mimecast

5 Email Threats Exposed

Business Email Compromise: The $55 Billion Scam

“Over 40% of successful social engineering attacks were Business Email Compromise (BEC)/CEO Fraud imposter attacks.”

Verizon DBIR 2024

Business Email Compromise is a rapidly growing threat to businesses worldwide. According to Coalition’s 2025 Cyber Claims Report, BEC and Fund Transfer Fraud (FTF) accounted for 60% of all of their cyber insurance claims last year, with BEC claim severity increasing by 23%.[1]

But why are BEC scams so successful?
These attacks exploit human vulnerability and organizational trust structures, often bypassing traditional security measures. They rely on psychological manipulation rather than technical hacking, making them uniquely dangerous.

1. https://www.darkreading.com/cyber-risk/email-based-attacks-cyber-insurance-claims

Humans Make Errors

Accidental users, risky behaviors

95%
of cybersecurity incidents traced to human error.

68%
of breaches involve non-malicious human element.[2]

BEC Pretexting: The Elaborate Deception

Malicious insiders, insider risk

69%
of data loss incidents are caused by employee data exfiltration.

$15M
The average cost of an insider data leak.[4]

Traditional BEC: The Direct Approach

Email compromise threats spoof executives, exploit organizational hierarchies, create urgent demands for financial transfers and payments

$55B
in losses due to business email compromise and phishing scams between 2013-2023.[3]

$35,000
Average, BEC incidents cost.[1]

Below, we'll walk you through **five real-world examples of BEC attacks and how they operate.** By understanding the tactics scammers use, your business can strengthen its defenses and significantly reduce the risk of falling victim to these schemes.

2. Verizon 2024 Data Breach Investigations Report

3. PSA from the FBI: Business email compromise $55BN in losses due to business email compromise and phishing scams between 2013-2023

4. Mimecast Annual Data Exposure Report 2024

Gift Card Scam
Executive impersonation tactic

Key Characteristics

Executive Impersonation:
The scammer pretends to be a high-ranking official, such the CFO or CEO, to increase credibility and urgency.

Positive Reinforcement:
The message often praises team performance and frames the request as a reward for employees, making the action seem both urgent and generous.

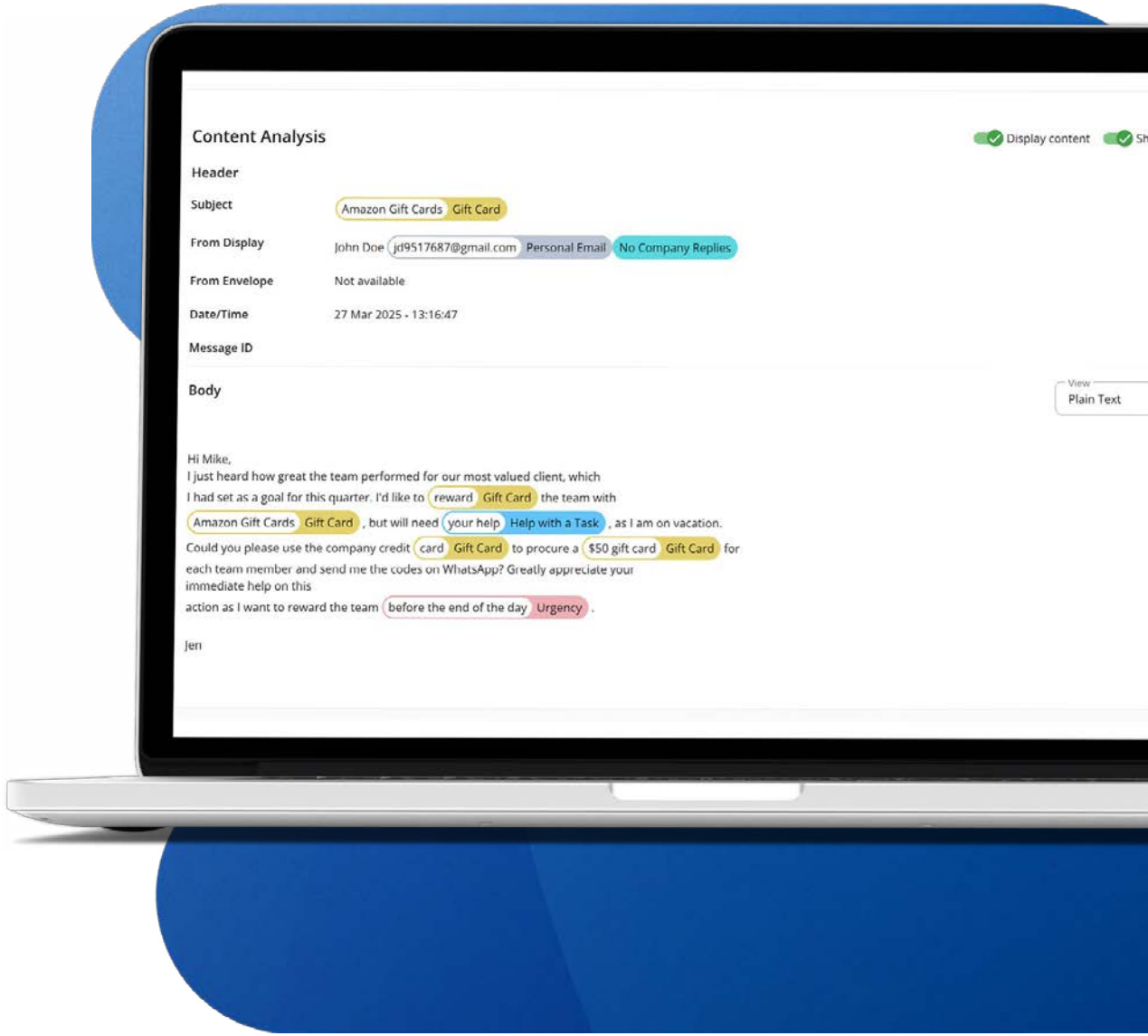
Alternative Communication Channels:
Instructions to send gift card codes via less secure platforms, like WhatsApp, are common to avoid detection.

Financial Analysis

Average gift card amount : **$50**
Count per email is **5** = **$250**

Frequency: 2/5

Loss: 2/5



Payroll Scam

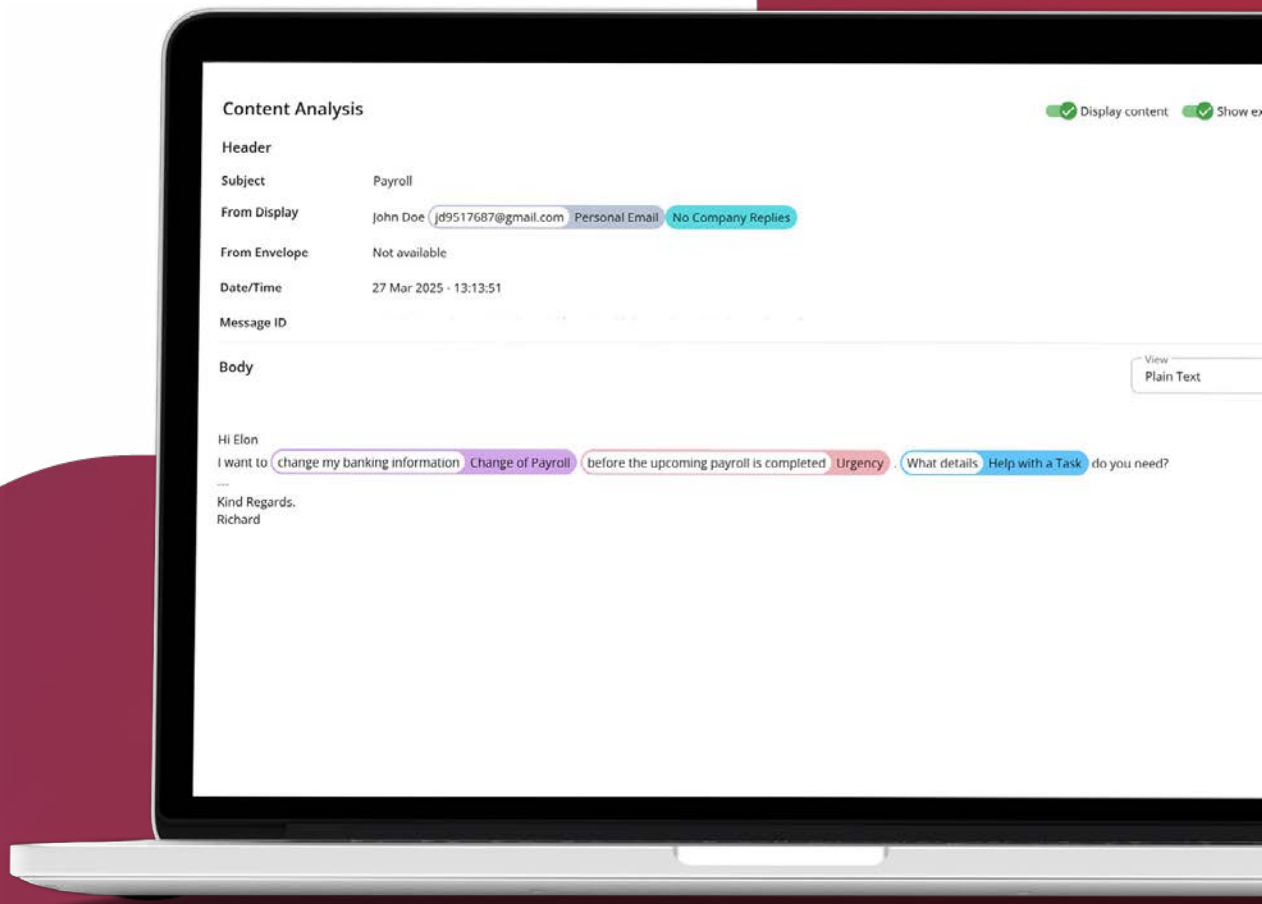
Growing threat to employee compensation

Key Characteristics

Executive Impersonation:
The scammer pretends to be an existing employee, using their name and possibly similar email addresses to gain trust.

Direct Deposit Redirect:
The primary aim is to change the banking details for payroll deposits, redirecting an employee's salary to the scammer's account.

Time Sensitivity:
The request is often made shortly before payroll processing deadlines to pressure payroll staff into acting quickly without thorough verification.



Financial Analysis

Average monthly employee salary in U.S. : **$5,000**

Frequency: 3/5

Loss: 5/5

Authority Scam
Urgency drives action

Key Characteristics

Executive Impersonation:
The scammer pretends to be a high-ranking manager or director, to exploit hierarchical trust.

Urgency and Secrecy:
The message claims urgency and requests a shift to a private communication channel, which is less monitored and more difficult to trace.

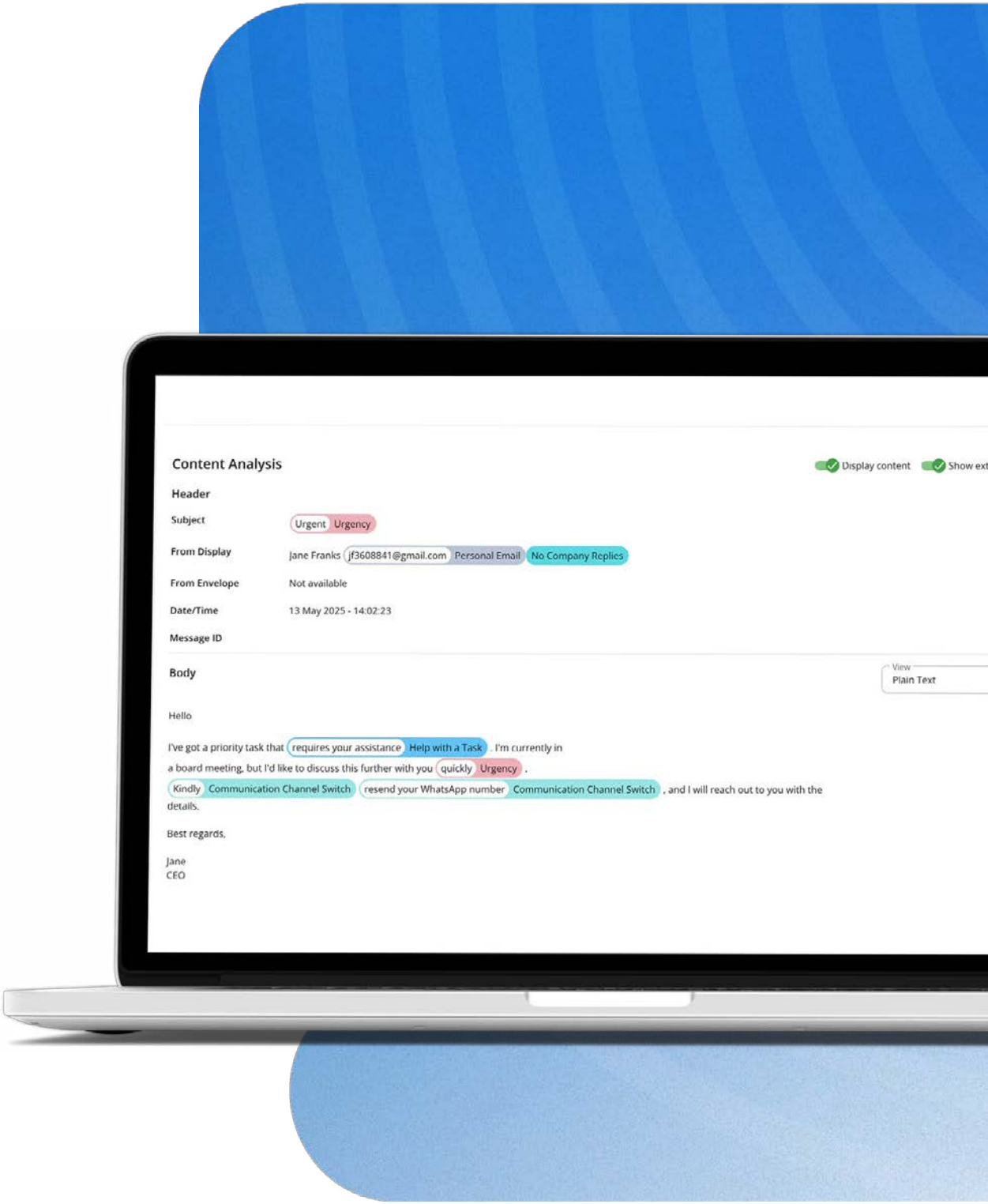
Minimal Initial Information:
Initial emails are vague to avoid suspicion but create a sense of importance, prompting the employee to respond quickly.

Financial Analysis

Average gift card demand : **$50**

Frequency: 5/5

Loss: 4/5



Fund Inheritance Scam

Advance fee on steroids

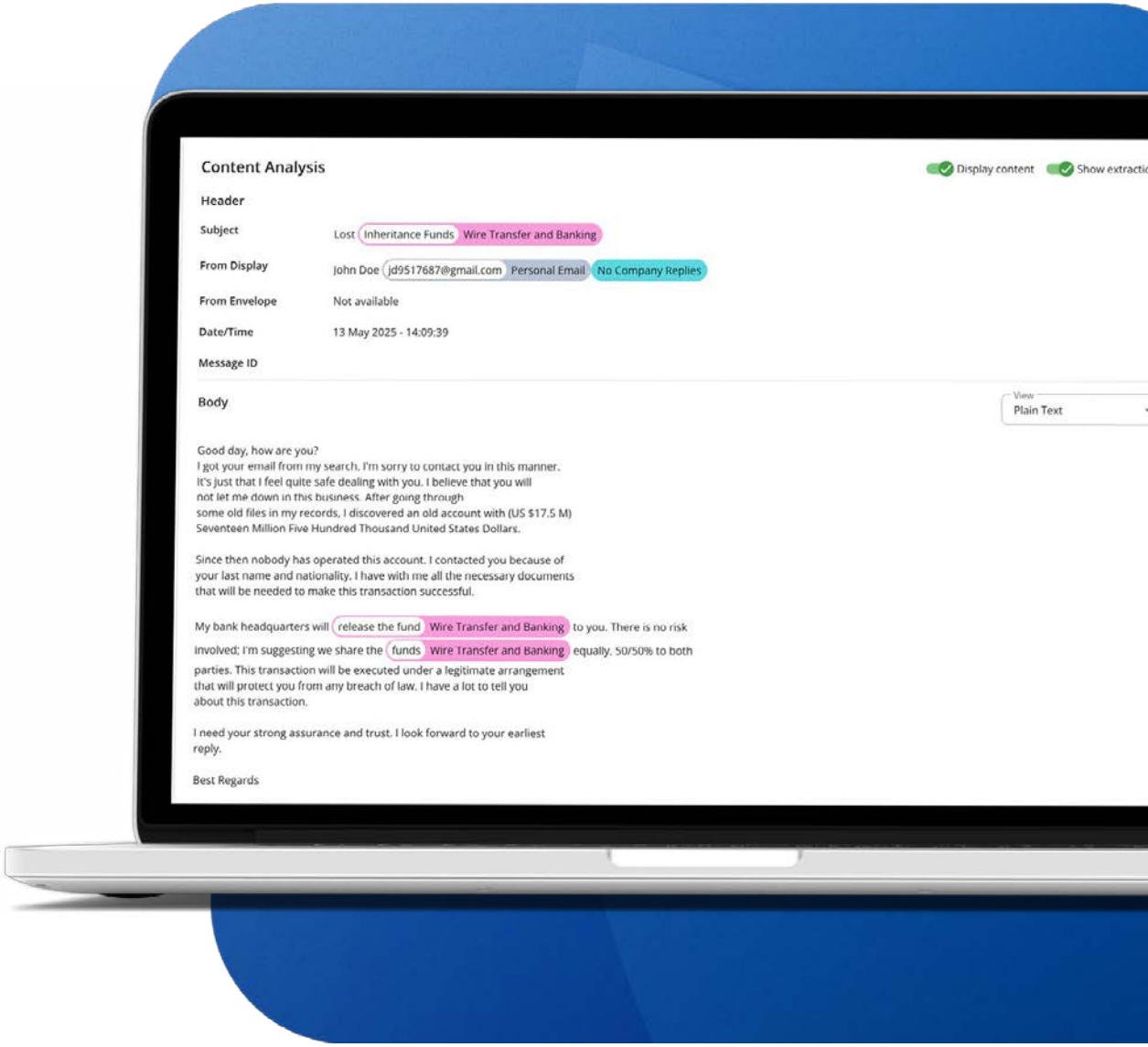
Key Characteristics

Deceased Client Narrative:
The scammer claims to be the account officer of a deceased client who left behind a significant unclaimed sum of money.

Surname Coincidence:
The recipient is told they share the same surname as the deceased, suggesting they could pose as a legitimate next of kin.

Promise of Partnership:
The email proposes a lucrative partnership, offering a share of the funds in exchange for help in transferring the money.

Assurance of Legitimacy:
The message assures the recipient that the transaction is legal and risk-free, attempting to build trust.



Financial Analysis

Average transaction in such emails : **$340**

Frequency: 2/5

Loss: 2/5

SEO Scam

Keywords are quick results

Key Characteristics

Unsolicited Offers:
Scammers send emails offering SEO services with blanket rates, such as $99 per month, promising top rankings on Google without any prior knowledge of the recipient's business or website specifics.

Urgency and Fear Tactics:
These emails often highlight supposed flaws in the recipient's website, creating a sense of urgency to prompt immediate action.

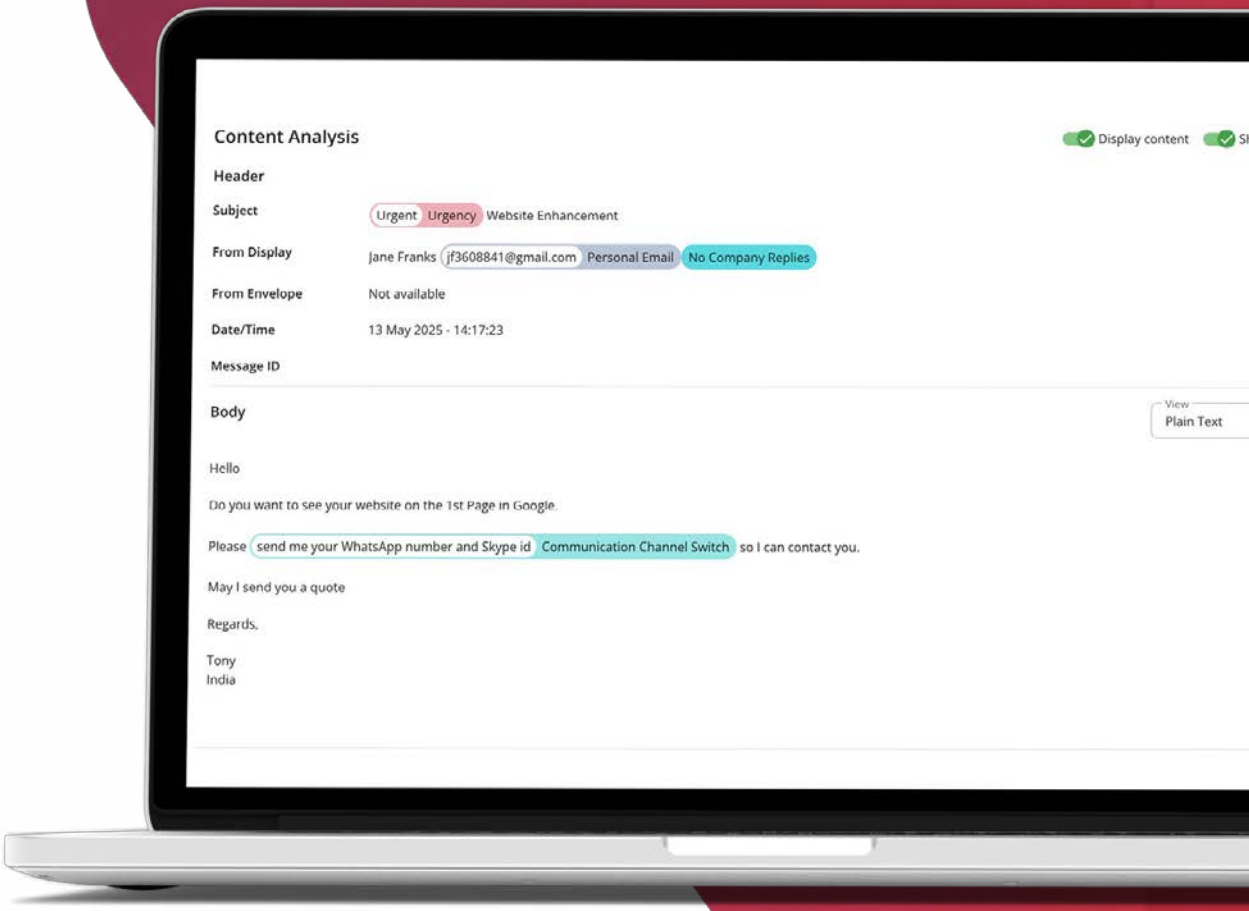
Switch to Less Secure Channels:
Scammers may request to continue communication on less secure platforms, increasing the risk of phishing or malware attacks.

Financial Analysis

Average transaction in such emails : **$120**

Frequency: 4/5

Loss: 3/5



“Email presents the largest risk for threats like phishing, and with more people working remotely than ever before, it’s even more critical to protect our email communications. That’s why we turned to Mimecast for help.”

Erik Hart, Chief Information Security Officer at Cushman & Wakefield

See How Mimecast Blocks BEC Threats

Business Email Compromise continues to evolve, which is why Mimecast takes the approach of pre- iltering and AI-powered security.

Connection
we solve IT

Contact your Connection Account Team for more information.
1.800.998.0067 ■ www.connection.com/Mimecast

3361271-1125

mimecast