Managing access to confidential emails: A case study of Virtru

Your N. Here
Your Institution

Second Name
Second Institution

Abstract

End-user adoption and usage of end-to-end encryption tools is an ongoing research topic. One such tool is Virtru–an encryption software that allows users to encrypt confidential emails and manage their access control using 4 features, namely expiration time, disable 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 study on 19 participants to understand user perceptions of Virtru 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 participants' first impression upon receiving a Virtru email was that it looked suspicious, especially when received from an unknown person. After participants were informed about the importance of Virtru, they were comfortable sharing medical, tax, and employee information via Virtru. Regarding access control management of the 3 types of confidential information, expiration time and disable forwarding were most useful for the participants in preventing unauthorized and continued access. While 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 practical implications of our findings.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, United States.

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 [2]. 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 [31]. People are more concerned about data leaks from recipients' devices rather than data during transit [32] [29].

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 [4, 6, 16, 26, 28, 30], user attitudes and concerns regarding the email encryption platform Virtru [3] has not yet been explored. Virtru encrypts messages and provides in-built access control at the same time. Therefore, we seek to understand user perceptions of Virtru and how they use its security features to manage access control to 3 types of confidential information, namely medical, tax, and employee personal information, if sent via email. More specifically, this paper investigates the following research questions:

- **RQ1:** What are users' first impressions when receiving an encrypted email using Virtru?
- **RQ2:** How comfortable are users with sharing various types of confidential information using Virtru, namely medical, tax, and employee?
- **RQ3:** How do users use Virtru's security 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 participants' first impression upon receiving an email encrypted with Virtru was that, due to its interface, it looked suspicious, especially when received from an unknown person. After participants were informed about the benefits of using Virtru, they were comfortable sharing medical, tax, and employee information forms via Virtru. However, they would be concerned if they shared these forms via regular email without Virtru. Regarding managing access control to the 3 types of confidential email information, expiration time and disabled forwarding were the most useful features for the participants for preventing unauthorized and continued access, and the only reasons for not using them were to prevent unforeseen accessibility issues by the recipient. While 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 3 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 if they set a longer expiration date, such as a year, to prevent future scenarios (e.g., taking screenshots by recipients or recipients' email accounts have been compromised). Our findings provide practical implications that could help users share confidential information via end-to-end encrypted communication mediums.

2 Virtru

Virtru is an end-to-end encryption platform that encrypts Gmail messages, attachments, and files stored in Google Drive, including Google Docs, Google Sheets, and Google Slides [3]. 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 (as shown in Figure 1) allow users to:

- Apply 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, the recipient will receive an email notification from Virtru. Unauthorized users will not be granted access.
- Apply Expiration Date to an encrypted email or file. Users can restrict access after a particular point in time. If a recipient tries to access the content after expiration, they will receive a prompt indicating their access is expired. Expiration can also be managed after an email has been sent.
- Apply 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 send 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.
- Apply Watermarking to a secure file. Recipients will only have access in the Secure Reader and will see their email address watermarked across the document. A recipient will not have the option to download the file.
- Apply Revoke (or reauthorize) Access. Virtru even allows the sender to revoke access to specific recipients granularly at any time. If recipient access is revoked, users will receive a prompt indicating their access has been removed.

Virtru uses a distributed architecture and unique symmetric keys for each email and file [1]. 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 [1]. In this way, data is kept private, even from Google or unauthorized parties. Although Virtru provides email transmission security, it does not protect against email account compromise.

In our study, we chose Virtu to understand how users manage access control to their confidential information since Virtru is easily integrated with users' existing Gmail accounts, provides end-to-end encryption and has automatic key management, has good usability [24], and has built-in access controls that can help Gmail users to control their emails after they are sent.

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. [4, 13]. To investigate the sensitive data-sharing practices, Dell [11] commissioned a global survey of 2,608 professionals handling

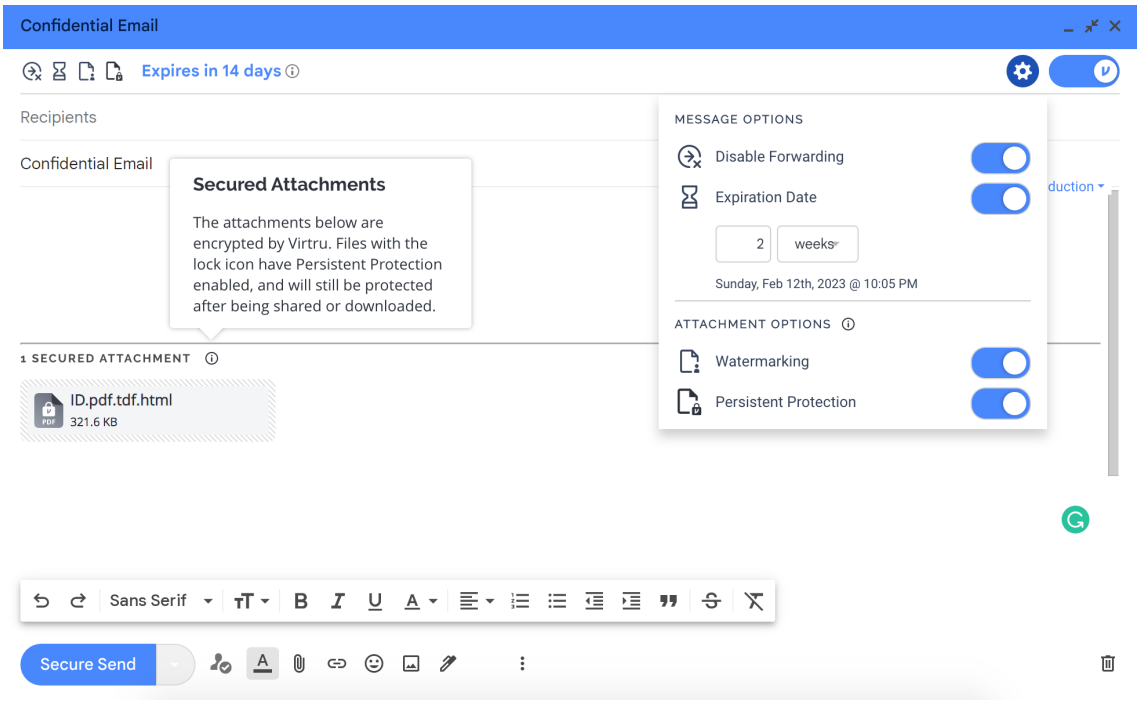

Figure 1: Virtru's email composition window along with its message security options.

sensitive data at companies. The survey results showed that 72% of employees are willing to share sensitive, confidential, or regulated company information without proper data security protocols in place. Also, Warford et al. [32] explored users' experiences with sending sensitive information via standard (unencrypted) email, which was the most common transmission method users used when they send their sensitive documents, such as their financial information, social security number, health information, and information related to their children. Users could share sensitive health information on social media (Facebook), which can negatively affect users' privacy [10, 18].

Recently, users have been using end-to-end encrypted messaging applications (e.g., Whatsapp, Signal) to communicate privately. Still, most users believed that SMS is more secure than WhatsApp and that they were not targeted by government and special service surveillance [14]. Despite using these secure messaging apps, users' decisions were affected more by peer influence than secure messaging apps' security features [13]. Even though WhatsApp users were informed that their messages are end-to-end encrypted, 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 towards 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. [12] 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. They also suggested that users discuss security topics to warn others against immediate novel security threats observed, or to collect details about solving an experienced problem. Two studies evaluated the differences in motivations for (not) following computer security practices [15] and smartphone security measures [5] based on the rational decision model. They found there were differences in users' perceptions regarding the benefits, risks, and costs associated with their decisions. Luca et al. [13] explored how much of a role security and privacy played in people's decisions to use a mobile secure instant messenger (IM). They advertised the messenger app Threema as more secure and private than a traditional mobile IM. They found that peer influence mainly motivated people to use a specific mobile IM, whereas the security and privacy of the application had a minor role.

In other studies [16, 23], 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 [16]. As a result of technical issues, usability issues, and social considerations, participants did not consider using it frequently. In another study [25], 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. [24] 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 (71.1). It also had well-designed tutorials, which made participants prefer to use it. We add to the existing literature by understanding users' perceptions of using end-to-end encrypted email and how they 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 computer security research community has endorsed using secure communication methods to protect confidential information. Personal messaging applications, such as WhatsApp and Telegram, have adopted end-to-end encryption. Abu-Salma et al. [4] explored users' knowledge, experience, and perception of different communication tools. They found that most 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. [16] conducted a study by interviewing a sample of users from an activist organization whose tasks require 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. Surprisingly, they found that participants perceived only "paranoid people" or "people who are up to no good" would use encryption. Furthermore, researchers [34] identified four mental models of encryption as a problem that illustrated how users perceived encryption's structure and functions.

Whitten and Tygar [33] in their seminal paper "Why Johnny Can't Encrypt" 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. [23] 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. [19] 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. At the same time, administrators often do not comprehend the interplay of functional protocol components. Recently, users began using Gmail's Confidential Mode (GCM) to share confidential emails, believing it encrypts them [6]. 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 an end-to-end encrypted email before our participants explored Virtru's security features.

4 Methodology

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 and Social media. All interested participants completed a screening survey to determine their eligibility, by ensuring they use Gmail accounts frequently, have sent emails containing confidential information before, are at least 18 years old, have the ability to install Virtru extension on their computers, and have never used Virtru/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. Participants who completed the study received $10 Amazon gift card. Our Institutional Review Board approved the study (IRB Protocol #XX-XXXX).

4.2 Demographics

We interviewed 19 participants. Each participant was asked a set of demographic questions, such as age, gender, employment status, any experience in working or studying computer related fields, and the highest level of education completed. The majority of our participants (52.6%) were aged 20–29 years. Whereas, 4 of them (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 8 participants were male (42.1%). 57.9% of our participants were students, 26.3% were both employees and students, but a few of them (15.8%) had full-time employment. Additionally, the majority of our participants had not had any experience in working or studying computer-related fields, and only 8 of them had experience in these fields. Regarding the highest level of education achieved, 9 of the participants had completed college or associate's degree, 7 had completed high school or equivalent, and 3 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 participants 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. Participants were first asked a set of questions on how they perceive the security and privacy of Gmail. After that, we asked participants to perform three tasks.

In the first task, we aimed to explore participants' perceptions of receiving Virtru's secured email as shown in Figure 2 since they had not used it before. We asked them to state their impression when they opened the encrypted email, their rating of how easy or difficult 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.

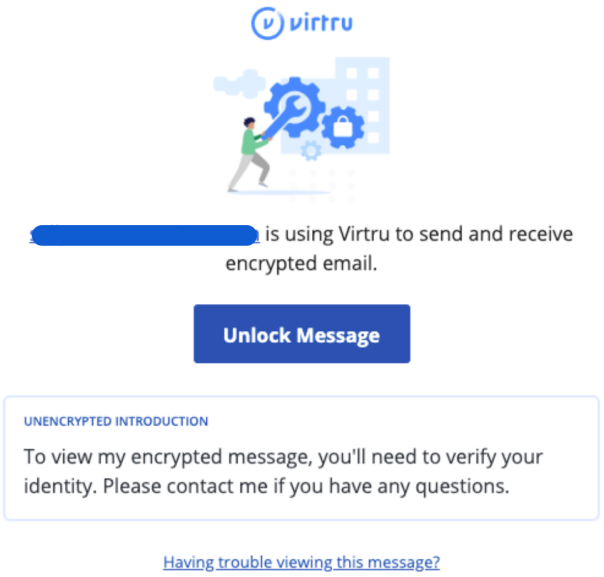

Figure 2: Virtru's secured email window

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

In the third task, participants were provided with three hypothetical scenarios to understand how users manage the access controls of Virtru's security features in the encrypted email and how they rate their satisfaction and concern once they share their confidential information via standard email and encrypted email. To perform this task, participants were first asked to download three documents/forms (employee information form, medical history form, and W-9 form)on their personal devices.We chose these documents since they are sensitive and people are familiar with health records, employment applications, and tax documents. Moreover, researchers [6] found most participants emailed their confidential information related to health, financial, and work-related documents using Gmail's Confidential Mode, which is integrated with Gmail. Thus, these forms have been filled out with artificial information as an example. We asked participants to imagine that information in all these forms, including sensitive information such as social security number, belongs 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 artificial information about an employee (e.g., employee ID, contact information). The given scenario was between the participants and 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 the HR a week before they joined the company, so HR could review it anytime during this week.
- For the medical history form, we included artificial information about a person's health history (e.g., Unhealthy Habits, Patient's Medical History). The given scenario was between the participants and Doctor's office. We asked them to imagine visiting a new doctor for the first time, and the new doctor's office needs their medical history form before they come to their appointment, which is three days later.
- For the W-9 form, we included artificial 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 hours.

All participants were asked to demonstrate how to change 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, disable forwarding, watermarking, and persistence protection. We used the randomizer function to change the scenario order for all participants since there were three scenarios.

Lastly, participants were asked to answer a set of demographic questions via the Qualtrics survey. The interview questions, scenarios, and instructions are listed in the appendix.

4.4 Analysis

We collected both quantitative and qualitative data. For the quantitative data, we used the Wilcoxon Signed-Ranks test (a non-parametric statistical hypothesis test [20]) to analyze the ordinal data for users' satisfaction and concerns regarding using standard email and an end-to-end encryption email. For the qualitative data, we utilized an inductive approach. The data was coded independently by two researchers. We then discussed, refined, and updated the two sets of coded data to resolve disagreements [21].

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, namely: 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 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), 2) describe what encryption means, 3) explain whether there is anyone besides the recipient, who can read and access the content of their email, and 4) explain whether Google gives the government direct access to their email if it is 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, still, several participants (26.3%, N=5) did not know what encryption was, but they had heard of it.

With regards 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).

Additionally, when asked whether participants thought there was anyone besides the recipient who could read and access the content of their email, we found that only 2 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 email. For example, two comments were: *"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/third-party who could access and read their emails. They stated that **hackers** (3/19), **Gmail/Google employees** (6/19), **university employees** (2/19, a comment is shown below), **third parties** (2/19), **government** (1/19), and **police** (1/19) could access their emails besides the intended recipients.

A comment was mentioned by P14 *"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."*

Regarding Google giving the government direct access to participant's email, if requested, we found that the majority of the participants (N=10, 52.6%) believed that Google gives the government access to their email when requested, 31.6% of participants (N=6) did not think so, and 15.8% did not know whether Google gives the government direct access to their email. We found 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 that 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: **required by law enforcement** (2/19), **depends on the requester** (1/19), and **needs user permission** (1/19).

Summary. Majority of our participants professed awareness of encryption technology, but they did not understand how it works. Some participants did not think anyone besides the recipient could read/access the content of their emails. However, when it comes to the government, the majority of participants believed that Google gives the government direct access to their email 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, ***What are users' first impressions when receiving an encrypted email using Virtru?***, we asked participants to explore the encrypted email since they did

not have any previous experience with sending/receiving encrypted emails. Virtru allows non-Virtru recipients to read an encrypted email without Virtru installed and access the email content via Virtru's Secure Reader. So, participants could perform this task without installing Virtru. Figure 2 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 are with the concept of "Encrypted Email," as described in this email.

Regarding the themes of participants' reactions when they first saw a Virtru-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 looked **suspicious** (7/19), seemed like **spam/phishing email** (4/19), or had **a confusing interface** (1/19). Those who had a positive impression said that it **needed verification** which felt safe (5/19), **encrypted email content** (2/19), seemed more **secure and serious** (4/19), and had **a 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."* 4 participants stated that they would **delete the email**, 2 participants would **mark as spam**, and 1 participant mentioned **block 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 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 4 participants mentioned that they would **contact 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 1 participant mentioned that they **feel Safe** when receiving this kind of email from a known entity.

Moreover, we found most of our participants (N=18, 94.8%) stated that it was (Somewhat/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 2). A few participants (N=4, 21.1%) were not at all familiar with the concept of "Encrypted Email" described in this email, whereas another 4 participants were slightly familiar with this concept.

Summary. For a majority of the participants, the first impression of a Virtru-encrypted email was that it **looks suspicious** and if they received any email like this from an unknown person, they would not open it. However, if the sender is a known entity, then most of the participants stated that they opened 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 in a Virtru email.

5.3 Sharing confidential information using Virtru

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

To answer the research question, ***"How comfortable are users with sharing various types of confidential information using Virtru, namely medical, tax, and employee?"***, participants were provided with three hypothetical scenarios to understand 1) how they utilize Virtru's security features to manage the access control for the encrypted email and 2) how they rate their satisfaction and concern once they share their confidential information via standard email and encrypted email. First, participants downloaded three documents (employee information form, medical history form, and W-9 form) on their personal devices. These forms have been filled out with artificial information as an example based on the given scenario. Therefore, we asked participants to imagine that the information in these forms, such as the social security number (SSN), belongs 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 consider it to include sensitive information, and rate this form's information sensitivity. All participants stated that they consider this employee information form to include sensitive information. They provided many examples of included sensitive information, such as employee ID, SSN, and contact information. We

	Sharing via standard email (Mean)	Sharing via Virtru's email (Mean)	Z score (Z)	p value (p)
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

Table 1: Participants' rating of satisfaction and concerns about sharing confidential information via standard email and end-to-end encrypted email

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, participants rated their satisfaction with sharing their SSN in the employee information form using their regular/standard email and Virtru's secured email. Also, they were asked to rate their concerns regarding sharing their SSN in the employee information form with HR using their regular/standard email and Virtru's secured email.

The Wilcoxon Signed-Ranks Test showed that the participants' satisfaction with sharing SSN in the employee information form via Virtru's secured email was rated higher by the participants compared to sharing via standard email, Z = -3.6, p< 0.001 (Table 1). Therefore, we found all participants (100%) rated their satisfaction (as Moderately/Very satisfied) if they shared their SSN with HR using Virtru compared to standard email (26.4% rated as Moderately/Very satisfied). Also, the test indicated that users were more concerned if they shared their SSN with HR via regular/standard email than Virtru's secured email, Z = -3.8, p< 0.001 (Table 1). Furthermore, 63.2% of the participants were not at all concerned if they shared their SSN with HR using Virtru compared to standard email (47.4% rated as "Very concerned").

5.3.2 Scenario 2: W-9 Tax form with 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 consider this employee information form to include sensitive information, such as SSN and account number. We found that 94.7% of participants rated this form's information sensitivity as "Very sensitive."

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

We used the Wilcoxon Signed-Ranks Test to compare participants' satisfaction with sharing sensitive information via standard email and Virtru. The test indicated that the participants' satisfaction with sharing SSN in the W-9 form via Virtru's secured email was rated higher than sharing SSN in this form via standard email, Z = -3.9, p< 0.001 (Table 1). Therefore, we found that all participants rated their satisfaction (as Moderately/Very satisfied) when sharing their SSN with the CPA using Virtru compared to standard email. We also conducted another Wilcoxon Signed-Ranks Test and found that the participants were more concerned if they shared their SSN with the CPA via regular/standard email compared to Virtru's secured email, Z = -3.7, p< 0.001 (Table 1). Therefore, we found that 68.4% of participants were "Not at all concerned" if they shared their SSN with the CPA using Virtru compared to standard email.

5.3.3 Scenario 3: Medical health form with Doctor's office

For the third scenario, we first asked 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 includes sensitive information (e.g., medical history, health habits, and SSN). We found that 78.9% of participants rated this form's information sensitivity as "Very sensitive."

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

We performed the Wilcoxon Signed-Ranks Test, which indicated that the participants' comfort with sharing SSN in the medical history form via Virtru's secured email was rated

higher compared to sharing it via standard email, Z = -3.8, p< 0.001 (Table 1). All participants rated their satisfaction as (Moderately/Very satisfied) if they shared their SSN with the doctor's office using Virtru compared to standard email Also, the test indicated that users were more concerned if they shared their SSN with the doctor's office via regular/standard email than Virtru's secured email, Z = -3.9, p< 0.001 (Table 1). We found that 73.7% of participants were "Not at all concerned" if they shared their SSN with the doctor's office using Virtru compared to standard email (52.6% rated as "Very concerned").

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

5.4 Virtru's security settings

To answer the research question, ***"How do users use Virtru's security features to manage access control to their confidential information?"***, participants were asked to open Virtru's secured email that they sent earlier and to review what Virtru's security options (e.g., set expiration time, enable disable forwarding, add watermarking, or add persistent protection) they enabled based on the given scenarios, as shown in Table 2. They were also asked to provide their reasons for selecting or not selecting Virtru's security features.

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

Table 2: Percentage of participants who did or did not select Virtru's four security options.

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 1 participant mentioned that he would choose this option to **avoid access afterward**. For the W-9 form, 13 participants mentioned selecting Expiration Time to **remove continued access** (e.g., a comment is shown below). Only 1 participant would select that because of the **urgency of document access**. For the medical form, 16 participants selected this feature to **allow access for limited time**.

A comment was mentioned by P7: *"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 hours, 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 bad impression** (e.g., a comment is shown below), and another participant shared that it was **not important** to him. For the W-9 form, 3 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 2 participants stated that this feature was **not needed**.

A comment was mentioned by P6: *"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/resharing**. This reason was most prominent for the employee form (13/19, a comment is shown below), the W-9 form (16/19), and the medical form (9/19).

A comment was mentioned by P6: *"because, as my public accountant, they should be the ones handling all my information. If they're sending my personal information out to other places. There's something wrong with that accountant, and I need to hire somebody else."*

Not Selected: The main reason for not selecting this option for the employee form was **enable sharing access** as stated by 4 participants. For the W-9 form, one participant mentioned they **trust recipient** and another one mentioned **allowing re-sharing** as the reasons for not selecting this option. For the medical form, their reasons were: **allow sharing with other departments** (5/19, a comment is shown below) and **other protections in place** (1/19). Moreover, some participants thought this feature was **not needed** for these documents: employee form (1/19), W-9 form (1/19), and medical form (3/19).

A comment was mentioned by P10: *"Because I thought that the doctors might need the information like to share the information 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 **extra layer of protection**, as stated by 3 participants for the employee form, 2 participants for the W-9 form, and 5 participants for the medical form (e.g., 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 medical form, 1 participant stated **distinguishing between the original document and its copy** as the reason for using this feature.

A comment was mentioned by P18: *" 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 3 participants for the employee form, 6 participants for the W-9 form, and 3 participants for the medical form mentioned it. Many participants shared that they thought this option was **not needed** for these documents: employee form (10/19), W-9 form (4/19), and medical form (9/19). Additionally, people did not select it **to avoid bad impression about access** (1/19), **document is already secure** (1/19) and, **inappropriate to use this feature** (1/19) for the employee form (e.g., a comment is shown below).

A comment was mentioned by P5: *"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 **extra layer of security** (employee form: 6/19, W-9 form: 9/19, medical form: 9/19) and **prevent unauthorized access** (employee form: 7/19, W-9 form: 8/19, medical form: 9/19). Additionally, one participant mentioned **prevent misuse of personal information** in the employee form. For the medical form, 4 people stated **preventing re-sharing** (e.g., a comment is shown below).

A comment was mentioned by P9: *"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/usability issues** for not using the Persistent Protection feature (e.g., a 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 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 a week, the medical history form needed to be accessed by Doctor's office for three days, and the W-9 needed to be accessed by CPA for 24 hours.

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 time. Participants provided their reasons for the possibility that their emails could be misused since there is **no trust in entities' attitudes** that allow them to misuse their information (12/19). For example, a comment is shown below.

P17: *"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, participants were concerned about **taking screenshots or copies of their information** by entities (3/19). For example, a comment is shown below.

P8: *"I believe that if I set the expiration date for a year, it gives them enough time to copy the entire text, or create a record for 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 numbers of participants expressed their concerns about the possibility that **someone could hack the entities' email accounts** and access their information if they set a long time (3/19). For example, a comment is shown below.

P16: *"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 4 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., a comment is shown below), and the **attachment features were enabled**, such as persistent protection and watermarking.

A comment was mentioned by P1: *"Because these emails are actually encrypted and not just sent out. It'd be a lot harder for them to be accessed by third-party sources 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 or authorized."*

We also asked participants how they would handle the situation if they accidentally sent an email to the wrong person and they realized it afterward. In this task, 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 Virtru's 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. For example, a comment is shown below.

P8: *"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."*

Other 9 participants directly pointed out the **Revoke Access button** on the top of the email window, as shown in Figure 3, which disables access to the email content and attachments. For example, a comment is shown below.

P19: *"Before Virtru... Google doesn't allow me to undo it after 30 seconds 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."*

Two participants stated that they would inform recipients that the email was sent by mistake. A comment was mentioned by P12: *"I would send them another email, or like reply to that email; that just this that's kind of a mistake; this email was sent by mistake."*

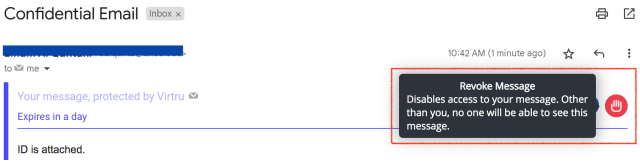

Figure 3: Revoke access button highlighted in red

6 Discussion

Perceptions of encryption concept. End-to-end encryption is still rarely used by non-expert users, even target groups, such as journalists [22]. 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 that *"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 [14, 17, 34]. Educating users about how encryption works with an accurate model is a challenging task. The researchers [34] recommend aligning communication efforts and designs with the functional models of encryption that users already possess.

Interaction with encrypted emails. Before informing our participants about Virtru, most of them had negative impressions when they first saw this encrypted email by stating that it seemed suspicious or a spam/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 [24], 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 participants composed an encrypted email for the first time, no one faced any difficulties after watching the video. They were comfortable using

Virtru's 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 (Virtru) rather than regular email. Also, they were more concerned about sharing their sensitive information via regular email without using Virtru. These findings confirmed prior work [7–9], 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 [27] 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 Virtru security features, to limit access to their medical, tax, and employee information in 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 recipient's attitudes as they may 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 [32].

7 Limitations and Future Work

Our work is not without limitations. Since most of our participants were recruited from the university, the results may be considered exploratory and cannot be generalized for all users. Including non-university participants, such as less tech-savvy users or employees' organizations who daily 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 the encrypted email, such as whether someone could access and read their email content. Further study is needed to ask detailed and less technical questions to measure users' understanding between point-to-point encryption and end-to-end encryption for secure communication mediums.

Virtru provides more controls to track the emails in the Control Center after they have been sent (e.g., checking if the email/file is accessed or shared by the recipients, providing validation reports, and listing all authorized recipients who access the email). It would be an interesting path to find out what happens beyond tracking users' sensitive information to evaluate the following questions.

- Do users review their confidential emails to check if they have been accessed by recipients?
- Are users concerned about their email if it stays in the recipient's email inbox based on the given expiration date?
- What are the users' expectations of email's deletion concept (e.g., Undo feature vs Revoke Access at any time)?

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

Besides end-to-end encrypting of our participants' forms, they were comfortable managing the access control of message features (Expiration date and disabled forwarding). However, some participants were confused about the attachment features (watermarking and persistent protection). Further study is needed to evaluate the impact of risk communication presenting scenarios highlighting the importance of using the attachment features tailored to specific populations. For example, a scenario shows how students watermarked with authorized recipients' names on their academic papers or school projects when shared with other students to prevent recipients from leaking their sensitive data. According to our participant, he preferred to use Watermarking feature to prevent plagiarism in his written academic papers or to share works with his ideas.

8 Conclusion

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 Virtru (end-to-end encryption platform) and how they use it to manage access control (expiration time, disable forwarding, persistent protection, and watermarking) to confidential information, such as medical, tax, and employee information if sent via email. Our results show that Virtru emails were perceived as suspicious, especially when they came from unknown senders. Medical, tax, and employee information was shared via Virtru after participants learned about its importance. The expiration time and disable forwarding features were most useful for preventing unauthorized access and continued access to the three types of confidential information. 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 a longer expiration date. Furthermore, our findings provided practical implications that could help users to share confidential information via end-to-end encrypted communication mediums.

References

[1] Encryption key management. https://www.virtru.com/encryption-key-management/?utm_campaign=2022_US_DataBreach_General&gclid=Cj0KCQiAw8OeBhCeARIsAGxWtUyk2j-CDf10x84XKRWd4XkaGCthgOfzZlVKe6CZiUgQzhgbOex9m7YaAiSiEALw_wcB. Accessed: 2023-01-27.

[2] How Much Sensitive Data Is Your Organization Sharing? - Virtru — virtru.com. https://www.virtru.com/blog/data-sharing-risk-calculator. [Accessed 06-Feb-2023].

[3] Virtru. https://www.virtru.com/google-workspace-encryption?hsLang=en. Accessed: 2023-01-27.

[4] Ruba Abu-Salma, M Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. Obstacles to the adoption of secure communication tools. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 137–153. IEEE, 2017.

[5] Elham Al Qahtani, Yousra Javed, Heather Lipford, and Mohamed Shehab. Do women in conservative societies (not) follow smartphone security advice? a case study of saudi arabia and pakistan. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 150–159. IEEE, 2020.

[6] Elham Al Qahtani, Yousra Javed, and Mohamed Shehab. User perceptions of gmail's confidential mode. *Proc. Priv. Enhancing Technol.*, 2022(1):187–206, 2022.

[7] Elham Al Qahtani, Lipsarani Sahoo, and Mohamed Shehab. The effectiveness of video messaging campaigns to use 2fa. In *International Conference on Human-Computer Interaction*, pages 369–390. Springer, 2021.

[8] Yusuf Albayram, Mohammad Maifi Hasan Khan, Theodore Jensen, and Nhan Nguyen. "... 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 *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, pages 49–63, 2017.

[9] Yusuf Albayram, John Liu, and Stivi Cangonj. Comparing the effectiveness of text-based and video-based delivery in motivating users to adopt a password manager. In *European Symposium on Usable Security 2021*, pages 89–104, 2021.

[10] Eman Asiri, Mohamed Khalifa, Syed-Abdul Shabir, Md Nassif Hossain, Usman Iqbal, and Mowafa Househ. Sharing sensitive health information through social media in the arab world. *International Journal for Quality in Health Care*, 29(1):68–74, 2017.

[11] Susan Brady. Survey shows sharing confidential data in the workplace is common, Jun 2017.

[12] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. The effect of social influence on security sensitivity. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 143–157, 2014.

[13] Alexander De Luca, Sauvik Das, Martin Ortlieb, Iulia Ion, and Ben Laurie. Expert and {Non-Expert} attitudes towards (secure) instant messaging. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 147–157, 2016.

[14] Sergej Dechand, Alena Naiakshina, Anastasia Danilova, and Matthew Smith. In encryption we don't trust: The effect of end-to-end encryption to the masses on user perception. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 401–415. IEEE, 2019.

[15] Michael Fagan and Mohammad Maifi Hasan Khan. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Twelfth symposium on usable privacy and security (SOUPS 2016)*, pages 59–75. USENIX Association Denver, CO, 2016.

[16] Shirley Gaw, Edward W Felten, and Patricia Fernandez-Kelly. Secrecy, flagging, and paranoia: adoption criteria in encrypted email. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 591–600, 2006.

[17] Nina Gerber, Verena Zimmermann, Birgit Henhapl, Sinem Emeröz, and Melanie Volkamer. Finally johnny can encrypt: But does this make him feel more secure? In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pages 1–10, 2018.

[18] Mowafa Househ. Sharing sensitive personal health information through facebook: the unintended consequences. In *User Centred Networked Health Care*, pages 616–620. IOS Press, 2011.

[19] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel Von Zezschwitz. " if https were secure, i wouldn't need 2fa"-end user and administrator mental models of https. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 246–263. IEEE, 2019.

[20] Thomas W MacFarland, Jan M Yates, Thomas W MacFarland, and Jan M Yates. Wilcoxon matched-pairs signed-ranks test. *Introduction to Nonparametric statistics for the biological sciences using R*, pages 133–175, 2016.

[21] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice. *Proceedings of the ACM on human-computer interaction*, 3(CSCW):1–23, 2019.

[22] Susan E McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. Investigating the computer security practices and needs of journalists. In *24th {USENIX} Security Symposium ({USENIX} Security 15)*, pages 399–414, 2015.

[23] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. Why doesn't jane protect her privacy? In *International Symposium on Privacy Enhancing Technologies Symposium*, pages 244–262. Springer, 2014.

[24] Scott Ruoti, Jeff Andersen, Luke Dickinson, Scott Heidbrink, Tyler Monson, Mark O'neill, Ken Reese, Brad Spendlove, Elham Vaziripour, Justin Wu, et al. A usability study of four secure email tools using paired participants. *ACM Transactions on Privacy and Security (TOPS)*, 22(2):1–33, 2019.

[25] Scott Ruoti, Jeff Andersen, Scott Heidbrink, Mark O'Neill, Elham Vaziripour, Justin Wu, Daniel Zappala, and Kent 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*, pages 4298–4308, 2016.

[26] Scott Ruoti, Jeff Andersen, Daniel Zappala, and Kent Seamons. Why johnny still, still can't encrypt: Evaluating the usability of a modern pgp client. *arXiv preprint arXiv:1510.08555*, 2015.

[27] Scott Ruoti, Tyler Monson, Justin Wu, Daniel Zappala, and Kent Seamons. Weighing context and trade-offs: How suburban adults selected their online security posture. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 211–228, 2017.

[28] Steve Sheng, Levi Broderick, Colleen Alison Koranda, and Jeremy J Hyland. Why johnny still can't encrypt: evaluating the usability of email encryption software. In *Symposium On Usable Privacy and Security*, pages 3–4. ACM, 2006.

[29] Stu Sjouwerman. 91blog.knowbe4.com. https://blog.knowbe4.com/bid/252429/91-of-cyber attacks-begin-with-spear-phishing-email. [Accessed 06-Feb-2023].

[30] Daniel J Solove. I've got nothing to hide and other misunderstandings of privacy. *San Diego L. Rev.*, 44:745, 2007.

[31] Chris Stokel-Walker. Almost no one encrypts their emails because it is too much of a hassle. https://www.newscientist.com/article/2289747-almost-no-one-encrypts-their-emails-because-it-is-too-much-of-a-hassle/. Accessed 06-Feb-2023.

[32] Noel Warford, Collins W Munyendo, Ashna Mediratta, Adam J Aviv, and Michelle L Mazurek. Strategies and perceived risks of sending sensitive documents. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 1217–1234, 2021.

[33] Alma Whitten and J Doug Tygar. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *USENIX security symposium*, volume 348, pages 169–184, 1999.

[34] Justin Wu and Daniel Zappala. When is a tree really a truck? exploring mental models of encryption. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 395–409, 2018.

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' 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 of 1 to 4? (1:Not at all familiar, 2:Slightly familiar, 3:Moderately familiar, 4:Very familiar)

[Researcher' Script] *You can stop sharing your screen!*

Task 2

[Researcher' 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' 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' 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 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 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 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 HRD via Virtru? (Not at all concerned, Slightly concerned, Moderately concerned, Very concerned)

Scenario [Researcher' 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' 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 W-9 Form based on this given scenario]

   Scenario [Researcher' 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 hours. 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 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' 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?

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.