Elham Al Qahtani, Yousra Javed*, and Mohamed Shehab

User Perceptions of Gmail's Confidential Mode

Abstract: Gmail's confidential mode enables a user to send confidential emails and control access to their content through setting an expiration time and passcode, pre-expiry access revocation, and prevention of email forwarding, downloading, and printing. This paper aims to understand user perceptions and motivations for using Gmail's confidential mode (GCM). Our structured interviews with 19 Gmail users at UNC Charlotte show that users utilize this mode to share their private documents with recipients and perceive that this mode encrypts their emails and attachments. The most commonly used feature of this mode is the default time expiration of one week, and the least used feature is the pre-expiry access revocation. Our analysis suggests several design improvements.

Keywords: Gmail Confidential Mode, Email, Encryption, Confidentiality, Privacy, User Perceptions, Ephemeral Communication

DOI 10.2478/popets-2022-0010
Received 2021-05-31; revised 2021-09-15; accepted 2021-09-16.

1 Introduction

Email content is not end-to-end encrypted by default, and therefore is vulnerable to unintended disclosure during transmission. Various tools exist for achieving email privacy through end-to-end encryption between email sender and receiver. Among these, GNU Privacy Guard is notable. Similarly, many email service providers provide support for Secure/Multipurpose Internet Mail Extensions (S/MIME) and Pretty Good Privacy (PGP) in their clients. However, studies on these tools have shown that end-users struggle with configuring end-to-end encryption on their emails [43, 46, 58].

Gmail—the most popular email service provider for personal and business use [33]—introduced the "confidential mode" in 2018 for ephemeral email communication and access control. This helps protect sensitive information from unauthorized access. Users can set a message expiration date, revoke message access at any time, and require an SMS verification code to access messages [21, 24]. The feature is available for use with various devices e.g., laptops, mobile phones, and tablets [22].

Gmail's confidential mode does not encrypt email content and uses its own mechanism for ensuring confidentiality. When this mode is used in an email, Gmail removes the email body and any attachments from the recipient's copy of the email. These are replaced with a link to the email's content. Gmail clients then make the linked content appear as if it is part of the email. Third-party mail clients display a link in place of the content [24, 35]. The confidential mode also prevents recipients from forwarding, copying, printing, or downloading messages, including attachments. However, it does not prevent recipients from taking screenshots or photos of the messages or attachments (similar to Snapchat). Recipients may still be able to copy or download these messages or attachments through other means such as saving the HTML page.

A wide amount of literature exists on the usability and effectiveness of end-to-end email encryption tools. However, to the best of our knowledge, user perceptions and motivations for sending private emails using other confidentiality tools, such as Gmail's confidential mode, have not been explored. This paper seeks to answer the following research questions:

1. What motivates users to use the confidential mode?
2. What are users' perceptions of confidential mode?
3. Do users understand the features of this mode i.e., expiration time, permission restriction, and pre-expiry access revocation?

We conducted a structured interview-based study with 19 Gmail users at a university who have experience with using its confidential mode feature. Our results show that users use this mode to share their confidential private documents with recipients and perceive that this mode encrypts their emails and attachments. The most commonly used feature of this mode is the default time expiration of one week, and the least used feature is the pre-expiry access revocation. Our analysis has several

Elham Al Qahtani: University of North Carolina at Charlotte, E-mail: ealqahta@uncc.edu
***Corresponding Author: Yousra Javed:** Illinois State University, E-mail: yjaved@ilstu.edu
Mohamed Shehab: University of North Carolina at Charlotte, E-mail: mshehab@uncc.edu

design implications. Firstly, the users should be made aware of GCM and its features while attaching files in emails. Similarly, mechanisms other than documentation should be developed to inform users regarding associated risks/limitations(e.g., screenshots and lack of encryption). Moreover, usability of some of the features can be improved. For instance, using a read receipt for "pre-expiry access revocation".

The remainder of this paper is organized as follows. Section 2 provides background on GCM. Section 3 presents the most relevant literature to this work. Section 4 describes the methodology of our study, and the results are presented in Section 5. Section 6 provides a discussion of our findings. Section 7 concludes our paper with the main takeaways.

2 Gmail's Confidential Mode

Google introduced a service in early 2018, namely Gmail Confidential Mode (GCM), which provides Gmail users with built-in access controls for their emails. The GCM icon is represented by a lock with a timer symbol, as shown in Figure 1 (a). Users can turn on the confidential mode by clicking on this icon. GCM's features allow Gmail users to do the following:

- Set an expiration date by specifying the amount of time the email will be accessible to the recipient.
- Set an SMS passcode (one-time passcode) to verify the recipients who can access the messages.
- Revoke access to messages before their scheduled expiration date.
- Prevent recipients from forwarding, copying, printing, or downloading message contents or attachments.

When users compose an email with "confidential mode" turned on, they can adjust the confidential mode's settings (as shown in Figure 1 (b)) by managing the expiration time and setting an SMS passcode. Once a user clicks the confidential mode button, it sets the default confidentiality features such as a default expiration time of one week. The subject line will remain, but the body text will disappear once the expiration date has elapsed. When Gmail users send a confidential email to recipients who use a different email service, such as Outlook.com, the recipient will receive an email containing a link with a one-time code generated by Google before viewing the message (see Figure 2). They can additionally be requested to confirm their identities by requiring a passcode sent to their phone number. However, the SMS passcode feature is limited to certain regions (America, Europe, Australia, and some countries in Asia) [21].

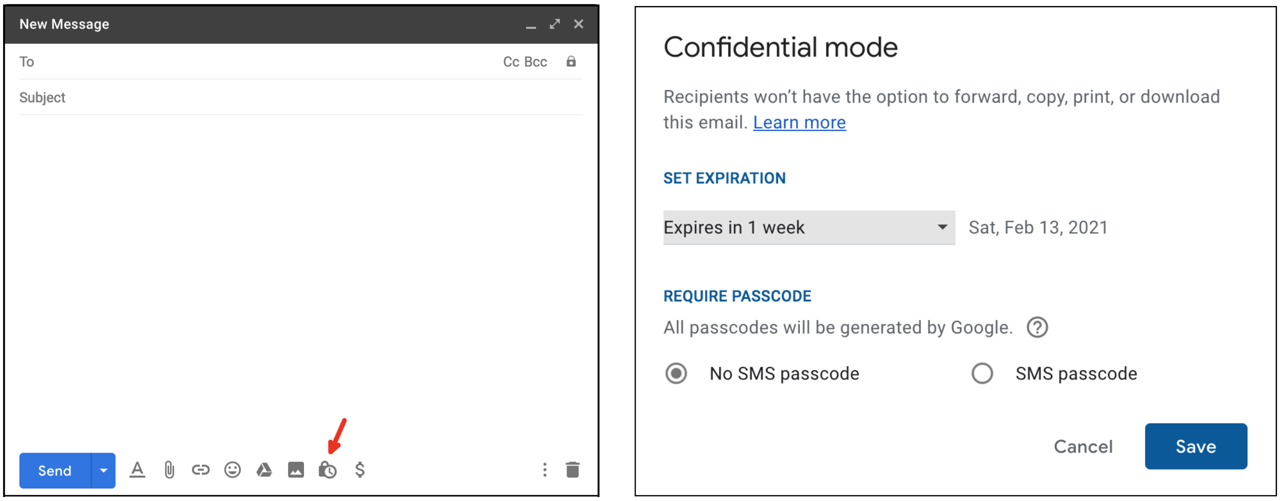
GCM therefore prevents unauthorized access by protecting emails that include sensitive information. However, there are limitations. A confidential email is sent over TLS, a secured subnetwork, however it is not completely secure, so emails sent outside an improperly configured server or containing individual attachments won't be encrypted [53]. Thus, confidential mode emails are not end-to-end encrypted. In addition, the confidential mode doesn't prevent recipients from taking screenshots or photos of the messages or attachments or saving the HTML page. Another issue is that Google will have access to recipient's phone number (to send the passcode) without their consent. Markert et al.[28] experimented with a phishing attack that mimicked the GCM's look and showed how attackers could obtain the one-time passcode (2FA) sent via SMS, which was received by Google's two-factor authentication. Motivated by the above factors, we investigated how users perceive email security and privacy when using GCM.

3 Related Work

The literature most relevant to our work falls under three categories: 1) adoption of security/privacy tools, 2) mental models of encryption and 3) ephemeral communication.

3.1 Adoption of Security Tools

Several factors and motivations behind the adoption of security tools in various contexts have been investigated. For instance, Alkaldi and Renaud [3] identified the factors such as poor advertisement and lack of trustworthiness, that impact users' decision to adopt smartphone password managers. Similarly, ease-of-use, required cognitive efforts, and trustworthiness have been identified as key factors that influence the adoption of two-factor authentication [11, 23, 37]. Other studies have looked at users' perceptions and motivations for (not) following computer security advice (updating software, using a password manager, using two-factor authentication, and changing passwords frequently) [15] and smartphone security advice (using a screen lock, updating the device's software, deleting suspicious text messages, and using secure Wi-Fi) [2].



Confidential mode

Recipients won't have the option to forward, copy, print, or download this email. Learn more

SET EXPIRATION

Expires in 1 week — Sat, Feb 13, 2021

REQUIRE PASSCODE

All passcodes will be generated by Google.

● No SMS passcode ○ SMS passcode

(a) Gmail's confidential mode button **(b)** Features (defaults) of Gmail's confidential mode

Fig. 1. Email composition window showing Gmail confidential mode

Abu-Salma et al. identified significant obstacles that influence users' decisions about not adopting secure communications and found that most participants did not understand end-to-end encryption, utilized incompatible tools, and had incorrect mental models about how encryption works [1]. Also, poor usability hinders the adoption of security and privacy tools. For instance, user interface design problems lead to users' failure to utilize secure tools for creating PGP encrypted emails [18, 58]. However, some of the secure messaging applications (e.g., WhatsApp and Signal) hide the encryption details, and the users are unable to perform the authentication ceremony without adequate instructions [52].

Other studies [19, 38] have examined the adoption and use of secure email tools by users, exploring why these tools are not widely adopted. For instance, researchers [19] have identified barriers that hinder the adoption of encrypted email in the workplace. The participants did not consider using it frequently due to technical factors, usability and social considerations. Another study [42] demonstrated that when secure email tools are integrated with webmail, such as Gmail, they have a greater chance of being adopted by average users.

We add to the existing literature by understanding users' motivations for using GCM features.

3.2 Mental Models of Encryption

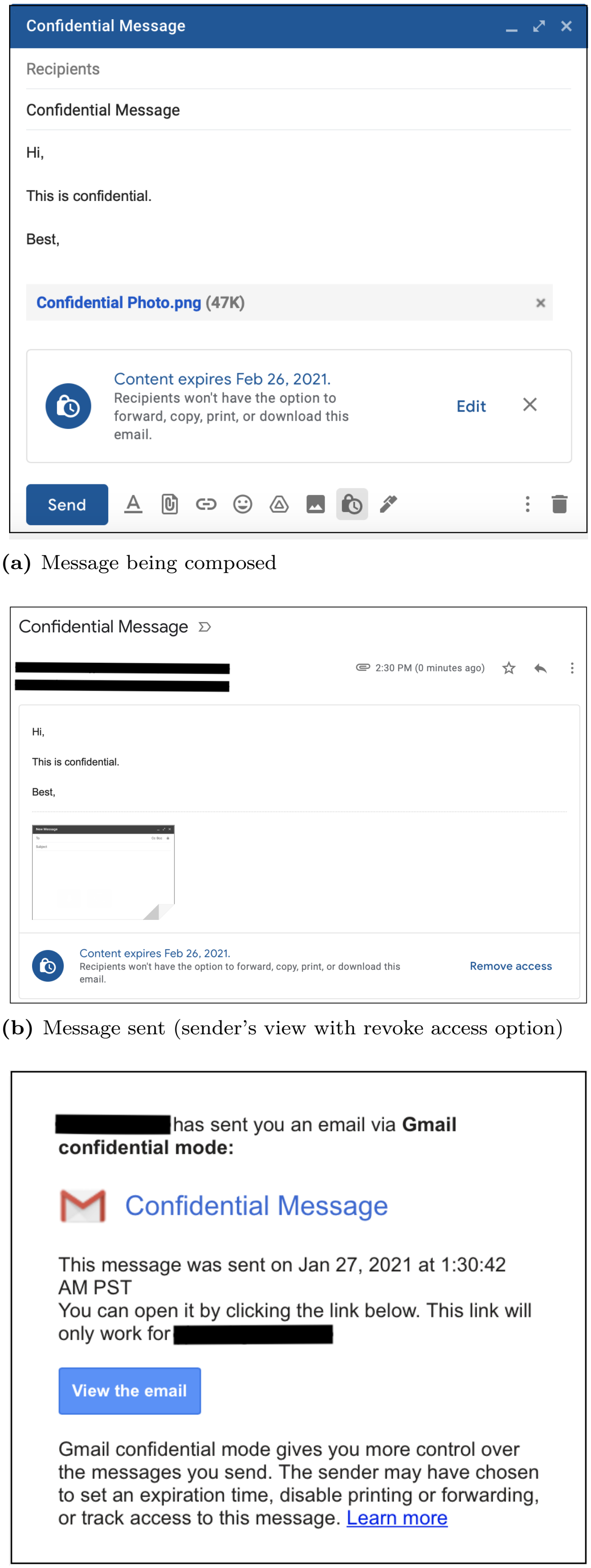
Human behavior depends on differences in perceptions and perceived intelligence [45]. Huang et al. [25] investigated the factors that influence people's perceptions of common security threats. They found that people's perceptions of information security are based on six factors: knowledge about threats, threats' impact on people, the ability to perceive the severity of a threat, the ability to control the threat, the possibility that the threat will occur, and awareness of threats.

Understanding users' mental models can help improve risk communication [7] and help them make the right security decisions [56]. Routi et al. found that users have a perception that using automatic encryption tools causes security issues whereas systems with manual encryption are trustworthy [44]. Wu et al. [59] identified users' (mis)conceptions about encryption in terms of functional (e.g., access control) and structural mental models. Another study showed that even after receiving educational training about end-to-end encryption, users were still confused about information integrity and authenticity [4]. Additionally, Krombholz et al. [27] identified the misconceptions about HTTPS by asking participants to think aloud while drawing their thoughts related to different scenarios.

We examined users' perceptions of GCM in terms of encryption, ephemerality, and access control.

3.3 Ephemeral Communication

Ephemeral content/self-destructing messages automatically disappear from the recipient side after the message has been viewed or after a certain amount of time has elapsed.



Confidential Message

Recipients

Confidential Message

Hi,

This is confidential.

Best,

Confidential Photo.png (47K)

Content expires Feb 26, 2021.
Recipients won't have the option to forward, copy, print, or download this email.

(a) Message being composed

Confidential Message

[redacted]

2:30 PM (0 minutes ago)

Hi,

This is confidential.

Best,

Content expires Feb 26, 2021.
Recipients won't have the option to forward, copy, print, or download this email.

(b) Message sent (sender’s view with revoke access option)

[redacted] has sent you an email via **Gmail confidential mode:**

Confidential Message

This message was sent on Jan 27, 2021 at 1:30:42 AM PST
You can open it by clicking the link below. This link will only work for [redacted]

Gmail confidential mode gives you more control over the messages you send. The sender may have chosen to set an expiration time, disable printing or forwarding, or track access to this message. Learn more

(c) Message sent (receiver’s view)

Fig. 2. Email composed using Gmail confidential mode

Ephemeral messaging is being widely used in social media applications such as Snapchat (direct messages and stories), Facebook (stories), and Instagram (stories) for achieving access control and privacy [51] [49]. Taking a screenshot of the content triggers a notification to the other party. Thus, these social media apps implement confidentiality [41] through the feature of self-destructing messages [29]. Similarly, some messaging applications such as WhatsApp have recently introduced a self-destruct feature, allowing a user to set an expiration time to a message [12].

Researchers have found that users adopt ephemeral content based on motivations such as fear of missing out, trust, immediacy, and social pressure to obtain gratification [5, 8]. The messages can also be captured by other methods [14] without alerting the receiver’s application. Self-destructing messages are not permanently deleted after their timeout [26, 31, 36, 39].

We extend this work by evaluating the email expiration feature of Gmail’ s Confidential Mode since the concept of ephemerality is new to emails.

4 Methodology

In order to understand the user perceptions and motivations of GCM, we conducted structured interviews with 19 participants from UNC Charlotte, who were aged 18 and above, had personal Gmail accounts, and had used GCM. The interview structure and format followed Watson et al.’s design for exploring user perceptions about Google+ circles [57]. Moreover, we used a usable security expert’s feedback to remove potential biases and misunderstandings in our questions.

4.1 Study Design

Eligible participants were invited to the usability lab on campus for in-person interviews or online meetings via Zoom. The participants who completed the study in-person, read and signed the consent form, whereas for the participants who were interviewed online, we verbally read the consent form and asked them if they agreed to participate.

We utilized our lab’s desktop computer for the in-person participants, while the online participants used their own devices during the study. In both settings, the audio was recorded. For the lab participants, audio was recorded using interviewer’s smartphone, while during Zoom interviews, the audio was recorded using Zoom's record feature which additionally recorded the entire session (with participant's permission) including instances where participants shared their screen. However, no personal/confidential information of the uninvolved persons was captured during screen sharing. For instance, during email composition, the message window was maximized to hide inbox emails from the background. Similarly, to show past GCM email, participants zoomed into a GCM email to show only the part that contained GCM icon or related statement such as "Content is expired". We only used the audio/ text(captions) files from Zoom interviews in our analysis and any video/screen share files automatically captured were deleted after data collection.

The collected data comprised participants' motivation for using GCM and their understanding of how it works. The participants were first asked a set of demographic questions (age, education, gender, job, and technical level) and questions regarding their motivations for using confidential mode, i.e., whether they used it for specific people or a particular content type, and why they used it. The interview questions are listed in the Appendix A.1.

Next, the participants performed a set of tasks, including, composing a confidential mode email and thinking aloud as they performed the task. We were interested in knowing what confidential mode meant to the participants, whether they confused it with encryption, and whether they understood the mode's features for achieving confidentiality.

In the last task, the participants were asked to review a few of their past confidential mode emails and answer a set of questions related to these emails. The remote participants were requested to share their screen. However, they stopped screen-sharing when viewing their past GCM emails. In this part, we investigated whether the participants understood the features of this mode for achieving confidentiality, permission restriction, expiration time, and pre-expiry access revocation:

- **Expiration Time:** We asked whether participants were aware that they could set an expiration date on the message and that the recipient would no longer be able to view the message after it expired.
- **Authentication:** We asked whether participants were aware that they could require an SMS passcode for the recipient to access messages.
- **Pre-Expiry Access Revocation:** We asked whether participants were aware that they could remove message access at any point before the set expiry time.
- **Permission Restriction:** We asked whether participants were aware that this mode ensures that the recipient does not forward, download, or print the email, but that the recipient could still take screenshots.

Therefore, we asked the participants whether they set an expiration date on the content, required an SMS passcode, revoked message access, and prevented the recipient from forwarding, downloading, or printing the content of and attachments to their emails. If a participant's response was yes, they were asked what they used these features for, why they chose them, and what was their confidence rating in using these features. Those who did not use these features were asked to explain why they decided not to use them.

Each interview session lasted for an average of 25 minutes. The participants were thanked for their time, and rewarded with a $5 Starbucks gift card. The study was approved by the university's Institutional Review Board (Protocol #19-0556).

4.2 Analysis Method

We collected qualitative data and utilized an inductive approach for our analysis. The audio of each interview was recorded and transcribed. Two researchers coded the transcribed audio data independently. The two sets of coded data were then compared and discussed to produce final codes after resolving any disagreements. For this reason, we did not conduct Cohen's Kappa test (inter-rater agreement). The entire codebook is added in the Appendix A.2.

4.3 Recruitment

Participants were recruited through a mass email sent via a research announcement to all faculty, staff, and students at our university. Interested individuals proved their eligibility in a privacy-preserving manner by only showing us the portion of a previous GCM email that included the GCM icon or statements such as "This message was sent via confidential mode" or "Content is expired".

4.4 Demographics

We interviewed 19 participants from UNC Charlotte as shown in Table 1. Participants were asked a set of demographic questions, such as age, gender, highest level of education completed, occupation and technical skill level.

The majority of our participants were female (N= 12, 63.2%), whereas 7 participants were male (36.8%). 17 of our participants were aged 18–39 years. Regarding the highest level of education achieved, 7 of the participants had completed high school, 4 had completed a bachelor's degree, 4 had completed a master's, 2 had completed associate's, and 1 had completed a doctorate. Our participants were mostly students, but few of them had full-time employment. Besides that, we did not collect any specific information about each student's major. However, the majority of those who answered the occupation question provided their major. Others also provided their current level of education with the highest level they have completed. 14 participants rated their technical skills as high, whereas 5 participants rated them as low (on a scale from 1 to 10) with 1 being low and 10 being high.

5 Results

We used an inductive approach to analyze the collected qualitative data. The coding procedures were described in Section 4.2. Below, we report the questions and the main codes derived from participants' responses.

After the participants answered demographic questions, they were asked about their email usage, i.e., which email service providers they used and how often they used them. All of our participants used Gmail. Other email services reported were Yahoo (5 participants), Hotmail (4 participants), and Outlook (4 participants). The majority of our participants used Gmail every day compared to the other email services.

We also asked the participants about their frequency of use of GCM. We wanted to know how long they had used GCM and how frequently they had used it. We found that most participants had used GCM since last year (2020), while four of them had been using it since 2019. A majority of our participants used GCM one or more times per week.

#	Age	Education	Gender	Occupation	Major[1]
P1	30	Master's	Female	PhD student	Information Systems
P2	20	High school	Female	Nursing assistant	-
P3	20	High school	Female	Student	-
P4	26	Bachelor's	Male	Student	Computer Science
P5	38	Master's	Female	Instructor/ Student	Computer Science
P6	19	Associate's	Male	Student	Mathematics and Computer Science
P7	22	Bachelor's	Female	Student	Computer Science and Business Administration
P8	29	Bachelor's	Female	Student	Chemical Engineering
P9	19	High school	Male	Student	Computer Science
P10	47	Doctorate	Male	Professor	Curriculum Instruction and Educational Policy
P11	34	Master's	Female	Student	Health Informatics
P12	22	Bachelor's	Male	Student	Criminal Justice
P13	19	High School	Female	Employee at restaurant/Student	Computer Science
P14	22	High School	Female	Student	Communications
P15	19	High School	Female	Student	Meteorology
P16	53	Bachelor's	Male	IT consultant	-
P17	30	Master's	Male	Student	Electrical and Computer Engineering
P18	19	High School	Female	Tax Associate	Accounting
P19	33	Associate's	Female	Student	Media Communications

Table 1. Participant demographics

[1] Major was not explicitly collected

5.1 Motivations for Using Gmail's Confidential Mode

To answer our first research question ***"What motivates users to use the confidential mode?"***, we asked participants what made them start using GCM. We believe that users' perceptions highlight how confidential emails have been approached, impacting their willingness to share confidential content and attachments.

Participants reported a variety of reasons for using GCM. The most pronounced reason was sharing confidential documents (12/19). The majority of our interviewees began using GCM for sending sensitive documents, including personal identification documents (e.g., driver's licenses, passports, financial statements, or medical records).

We also noticed that participants used GCM to prevent unauthorized access (4/19). They were concerned about unauthorized people accessing their confidential documents or accidental sharing with the wrong people. Participants used GCM's default time expiration after one week, to allow recipients to access information temporarily (4/19).

> **P8**: *"Initially, when I wanted to share my information with a third party where I didn't want them to have that for a long time, I used it when I wanted to add my name to the existing new lease. So they asked me for some documents ... but I didn't want them to have it for too long so I sent it through confidential mode so they could just view it. ... After some time it just expires."*

Another reason given by interviewees for using GCM was curiosity (3/19), which led them to explore GCM's security features to make better security decisions. For instance,

> **P5**: *"Actually, I'm curious about my confidentiality. ... So that's what raised my attention. I felt like it will meet my requirements specially when I send some really critical information and I don't want the other person to reuse it in a different way than as I had wanted."*

A few participants mentioned that they started using GCM thinking that it was encrypted. For example, **P15** stated that she was confident that she was sending an encrypted email with confidential mode when sharing patient information related to the Health Insurance Portability and Accountability Act (HIPAA). Also, two participants valued their data privacy when sharing confidential content. They clarified that it provided more privacy to their email content and attachments, perceiving that no one would see the email except the recipients.

Furthermore, a number of participants expressed that their motivation for utilizing GCM was remote confidential information sharing since they could not hand over important documents physically once the pandemic started. Another participant **(P16)** received a suggestion to use GCM from his work colleague. He then suggested this mode to other people.

Next, we asked the participants what type of email content they used GCM for. We found that 19 participants used GCM to send private documents, which was similar to their motivation for using GCM. These documents included legal documents between two companies, work-related documents, financial records, personal information (e.g., private pictures, as shown in the quote below), governmental and tax documents, and medical information (e.g., patient records, pet files, immunization records). Also, participants used GCM to share private non-work-related documents with family members, such as parents and spouses (3/19).

> **(P5)**: *"I would say things that should be really very private between me and the person that I send them to. Sometimes I may do that if I'm sending pictures of mine. I would really like to keep their privacy, and I don't want them to be kept forever. So, mainly they are for personal information."*

Our study found that participants attached various files or documents, such as PDFs, Excel files, scanned images, Word files, and text messages in their GCM emails.

Next, the participants were asked to whom they sent GCM emails and why they chose to share with them. We observed that participants sent confidential emails to several recipients. This included family members and close relatives (11/19) (e.g., parents, spouses, partners, or friends), administrative team members (7/19) (e.g., upper management, company manager, government officials, school offices, or admissions officers), financial employees (7/19) (e.g., financial managers or bank consultants), for teamwork (3/19) (e.g., clients, classmates, teammates), medical personnel (2/19) (e.g., doctors, veterinarians), and a leasing office (1/19).

Participants also stated their reasons for sharing confidential emails with these recipients. A number of participants mentioned that they couldn't physically share confidential documents once the pandemic had started (4/19), so GCM served as a solution. Another reason (4/19) was that the administrative team (e.g., company manager, admissions officers) requested that they share confidential documents that related to their work. Participants also reported that the recipients of these documents requested them to be sent privately (3/19). Moreover, a few participants either trusted the receiver (2/19) or used GCM to prevent unauthorized access (2/19). One participant (P5) also mentioned that she could use GCM to achieve privacy while using the internet without using a VPN:

(P5): *"So once the pandemic started, it gave me time to be able to just try all these things out, different services and such. I had privacy concerns, because I just hadn't been using internet, without a VPN. There was, I think, a few years ago there was like a wave of hacks of personal emails and that's what kind of like inspired me to look into kind of making sure that my information is private."*

Table 2 summarizes the themes of participants' motivations, the type of content that is used in GCM emails, and the type of recipients who received GCM emails.

Motivation for Using GCM	**# Participants**
Sharing confidential documents	(12/19)
Prevent unauthorized access	(4/19)
Encryption	(2/19)
Curiosity	(3/19)
Replacement for physical	(2/19)
Information sharing during pandemic	(2/19)
Requirement of sharing work documents	(1/19)
Type of content in GCM	**# Participants**
Private non-work-related documents	(3/19)
Work-related documents	(5/19)
Financial records	(5/19)
Governmental and tax documents	(3/19)
Legal documents	(1/19)
Medical documents	(2/19)
Type of recipients in GCM	**# Participants**
Family members and close relatives	(11/19)
Administrative team members	(7/19)
Financial employees	(7/19)
Teamwork at school office	(3/19)
Medical personnel	(2/19)
Leasing office staff	(1/19)

Table 2. Summary of motivations for using GCM along with the type of content and recipients in GCM emails

5.2 Perceptions of GCM

Our second research question was ***"What are users' perceptions of confidential mode?"*** We asked the participants to compose a confidential email related to this interview experience and think aloud as they complete this task. After the task was completed, participants were asked how the confidentiality was being achieved, and whether the composed email was encrypted. We asked participants to perform this task as it would enable them to articulate their best understanding of the topic and discuss their thoughts on how confidentiality could be achieved in this mode and whether the composed email was encrypted or not.

Participants showed us how they composed the email in confidential mode. They started by clicking on the button of the confidential mode. After seeing the GCM settings dialog box, they started explaining how they use them. They demonstrated how they could modify these settings. For example, some participants changed the default expiration date or chose not to use SMS passcode when they used this mode. We found that participants experienced the GCM as intuitive to use. The features' evaluation is discussed in depth in the following sections and Table 3 summarizes participants' perceptions of GCM regarding achieving confidentiality and encryption.

5.2.1 Confidentiality

When asked how confidentiality was achieved in this mode, many participants explained that it was accomplished by using one of the confidential mode features. These included setting an expiration date (8/19); enabling authentication (4/19); disabling options to forward, copy, print, and download the emails (9/19); and including confidential links (2/19). One participant also mentioned that GCM is achieving confidentiality by enabling a high level of encryption. Each theme is described in detail below.

Setting an Expiration Date. Participants explained that confidentiality in this mode is achieved by choosing an expiration date. This feature prevents a recipient from being able to view confidential messages after a certain time. For example, one of the participants **(P2)** commented, *"I usually set my confidential mode to expire like within a week. So, I know that they've gotten it, but then the email, like after a week expires."*

Enabling Authentication. Four participants clarified that the confidentiality of the message was achieved through the use of second factor for authentication (SMS passcode generated by Google). The recipients received an SMS passcode through a text message to access their confidential messages. For instance, one participant **(P18)** mentioned: *"Because this information cannot be leaked or be handed to the wrong people so in case this email is being sent to the wrong recipient,* *or in case of anything, due to the passcode, they cannot access it."*

Enabling a High Level of Encryption. One participant **(P6)** mentioned the availability of stronger encryption when a GCM email was sent: *"When the email is normally sent, there's the basic encryption, that it goes through, but [it] is saved permanently. But this one has a high degree of encryption."*

Including a Confidential Link. Two participants mentioned that including a link to content in their email meant it was confidential and that the link expired after a certain amount of time. For instance, one of them **(P16)** commented: *" Instead of whatever it is that I'm sending to them... [and they are] receiving a copy of it, and having that copy reside physically on their computer, they're just getting a link to whatever it is I'm sending them and can be expired."*

Disabling Options to Forward, Copy, Print, and Download. Participants also perceived that confidentiality was maintained by preventing recipients from accidentally sharing their emails (e.g., forwarding, copying, printing, and downloading). For example, one **(P5)** said: *"Disabling the ability of the receiver to edit or share this email with others.... So besides confidentiality, which I consider keeping my private information with high privacy.... So, there will be high integrity and confidentiality. So I would feel really secured with that option."*

5.2.2 Encryption

Participants were asked whether their email was encrypted. If they thought so, they explained how it was encrypted and why. We found that 11 participants perceived that their GCM email was encrypted, whereas 5 participants were not sure if it was encrypted. Surprisingly, only 3 participants stated that sending an email in confidential mode does not mean that it is encrypted. Table 3 summarizes user perceptions regarding confidentiality and encryption in GCM.

Encrypted: Participants were convinced that email in this mode was encrypted due to their trust in Google services. For instance, one participant **(P12)** said: *"Yes, I believe so. I'd say, you know, I trust Google, and I have faith and confidence in the services that they provide."* Other participants perceived it as encrypted since it used security features such as an SMS passcode or time expiration. For example, one **(P7)** noted that, *"by pushing that button it is being encrypted and by doing so in a certain amount of days, it will get deleted itself."*

Not Sure: A number of participants were unsure whether GCM emails were encrypted since they had no knowledge of the hidden process of how confidentiality worked. For example, one **(P10)** stated: *"I don't know enough about the sort of inner working of the mode, whether it's truly encrypted but my guess is that it is an extra layer of [secure link], I mean that's where you keep the confidentiality.... I don't think I know quite enough about how confidentiality works and if it's truly all encrypted, or there's a secure socket kind of secure SSL layer."*

Not Encrypted: Surprisingly, 3 participants assured that the GCM email was not encrypted because of their understanding of encryption and decryption as one stated below:

P16: *"The email is not encrypted, because of a few reasons. If it was encrypted, the recipient would have to know how to decrypt it. And that's unlikely. And just the way that Gmail confidential mode works, it doesn't really work by encryption. It works by sending them a link to whatever it is I'm sending them, which will remain on a Google server."*

Confidentiality in GCM	**# Participants**
By setting an expiration date	(8/19)
By enabling authentication	(4/19)
By disabling options to forward, copy, print	(9/19)
By including confidential links	(2/19)
By enabling a high level of encryption	(1/19)
Encryption in GCM	**# Participants**
Via security features	(11/19)
Unsure	(5/19)
Does not exist	(3/19)

Table 3. Summary of user perceptions of GCM regarding achieving confidentiality and encryption

5.3 Security Features of GCM

To answer our third research question, ***"Do users understand the individual features of GCM i.e., permission restriction, expiration time, and pre-expiry access revocation?"***, we asked participants to evaluate their last few (1 to 3) emails that they sent in confidential mode and answer a set of questions related to their use of each feature, as shown below. We wanted to know whether participants used these features in their emails and, if so, why they used them (if any), why they chose not to use them (if any), and what confidence they had in using these features on a scale from 1 to 5, where 5 indicated high confidence. The questions are included in the Appendix section A.1. Table 4 summarizes participants' reasons for (not) using GCM features.

5.3.1 Expiration Time

Gmail users can set an expiration time after which the email will not be visible to the recipients. The expiry date options include one day, one week, one month, three months, or five years. We found that 15 of our participants had set an expiration date on the content in their last emails, whereas the other three did not.

Participants who responded yes, were asked what this feature meant and why they chose to use it. They reported that they used this feature to prevent unauthorized access (4/15), to have temporal access (10/15), and to set content restrictions (1/15).

Participants set an expiration time to the confidential email within a week, including attachments, such as identification documents, to prevent unauthorized people from accessing it and misusing the content. Also, participants explained that setting an expiration time in the emails containing confidential documents prevents unauthorized access even if the user's email account is accidentally left logged in at multiple devices/locations.

One participant **(P8)** explained that she used this feature to restrict the recipient from downloading, printing, or using the information later. Also, a number of participants specified the expiry time in terms of hours or days. They stated that sensitive information (such as medical documents, tax documents, family gifts, and personal documents) would disappear and would no longer be vulnerable to any data leaks or information hacking. For instance,

P5: *"Because I wanted this data to not be available for long term storage. And because it will be invalid after sometime. So, I use that feature to make sure it will only be available within the time I designated. I would like to get this picture destroyed as soon as possible. This may encourage me to share some private pictures but for very a short time to make sure it will not be abused by others."*

Participants expressed their confidence in setting an expiration time as follows. Seven participants were strongly confident (5) using this feature (see the quote from **P5**), whereas four and three participants expressed their confidence at 4 and 3, respectively. One participant **(P1)** rated her confidence at 2.5 stating that she was unsure whether the confidential email was still in the cloud after the expiration date.

Few participants did not choose a short expiration time because of the concern that emails might delete themselves before they were read by recipients or because of the type of email account this email was used for (work vs. personal accounts).

5.3.2 Authentication

Gmail users can set an SMS passcode (a one-time passcode) generated by Google to verify the recipients who can access the confidential messages. We found that 8 participants required an SMS passcode in their emails, whereas 11 participants did not select an SMS passcode in their GCM emails.

Participants set passcodes for recipients to prevent unauthorized access to their emails (4/8),to use two-factor authentication for extra security (2/8), to ensure email privacy (2/8), and to ensure message safety (1/8).

Participants who required an SMS passcodes for the recipients stated their confidence in setting them. Three participants were extremely confident about using this feature, whereas four participants expressed strong confidence. One participant, **(P1)**, expressed only moderate confidence in the technology.

Eleven participants explained why they did not use an SMS passcode in their GCM email. The themes that emerged from their responses were as follows: using another security tool (1/11), using for specific accounts (1/11), avoiding any confusion (2/11), being convenient (4/11), trusting the recipient (1/11), considering it unnecessary (1/11), and not knowing the passcode (1/11).

For example, one participant **(P7)** utilized another security tool, stating that she used VPN to secure the messages when sending emails to recipients. Another reason an SMS passcode was not used in the confidential email was that it was only used on a work account, and not on a personal email account, as one participant **(P11)** commented, *"So it was my company requirement, it was not my personal thing, so I just abide by what they told me to follow."*

In addition, a number of participants did not utilize an SMS passcode in their GCM emails to avoid confusion due to the recipients' low technical expertise. Other participants stated that choosing not to use an SMS passcode made it more convenient and comfortable for recipients to access their confidential email. Also, one participant stated that this feature was not needed in the confidential email.

Another theme that emerged from participants' responses was the trust between the receiver and sender. For example, one participant **(P2)** trusted his family members and said:

> *"So we all trust each other that, you know, we're not going to need to have a text message sent to our phone in order to access the email.... We want a way that no one accidentally sends something by mistake. So that's why the SMS just seemed like an additional step that wasn't necessary for our purposes."*

5.3.3 Pre-Expiry Access Revocation

Confidential mode allows Gmail users to remove access to email content early before it expires. We found that most participants (14) did not revoke message access in any of their last emails. Further, five participants did not know what revoking message access meant and its purpose. Only one participant used this feature once, thinking that the receiver might not open their email.

Fourteen participants did not revoke email access before the expiration date for the following reasons: trusted the recipients (5/14), there was already an access restriction (e.g., expiration date) (4/14), and thought it was unnecessary (4/14). One participant also stated that content was not super sensitive (birth certificates (1/14)) and thus did not require revoking access.

Therefore, some participants already trusted and knew the identity of recipients, such as friends, administrators, or family members, which led them not to choose message access revocation before it expired. Also, a number of participants expressed that setting an expiration time for their confidential email was adequate for achieving the goal of using GCM. For example,

P16: *"I just didn't need to use it, I felt like the expiration date would be adequate. I didn't know when the person was going to look at the message. And I didn't want to keep up with it, it was easier to just let it expire instead of having to actively revoke it."*

A few participants stated that they were not aware of pre-expiry access revocation and how it works. Moreover, they did not understand the primary purpose of using this feature in general. Other participants found no reason to revoke message access in their confidential email, and they did not need to utilize this feature. For instance,

P18: *"I didn't see it [as] 100% necessary. If its in confidential mode, there shouldn't be a reason to revoke it unless it was the wrong recipient or we have to do anything like that, then that's another issue."*

5.3.4 Permission Restriction

GCM allows users to prevent the recipient from forwarding, copying, printing, or downloading message contents. We asked our participants about their experiences with preventing recipients from forwarding, downloading, or printing their last emails. As a result, 14 participants stated that the confidential mode would prevent recipients from doing that. However, 5 participants said that this mode would not prevent recipients from doing that.

We asked those who mentioned that recipients couldn't forward, download, or print emails about how this was accomplished. The majority of participants (10/14) stated that GCM by default prevents recipients from forwarding, copying, printing, or downloading message content or attachments. Also, some participants (3/14) were unsure whether recipients could forward, copy, print, or download message content or attachments in their last emails since they considered alternative methods that the recipients might use. Another participant stated that the sharing of private information among employees is done by following workplace rules such as not printing or forwarding confidential documents. For example, one participant **(P7)** mentioned:

> *"So, most of the time it is a work culture and kind of expected that we do not print the private information that you know may end up in an unauthorized person's hands, so most of the time it is known but I've never been in a situation where I've had to tell someone that please do not print this."*

Participants were also asked whether there were other ways in which the recipients could copy the content in their email. The methods identified by the participants were as follows: screenshots taken from the computer or smartphone screen (12/14), third-party programs to bypass security (1/14), and screen records using recording tools (1/14).

Even though participants mentioned other methods that recipients might use to capture the confidential content, many of them were still moderately confident. Participants stated their confidence on a scale from 1 to 5 (where 5 was strongly confident), about ensuring that the recipient could not forward, download, or print the email. Four participants were strongly confident since they trusted the receiver, while seven were moderately confident at a level of 3.

On the other hand, a few participants stated that they were unsure whether this mode would prevent recipients from forwarding, downloading, or printing the content. They believed that it was not required to prevent recipients (family members) from sharing or downloading the content. For example,

> **P9**: *"So I never really had to prevent them from sharing or something like that, but for my personal documents, it is my family that accesses the files, and I never did that with my family and classmates."*

6 Discussion

6.1 User Understanding/Expectations of GCM

According to the Electronic Frontier Foundation (EFF) [20], *"Google can see the contents of your messages and has the technical capability to store them indefinitely, regardless of any 'expiration date' you set. In other words, Confidential Mode provides zero confidentiality with regard to Google."* Our participants stated that confidentially is being achieved when GCM is used by clicking the "confidential mode" button and selecting one of its features. They expected confidentiality with regards to recipients and that the email will be fully deleted from recipient's inbox after expiration time. They also had expectations with regards to Google, but assumed that Google will have access to their email content. According to most participants, their GCM is encrypted and secure, and only receivers can read their confidential emails until they expire, after which the recipients will no longer have access to these emails. Some participants, however, indicated that Google also reads their encrypted emails in addition to the recipients before the time limit has expired. Thus, participants had a low understanding of encryption and confidentiality.

Table 5 summarizes the levels of participants' understanding of each GCM feature, interpreted from their open-ended responses on what each feature is, why they chose it, how they use it, and their confidence in correctly using it. High-understanding refers to correctly answering all four questions, medium-understanding refers to answering half of these questions correctly, whereas low-understanding means answering less than 2 questions correctly. "Usage" term represents the portion of participants who used this feature and not how frequently they used it. These levels were finalized with mutual agreement between the two coders. Participants trusted Google services, believing that GCM was encrypted and that its features (SMS code and expiration time) implemented the encryption process. Their trust in Google services confirms the findings of the Watson et al. study [57], who stated that participants who used

(Using) Expiration Time	**# Participants**
Prevent unauthorized access	(4/15)
Grant temporal access	(10/15)
Set content restrictions	(1/15)
(Not using) Expiration Time	**# Participants**
Email deletion	(2/4)
Type of email account	(2/4)
(Using) Authentication	**# Participants**
Prevent unauthorized access to emails	(4/8)
Use 2F authentication for extra security	(2/8)
Ensure email privacy	(2/8)
Ensure message safety	(1/8)
(Not using) Authentication	**# Participants**
Using another security tool	(1/11)
Using it for specific accounts	(1/11)
To Avoid any confusion	(2/11)
Being convenient	(4/11)
Trusting the recipient	(1/11)
Unnecessary	(1/11)
Not knowing the passcode	(1/11)
(Using) Pre-expiry Access Revocation	**# Participants**
Receiver might never open email	(1/1)
(Not Using) Pre-expiry Access Revocation	**# Participants**
Trust the recipients	(5/14)
Other access restrictions exist	(4/14)
It is unnecessary	(4/14)
Content is not super sensitive	(1/14)
(Using) Permission Restriction	**# Participants**
Provided by GCM by default	(10/14)
Following workplace rules	(1/14)
Recipients use alternative methods	(3/14)
(Not using) Permission Restriction	**# Participants**
Not required to prevent recipients from sharing or downloading content	(5/5)

Table 4. Summary of participants' reasons for (not) using GCM features

	Expiration time	Pre-expiry access revocation	SMS passcode authentication	Permission restriction	Encryption
Understanding	High	Low	High	Medium	Low
Usage	High	Low	Low	High	NA

Table 5. A summary of participant understanding and usage rating of GCM features

Google+ had a higher level of trust in Google with regard to their personal information.

The majority of the participants had a higher understanding of the expiration time and SMS passcode features for achieving confidentiality, as shown in Table 5. In contrast, participants had a moderate understanding of GCM's pre-expiry access revocation. Moreover, participants had a good comprehension of GCM's authentication feature, and that it was enabled based on their preferences. Many participants set an SMS passcode (one-time passcode) in their emails for adding a security layer to prevent unauthorized access and ensure message safety and privacy. The expiration time feature was also well understood by the participants. They did not revoke access to messages after setting an expiration date, believing that there was no need to do so or preventing such a scenario where the message was deleted before it had been viewed. Participants agreed that the confidential mode prevented recipients from forwarding, copying, printing, and downloading message contents through the permission restriction feature. However, when they started to think about other methods of capturing confidential documents (e.g., screenshots), they strongly relied on the trust relationship with the recipient. They believed that there was no need to revoke access to messages for trusted recipients.

6.2 GCM Usage

Our participants were able to compose a confidential email using GCM with an expiration time and permission restriction without any issues. However, it appeared that participants did not set an SMS passcode when they used this mode since setting an SMS passcode was inconvenient to use especially when the recipients are older and less tech savvy. Moreover, some did not revoke access to a message after setting an expiration date in order to prevent a scenario where it was deleted before the recipient had viewed the message.

Table 5 (the second row) shows that a majority of the participants frequently used the expiration time and permission restriction, whereas they used the other features (access revocation and authentication) less frequently due to usability issues.

The types of confidential private documents shared included tax documents, passports, financial statements, medical records, and photos. Therefore, participants used GCM for sharing sensitive documents both in person-to-person and person-to-business context. The documents included both non-work and work-related documents. The non-work documents were shared with close friends and relatives, such as parents, spouses, and partners. On the other hand, many participants shared work related documents with formal relationships, such as an office team. Users who shared work-related documents were more concerned about the third-party threats e.g., entities other than Gmail and the recipient gaining access to email content.

Many participants began to use GCM after the onset of the COVID-19 pandemic as they faced difficulties in sharing their sensitive documents physically. They aimed to prevent access by the wrong person. Furthermore, due to the deletion of these documents from recipients' inboxes, recipients can only temporarily access the information.

6.3 Design Implications

There are certain risks when users send private information via the confidential mode (GCM), contrary to users' belief that it is end-to-end encrypted and completely confidential. Moreover, certain GCM features are less used to avoid unforeseen circumstances. Therefore, our findings suggest several design improvements.

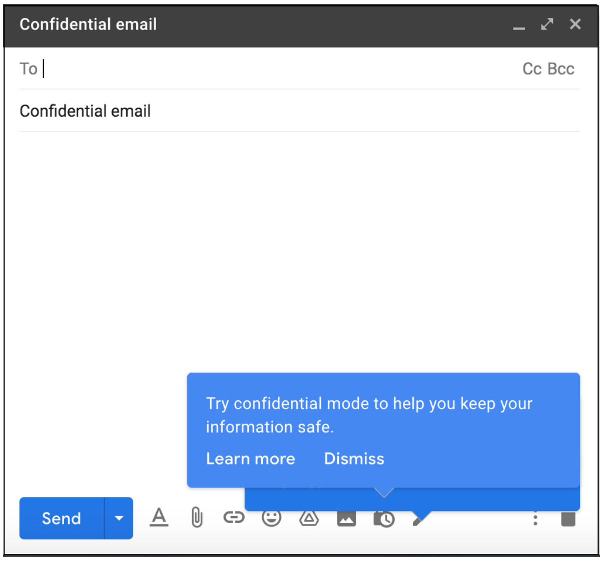
- **Improve risk communication**
  Effective risk communication involves delivering the risk information in a way that motivates users to make secure decisions [10, 30, 40]. For instance, the walk-through technique provides instructions on what users can do through the interaction. It has been used to support users learnability and improve the code quality and user experience of using new systems [6, 16]. In our study, we found that some of the participants believed that GCM uses a high level of encryption for their messages and attachments. Thus, we suggest that Gmail users should be informed that GCM does not add end-to-end encryption via a walk-through of the GCM features

(for new users) together with the misconceptions we found in our study.

Another approach to inform Gmail users that GCM does not add end-to-end encryption is by showing an icon of broken/non-existent email encryption. For example, in security warnings, engaging users through meaningful cues (such as icons and words) allows them to comprehend the context of the messages [60].

- **Provide the GCM email sender with a read receipt**

  We found that participants did not revoke access to messages after setting an expiration date in order to prevent a scenario where the message was deleted before it had been viewed. Therefore, we recommend that the sender be informed once the recipient has read the confidential message and clicked on the link e.g., by providing a read-receipt to the sender (similar to WhatsApp's blue-tick idea [9]). Secondly, a machine-learning based approach (similar to Pielot et al. [34]) can be used to estimate the amount of time after which the recipient is likely to read the email (based on recipient's past phone usage). This information can assist the sender in revoking access after the email has been sent or in choosing the appropriate expiration time while sending the GCM email.



Confidential email

Try confidential mode to help you keep your information safe.

Fig. 3. A notification message is shown if a user has not turned on the confidential mode in the past

- **Add watermarking feature in the email attachments**

  Watermark refers to a piece of hidden information (for example, text, image), which can be more or less transparent to the original document while providing individualized tracking for sensitive documents, copyright protection, and data authentication (e.g., ownership proof, copying prevention) [47]. We found that GCM does not prevent recipients from taking screenshots/photos of the received messages and attachments. The attachments (e.g., PDF, images) could be watermarked to prevent recipients from leaking sensitive photos similar to the feature provided by the email encryption tool Virtru [54], i.e., when documents are shared externally, they can be watermarked with authorized recipients' names, helping prevent data leaks and giving senders another mechanism to keep the sensitive data protected [48].

- **Improve the notification message about using GCM when including email attachments.**

  Gmail users who have not turned on the confidential mode in the past receive a notification message especially when they attach files to their emails, asking them to try using GCM to keep their information safe. Figure 3 shows Gmail's existing notification displayed (once) to Gmail users who have never used GCM. We recommend modifying it by including short description of confidential mode features (e.g., expiration date, access revocation before the expiration date) to its increase usage. The notification can be ignored if it provides no value to the user [32]. On the other hand, relevant and timely notifications have the power to reach users and capture their attention [55].

6.4 Limitations and Future Work

Our work is not without limitations. Firstly, there is a demographic bias in our sample. A majority of the participants were young (less than 30 years) due to recruitment from a university. The sample size is also small and not gender-balanced since the pandemic caused difficulties in recruiting/determining eligibility of participants over MTurk via GCM email screenshots. The high level of technical skill reported could be a result of participants being recruited from campus. An area of improvement would be to expand the study by including non-university participants in order to get a more diverse sample.

Secondly, we did not use a standardized questionnaire such as the Affinity for Technology Interaction

(ATI) [17], the Security Behavior Intentions Scale (SeBIS) [13] or the Internet Skills Scale [50] to measure technical expertise since our main goal was not to compare the perceptions of technical experts and non-experts. However, this can be a future extension of this work.

Moreover, since UNC Charlotte has disabled Gmail's confidential mode, the faculty, staff, and students can't send Gmail messages in confidential mode using their university accounts. Therefore, our participants used their personal Gmail accounts for the study.

The encryption question asked from the participant to get their perception of whether GCM uses encryption may be too simplistic and not account for real-world nuances. A more detailed approach could have been a less technical or indirect way of asking the same question.

There are several future directions for this work. It is possible to expand it via a quantitative online study. The questions for such study can be based on the findings from the interviews. Another interesting path could involve a simple browser extension that directly inserts risk communication notifications into Gmail's web interface. The effectiveness of these notifications could also be measured.

7 Conclusion

We conducted a qualitative interview-based study with 19 Gmail users, investigating their motivations for using confidential mode as well as their understanding of each feature for achieving confidentiality (e.g., permission restriction, expiration time, authentication, and pre-expiry access revocation).

The participants used GCM to share their confidential/private documents with recipients both in person-to-person and person-to-business context. Moreover, they perceived GCM to be end-to-end encrypted and confidential. The most commonly used feature of confidential email was the default time expiration within a week, and the least used feature was the pre-expiry access revocation.

Our analysis has several design implications. Firstly, the users should be made aware of GCM and its features while attaching files in emails. Similarly, mechanisms other than documentation should be developed to inform users regarding associated risks. Moreover, usability of some of the features can be improved. For instance, using a read receipt for "pre-expiry access revocation".

8 Acknowledgements

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

[1] 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.

[2] 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.

[3] Nora Alkaldi and Karen Renaud. Why do people adopt, or reject, smartphone password managers? 2016.

[4] Wei Bai, Michael Pearson, Patrick Gage Kelley, and Michelle L Mazurek. Improving non-experts' understanding of end-to-end encryption: An exploratory study. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 210–219. IEEE, 2020.

[5] Joseph B Bayer, Nicole B Ellison, Sarita Y Schoenebeck, and Emily B Falk. Sharing the small moments: ephemeral social interaction on snapchat. *Information, Communication & Society*, 19(7):956–977, 2016.

[6] Maya Cakmak and Leila Takayama. Teaching people how to teach robots: The effect of instructional materials and dialog design. In *Proceedings of the 2014 ACM/IEEE international conference on Human-robot interaction*, pages 431–438, 2014.

[7] L Jean Camp. Mental models of privacy and security. *IEEE Technology and society magazine*, 28(3):37–46, 2009.

[8] Kuan-Ju Chen and Hoi Ling Cheung. Unlocking the power of ephemeral content: The roles of motivations, gratification, need for closure, and engagement. *Computers in Human Behavior*, 97:67 – 74, 2019.

[9] Karen Church and Rodrigo De Oliveira. What's up with whatsapp? comparing mobile instant messaging behaviors with traditional sms. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*, pages 352–361, 2013.

[10] National Research Council et al. Improving risk communication. 1989.

[11] Emiliano De Cristofaro, Honglu Du, Julien Freudiger, and Greg Norcie. A comparative usability study of two-factor authentication. *arXiv preprint arXiv:1309.5344*, 2013.

[12] Tech Desk. New whatsapp feature brings self-destructing messages: How it works. https://indianexpress.com/article/technology/social/whatsapp-self-destructing-message-available-how-to-use-6316569/, 2020. Last accessed 8 February 2021.

[13] Serge Egelman and Eyal Peer. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pages 2873–2882, 2015.

[14] Rip Empson. Not-so-ephemeral messaging: New snapchat "hack" lets users save photos forever. https://techcrunch.com/2013/01/22/not-so-ephemeral-messaging-new-snapchat-hack-lets-users-save-photos-forever/, 2013. Last accessed 2 February 2021.

[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, 2016.

[16] Michael E Fagan. Design and code inspections to reduce errors in program development. *IBM Systems Journal*, 38(2.3):258–287, 1999.

[17] Thomas Franke, Christiane Attig, and Daniel Wessel. A personal resource for technology interaction: development and validation of the affinity for technology interaction (ati) scale. *International Journal of Human–Computer Interaction*, 35(6):456–467, 2019.

[18] Simson L Garfinkel and Robert C Miller. Johnny 2: a user test of key continuity management with s/mime and outlook express. In *Proceedings of the 2005 symposium on Usable privacy and security*, pages 13–24, 2005.

[19] 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.

[20] Gennie Gebhart and Cory Doctorow. Between you, me, and google: Problems with gmail's "confidential mode". https://www.eff.org/deeplinks/2018/07/between-you-me-and-google-problems-gmails-confidential-mode, 2018. Last accessed 5 February 2021.

[21] Google. Protect gmail messages with confidential mode. https://support.google.com/a/answer/7684332?hl=en. Last accessed 10 January 2021.

[22] Google. Send & open confidential emails. https://support.google.com/mail/answer/7674059?hl=en&co=GENIE.Platform%3DAndroid&oco=1, 2018. Last accessed 10 January 2021.

[23] Nancie Gunson, Diarmid Marshall, Hazel Morton, and Mervyn Jack. User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking. *Computers & Security*, 30(4):208–220, 2011.

[24] Todd Haselton. How to send self-destructing messages in gmail. https://www.lifewire.com/send-self-destructing-messages-gmail-4691876, 2018. Last accessed 5 February 2021.

[25] Ding-Long Huang, Pei-Luen Patrick Rau, and Gavriel Salvendy. A survey of factors influencing people's perception of information security. In *International Conference on Human-Computer Interaction*, pages 906–915. Springer, 2007.

[26] Christopher Kotfila. This message will self-destruct: The growing role of obscurity and self-destructing data in digital communication. *Bulletin of the Association for Information Science and Technology*, 40(2):12–16, 2014.

[27] 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.

[28] Philipp Markert, Florian Farke, and Markus Dürmuth. View the email to get hacked: Attacking sms-based two-factor authentication. *WAY*, 2019.

[29] Agnieszka McPeak. Self-destruct apps: Spoliation by design. *Akron L. Rev.*, 51:749, 2017.

[30] M Granger Morgan, Baruch Fischhoff, Ann Bostrom, Cynthia J Atman, et al. *Risk communication: A mental models approach*. Cambridge University Press, 2002.

[31] Radia Perlman. The ephemerizer: Making data disappear, 2005.

[32] Xuan-Lam Pham, Thi-Huyen Nguyen, Wu-Yuin Hwang, and Gwo-Dong Chen. Effects of push notifications on learner engagement in a mobile learning app. In *2016 IEEE 16th International Conference on Advanced Learning Technologies (ICALT)*, pages 90–94. IEEE, 2016.

[33] Andy Phan. 6 of the best email service providers in 2021. https://www.currentware.com/best-email-service-providers-2021/, 2021. Last accessed 19 February 2021.

[34] Martin Pielot, Rodrigo De Oliveira, Haewoon Kwak, and Nuria Oliver. Didn't you see my message? predicting attentiveness to mobile instant messages. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 3319–3328, 2014.

[35] Justin Pot. How the new confidential mode works in gmail. https://www.howtogeek.com/352025/how-the-new-confidential-mode-works-in-gmail/, 2018. Last accessed 10 January 2021.

[36] Joel Reardon, David Basin, and Srdjan Capkun. Sok: Secure data deletion. In *2013 IEEE symposium on security and privacy*, pages 301–315. IEEE, 2013.

[37] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. A usability study of five two-factor authentication methods. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 2019.

[38] 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.

[39] Franziska Roesner, Brian T Gill, and Tadayoshi Kohno. Sex, lies, or kittens? investigating the use of snapchat's self-destructing messages. In *International Conference on Financial Cryptography and Data Security*, pages 64–76. Springer, 2014.

[40] Bernd Rohrmann. Risk perception, risk attitude, risk communication, risk management: A conceptual appraisal. In *15th Internaional Emergency Management Society (TIEMS) Annual Conference*, volume 2008, 2008.

[41] Ira S Rubinstein. Regulating privacy by design. *Berkeley Tech. LJ*, 26:1409, 2011.

[42] 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.

[43] 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.

[44] Scott Ruoti, Nathan Kim, Ben Burgon, Timothy Van Der Horst, and Kent Seamons. Confused johnny: when automatic encryption leads to confusion and mistakes. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, pages 1–12, 2013.

[45] Gavriel Salvendy. *Human factors and Ergonomics*. Lawrence Erlbaum Associates, 1999.

[46] 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.

[47] Prabhishek Singh and Ramneet Singh Chadha. A survey of digital watermarking techniques, applications and attacks. *International Journal of Engineering and Innovative Technology (IJEIT)*, 2(9):165–175, 2013.

[48] Editorial Team. Enhanced control over files with document watermarking. https://www.virtru.com/blog/digital-watermarking/. Last accessed 28 August 2021.

[49] Sonja Utz, Nicole Muscanell, and Cameran Khalid. Snapchat elicits more jealousy than facebook: A comparison of snapchat and facebook use. *Cyberpsychology, Behavior, and Social Networking*, 18(3):141–146, 2015.

[50] Alexander JAM Van Deursen, Ellen J Helsper, and Rebecca Eynon. Development and validation of the internet skills scale (iss). *Information, Communication & Society*, 19(6):804–823, 2016.

[51] Christof van Nimwegen and Kristi Bergman. Effects on cognition of the burn after reading principle in ephemeral media applications. *Behaviour & Information Technology*, 38(10):1060–1067, 2019.

[52] Elham Vaziripour, Justin Wu, Mark O'Neill, Jordan Whitehead, Scott Heidbrink, Kent Seamons, and Daniel Zappala. Is that you, alice? a usability study of the authentication ceremony of secure messaging applications. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 29–47, 2017.

[53] Virtru. The definitive guide to gmail encryption. https://www.virtru.com/blog/gmail-encryption/, 2019. Last accessed 26 May 2021.

[54] Virtru. Demystifying gmail confidential mode. https://www.virtru.com/resource/demystifying-confidential-mode/, 2019. Last accessed 26 May 2021.

[55] Ian Warren, Andrew Meads, Satish Srirama, Thiranjith Weerasinghe, and Carlos Paniagua. Push notification mechanisms for pervasive smartphone applications. *IEEE Pervasive Computing*, 13(2):61–71, 2014.

[56] Rick Wash and Emilee Rader. Influencing mental models of security: a research agenda. In *Proceedings of the 2011 New Security Paradigms Workshop*, pages 57–66, 2011.

[57] Jason Watson, Andrew Besmer, and Heather Richter Lipford. + your circles: sharing behavior on google+. In *Proceedings of the eighth symposium on usable privacy and security*, pages 1–9, 2012.

[58] 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.

[59] 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.

[60] Zarul Fitri Zaaba and Teo Keng Boon. Examination on usability issues of security warning dialogs. *Age*, 18(25):26–35, 2015.

A Appendix

A.1 Script for In-Person Interview

Good morning/afternoon!

Thank you for coming. My name is Elham Al Qahtani - I am a Ph.D. student working under Dr. Mohamed Shehab's supervision. This study focuses on Gmail users who have sent confidential mode emails. The purpose of the study is to gather information about user motivations for using Gmail's confidential mode in emails and their understanding of how it works. Please read the consent form before we start. If you agree to participate, you will first sign/confirm your agreement and answer a set of demographic and motivation of use questions, you will then perform a few tasks such as composing an email and reviewing a set of your past emails. After that, you will be asked a second set of questions related to these emails. The session will last around 25 minutes. You will receive a $5 Starbucks card as a reward for your participation.

Demographic questions:

1. How old are you?
2. What is the highest level of education you have completed?
3. What is your gender?
4. What is your occupation?
5. What is your technical expertise on a scale from 1-10 where 10 is very technical?

Email and GCM usage questions:

1. Which email service providers do you use?
2. How often do you use each?
3. How long have you been using Gmail confidential mode?
4. How often do you use Gmail confidential mode?

Let's now focus on your motivations for using Gmail's confidential mode

1. What made you start using Gmail confidential mode?
2. How are you using Gmail confidential mode in your emails?
3. What type of email content do you use Gmail confidential mode for?
4. What type of documents or files do you attach in these emails?
5. Who do you send these emails to?
6. Why did you decide to share these emails with them?

Task: Could you show me how you would compose a confidential email for someone about this interview experience. Please think aloud as you perform this task

1. When you use this mode, how is confidentiality being achieved?
2. Is your email encrypted? How and Why?

Task: Now please review the last few emails (1 to 3 emails) that you sent in confidential mode. The next set of questions are related to the emails the reviewed emails:

1. Did you require an SMS passcode in any of these emails?
   - If participant said "Yes"
     - What is it for? Why did you choose it?
     - Do you require an SMS passcode for the recipient to access messages?
     - Can you state your confidence in requiring passcode feature on a scale from 1-5, where 5 is strongly confident?
   - If participant said "No"
     - Could you explain why you chose not to use this feature?
2. Did you set an expiration date on the content in any of these emails?
   - If participant said "Yes"
     - What is it for? Why did you choose it?
     - Can you state your confidence in setting an expiration date on the content of your email on a scale from 1-5, where 5 is strongly confident?
   - If participant said "No"
     - Could you explain why you chose not to use this feature?
3. Did you revoke message access in any of these emails?
   - If participant said "Yes"
     - What is it for? Why did you do it?
     - Can you state your confidence in revoking message access at any time on a scale from 1-5, where 5 is strongly confident?
   - If participant said "No"
     - Could you explain why you chose not to use this feature?
   - If the participant said "Yes"
     - Please explain how you achieved that?
     - Do you think there are other ways that the recipient can use to copy the content in your email? Can you tell me how?
     - Can you state your confidence in ensuring that the recipient doesn't forward, download, or print the email on a scale from 1-5, where 5 is strongly confident?
   - If participant said "No"
     - Could you explain why you were able to do so?

Thank you for your participation

A.2 Codebook With Code Frequencies

Code	Description	Frequency
Motivation: Sharing confidential documents	Send sensitive documents to recipients (e.g., driver's licenses, financial statements)	12
Motivation: Prevent unauthorized access	The unauthorized user gains access to confidential documents using different methods	4
Motivation: Encryption	The perception that users are sending an encrypted email with confidential mode	2
Motivation: Curiosity	Explore the security features to make better security decisions	3
Motivation: Replacement for physical sharing	Share confidential information remotely since they are unable to deliver important documents physically	2
Motivation: Sharing during pandemic	Share confidential information during the pandemic	2
Motivation: Work requirement	Sharing confidential information via GCM is a work requirement	1

Code	Description	Frequency
Content: Non-work-related documents	Share non work-related documents with close friends and relatives	3
Content: Work-related documents	Share documents related to work	5
Content: Financial records	Share financial documents (e.g., bank statements)	5
Content: Governmental documents	Share governmental documents (e.g., tax documents)	3
Content: Legal documents	Share legal documents (e.g., contracts)	1
Content: Medical documents	Share medical documents (e.g., patient records)	2
Recipients: Family and relatives	Send confidential emails to family members and close relatives (e.g., parents, friends)	11
Recipients: Administrative team	Send confidential emails to administrative team members (e.g., company manager)	7
Recipients: Financial employees	Send confidential emails to financial employees (e.g., bank consultants)	7
Recipients: Teamwork at school	Send confidential emails for teamwork (e.g., classmates)	3
Recipients: Medical personnel	Send confidential emails to medical personnel (e.g., veterinarians)	2
Recipients: Leasing office staff	Send confidential emails to a leasing office	1
Sharing-with-recipients: Sharing during pandemic	Sharing confidential information once the pandemic started	4
Sharing-with-recipients: Requested by administrative team	Administrative team request users to share confidential documents that are related to their work	4
Sharing-with-recipients: Requested by recipients	Recipients request users to privately share confidential documents	3
Sharing-with-recipients: Trust the receiver	Users trust recipients when they share confidential documents	2
Sharing-with-recipients: Prevent unauthorized access	Prevent unauthorized users from accessing confidential documents	2
Sharing-with-recipients: Achieve privacy	Users achieve privacy without using a VPN when GCM is used	1
Confidentiality: Setting an expiration date	The expiration date ensures confidentiality	8
Confidentiality: Enabling authentication	Authentication ensures confidentiality by using SMS passcode	4
Confidentiality: Disabling options to forward, copy, print	Enabling confidential mode prevents forward, copy, print	9
Confidentiality: Including confidential links	Include a link to the content that expires after a certain period of time	2
Confidentiality: Enabling encryption	Using GCM with high-level encryption	1
Encryption: Via security features	The security features of GCM ensure that email is encrypted	11
Encryption: Unsure	Unsure whether the email is encrypted or not	5
Encryption: Does not exist	GCM email is not encrypted	3
Expiration-Time: Prevent unauthorized access	Using the time limit feature, users prevent unauthorized people from viewing emails for as long as they need.	4
Expiration-Time: Have temporal access	The time limit feature enables temporary access to the confidential email by recipients	10
Expiration-Time: Set content restrictions	The time limit feature restricts the recipient from downloading, printing, or using the confidential information	1
No-Expiration-Time: Email deletion	Due to the possibility that emails might get deleted before the recipients read them, users don't use the feature	2
No-Expiration-Time: Type of email account	Users do not use this feature due to the type of account they have (e.g., personal or work)	2
SMS passcode: Prevent unauthorized access	Users set an SMS passcode for recipients to prevent unauthorized access to their emails	4
SMS passcode: For extra security	Users set an SMS passcode to use two-factor authentication for extra security	2
SMS passcode: Ensure email privacy	Users set an SMS passcode to ensure email privacy	2

Code	Description	Frequencies
SMS passcode: Ensure message safety	Users set an SMS passcode to ensure content safety	1
No-SMS passcode: Using another security tool	Users do not set an SMS passcode because other security tools are in place	1
No-SMS passcode: Using for specific accounts	Users do not set an SMS passcode for specific email account (e.g., personal or work)	1
No-SMS passcode: Avoiding confusion	Users do not set an SMS passcode to avoid any confusion due to the recipients' low technical expertise	2
No-SMS passcode: Being convenient	Users do not set an SMS passcode because it is more convenient for recipients to access their confidential email	4
No-SMS passcode: Trusting the recipient	Users do not set an SMS passcode because of the trust between the receiver and sender	1
No-SMS passcode: Unnecessary	Users do not set an SMS passcode perceiving that this feature is not needed in the confidential email	1
No-SMS passcode: Not knowing an SMS passcode	Users do not set an SMS passcode because they are not aware about it	1
No-Access Revocation: Trusting the recipient	Users do not revoke access to messages before their scheduled expiration date due to the trust between the receiver and sender	5
No-Access Revocation: Using access restriction	Users do not revoke access to messages since other GCM features are being used (e.g., expiration time)	4
No-Access Revocation: Unnecessary	Users do not revoke access to messages perceiving there is no reason or need to revoke message access in their confidential email	4
No-Access Revocation: Not super sensitive	Users do not revoke access to messages perceiving that the content is not super sensitive (e.g., birth certificates)	1
No knowledge-Access Revocation: Not aware	Users do not know what revoking message access meant and its purpose	5
Permission-Restriction: Default settings	Users perceive that GCM by default prevents recipients from forwarding, copying, printing, or downloading message content or attachments	10
Permission-Restriction: Following workplace rules	In the workplace, employees share private information based on defined rules	1
Permission-Restriction: Recipient use alternative methods	Users are unsure whether recipients could forward, copy, print, or download message content or attachments due to alternative methods that the recipients might use	3
Copy-Content: Screenshots	Users perceive that recipients could copy the content in their email using screenshots	12
Copy-Content: Third-party programs	Users perceive that recipients could copy the content in their email using third-party programs	1
Copy-Content: Screen records	Users perceive that recipients could copy the content in their email using recording tools	1