Edge Hill University

The Department of Computer Science

CIS2711
Fundamentals of Digital Forensics

Level 5

Coursework 1 – Portfolio 1

Thomas William Mason
26040247

Table of Contents

Task 1: Digital Forensic Investigation of Data Exfiltration Case

Section A: Document the Chain of Custody Process

Table 1: The Chain of Custody

Item No.	Date & Time	Released by (Signature & ID)	Received by (Signature & ID)	Comments/ Location
1	19/02/2025 3:33 PM	Jean Jones	Thomas Mason	Downloaded disk images nps-2008-jean.E01 and nps-2008-jean.E02.
2	19/02/2025 5:47 PM	Jean Jones	Thomas Mason	Both disk images were uploaded to the Autopsy software, a powerful tool for forensic investigation.
3	19/02/2025 7:13 PM	Jean Jones	Thomas Mason	Client's email was investigated from '/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst'
4	20/02/2025 10:36 AM	Jean Jones	Thomas Mason	Analysis was completed and returned to the client.

Section B: Examine the Disk Image and Analyse Files of Interest

Table 2: Metadata Table

Sr No.	Timestamps (creation, modification, last accessed)	Description	Screenshot
1	Creation: 2008-07-20 02:28:04 BST Modification: 2008-07-20 02:28:04 BST Last Accessed: 2008-07-20 02:28:04 BST	The *m57biz.xls* file is within the recently accessed files and is saved under *'Documents and Settings/Jean/Recent/'* This shows where the file was initially saved.	**Metadata** Name: /img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Recent/m57biz.lnk Type: File System MIME Type: application/octet-stream Size: 468 File Name Allocation: Allocated Metadata Allocation: Allocated Modified: 2008-07-20 02:28:04 BST Accessed: 2008-07-20 02:28:04 BST Created: 2008-07-20 02:28:04 BST Changed: 2008-07-20 02:28:04 BST MD5: 267c4ad8a74c278fa0d5013342b43b64 SHA-256: 862a9e36e9ae10ee821817bf96b65ca04b966b20455bc20f61b8a334730825d8 Hash Lookup Results: UNKNOWN Internal ID: 12828
2	Creation: 2008-07-20 02:27:42 BST Modification: 2008-07-20 02:28:04 BST Last Accessed: 2008-07-20 02:28:04 BST	The same *m57.xls* file is also in the recent documents. However, it is now saved under *'Jean/Application/Data /Microsoft/Office/Recent/'* This now shows the file was uploaded to Jean's Microsoft account, and it was possibly uploaded to Outlook as an email attachment.	**Metadata** Name: /img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/m57biz.LNK Type: File System MIME Type: application/octet-stream Size: 408 File Name Allocation: Allocated Metadata Allocation: Allocated Modified: 2008-07-20 02:28:04 BST Accessed: 2008-07-20 02:28:04 BST Created: 2008-07-20 02:27:42 BST Changed: 2008-07-20 02:28:04 BST MD5: e0250a439c4b606dbb982c2902ff672c SHA-256: d5b44c949e5459f37302d17cb391ec33cd3d6b8c962d8e9453c7cbd4b9465312 Hash Lookup Results: UNKNOWN Internal ID: 3689

- No deleted files were found as suspicious or of interest for this investigation.

Section C: Digital Forensic Analysis

1. **What was the timestamp when Jean created the spreadsheet? (Hint: filename: m57biz.xls)**

The timestamp for the m57biz.xls file is 2008-07-20 02:28:04 BST, and the file path is within the Documents and Settings. The hash values are essential as they uniquely identify every file in the directory through hexadecimal numbers. If the file were to change even by a singular letter, it would generate a new hash value; in this case, the hash format is SHA-256, which is a 256-bit value (Forensic Discovery, 2025).

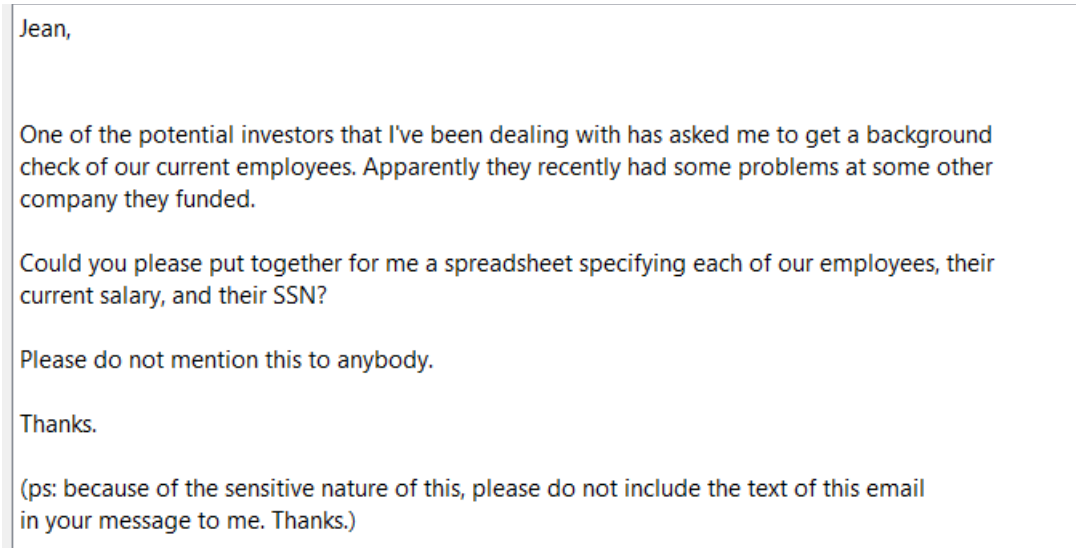
Type	Value	Source(s)
Path	C:\Documents and Settings\Jean\Desktop\m57biz.xls	RecentAct
Path ID	4014	RecentAct
Date Acce	2008-07-20 02:27:42 BST	RecentAct
Source File Path	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/m57biz.LNK	
Artifact ID	-9223372036854775796	

Metadata

Name:	/img_nps-2008-jean.E01/vol_vol2/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/m57biz.LNK
Type:	File System
MIME Type:	application/octet-stream
Size:	408
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2008-07-20 02:28:04 BST
Accessed:	2008-07-20 02:28:04 BST
Created:	2008-07-20 02:27:42 BST
Changed:	2008-07-20 02:28:04 BST
MD5:	e0250a439c4b606dbb982c2902ff672c
SHA-256:	d5b44c949e5459f37302d17cb391ec33cd3d6b8c962d8e9453c7cbd4b9465312
Hash Lookup Results:	UNKNOWN
Internal ID:	3689

2. How was the spreadsheet transferred from the company's laptop to the competitor's website? (Hint: email records can be related)

An attacker spoofed the organisation's email, sending a spear phishing mail to Jean (which can be seen within the Headers) titled 'background checks' and requesting a file containing the names, salaries, and social security numbers of all the current employees. The attacker later sends another email urgently requesting the data with a different return path of 'tuckgorge@gmail.com', to which Jean sends the confidential information and receives an email in return from the attacker thanking Jean.



Jean,

One of the potential investors that I've been dealing with has asked me to get a background check of our current employees. Apparently they recently had some problems at some other company they funded.

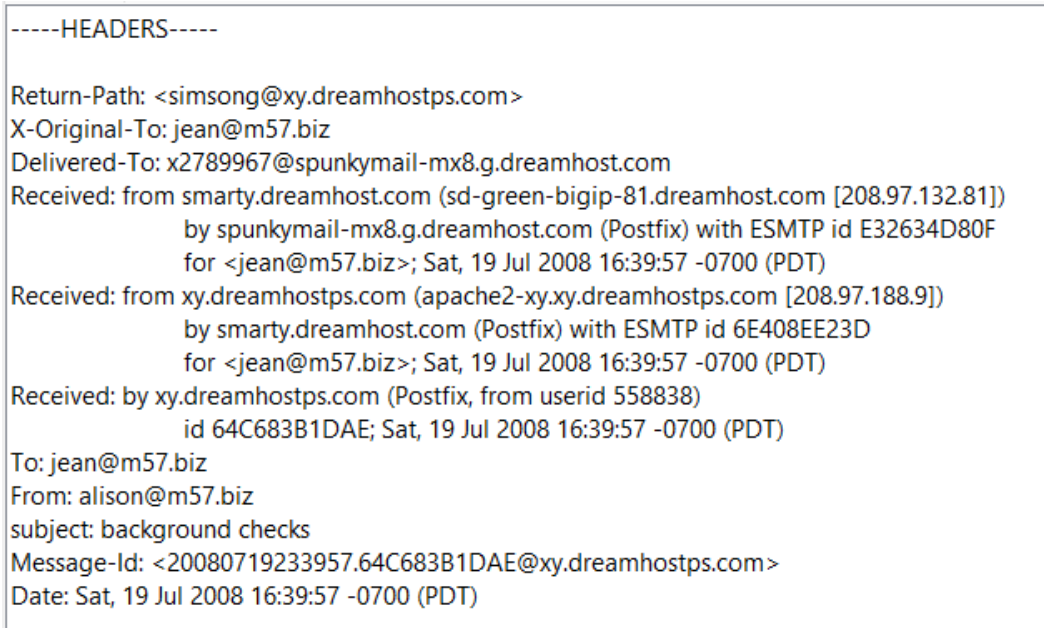
Could you please put together for me a spreadsheet specifying each of our employees, their current salary, and their SSN?

Please do not mention this to anybody.

Thanks.

(ps: because of the sensitive nature of this, please do not include the text of this email in your message to me. Thanks.)

Image 1 – Shows the original phishing email sent to Jean.



```
-----HEADERS-----

Return-Path: <simsong@xy.dreamhostps.com>
X-Original-To: jean@m57.biz
Delivered-To: x2789967@spunkymail-mx8.g.dreamhost.com
Received: from smarty.dreamhost.com (sd-green-bigip-81.dreamhost.com [208.97.132.81])
                by spunkymail-mx8.g.dreamhost.com (Postfix) with ESMTP id E32634D80F
                for <jean@m57.biz>; Sat, 19 Jul 2008 16:39:57 -0700 (PDT)
Received: from xy.dreamhostps.com (apache2-xy.xy.dreamhostps.com [208.97.188.9])
                by smarty.dreamhost.com (Postfix) with ESMTP id 6E408EE23D
                for <jean@m57.biz>; Sat, 19 Jul 2008 16:39:57 -0700 (PDT)
Received: by xy.dreamhostps.com (Postfix, from userid 558838)
                id 64C683B1DAE; Sat, 19 Jul 2008 16:39:57 -0700 (PDT)
To: jean@m57.biz
From: alison@m57.biz
subject: background checks
Message-Id: <20080719233957.64C683B1DAE@xy.dreamhostps.com>
Date: Sat, 19 Jul 2008 16:39:57 -0700 (PDT)
```

Image 2 - Shows email headers from the attacker and the return path showing an anonymous email.

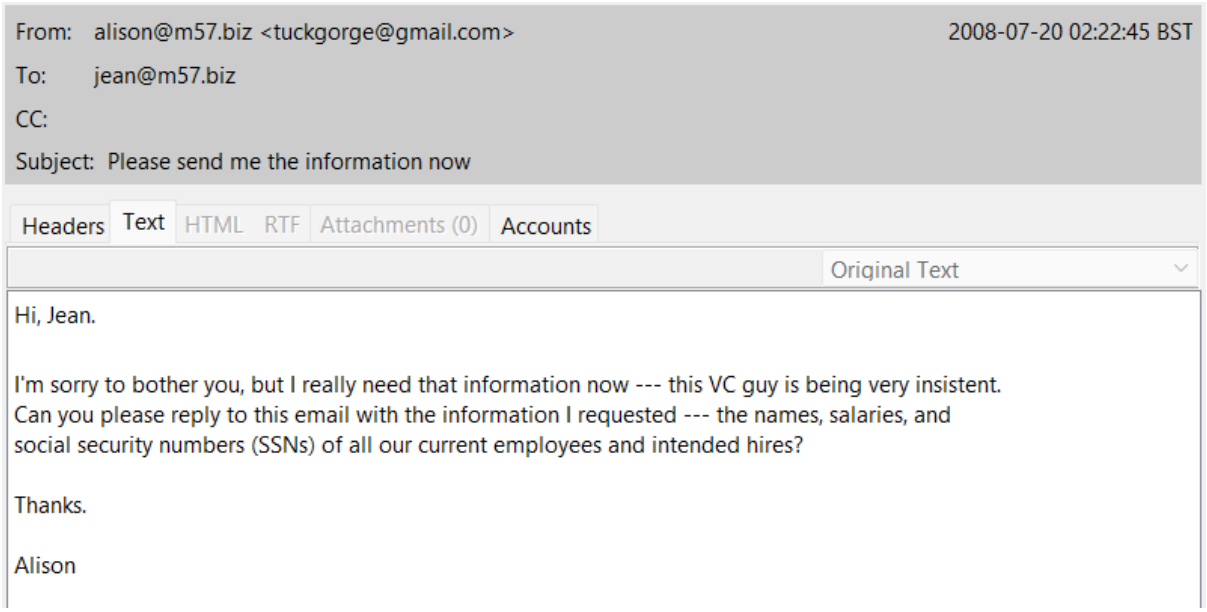


Image 3 – Shows the attacker being persistent and altering the return path to *tuckgorge@gmail.com*.

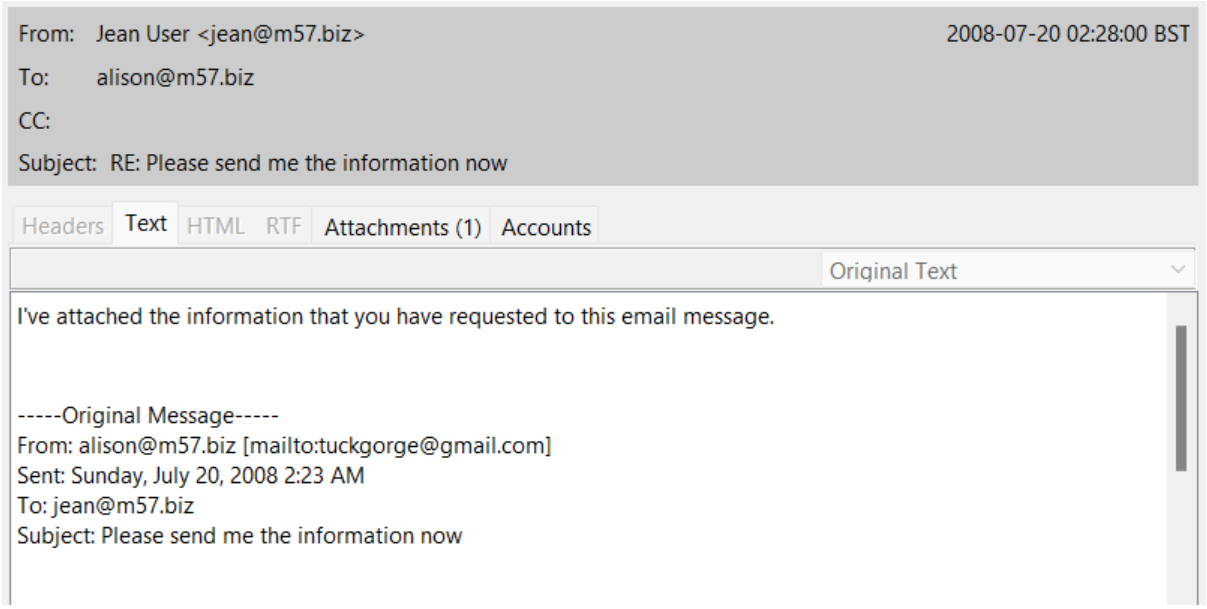


Image 4 – Shows Jean returning the email with the attachment included.

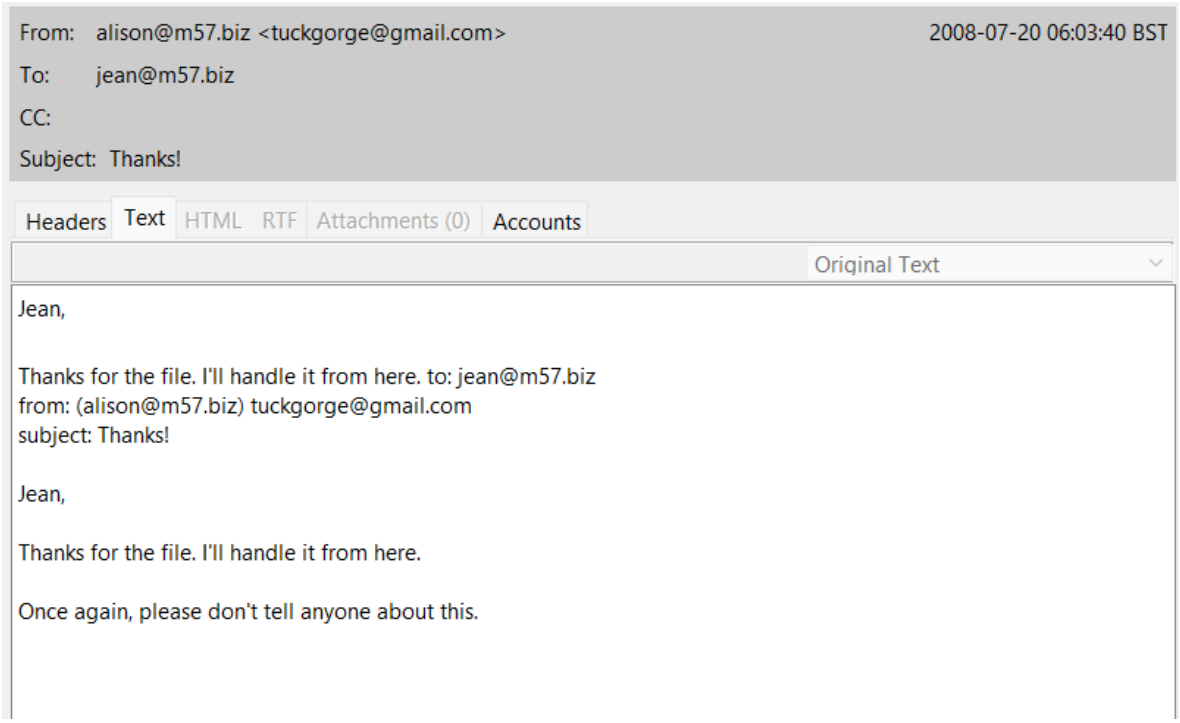


Image 5 – Shows the attacker replying to the email confirming the confirmation of the attachment and telling her not to tell anyone.

3. Is there any collusion in the company?

The forensic investigation concludes that Jean was spear-phished into the leak of the sensitive information. However, there was no direct link that suggests she was associated with the attacker or breach of the data, as Jean was aware of Alison's using another email address, as seen in image 6. Overall, Alison's statement matches the email being spoofed, and the leak could be attributed to a lack of care, training, and security within the company.

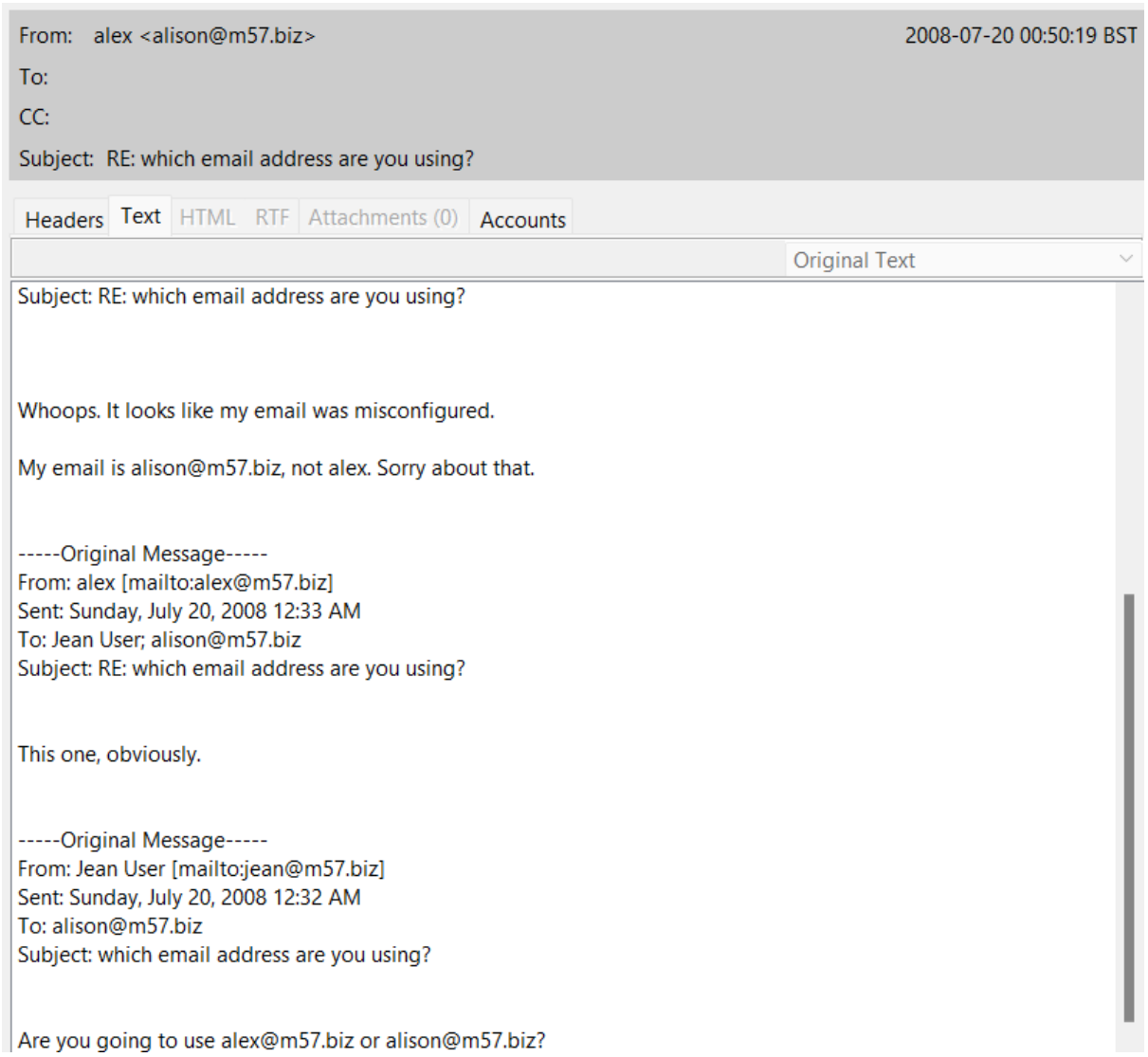


Image 6 – Shows Jean's confusion about Alison's email address being changed.

Section D. Findings

In the forensic investigation, a systematic approach was used to collect, analyse and present the evidence to the organisation. Firstly, the data was gathered and ensured to follow the NIST guidelines and ACPO principles, preserving the evidence and ensuring its integrity and accuracy. It was then uploaded onto the Autopsy software, where the recent documents, deleted files and Emails were analysed. After filtering the emails to date order, the email history was recited in chronological order from Jean's inbox; this gave a more accurate picture of the timeline of events and how the file was sent.

Date	Time	Description
19th July 2008	16:33:13	Jean is confused about which email address Alison is using. – Image 6.
19th July 2008	16:39:57	Jean receives an email requesting sensitive information titled "background checks". – Image 1.
19th July 2008	16:50:20	Alison is confused as to why Jean said, "Sure thing," as it was a reply confirming the sensitive information to be sent from Image 1.
19th July 2008	18:22:45	The spear phisher requests the data urgently again and alters the return path to *tuckgorge@gmail.com*. – Image 3.
19th July 2008	18:28:00	Jean returns the sensitive data to the attacker. – Image 4.
19th July 2008	22:03:40	The attacker thanks Jean and once again tells her not to tell anyone. – Image 5.

Table 3: Timeline of Events

There are multiple approaches the business can take to prevent this incident from happening again. Firstly, they could invest in using advanced email filtering to detect suspicious activity, which can analyse the inbound and outbound emails and block an email based on the content (proofpoint, 2025).

Another approach for the business could be employee awareness training and simulating a real-world attack to teach the staff to identify spear phishing emails such as strange or unexpected requests and to act quickly and promptly. Employee training needs to be kept up to date as malicious attackers are continuously improving their techniques (CISA, 2025).

References

CISA, 2025. *Teach Employees to Avoid Phishing.* [Online]
Available at: https://www.cisa.gov/secure-our-world/teach-employees-avoid-phishing
[Accessed 19 02 2025].
Forensic Discovery, 2025. *Hash Values are the DNA of Digital Evidence.* [Online]
Available at: https://forensicdiscovery.expert/hash-values-are-the-dna-of-digital-evidence/
[Accessed 19 02 2025].
proofpoint, 2025. *What Is Email Filtering?.* [Online]
Available at: https://www.proofpoint.com/uk/threat-reference/email-filtering
[Accessed 19 02 2025].