doctor's office; please go to the sent email/sent folder and open it. Make sure to share your screen after you open this email.
(Note: we asked participants the same questions in the first scenario.)

- After completing all the scenarios, do you think these emails you sent can be misused if you set a longer expiration date, such as a year?
  Why?
- How would you handle the situation if you accidentally sent an email to the wrong person and you realized it afterward?
  Can you please demonstrate how you would change the security setting using one of the emails you sent? You can share your screen. Could you think aloud while performing this task?

(Researcher's Script) *You can stop sharing your screen!*

(Note: The researcher shared a survey link with participants to answer demographic questions.)

- How old are you?
- What is your gender?
- How would you describe your employment status?
- Do you have any experience working in or studying computer-related fields?
- What is the highest level of education you have completed or degree you have earned?

Appendix B. Video Transcript

The major drawback of traditional email is that you can't control information once it's sent. This makes sending sensitive information through traditional email especially risky: Recipients may be hacked, or you may send an email to the wrong person. However, there are ways to ensure emails containing sensitive information aren't intercepted. To protect sensitive emails from unauthorized access or accidental sharing, you should use Virtru. Google recommends using Virtru to control access to sensitive emails. Virtru encrypts the content and attachments in your email; thus, once your email reaches the mail server, it cannot be read by anyone, such as Google, hackers, or third parties in the relay chain between you and your recipient. Importantly, Virtru allows you to set a message expiration date by specifying the amount of time the email will be accessible to the recipient. You can also revoke message access in case you send an email to the wrong person by using the access controls provided. Additionally, you can disable forwarding to the message unreadable if it has been forwarded. You also can add a watermark on the attachments and require authentication if the attachment is shared or downloaded to the recipient's computer. Also, you can apply persistent file protection to your encrypted attachments which restricts access to only authorized users even if it is shared or downloaded in their devices.

Virtru works using a browser plugin. First, navigate to Virtru Email Protection for Gmail in the Chrome Web Store and select Add to Chrome, When prompted, click Add extension Once Virtru is successfully installed, enabling Virtru during email composition is easy. You will automatically be prompted to activate upon opening Gmail. Select the Activate button to begin the activation process. Click Done to begin sending secure messages! You will receive a brief tour showing you how to send your first secure message. Click Compose to continue. In the Compose window, you can toggle Virtru protection by selecting the toggle in the top right corner. Click on the setting icon to add additional security options. You can control access to your protected message by setting an expiration

date, disabling forwarding, or watermarking attachments. Lastly, hit Secure Send and your message will be delivered securely.

References

1. How Much Sensitive Data Is Your Organization Sharing?—Virtru—virtru.com. Available online: https://www.virtru.com/blog/data-sharing-risk-calculator (accessed on 6 February 2023).
2. Stokel-Walker, C. Almost No One Encrypts Their Emails Because It Is Too Much of a Hassle. Available online: https://www.newscientist.com/article/2289747-almost-no-one-encrypts-their-emails-because-it-is-too-much-of-a-hassle/ (accessed on 6 February 2023).
3. Warford, N.; Munyendo, C.W.; Mediratta, A.; Aviv, A.J.; Mazurek, M.L. Strategies and perceived risks of sending sensitive documents. In Proceedings of the 30th USENIX Security Symposium (USENIX Security 21), Virtual, 11–13 August 2021; pp. 1217–1234.
4. Sjouwerman, S. 91blog.knowbe4.com. Available online: https://blog.knowbe4.com/bid/252429/91-of-cyberattacks-begin-with-spear-phishing-email (accessed on 6 February 2023).
5. Solove, D.J. I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev.* **2007**, *44*, 745.
6. Gaw, S.; Felten, E.W.; Fernandez-Kelly, P. Secrecy, flagging, and paranoia: Adoption criteria in encrypted email. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Montreal, QC, Canada 22–27 April 2006; pp. 591–600.
7. Abu-Salma, R.; Sasse, M.A.; Bonneau, J.; Danilova, A.; Naiakshina, A.; Smith, M. Obstacles to the adoption of secure communication tools. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–24 May 2017; pp. 137–153.
8. Ruoti, S.; Andersen, J.; Zappala, D.; Seamons, K. Why Johnny still, still can't encrypt: Evaluating the usability of a modern PGP client. *arXiv* **2015**, arXiv:1510.08555.
9. Sheng, S.; Broderick, L.; Koranda, C.A.; Hyland, J.J. Why johnny still can't encrypt: Evaluating the usability of email encryption software. In Proceedings of the Symposium On Usable Privacy and Security, Pittsburgh, PA, USA, 12–14 July 2006; pp. 3–4.
10. Al Qahtani, E.; Javed, Y.; Shehab, M. User Perceptions of Gmail's Confidential Mode. *Proc. Priv. Enhancing Technol.* **2022**, *2022*, 187–206.
11. Clark, J.; van Oorschot, P.C.; Ruoti, S.; Seamons, K.; Zappala, D. SoK: Securing email—A stakeholder-based analysis. In Proceedings of the Financial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, 1–5 March 2021; Revised Selected Papers, Part I 25; Springer: Berlin/Heidelberg, Germany, 2021; pp. 360–390.
12. Virtru. Available online: https://www.virtru.com/data-protection-platform/email-encryption/gmail#:~:text=End%2Dto%2DEnd%20Encryption%2C%20Simplified&text=Virtru%20equips%20you%20to%20secure,Set%20expiration%20dates (accessed on 27 January 2023).
13. Ruoti, S.; Andersen, J.; Dickinson, L.; Heidbrink, S.; Monson, T.; O'neill, M.; Reese, K.; Spendlove, B.; Vaziripour, E.; Wu, J.; et al. A usability study of four secure email tools using paired participants. *ACM Trans. Priv. Secur. (TOPS)* **2019**, *22*, 1–33.
14. UM, T.S. Virtru: Added Security for Your U-M GMail. 2023. Available online: https://safecomputing.umich.edu/protect-the-u/safely-use-sensitive-data/virtru (accessed on 29 September 2023).
15. CRUZ, U.S. Virtru for Sharing Sensitive Data on and Off Campus. 2023. Available online: https://its.ucsc.edu/virtru/ (accessed on 29 September 2023).
16. He, W.; Akhawe, D.; Jain, S.; Shi, E.; Song, D. Shadowcrypt: Encrypted web applications for everyone. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, 3–7 November 2014; pp. 1028–1039.
17. Vaziripour, E.; O'Neill, M.; Wu, J.; Heidbrink, S.; Seamons, K.; Zappala, D. Social Authentication for {End-to-End} Encryption. In Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), Denver, CO, USA, 22–24 June 2016.
18. Virtru Encryption Key Management. Available online: https://www.virtru.com/encryption-key-management/?utm_campaign=2022_US_DataBreach_General&gclid=Cj0KCQiAw8OeBhCeARIsAGxWtUyk2j-CDf10x84XKRWd4XkaGCthgOfzZlVKe6CZiUgQzhgbOex9m7YaAiSiEALw_wcB (accessed on 27 January 2023).
19. Ferreira, L.; Anacleto, J. Usability in Solutions of Secure Email—A Tools Review. In Proceedings of the Human Aspects of Information Security, Privacy and Trust: 5th International Conference, HAS 2017, Held as Part of HCI International 2017, Vancouver, BC, Canada, 9–14 July 2017; Proceedings 5; Springer: Berlin/Heidelberg, Germany, 2017; pp. 57–73.
20. Hogan, B. Virtru Review: Easily Protect Data Wherever It's Created or Shared. Available online: https://www.softwarepundit.com/virtru-review (accessed on 29 September 2023).
21. Ruoti, S.; Andersen, J.; Hendershot, T.; Zappala, D.; Seamons, K. Private webmail 2.0: Simple and easy-to-use secure email. In Proceedings of the 29th Annual Symposium on User Interface Software and Technology, Tokyo, Japan, 16–19 October 2016; pp. 461–472.
22. Tutanota. 2023. Available online: https://tutanota.com (accessed on 29 September 2023).
23. PGP (Mailvelope). 2023. Available online: https://mailvelope.com/en (accessed on 29 September 2023).
24. Proton Mail. 2023. Available online: https://proton.me/mail (accessed on 29 September 2023).
25. Gmail Confidential Mode. 2023. Available online: https://support.google.com/mail/answer/7674059?sjid=16859918329907772900-NA (accessed on 29 September 2023).

26. De Luca, A.; Das, S.; Ortlieb, M.; Ion, I.; Laurie, B. Expert and Non-Expert Attitudes towards (Secure) Instant Messaging. In Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), Denver, CO, USA, 22–24 June 2016; pp. 147–157.
27. Brady, S. Survey Shows Sharing Confidential Data in the Workplace is Common. 2017. Available online: https://totalsecurityadvisor.blr.com/cybersecurity/survey-shows-sharing-confidential-data-workplace-common/ (accessed on 29 September 2023).
28. Asiri, E.; Khalifa, M.; Shabir, S.A.; Hossain, M.N.; Iqbal, U.; Househ, M. Sharing sensitive health information through social media in the Arab world. *Int. J. Qual. Health Care* **2017**, *29*, 68–74.
29. Househ, M. Sharing sensitive personal health information through Facebook: The unintended consequences. In *User Centred Networked Health Care*; IOS Press: Clifton, VA, USA, 2011; pp. 616–620.
30. Dechand, S.; Naiakshina, A.; Danilova, A.; Smith, M. In encryption we don't trust: The effect of end-to-end encryption to the masses on user perception. In Proceedings of the 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, 17–19 June 2019; pp. 401–415.
31. Das, S.; Kim, T.H.J.; Dabbish, L.A.; Hong, J.I. The effect of social influence on security sensitivity. In Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS 2014), Menlo Park, CA, USA, 9–11 July 2014; pp. 143–157.
32. Fagan, M.; Khan, M.M.H. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In Proceedings of the Twelfth symposium on usable privacy and security (SOUPS 2016), Denver, CO, USA, 22–24 June 2016; pp. 59–75.
33. Al Qahtani, E.; Javed, Y.; Lipford, H.; Shehab, M. Do women in conservative societies (not) follow smartphone security advice? a case study of saudi arabia and pakistan. In Proceedings of the 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genova, Italy, 7–11 September 2020; pp. 150–159.
34. Renaud, K.; Volkamer, M.; Renkema-Padmos, A. Why doesn't Jane protect her privacy? In *International Symposium on Privacy Enhancing Technologies Symposium*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 244–262.
35. Ruoti, S.; Andersen, J.; Heidbrink, S.; O'Neill, M.; Vaziripour, E.; Wu, J.; Zappala, D.; Seamons, K. "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, San Jose, CA, USA, 7–12 May 2016; pp. 4298–4308.
36. Wu, J.; Zappala, D. When is a tree really a truck? exploring mental models of encryption. In Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018), Baltimore, MD, USA, 12–14 August 2018; pp. 395–409.
37. Whitten, A.; Tygar, J.D. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. *USENIX Secur. Symp.* **1999**, *348*, 169–184.
38. Krombholz, K.; Busse, K.; Pfeffer, K.; Smith, M.; Von Zezschwitz, E. "If HTTPS Were Secure, I Wouldn't Need 2FA"-End User and Administrator Mental Models of HTTPS. In Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 19–23 May 2019; pp. 246–263.
39. MacFarland, T.W.; Yates, J.M.; MacFarland, T.W.; Yates, J.M. Wilcoxon matched-pairs signed-ranks test. In *Introduction to Nonparametric Statistics for the Biological Sciences Using R*; Springer: Cham, Switzerland; 2016; pp. 133–175.
40. McDonald, N.; Schoenebeck, S.; Forte, A. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proc. ACM Hum.-Comput. Interact.* **2019**, *3*, 1–23.
41. McGregor, S.E.; Charters, P.; Holliday, T.; Roesner, F. Investigating the computer security practices and needs of journalists. In Proceedings of the 24th USENIX Security Symposium (USENIX Security 15), Washington, DC, USA, 12–14 August 2015; pp. 399–414.
42. Gerber, N.; Zimmermann, V.; Henhapl, B.; Emeröz, S.; Volkamer, M. Finally johnny can encrypt: But does this make him feel more secure? In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018; pp. 1–10.
43. Albayram, Y.; Liu, J.; Cangonj, S. Comparing the Effectiveness of Text-based and Video-based Delivery in Motivating Users to Adopt a Password Manager. In Proceedings of the European Symposium on Usable Security 2021, Karlsruhe, Germany, 11–12 October 2021; pp. 89–104.
44. Albayram, Y.; Khan, M.M.H.; Jensen, T.; Nguyen, N. "... better to use a lock screen than to worry about saving a few seconds of time": Effect of Fear Appeal in the Context of Smartphone Locking Behavior. In Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), Santa Clara, CA, USA, 12–14 July 2017; pp. 49–63.
45. Al Qahtani, E.; Sahoo, L.; Shehab, M. The Effectiveness of Video Messaging Campaigns to Use 2FA. In *International Conference on Human-Computer Interaction*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 369–390.
46. Ruoti, S.; Monson, T.; Wu, J.; Zappala, D.; Seamons, K. Weighing context and trade-offs: How suburban adults selected their online security posture. In Proceedings of the Symposium on Usable Privacy and Security (SOUPS), Santa Clara, CA, USA, 12–14 July 2017; pp. 211–228.