Major Project

By Bhavesh Mohinani

CS04B9

ACKNOWLEDGEMENT

I would like to express my special thanks of gratitude to our InfoSec trainer "Mr.Animesh Roy" for their able guidance and support in completing my project.

I would also like to extend my gratitude to Verzeo and my group members for providing me with all the facility that was required. Due to pratical exams being conducted at the submission time, this document couldn't be send on time kindly forgive us for any kind of disturbances or problems

DATE: Bhavesh Mohinani

bhaveshmohinani121005@gmail.com

01-05-2020 CS04B9

OVERVIEW OF THE REPORT

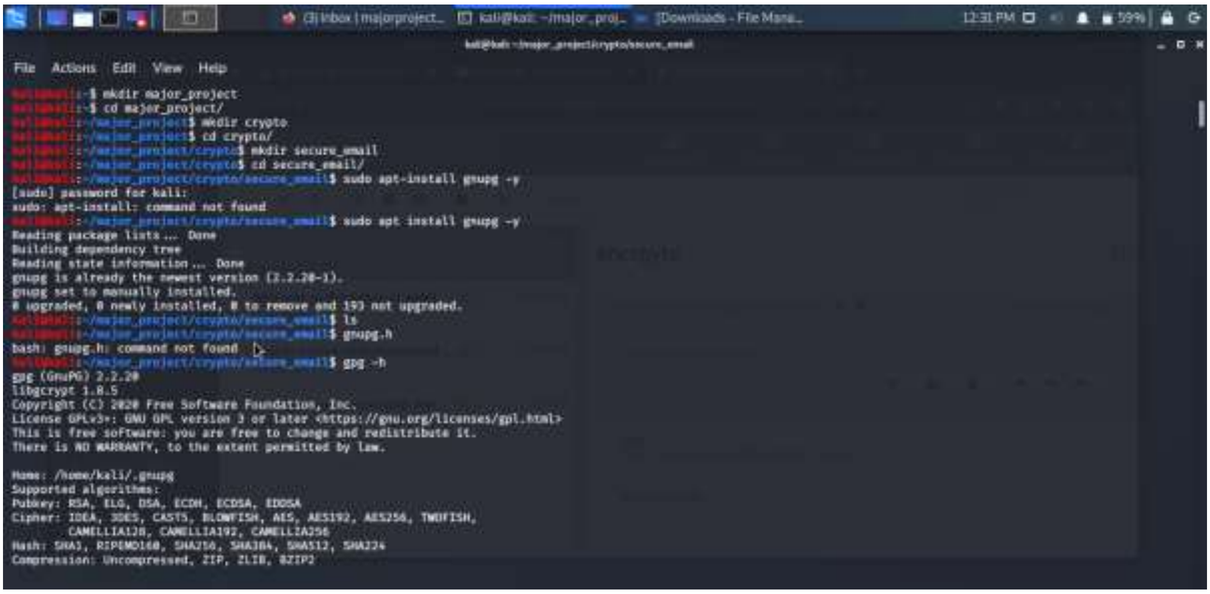
This report contains brief procedures of the activities.

Activity is based on the sending mail using pgp and python.

Based on the activities done the answers for the discussions and assessment is being written.

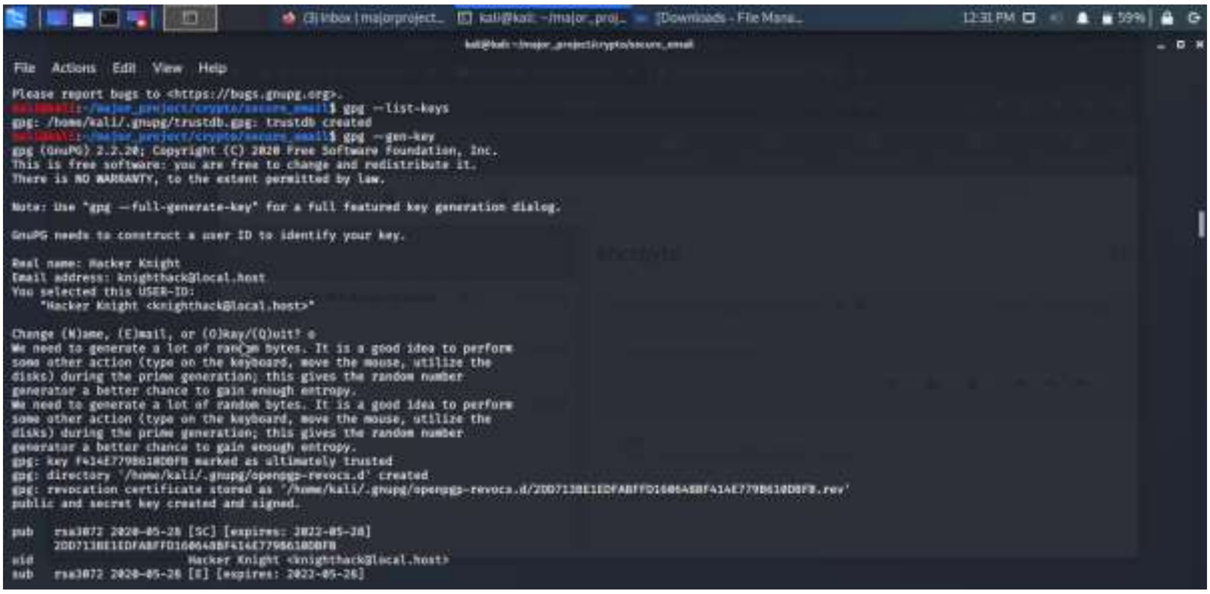
ACTIVITY 1:-

In this activity a mail is to be sent using pgp. First a directory is created in which gnupg is installed.



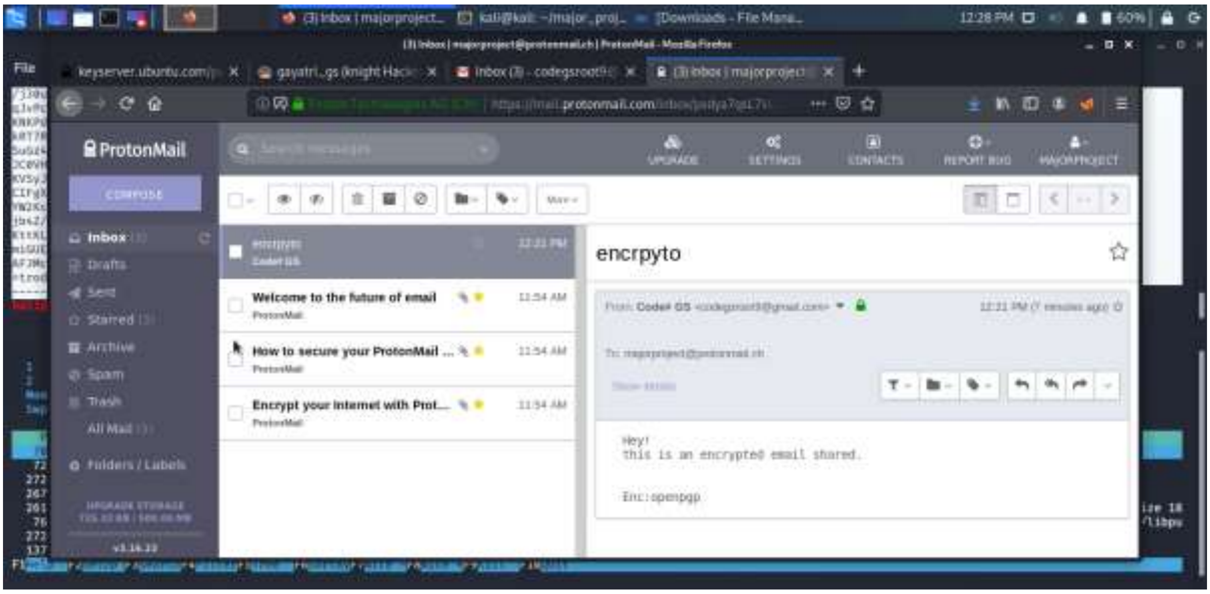
```
kali@kali:~$ mkdir major_project
kali@kali:~$ cd major_project/
kali@kali:~/major_project$ mkdir crypto
kali@kali:~/major_project$ cd crypto/
kali@kali:~/major_project/crypto$ mkdir secure_email
kali@kali:~/major_project/crypto$ cd secure_email/
kali@kali:~/major_project/crypto/secure_email$ sudo apt-install gnupg -y
[sudo] password for kali:
sudo: apt-install: command not found
kali@kali:~/major_project/crypto/secure_email$ sudo apt install gnupg -y
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
gnupg is already the newest version (2.2.20-1).
gnupg set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 193 not upgraded.
kali@kali:~/major_project/crypto/secure_email$ ls
kali@kali:~/major_project/crypto/secure_email$ gnupg.h
bash: gnupg.h: command not found
kali@kali:~/major_project/crypto/secure_email$ gpg -h
gpg (GnuPG) 2.2.20
libgcrypt 1.8.5
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Home: /home/kali/.gnupg
Supported algorithms:
Pubkey: RSA, ELG, DSA, ECDH, ECDSA, EDDSA
Cipher: IDEA, 3DES, CAST5, BLOWFISH, AES, AES192, AES256, TWOFISH,
        CAMELLIA128, CAMELLIA192, CAMELLIA256
Hash: SHA1, RIPEMD160, SHA256, SHA384, SHA512, SHA224
Compression: Uncompressed, ZIP, ZLIB, BZIP2
```

Then an email id is created and then followed by a key is generated. This key is signed and then it is encrypted and uploaded to key server.



```
Please report bugs to <https://bugs.gnupg.org>.
kali@kali:~/major_project/crypto/secure_email$ gpg --list-keys
gpg: /home/kali/.gnupg/trustdb.gpg: trustdb created
kali@kali:~/major_project/crypto/secure_email$ gpg --gen-key
gpg (GnuPG) 2.2.20; Copyright (C) 2020 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: Hacker Knight
Email address: knighthack@local.host
You selected this USER-ID:
    "Hacker Knight <knighthack@local.host>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? o
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: key F414E779B610D0FB marked as ultimately trusted
gpg: directory '/home/kali/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/kali/.gnupg/openpgp-revocs.d/2DD713BE1EDFABFFD1606ABBF414E779B610D0FB.rev'
public and secret key created and signed.

pub   rsa3072 2020-05-26 [SC] [expires: 2022-05-26]
      2DD713BE1EDFABFFD1606ABBF414E779B610D0FB
uid                      Hacker Knight <knighthack@local.host>
sub   rsa3072 2020-05-26 [E] [expires: 2022-05-26]
```

After this public key , the protonmail account is imported and encrypted and sent. Protonmail will automatically decrypt the message.



encrpyto

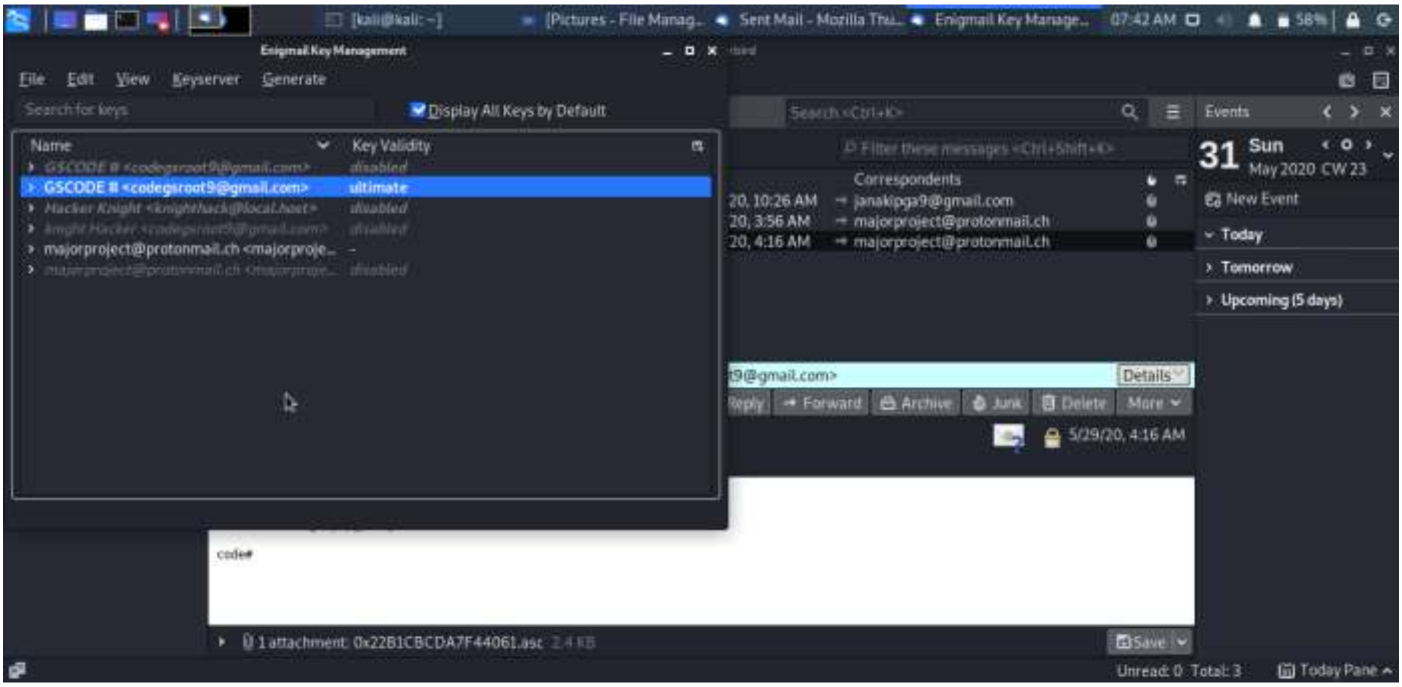
From: Code# GS <codegsroot9@gmail.com>
12:21 PM (7 minutes ago)

To: majorproject@protonmail.ch

```
Hey!
this is an encrypted email shared.

Enc:openpgp
```

Subject	Time
Welcome to the future of email ProtonMail	11:54 AM
How to secure your ProtonMail ... ProtonMail	11:54 AM
Encrypt your internet with Prot... ProtonMail	11:54 AM

Another method is to send a pgp message using thunderbird. It is installed and setup and Protonmail pgp certificate is imported. A message is sent to protonmail using the public key.



Enigmail Key Management

☑ Display All Keys by Default

Name	Key Validity
GSCODE # <codegsroot9@gmail.com>	disabled
GSCODE # <codegsroot9@gmail.com>	ultimate
Hacker Knight <knighthack@local.host>	disabled
knight Hacker <codegsroot9@gmail.com>	disabled
majorproject@protonmail.ch <majorproje...	-
majorproject@protonmail.ch <majorproje...	disabled

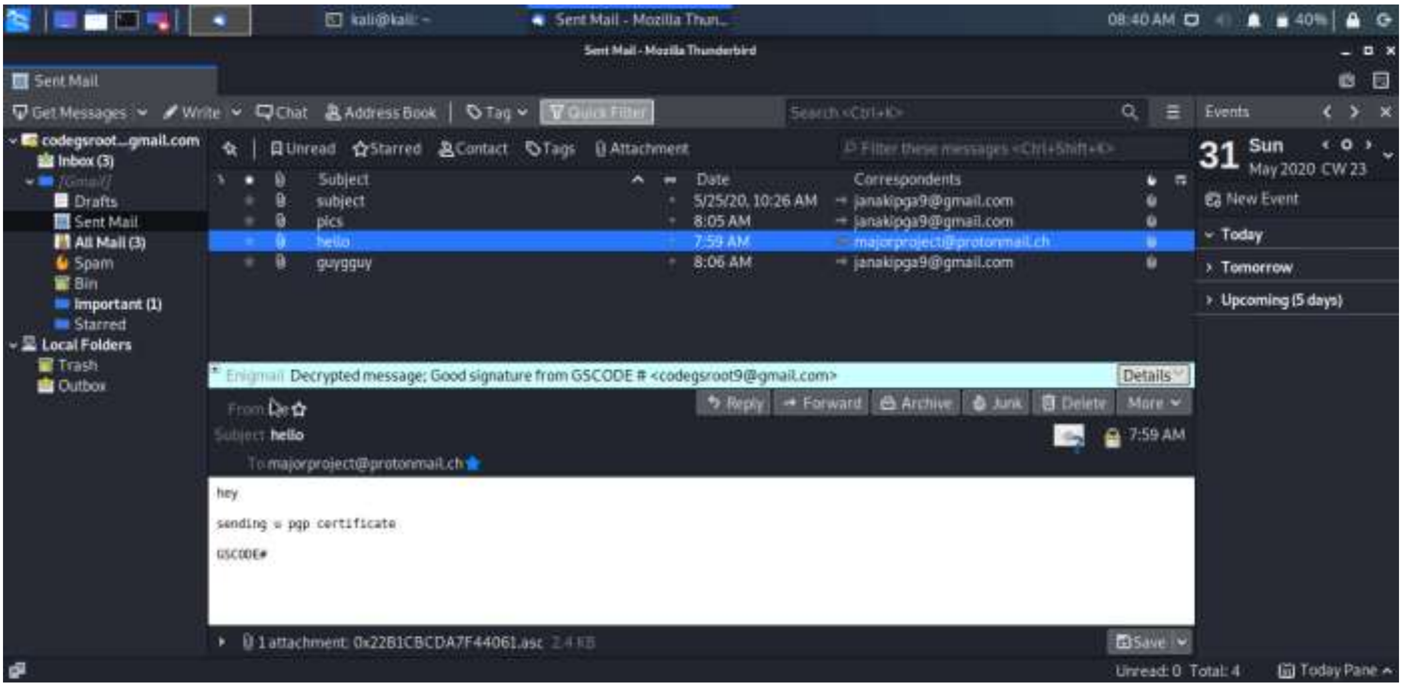
	Correspondents
20, 10:26 AM	janakipga9@gmail.com
20, 3:56 AM	majorproject@protonmail.ch
20, 4:16 AM	majorproject@protonmail.ch

5/29/20, 4:16 AM

code#

1 attachment: 0x22B1CBCDA7F44061.asc 2.4 KB

Unread: 0 Total: 3



Sent Mail - Mozilla Thunderbird

Subject	Date	Correspondents
subject	5/25/20, 10:26 AM	janakipga9@gmail.com
pics	8:05 AM	janakipga9@gmail.com
hello	7:59 AM	majorproject@protonmail.ch
guygguy	8:06 AM	janakipga9@gmail.com

Enigmail Decrypted message; Good signature from GSCODE # <codegsroot9@gmail.com>

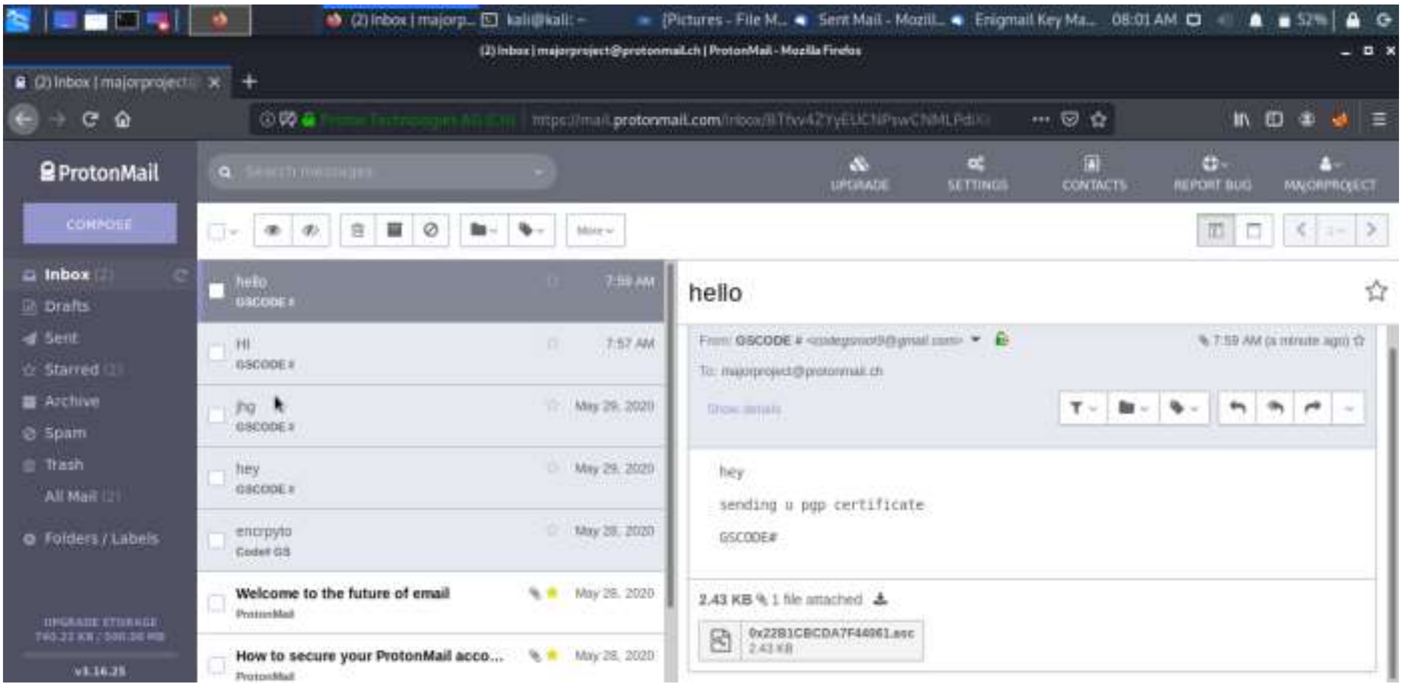
Subject hello

To majorproject@protonmail.ch

```
hey

sending u pgp certificate

GSCODE#
```

1 attachment: 0x22B1CBCDA7F44061.asc 2.4 KB

This is decrypted message by protonmail.



(2) Inbox | majorproject@protonmail.ch | ProtonMail - Mozilla Firefox

https://mail.protonmail.com/inbox/

Subject	Sender	Date
hello	GSCODE #	7:59 AM
HI	GSCODE #	7:57 AM
jhg	GSCODE #	May 29, 2020
hey	GSCODE #	May 29, 2020
encrpyto	Code# GS	May 28, 2020
Welcome to the future of email	ProtonMail	May 28, 2020
How to secure your ProtonMail acco...	ProtonMail	May 28, 2020

hello

From: GSCODE # <codegsroot9@gmail.com> 7:59 AM (a minute ago)

To: majorproject@protonmail.ch

```
hey

sending u pgp certificate

GSCODE#
```

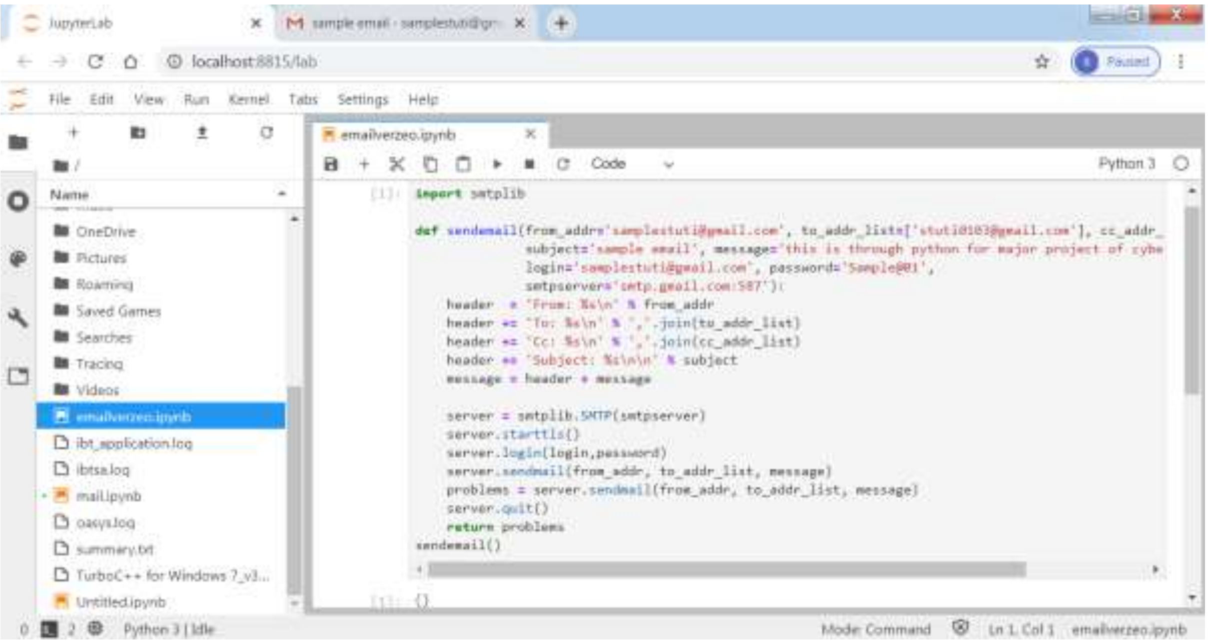
2.43 KB 1 file attached

0x22B1CBCDA7F44061.asc 2.43 KB

Activity 2:-

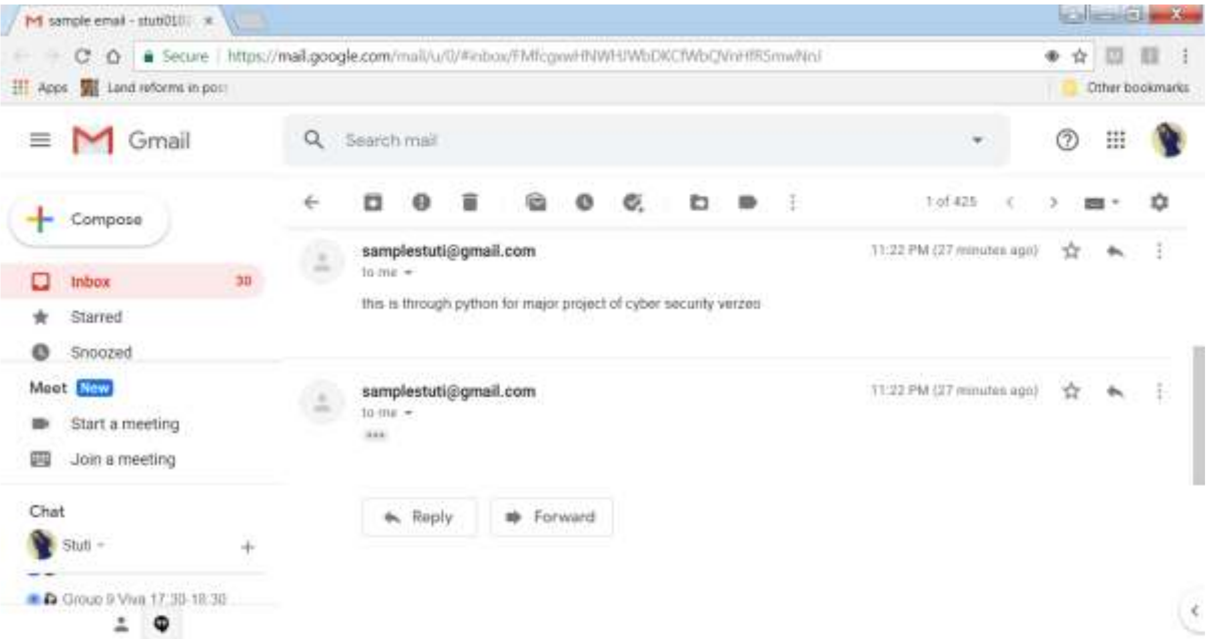
Send e-mail using python:-

Sent the email using following code:



```
[1]: import smtplib

     def sendemail(from_addr='samplestuti@gmail.com', to_addr_list=['stuti0103@gmail.com'], cc_addr_
                   subject='sample email', message='this is through python for major project of cybe
                   login='samplestuti@gmail.com', password='Sample@01',
                   smtpserver='smtp.gmail.com:587'):
         header  = 'From: %s\n' % from_addr
         header += 'To: %s\n' % ','.join(to_addr_list)
         header += 'Cc: %s\n' % ','.join(cc_addr_list)
         header += 'Subject: %s\n\n' % subject
         message = header + message

         server = smtplib.SMTP(smtpserver)
         server.starttls()
         server.login(login,password)
         server.sendmail(from_addr, to_addr_list, message)
         problems = server.sendmail(from_addr, to_addr_list, message)
         server.quit()
         return problems
     sendemail()

[1]: {}
```

Received the e-mail as:-

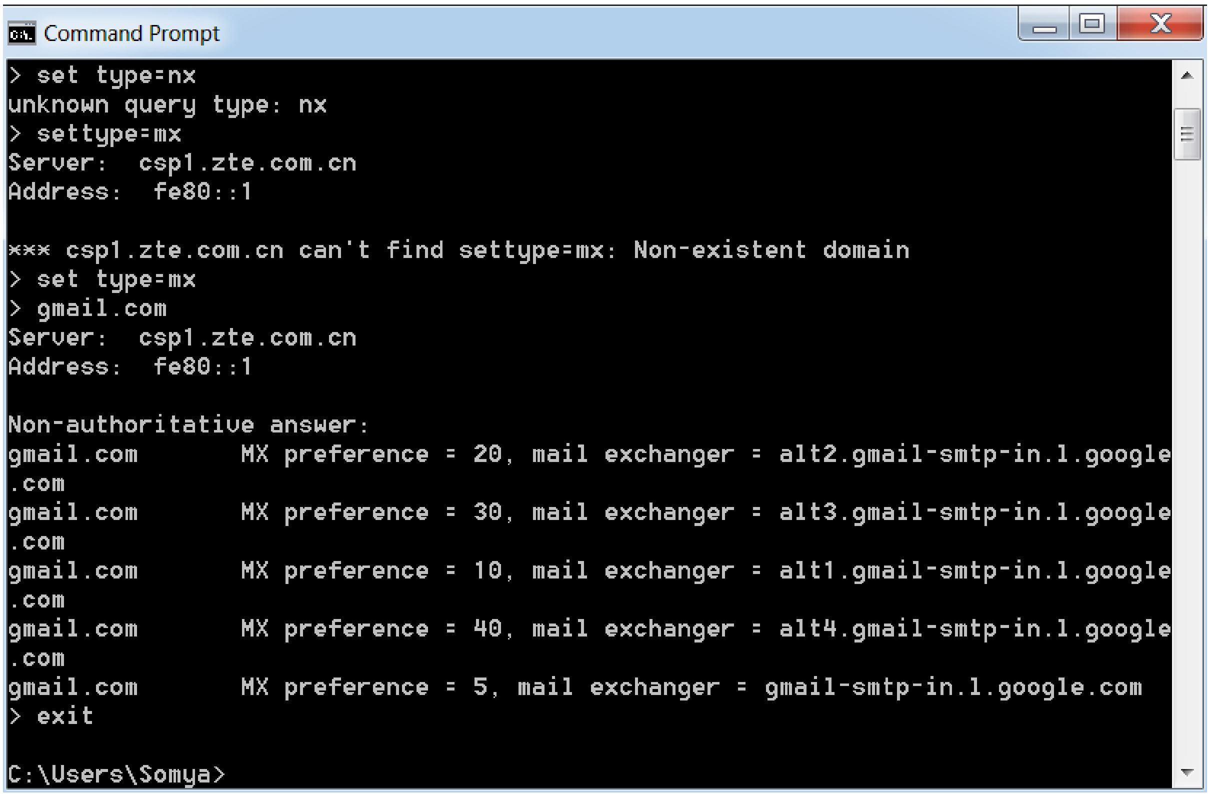


samplestuti@gmail.com 11:22 PM (27 minutes ago)
to me

this is through python for major project of cyber security verzeo

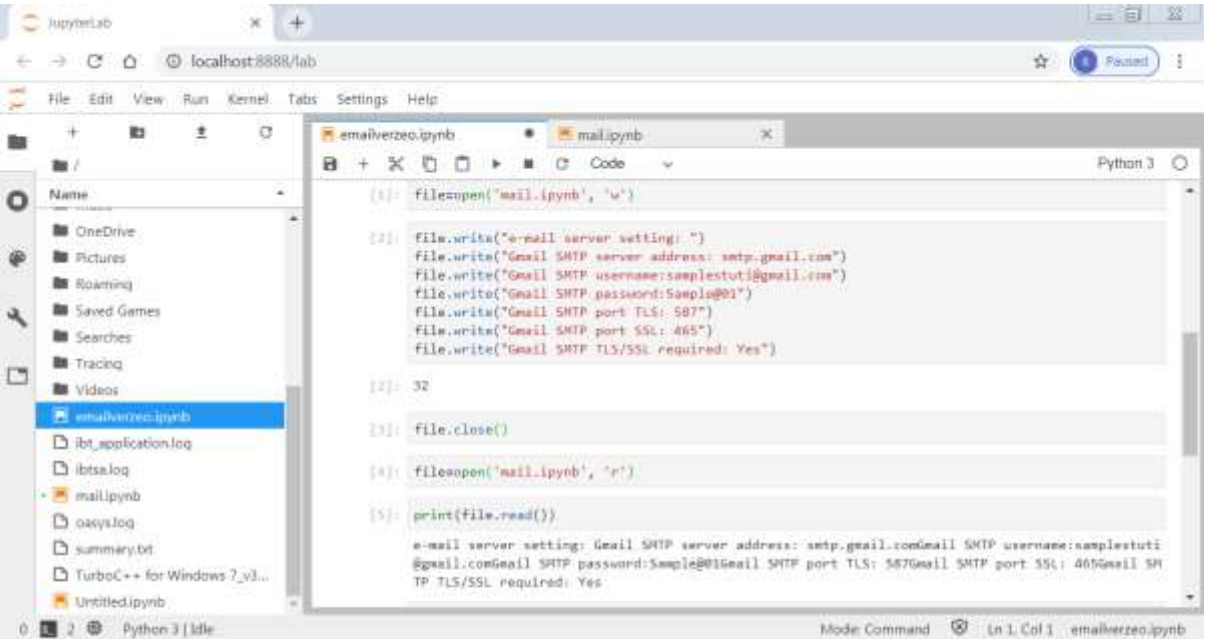
samplestuti@gmail.com 11:22 PM (27 minutes ago)
to me

Email server setting :-



```
> set type=nx
unknown query type: nx
> settype=mx
Server:  csp1.zte.com.cn
Address:  fe80::1

*** csp1.zte.com.cn can't find settype=mx: Non-existent domain
> set type=mx
> gmail.com
Server:  csp1.zte.com.cn
Address:  fe80::1

Non-authoritative answer:
gmail.com       MX preference = 20, mail exchanger = alt2.gmail-smtp-in.l.google
.com
gmail.com       MX preference = 30, mail exchanger = alt3.gmail-smtp-in.l.google
.com
gmail.com       MX preference = 10, mail exchanger = alt1.gmail-smtp-in.l.google
.com
gmail.com       MX preference = 40, mail exchanger = alt4.gmail-smtp-in.l.google
.com
gmail.com       MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com
> exit

C:\Users\Somya>
```

Update in python file:-



```
[1]: file=open('mail.ipynb', 'w')

[2]: file.write("e-mail server setting: ")
     file.write("Gmail SMTP server address: smtp.gmail.com")
     file.write("Gmail SMTP username:samplestuti@gmail.com")
     file.write("Gmail SMTP password:Sample@01")
     file.write("Gmail SMTP port TLS: 587")
     file.write("Gmail SMTP port SSL: 465")
     file.write("Gmail SMTP TLS/SSL required: Yes")

[2]: 32

[3]: file.close()

[4]: file=open('mail.ipynb', 'r')

[5]: print(file.read())

     e-mail server setting: Gmail SMTP server address: smtp.gmail.comGmail SMTP username:samplestuti
     @gmail.comGmail SMTP password:Sample@01Gmail SMTP port TLS: 587Gmail SMTP port SSL: 465Gmail SM
     TP TLS/SSL required: Yes
```

Can you e-mail multiple people?

Yes, we can send e-mail to multiple people.

For this we store a list of recipients in some variable receivers, and then use for loop to send each recipient separately but ultimately we can send the mail to all the recipients.

Could you pull the list of people to email from an external file?

Yes.

For this we can read the data of file and store in form of list in some variable and then we can use loop to send emails as above.

How can you personalize the email for the recipient?

Using python, we can send mail according to person's need, personalized messages and attachments also.

When we are sending mail to a list of recipients, then according to my research, we cannot personalize the mail much.

starttls() functions of smtplib class is used to encrypt the mail.

Assessment questions

1. Why do email services "read" your email? What is their goal?

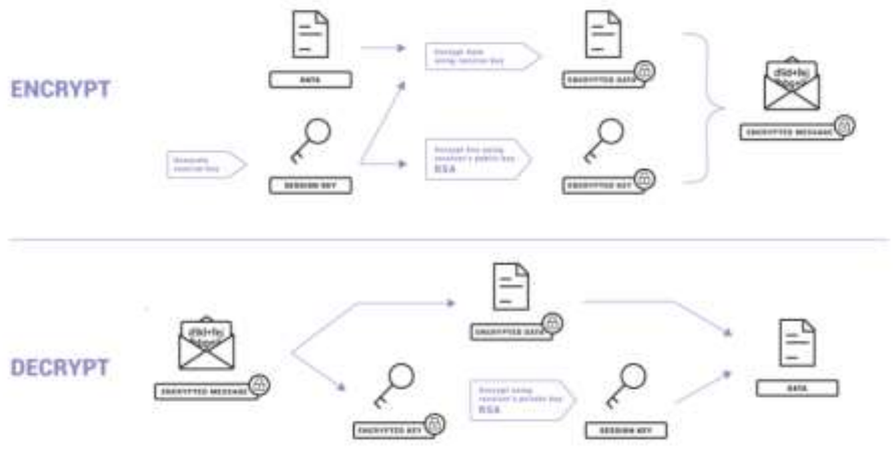
Worldwide, more than one billion people use Gmail, Google's free email service. "Is Gmail reading my email?" is a common question because Google is very good at targeting ads to users, and especially to those who use its services, like Gmail and YouTube. Gmail users often think Google is reading their messages because topics found in them sometimes appear in ads in their inbox, in search results, or in suggested videos on YouTube.

So does Gmail read your emails? The answer depends on what you mean by "reading." If you imagine a person sitting at a computer screen reading your email messages, then no, Gmail does not read them. However, computers do scan and analyze your incoming, outgoing, and stored messages.

Google has faced harsh criticism for this practice and has been targeted with lawsuits. But the company argues that scanning each email is necessary to provide a free and safe service to the public. Privacy advocates disagree, pointing out that Google scans emails from non-Gmail users who have not agreed to the company's privacy policy or Gmail terms of service. Critics also argue that other free email services, notably Microsoft's Outlook.com service, do not scan customer emails to create targeted advertising.

2. How does PGP secure email differently than GMail?

PGP is a cryptographic method that lets people communicate privately online. When you send a message using PGP, the message is converted into unreadable ciphertext on your device before it passes over the Internet. Only the recipient has the key to convert the text back into the readable message on their device. PGP also authenticates the identity of the sender and verifies that the message was not tampered with in transit. It's useful to see a diagram to understand how PGP encryption works. As you can see, PGP uses a combination of **symmetric key encryption** (i.e., a single-use session key encrypts and decrypts the message) and **public key encryption** (i.e., the keys unique to the recipient encrypt and decrypt the session key).



3. Why don't people use services like PGP more often?

Pretty Good Privacy (PGP) is an encrypted email solution that masks your messages before you send them. PGP works using public key cryptography, meaning that every user has their own key pair — one private key, and one public key. The private key is used to decrypt messages, while the public key is used to encrypt them.

Your public key can be openly shared with just about anyone without incurring any risk. Even if a potential bad guy were to obtain your public key, they wouldn't be able to decrypt your messages. For that, they would need to access the private key, which only you have. While PGP is very secure, it's also a huge hassle. If you're going to send someone an encrypted message, not only do they have to be using PGP, but you also have to exchange keys first. Likewise, once you have a collection of keys, it's up to you to hold on to them. If they get corrupted, or if your computer goes up in smoke, you have to repeat the process.

In light of the whole NSA leaks etc, I have to ask why we don't use PGP widely. Is it just because it's too difficult or is it because we never thought our emails were ever something to be kept private or just that there was never a need to produce tools to make the technology accessible.

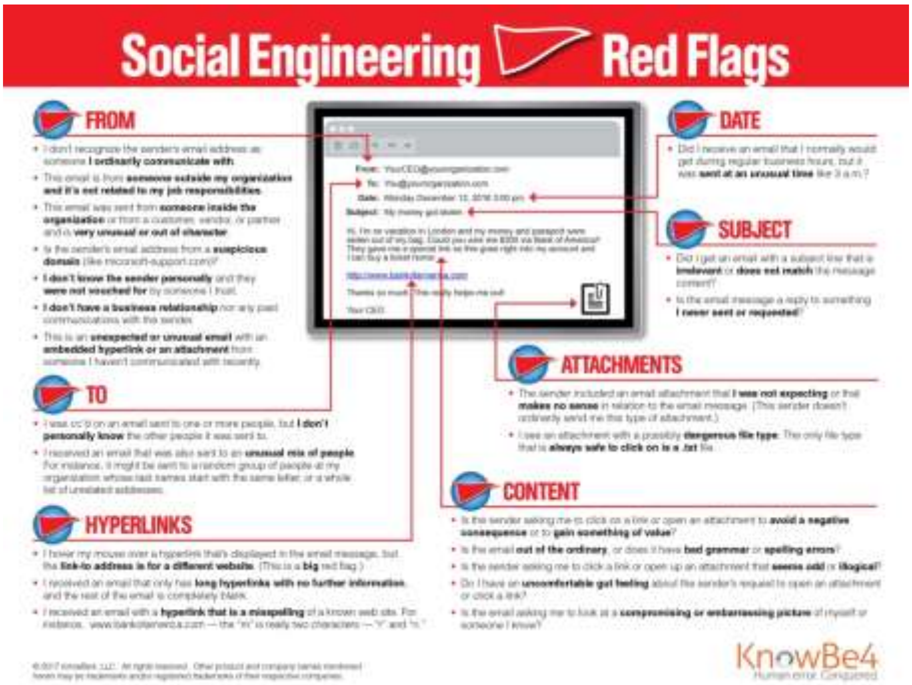
4. What is phishing?

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

The information is then used to access important accounts and can result in identity theft and financial loss.

Common Features of Phishing Emails

1. Too Good To Be True - Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people’s attention immediately. For instance, many claim that you have won an iPhone, a lottery, or some other lavish prize. Just don't click on any suspicious emails. Remember that if it seems to good to be true, it probably is!
2. Sense of Urgency - A favorite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time. Some of them will even tell you that you have only a few minutes to respond. When you come across these kinds of emails, it's best to just ignore them. Sometimes, they will tell you that your account will be suspended unless you update your personal details immediately. Most reliable organizations give ample time before they terminate an account and they never ask patrons to update personal details over the Internet. When in doubt, visit the source directly rather than clicking a link in an email.
3. Hyperlinks - A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it. It could be completely different or it could be a popular website with a misspelling, for instance www.bankofarnerica.com - the 'm' is actually an 'r' and an 'n', so look carefully.
4. Attachments - If you see an attachment in an email you weren't expecting or that doesn't make sense, don't open it! They often contain payloads like ransomware or other viruses. The only file type that is always safe to click on is a .txt file.
5. Unusual Sender - Whether it looks like it's from someone you don't know or someone you do know, if anything seems out of the ordinary, unexpected, out of character or just suspicious in general don't click on it!



Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with.**
- This email is from **someone outside my organization and it's not related to my job responsibilities.**
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character.**
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people.** For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website.** (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information,** and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

From: YourCEO@yourorganization.com
To: You@yourorganization.com
Date: Monday December 12, 2016 3:00 pm
Subject: My money got stolen

Hi, I'm on vacation in London and my money and passport were stolen out of my bag. Could you wire me $300 via Bank of America? They gave me a special link so this goes right into my account and I can buy a ticket home.

http://www.bankofarnerica.com

Thanks so much. This really helps me out!

Your CEO

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested?**

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type.** The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value?**
- Is the email **out of the ordinary,** or does it have **bad grammar** or **spelling errors?**
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical?**
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

5. *What is spear-phishing?*

Spear phishing is a targeted version of phishing.

The phishing message is directed to a specific person, in the hope that they will disclose information that allows an attacker to gain an initial foothold within an organisation.

Cybercriminals may use data that someone has posted online to add credibility to the message.

This may include information posted on a company web site, snippets of information that people disclose in social networks or things they publish in public forums.

For example, if the sales director of a company tweets about his holiday in Greece, or his business trip to Berlin, this can be referred to in an e-mail to make it look legitimate.

Similarly, an e-mail may be spoofed to look like it has come from a trusted colleague.

If, for example, it appears to be from a colleague in IT, it's likely that an employee will respond to the e-mail.

The widespread use of social networks, and our tendency sometimes to over-share, has given cybercriminals more raw data for developing spear phishing attacks.

DISCUSSIONS QUESTIONS

What could you do to ensure privacy when sending email?

Encrypt your important emails: Without email encryption, hackers can easily intercept, open and Read your emails. Though not a commonly held thought, email is basically insecure from privacy breaches. This includes attached documents as well. Encryption works like a lock box with two keys allowing encryption to work. First, you have your public key. This key is a series of numbers and letters you share with those who you want to be able to open your encrypted emails on the other end.

Your private key is what you keep for yourself and never give up. When you encrypt your email, anyone who intercepts it will be unable to read or interpret them. They will appear as garbled text with all pertinent information such as photos, credit card numbers, names and address obscured and unrecognizable as a valid email.

What are the steps to encrypting your email? There are three:

First, I recommend using PGP, Pretty Good Privacy, to encrypt your messages. PGP is a free service and using it is the first step in sending secure, encrypted emails.

Next, you'll need to generate your public and private key pairs. GNU Privacy Guard is my choice and is an extension of OpenPGP. It's both free and easy to implement.

Lastly, we will put the configured and generated key pairs to work. Depending upon your email browser preferences, you can use either Thunderbird or Postbox to encrypt your actual messages.

To use, you'll simply scroll to the "OpenPGP" menu and choose the option to either "Sign Message" or "Encrypt Message." Choose both for maximum email security.

What expectation of privacy do you have when sending e-mail?

Sensitive data must be protected: Communicating with traditional email is not secure. It only takes one email-related security breach to cause inadvertent disclosure of confidential or sensitive messages and files. With identity theft, hackers and private communication taking place online, it’s a risk that shouldn’t be taken.

Email should be delivered to the right person: During sending an email it expected that the intended person is getting mails. It is also expected that the email is transmitted to its receiver without getting halted or interrupted or denied and is delivered.

Receiver is not sharing the confidential information with others: While sending a confidential email it is expected that the receiver is not sharing the information with others.

If you had a secret message to send, how would you do it?

You can send secret messages by email or text. You can also encode messages or make up your own secret language. Keep reading to find out how to write secret messages and how to pass them to your cohorts without getting caught.

1. You can write your email message in code. If someone is snooping through your phone or your computer, they won't be able to read the message. Keep reading for secret code ideas.
2. There are sites that will send encrypted emails that are more secure than regular email. The recipient will need to know the password for most of them.
3. If you want to send an anonymous email that doesn't tell who the sender is, there are several sites you can use. These sites will also send emails that won't reveal the sender
4. Sent emails aren't always secure. But if you need to send a private email to someone, you can create a fake email account. Share the login and password with the person who is receiving the message. Compose an email message, but save it in the drafts folder instead of sending it. The other person will be able to read it. And since the email was never sent, it isn't traceable.

How could you automate e-mailing many people?

It all depends on what kind of emails you want to automate.

Generally, there are three types of emails:

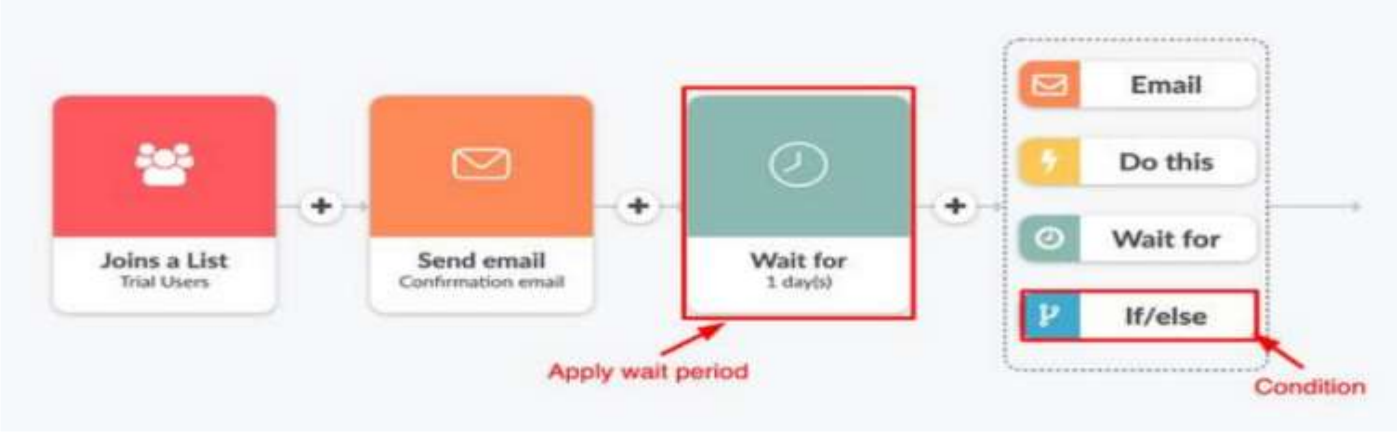
1. Marketing emails (Inbound) - they’re meant to inform a large group of people who agreed to receive a message from you, you don’t expect recipients to reply to your email

2. Outbound emails - they’re meant to get responses from people either to strike a deal, get something from them, introduce yourself and your business

3. Email notificators - welcome or error messages that go out from the system.

If you want to automate marketing emails, use MailChimp or Freshmail.

If you want to automate outbound emails, use hubsell.



4 Steps to Awesome Email Automation

Step 1: <u>Create a plan</u>: marketers know the first step in any good campaign is creating a blueprint for success. In this case, you'll need a plan to guide your automation campaign.

Step 2: <u>Automation that's right for you</u>: There are three basic types of email service providers: freemium, mid-tier, and enterprise. But which is right for you?

Step 3: <u>Set up your workflow</u>: Once you've selected a system to power your email automation, set up the automated email messages you want to send your subscribers.

Step 4: <u>Measure</u>: The last step—which is ongoing— is testing and refining your efforts.

<u>THANKYOU</u>