



# Why RMail for BEC

The Missing Layer in Your Security Stack



## ▶ Customer Stories

**Applied Systems is the world's largest insurance agency management platform. Their customers have trusted RMail email security for more than a decade. Now Applied Systems is building the newest RMail innovations – its AI-infused impostor email and human error protection suite – into its main platforms, OEM-esque.**

[www.RMail.com](http://www.RMail.com)

## What is Business Email Compromise?

Business Email Compromise (BEC) is a social engineering, targeted cyber attack designed to trick individuals into sending sensitive information or money to the attacker, often through the use of phishing and spear-phishing techniques.

BEC attacks can target both **inbound and outbound** emails, meaning that emails can be intercepted both at the sender and at the recipient, making them particularly difficult to detect and prevent.

## Perfect Harmony, Enhance the Outbound

### Keep your existing inbound email security – and even your outbound DLP.

RMail harmoniously extends your existing email security systems, adding Email Eavesdropping™ detection, even at your recipient's end, personalized eSecurity training and awareness integrated into the email client, DLP automation at the client and server levels, and more.

RMail seamlessly installs into Microsoft Outlook, Gmail, Salesforce and more, and can also be installed at the server level.

## Key Capabilities

- Detects cybercrimes in progress targeting you **even at your recipient**.
- Empowers Admins to automate DLP in the inbox and at the server level.
- Delivers **personalized secure email recommendations** to your users in the moment of sending.
- Detects and alerts for lookalike domains and other trickery.
- Allows users to un-send sensitive content from the email body.
- Empowers recipients to **authenticate invoices**.

# \$2.7 billion

Lost yearly to BEC attacks

- FBI, IC3 report. 2023.

## Key Features

### Email Eavesdropping™ Alerts

#### Email Activity Report

#### Email Eavesdropping™ Alert

Original Recipient: David.Smith@northwestinsurance.com

Security: **Red**

Opens: **3**

Locations: **2**



Email Age: 15 days 1 hour 4 minutes

Risk Details: All Activities

**Pre-empt cybercrime.**  
**After the hook is in, before the steal.**

| Time (UTC)          | Activity   | Location     | Country | Network Addr. | Network       | Risk  |
|---------------------|------------|--------------|---------|---------------|---------------|-------|
| 09/15/2022 08:12:48 | Open (VPN) | Ikeja, Lagos | Nigeria | 41.67.191.255 | Netcom Africa | Red   |
| 09/13/2022 17:06:22 | Open       | Boston, MA   | USA     | 94.92.53.178  | Verizon       | Green |
| 09/13/2022 12:54:18 | Open       | Boston, MA   | USA     | 94.52.53.178  | Verizon       | Green |

#### Original Message Details

Subject: Weekly analysis

Original Send Time: 09/13/2022 03:20:00 UTC

Transaction ID: A4BD52B62EE9862A5FDD8B8F336A99E2D69FEF54A

#### Metadata:

[IP Address: 41.67.191.255] [Time Opened: 09/15/2022 08:12:48 AM] [REMOTE\_HOST: 192.168.10.153] [HTTP\_HOST: open.r1.rpost.net] [SCRIPT\_NAME: /open/images/LGy25hw0Z65CNlyOLyZCLCuMKdk95gm4vir26bBCMDlx.gif] HTTP\_ACCEPT: \*/\* HTTP\_ACCEPT\_ENCODING:gzip, deflate HTTP\_HOST:open.r1.rpost.net HTTP\_USER\_AGENT:Mozilla/4.0 (compatible; ms-office; MSOffice 16) HTTP\_X\_FORWARDED\_FOR:183.82.2.55 HTTP\_X\_FORWARDED\_PROTO:https HTTP\_X\_FORWARDED\_PORT:443 HTTP\_X\_AMZN\_TRACE\_ID:Root=1-632d2601-68f7d3e527e10ac35f151b35 HTTP\_UA\_CPU:AMD64 Accept: \*/\* Accept-Encoding: gzip, deflate Host: open.r1.rpost.net User-Agent: Mozilla/4.0 (compatible; ms-office; MSOffice 16) X-Forwarded-For: 183.82.2.55 X-Forwarded-Proto: https X-Forwarded-Port: 443 X-Amzn-Trace-Id: Root=1-632d2601-68f7d3e527e10ac35f151b35 ua-cpu: AMD64 /LM/W3SVC/5/ROOT 256 2048 C=US, S=VA, L=Herndon, O=Network Solutions L.L.C., CN=Network Solutions DV Server CA 2 CN=tracking.rpost.com 0 CGI/1.1 on 256 2048 C=US, S=VA, L=Herndon, O=Network Solutions L.L.C., CN=Network Solutions DV Server CA 2 CN=tracking.rpost.com 5 /LM/W3SVC/5 192.168.10.186 /open/images/LGy25hw0Z65CNlyOLyZCLCuMKdk95gm4-vir26bBCMDlx.gif 192.168.10.153 192.168.10.153 46808 GET /open/images/LGy25hw0Z65CNlyOLyZCLCuMKdk95gm4vir26bBCMDlx.gif open.r1.rpost.net 443 1 HTTP/1.1 Microsoft-IIS/8.5 /open/images/LGy25hw0Z65CNlyOLyZCLCuMKdk95gm4vir26bBCMDlx.gif \*/\* gzip, deflate open.r1.rpost.net Mozilla/4.0 (compatible; ms-office; MSOffice 16) 183.82.2.55 https 443 Root=1-632d2601-68f7d3e527e10ac35f151b35 AMD64

RPost patented (rpost.com/patents) including US patent applications 17663425, 63/201,857, 63/366,685, 63/366,661 and other applications.

(M) = activity determined to be on a mobile device.

(VPN) = activity was detected at an anonymizing VPN endpoint location.

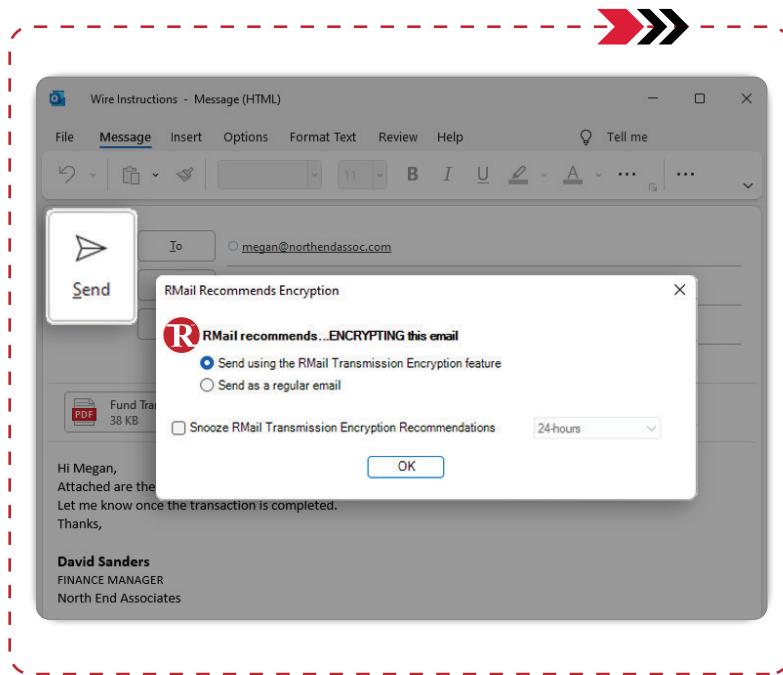
Location = registered location of the detected network.

Network = registered network associated with the internet protocol.

With Email Eavesdropping™ alerts, admins and senders can receive real time notifications if RMail detects that an outgoing email is being monitored by someone other than the intended reader. These alerts include all the email forensics so that IT security specialists can validate and take immediate action, before the cybercriminal lures users into mis-wiring money to the criminal's bank.

## Email Security

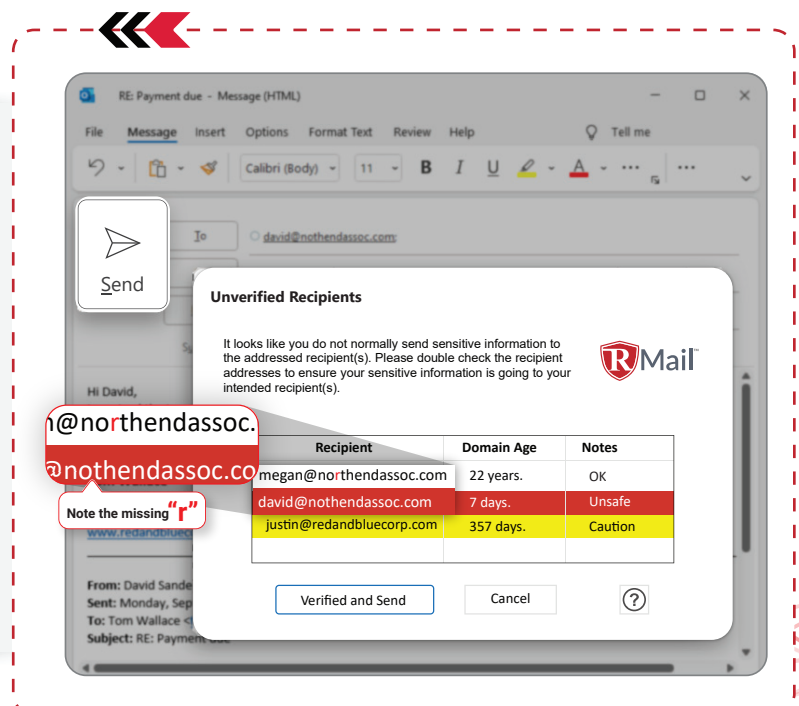
### RMail Recommends™



At the click of the Outlook Send button, RMail recommends the sender the appropriate RMail feature based on message content and attachments. IT admins can customize recommendations or even make certain features mandatory.

### Impostor Email Detection

At the click of the Outlook Send button, RMail presents the full email address of each recipient to make it easy for senders to re-verify that they are about to send the right message to the right recipient. And, if RMail identifies any cybercriminal trickery in the email addresses, such as clever domain misspells or tricky message header reply-to pivots, it instantly alerts the sender.



## Email Security

### Secure Large File Share™

Senders can securely attach and send up to 1GB of files right from inside the Outlook compose window to any recipient with encryption and configurable self-purging options -- or any of the RMail web applications.

### Digital Seal®

RMail Digital Seal® makes it easy for a recipient to verify origin and authorship of an email (for example, an email carrying an invoice) and re-create a copy of the original message content instantly. This empowers the recipient to verify authenticity of payment information in real-time, anytime, before paying.

### Redact+

RMail empowers senders to redact certain content from the message body, eliminating the risk of your organization's sensitive information being exposed in email threads or if the recipient's email account is compromised.



RPost© Copyright 1999-2023.  
RPost trademarks are registered and unregistered.

---

[www.RMail.com](http://www.RMail.com)