RMail™
By RPOST

Email Security

Targeted Attack Pre-Emption
Features Spotlight

Explore Our
Secure Email
Services

Email Privacy &
Compliance

Human Error
Prevention & DLP

APPLIED

▶▶ 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 plus dynamically simplified email encryption – into its main platforms, OEM-esque.

Targeted Attack
Pre-emption

Certified Proof of
Content Delivered

Outbound AI
Security Stack

California	70+	100%	190+	
R&D	Patents	AI-Infused	Countries	www.RMail.com

Email Privacy & Compliance

SMARTR Email Encryption
Dynamically adapting encrypted email ensures elegantly easy; simple for recipient means happy sender. Far beyond opportunistic TLS, RMail encrypted email service smartly adapts to provide peace-of-mind with end-to-end encryption, secure file sharing, auditable proof of fact of GDPR and HIPAA privacy compliance, email thread security monitoring, and more.

Human Error Prevention & DLP

Mutating the DNA of Data Leaks
Automatically sensitize users of their need to treat certain messages differently, seamlessly and in the flow of email and work, with in-the-moment-of-sending, bite sized insights and alerts. Empower your people and prevent data loss with AI-Infused and automated rules-based email compliance and security recommendations.

Targeted Attack Pre-emption

Intercepting the Human Instinct to Please
Nip cybercriminal-induced mis-wires (a/k/a wire fraud) with real-time alerts that expose whose email account is being eavesdropped on, which email addresses have tricky lookalike domains, and when a reply is about to be hijacked--must-have additional layers for your Business Email Compromise defense. Outbound Pre-Crime™ email security at its finest!

Certified Proof of Content Delivered

Proof of Who Said What When, by Email
Gain insights of the overall journey of your email, how popular who read what when, and receive forensic certified proof.

Outbound AI Security Stack

Perfect Harmony, Enhance the Outbound
Keep your existing inbound email security – and even your outbound DLP if you so choose. Add RMail outbound security gateway, in-the-inbox integrated cloud email security, and in-the-ether e-security content controls: all, some or one. RMail harmoniously extends your existing email security systems, adding elegantly-easy encryption user experiences, unique BEC targeted attack detection, and more, with AI DLP automation.

Why We Are Unique

Our features provide the best user experience. Our prices make us the most affordable. And our services connect elegantly inside your existing email programs and business systems.

Breadth of Services
RMail empowers you; all of the functionality you need, all in one installation onto the platforms you're already using -- email encryption, certified proof, AI-infused human e-security error prevention, in-the moment personalized e-security training, and much more.

Simplicity
We understand that the power of e-security technology resides in user adoption. That is why RMail is built with AI that automatically sensitizes users to today's e-security and e-compliance needs, subtly nudging them to make the right email-related e-security decisions. Securing your business has never been easier.

Legal Proof®
Each message comes with a Registered Receipt™ email record; the global standard for court-accepted, timestamped proof of secure delivery of emails — and its attachments. This record is durable (it may be forwarded, retaining its self-authenticating integrity), and is self-contained (it does not require any other record to be stored anywhere).

Friendlier Service
Excellent technology is key, outstanding service is gold. Getting both in a single package is pure bliss. Our teams are more knowledgeable and friendlier to work with. That is why our customers rate us with 99% satisfaction scores and 5-star accolades.

Thank you, to the more than **25 million people** the world over, who have put their trust in our team and technology, **since 2000**.

RMail Security Flow

RMail Outbound Cloud Security Platform most often acts as an extension of one's existing inbound email security filters and outbound DLP services, with specialized Email Eavesdropping™ protection, elegantly easy and automated email encryption, and more.
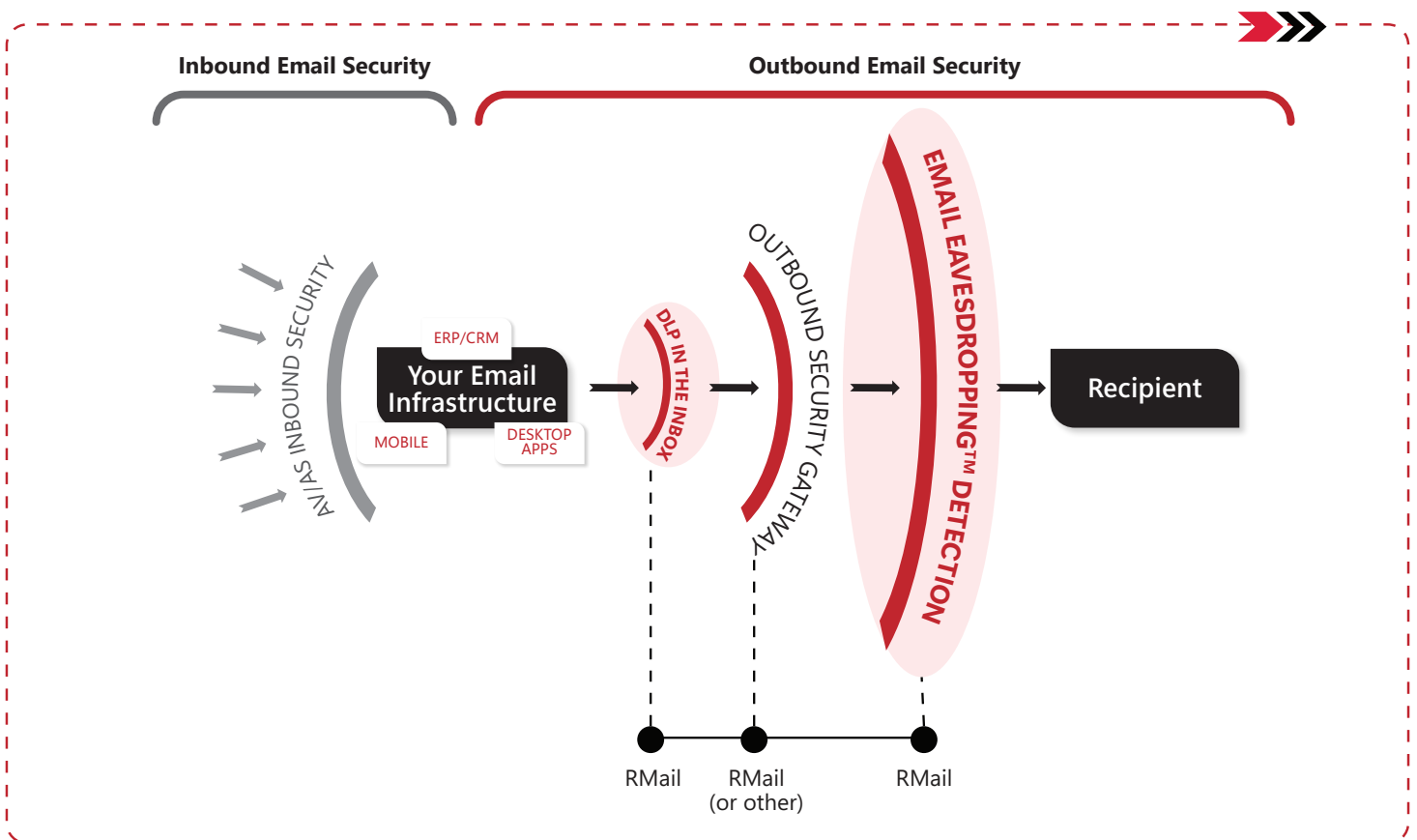

RMail services detect when a message should be sent encrypted and automatically transform it into a secure message that recipients can view with ease.

With Email Eavesdropping™ threat hunting, senders have peace-of-mind that they will be alerted in real time if a cybercriminal has compromised their recipient's email inbox, which is often the main step in lures leading to mis-wires.

RMail then sends aggregate Email Eavesdropping™ red-alerts to administrators and, if desired, to their managed security service provider as well.
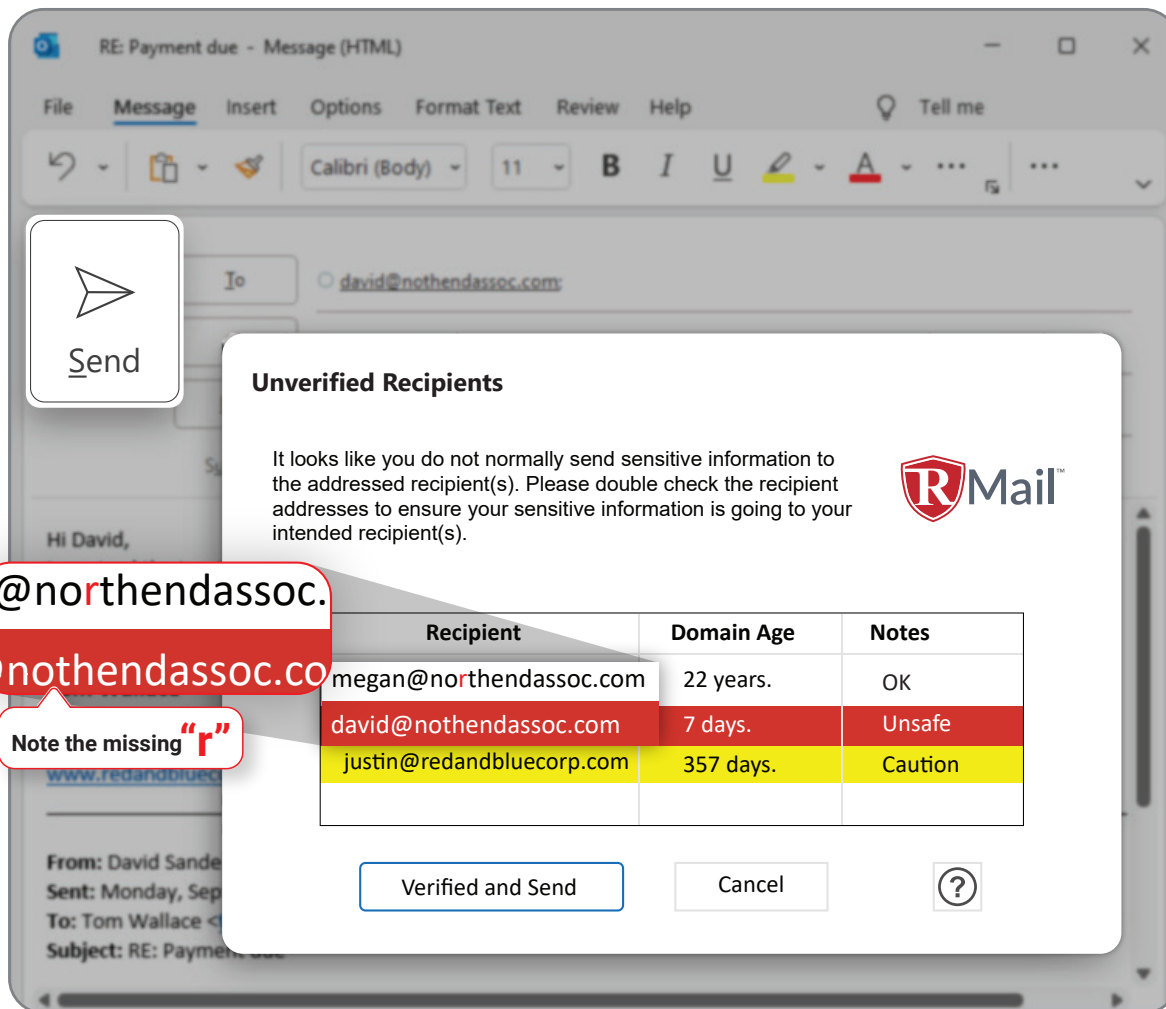
All-in-One in the Inbox
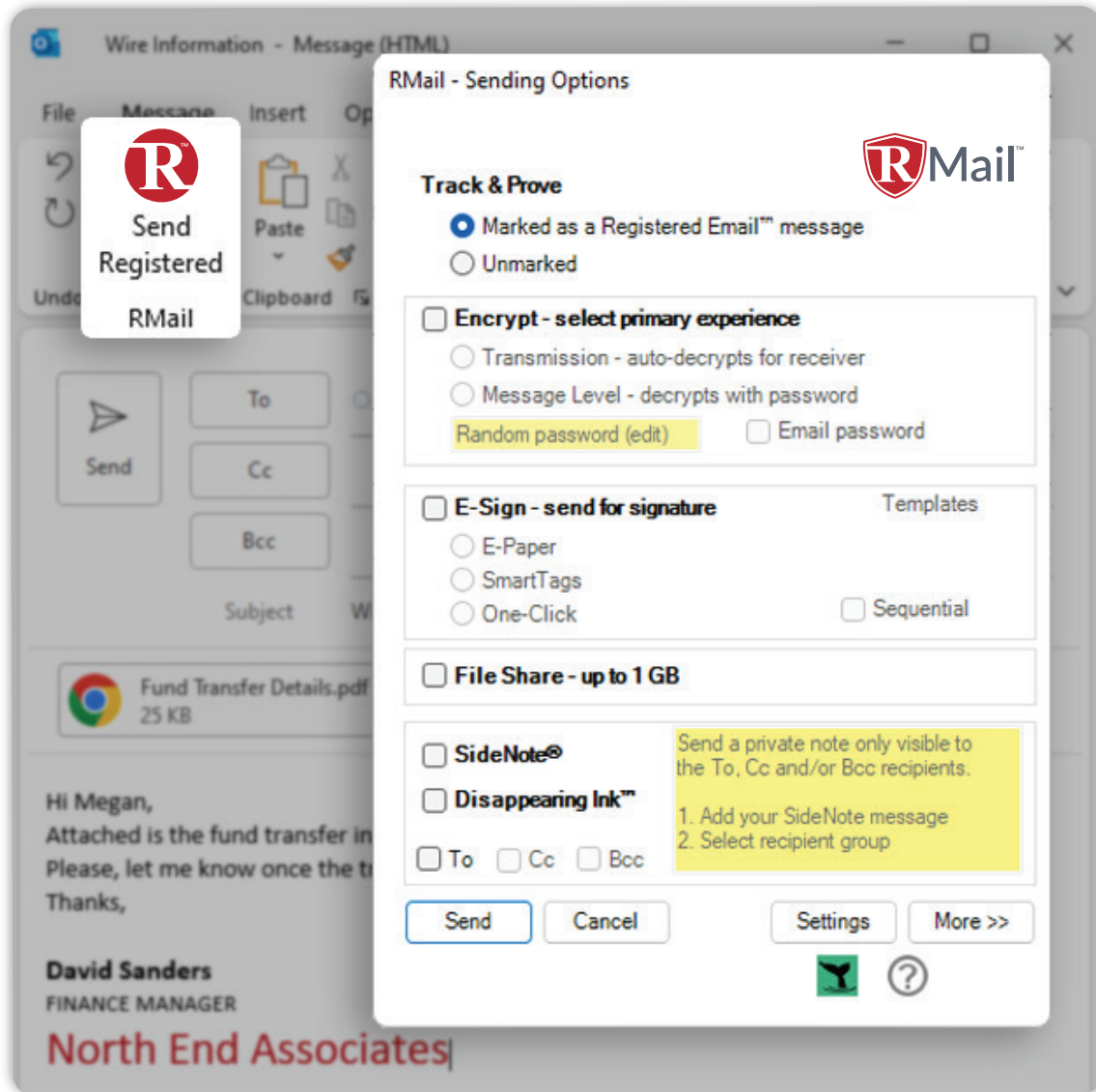
RMail installs seamlessly into Microsoft Outlook, Gmail, Salesforce and more to empower users with its full set of email security, DLP, privacy compliance and productivity tools at the click of a button.

RMail Recommends™ DLP in the Desktop
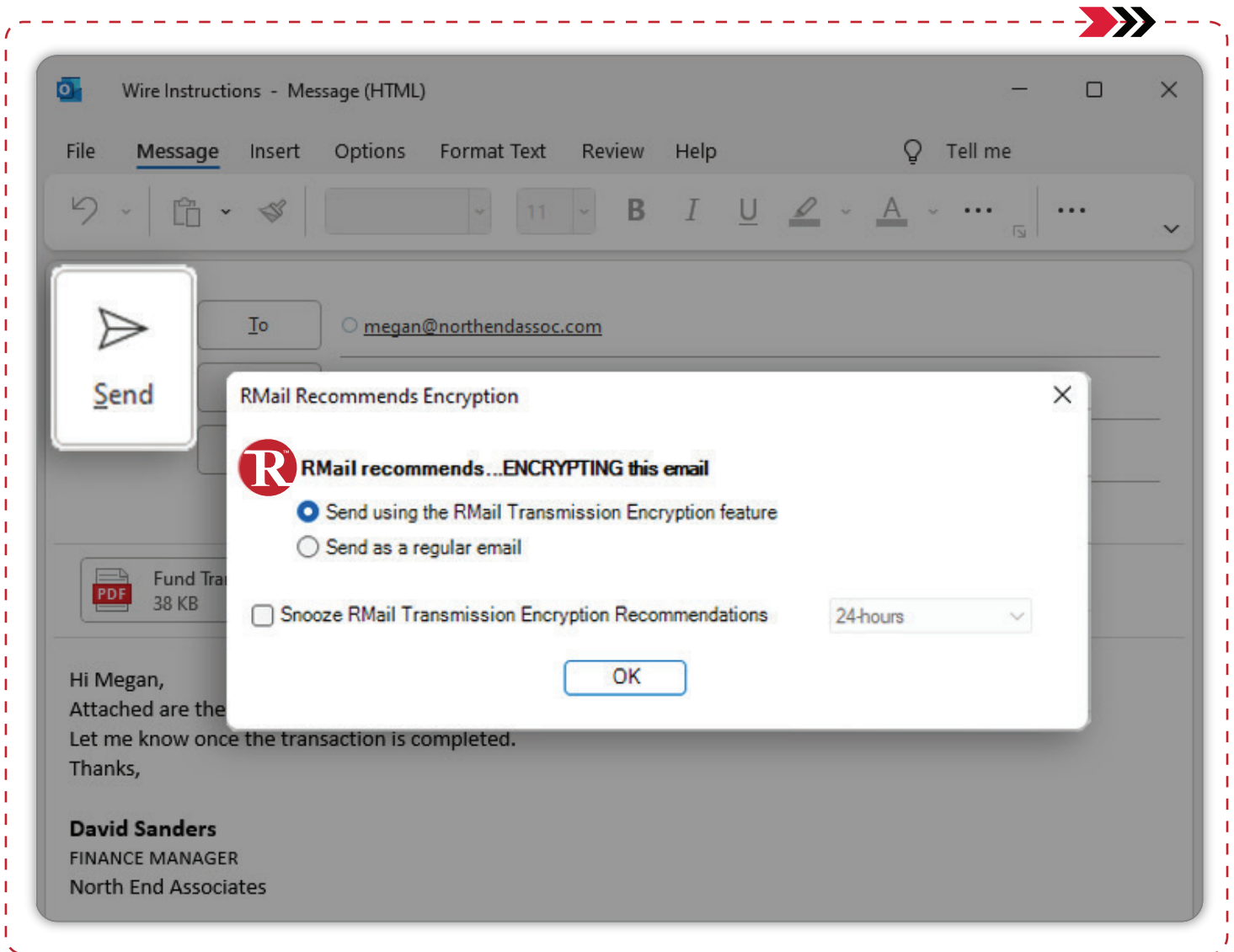
RMail automatically sensitizes users to the need to treat certain email with special care; and then transforms the message with specialized security in mind. This is true DLP in the desktop, no server settings or routings needed. For the sender, it's just like sending any other email. For IT admins, it's peace of mind with pure email security and compliance bliss.

Right Recipient™: Lookalike Domain™ Detector

In this example, the cybercriminal has newly purchased a domain with one letter different -- missing the "r" – to effectively hijack the reply and continue corresponding, posing as a long-time contact.

Unverified Recipients

It looks like you do not normally send sensitive information to the addressed recipient(s). Please double check the recipient addresses to ensure your sensitive information is going to your intended recipient(s).

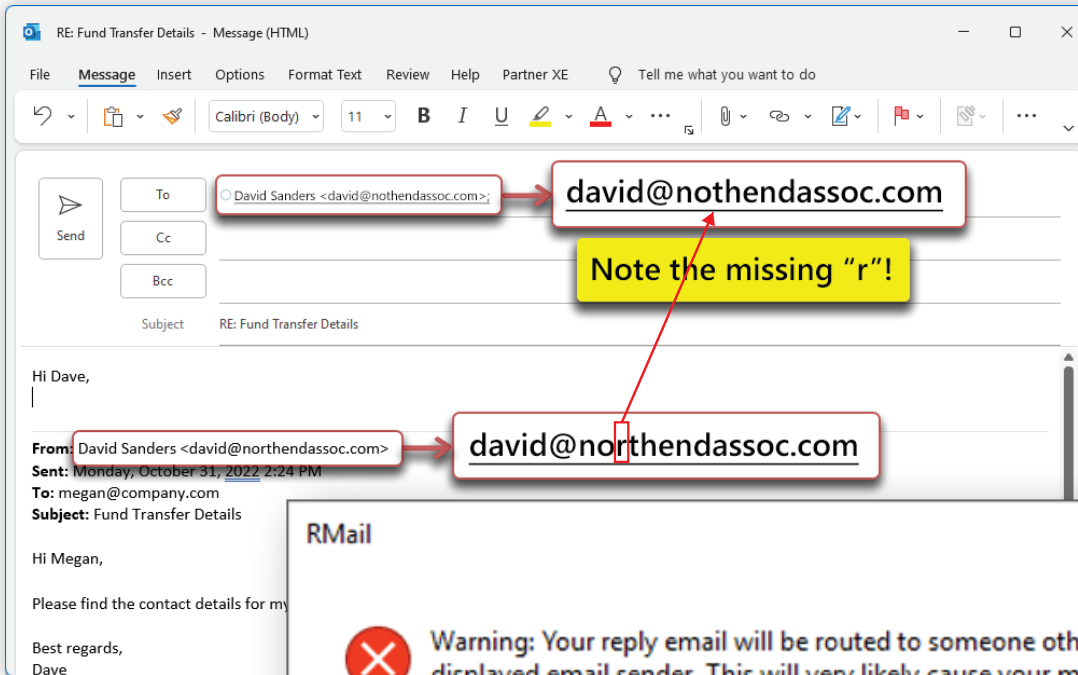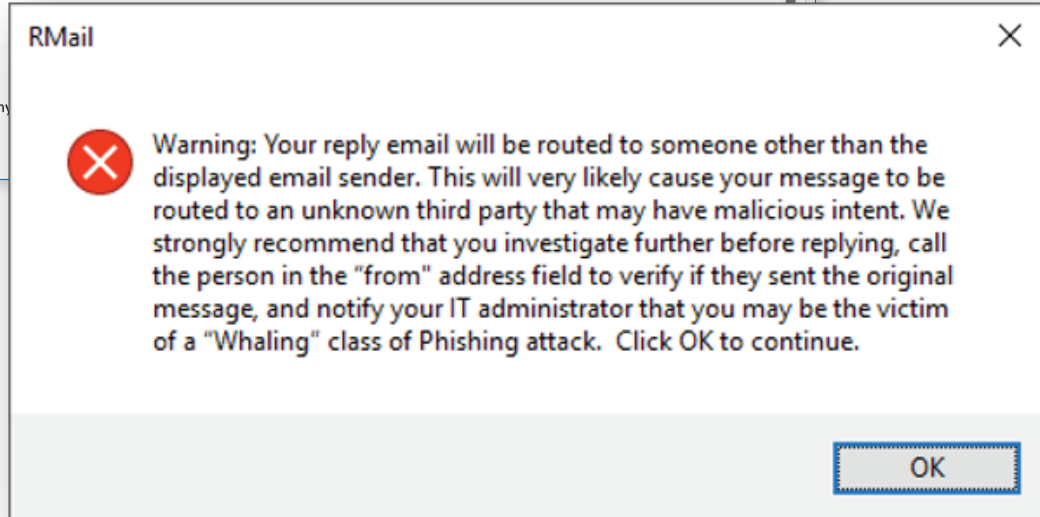| Recipient	Domain Age	Notes
megan@northendassoc.com	22 years.	OK
david@nothendassoc.com	7 days.	Unsafe
justin@redandbluecorp.com	357 days.	Caution

Verified and Send   Cancel   ?

Note the missing "r"

After an email is deemed important enough to send in a special RMail way, 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.

Right Recipient™: Reply Hijack™ Alerts

RE: Fund Transfer Details - Message (HTML)

File   Message   Insert   Options   Format Text   Review   Help   Partner XE   ♀ Tell me what you want to do

Calibri (Body)   11   **B** *I* U ...

To: ○ David Sanders <david@nothendassoc.com>;

→ david@nothendassoc.com

Cc:

Bcc:

Subject: RE: Fund Transfer Details

Note the missing "r"!

Hi Dave,

From: David Sanders <david@northendassoc.com>
Sent: Monday, October 31, 2022 2:24 PM
To: megan@company.com
Subject: Fund Transfer Details

→ david@northendassoc.com

Hi Megan,

Please find the contact details for my

Best regards,
Dave

The lookalike reply domain is not visible to human eyes until after the sender clicks reply, at which time it is very difficult for the sender to spot.

RMail   ✕

❌ Warning: Your reply email will be routed to someone other than the displayed email sender. This will very likely cause your message to be routed to an unknown third party that may have malicious intent. We strongly recommend that you investigate further before replying, call the person in the "from" address field to verify if they sent the original message, and notify your IT administrator that you may be the victim of a "Whaling" class of Phishing attack. Click OK to continue.

OK

This feature will alert senders **after the hook is in, before the steal,** in-the-moment of replying or forwarding a message, if RMail detects a message will pivot from the intended recipient.

This method, combined with the utilization of impostor domains, is one of the most common ways in which cybercriminals hijack a thread, and one of the first steps towards wire fraud.

SMART**R**™ Encryption
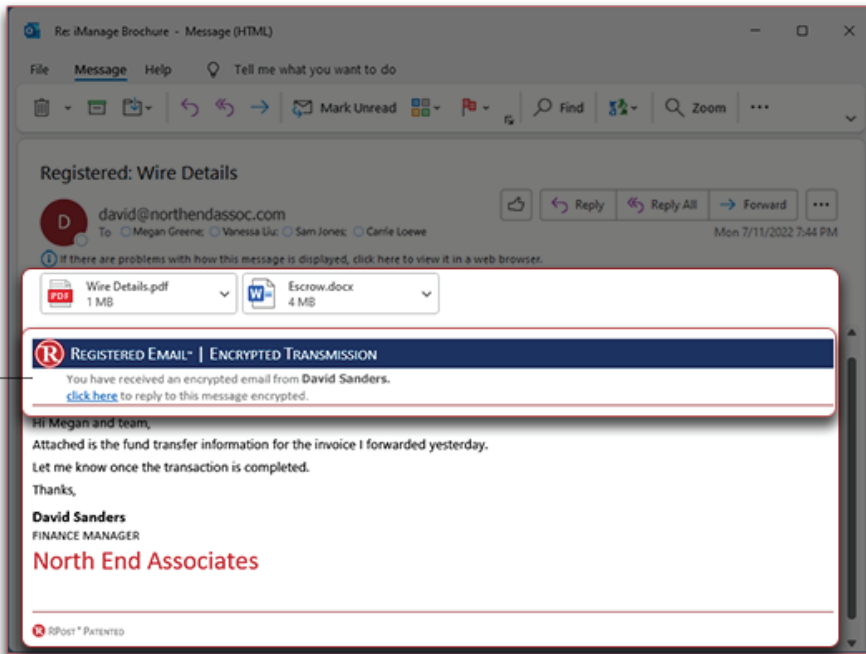
Transmission Preferred Encryption: RMail's default settings first attempt transmission level encryption at the minimum sender-acceptable security level, and deliver the encrypted email right to the recipient's inbox, providing the same familiar user experience as a normal email: **without any logins, links or need to create an account.** Recipients even have the option to reply encrypted.

R **REGISTERED EMAIL™ | ENCRYPTED TRANSMISSION**

You have received an encrypted email from **David Sanders.**
click here to reply to this message encrypted.

Benefits:
- The banner adds confidence for the receiver that the information was shared securely
- Familiar user experience
- No logins, links or need to create an account

click here to reply to this message encrypted.
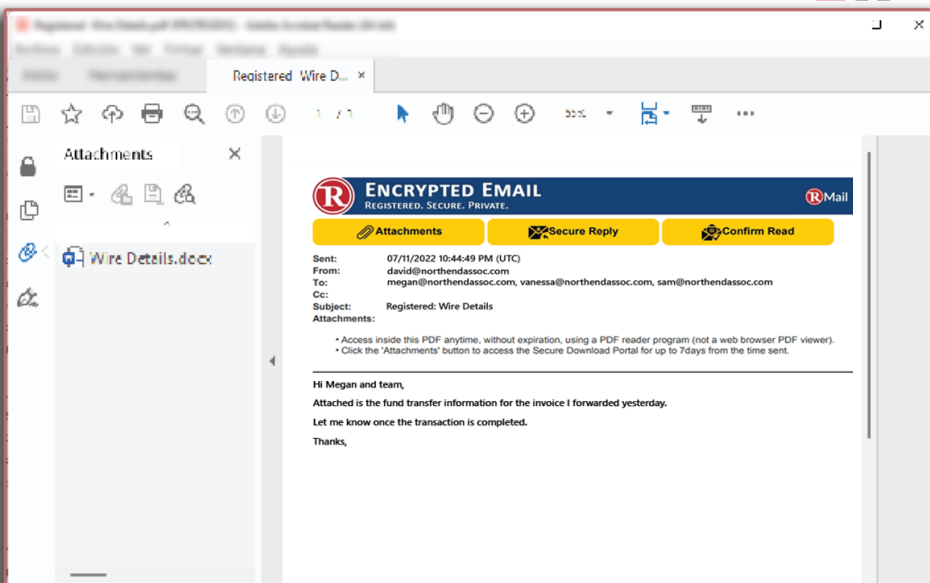
Benefits:
- Recipient can reply encrypted
- Option to attach up to 200MB of files securely in the reply

SMARTR™ Encryption
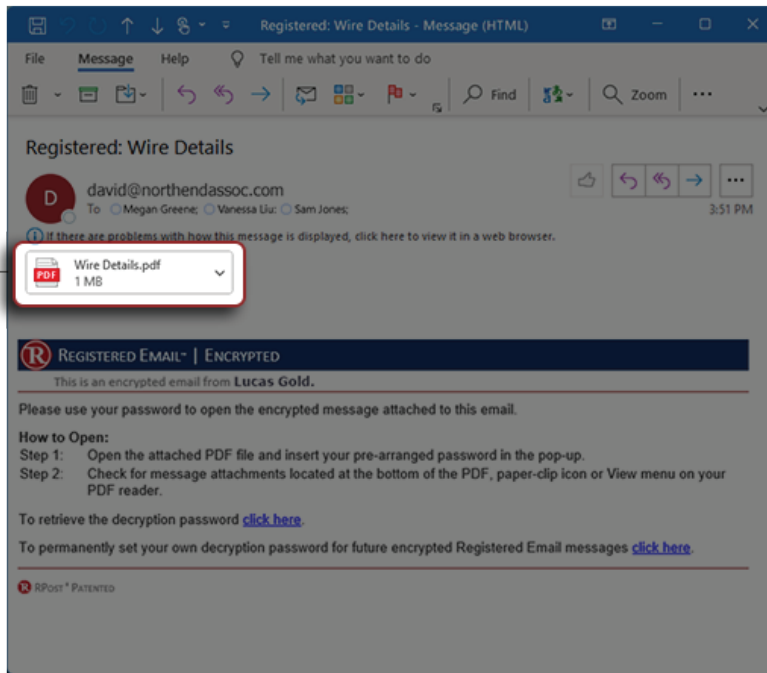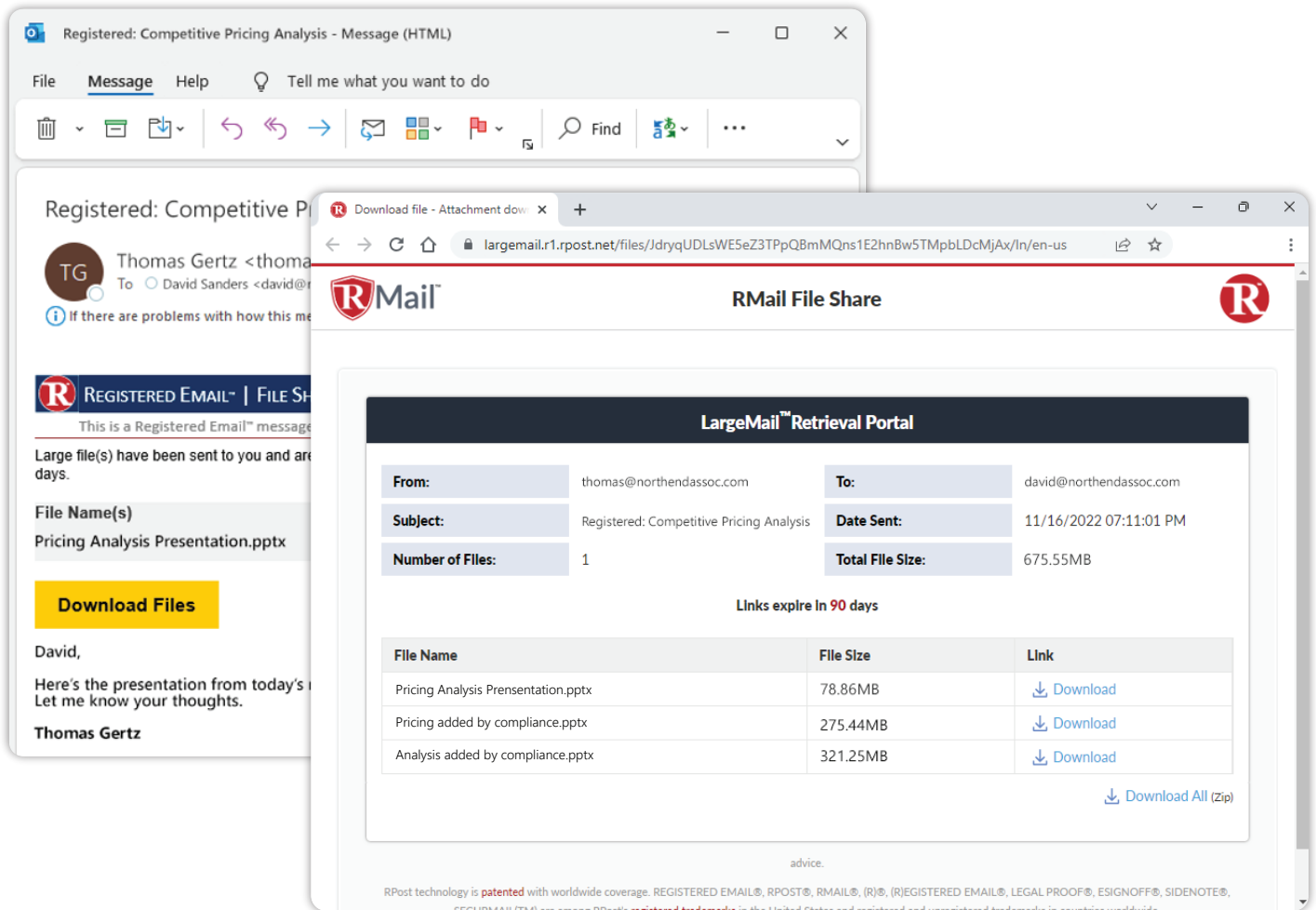

Message Level Encryption

RMail dynamic encryption engine detects whether the recipient's server is able to receive the email at the minimum sender-acceptable security level and, if not, automatically reverts to message level encryption, wrapping the email and any attachments inside an AES-256-bit encrypted PDF package, delivered into the recipient's inbox, with automated decryption password management.

Benefits:

- Message and attachments remain encrypted at rest in the recipient's inbox
- Familiar and easy PDF user experience for reader
- The email opens in any browser or PDF reader
- Digitally signed, integrity visible in the PDF reader
- Recipient can access the attachments in any browser with a simple click, or directly in their PDF reader

Secure Large File Share™ Send Up to 1GB from within Outlook

Senders can easily attach and track up to 1GB of files right from inside the Outlook compose window -- or any of the RMail web applications. Senders can send large files securely to any recipient with encryption and configurable self-purging options (from 1 to 90 days) through a secure web container that eliminates the risk of download recipients being able to see sender's cloud storage file structure.

Plus, files auto-purge after 1 to 90 days (configurable) and can be killed early at any time by the sender. No files linger on the Internet – pure compliance bliss.

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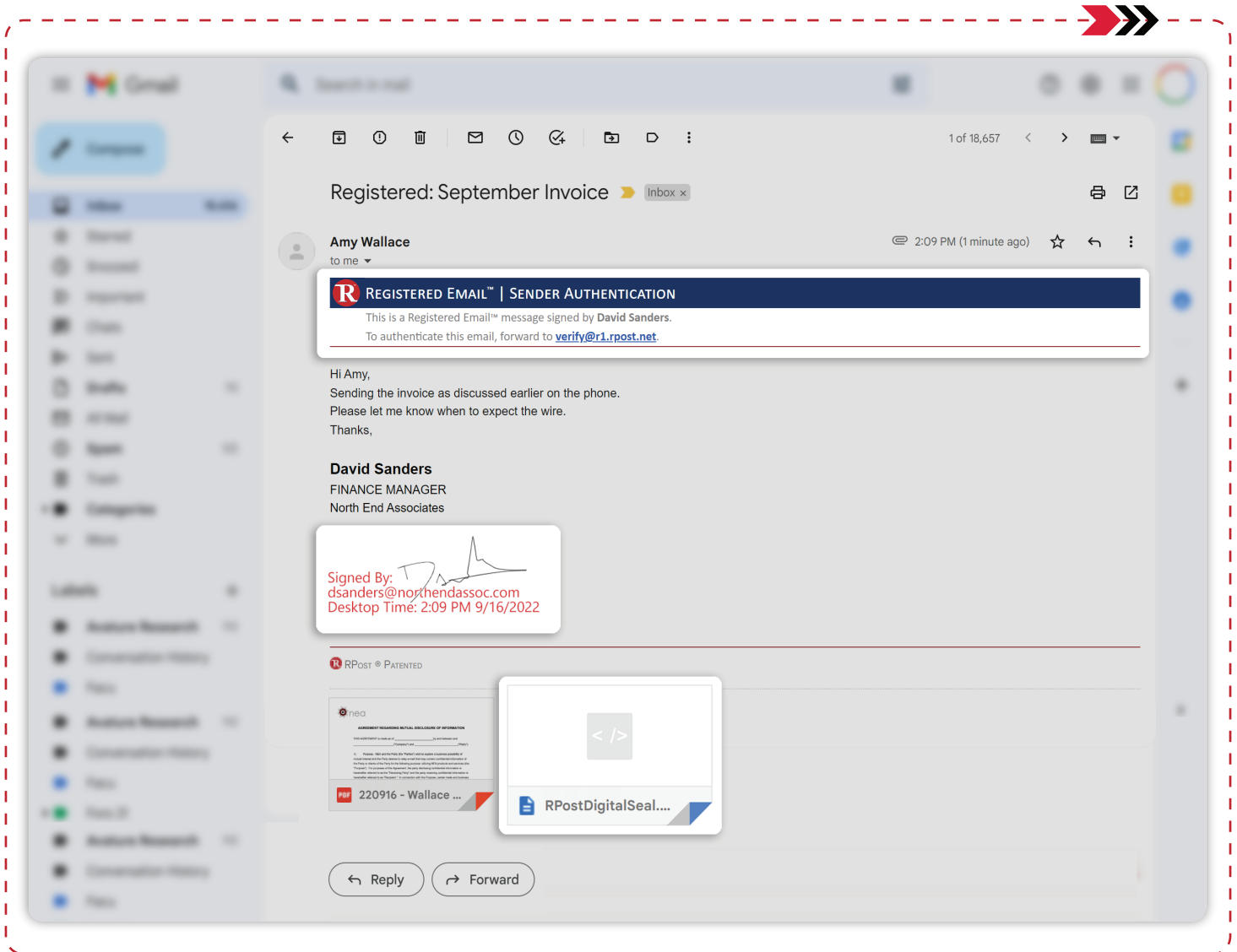
RMail Digital Seal® authentication makes it easy for a recipient to verify origin and authorship of an email (for example, an email carrying an invoice) and re-create a copy of the original message content instantly. This empowers the recipient of the invoice to verify authenticity of payment information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

Redact+ Protect-the-Thread™ With In-the-Message DLP
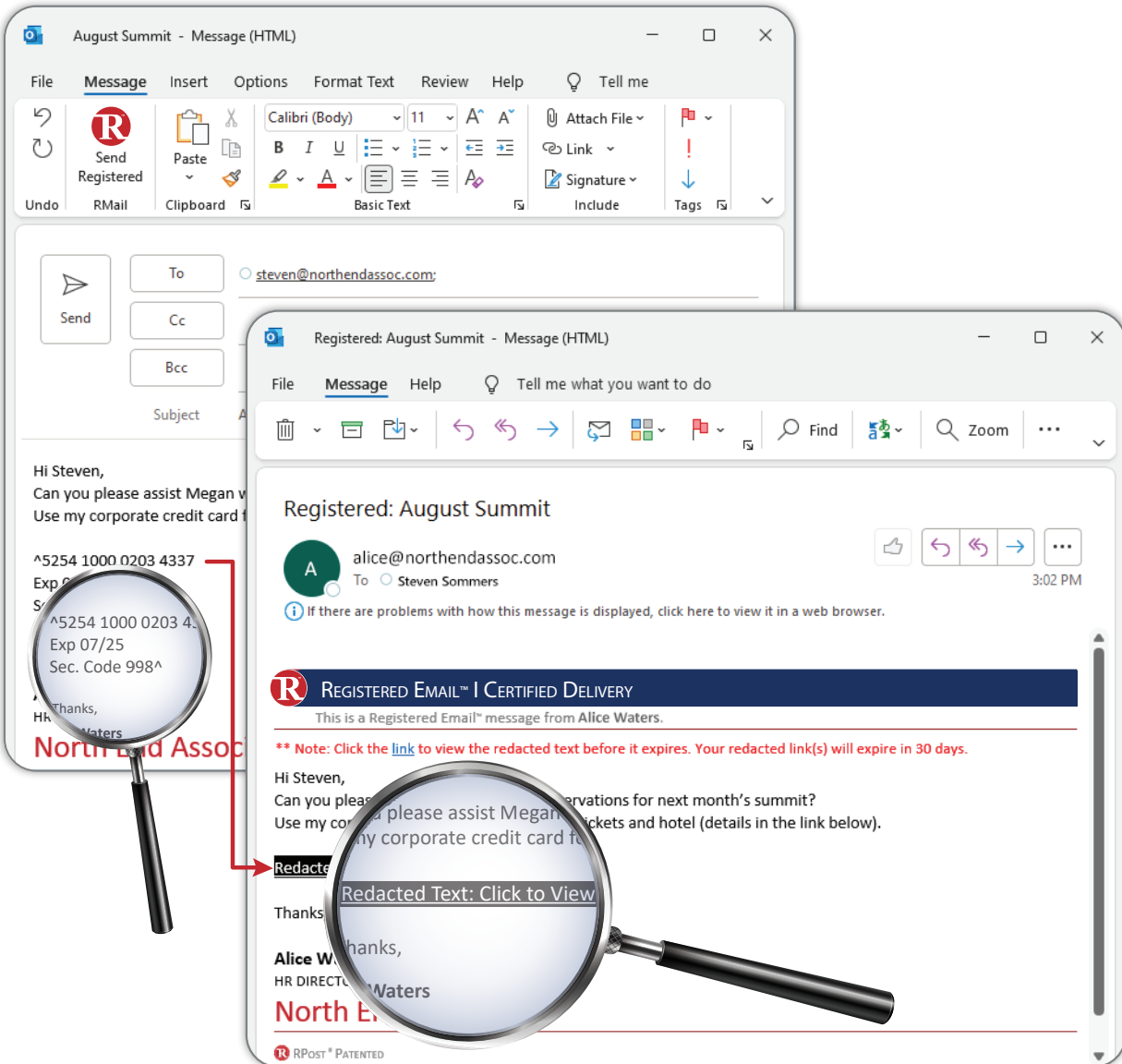
Senders are now empowered to ensure that certain content of an email – like payment details, negotiated terms, or other sensitive content – is redacted from the message body. It protects the sender by automatically cleansing the email thread of sensitive content while at the recipient regardless of how a recipient replies or who they forward the message to.

RMail™ By RPOST

Double Blind Cc™ & Private SideNote®

AS SENT
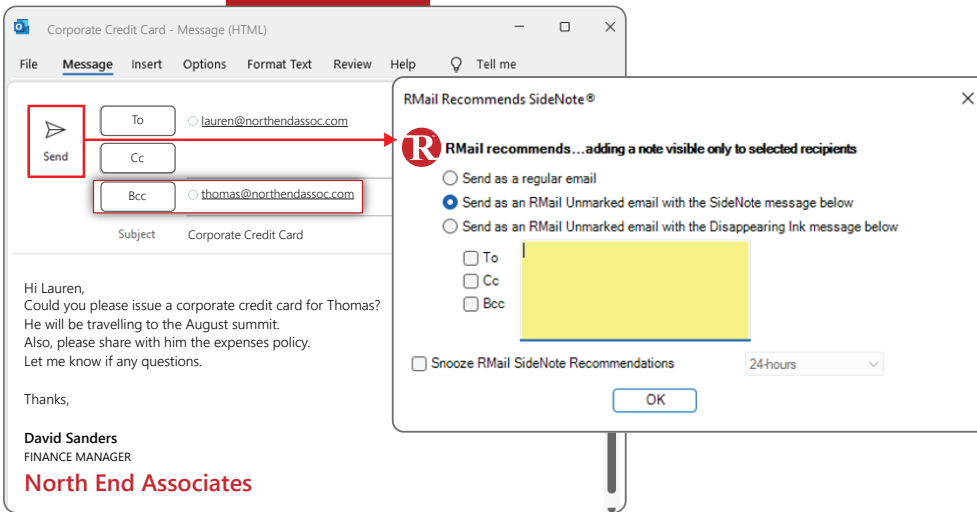
In the normal process of sending an email, RMail AI detects whether it may be useful for senders to add contextual SideNote® message visible only to selected recipients. When used in combination with Disappearing Ink™, that note can be set to disappear after read, without any trace.

AS RECEIVED

Senders can redact addresses in the To/Cc fields, such that recipients in Bcc can see who was copied but cannot inadvertently <u>reply to all</u>, exposing that they were blind copied.
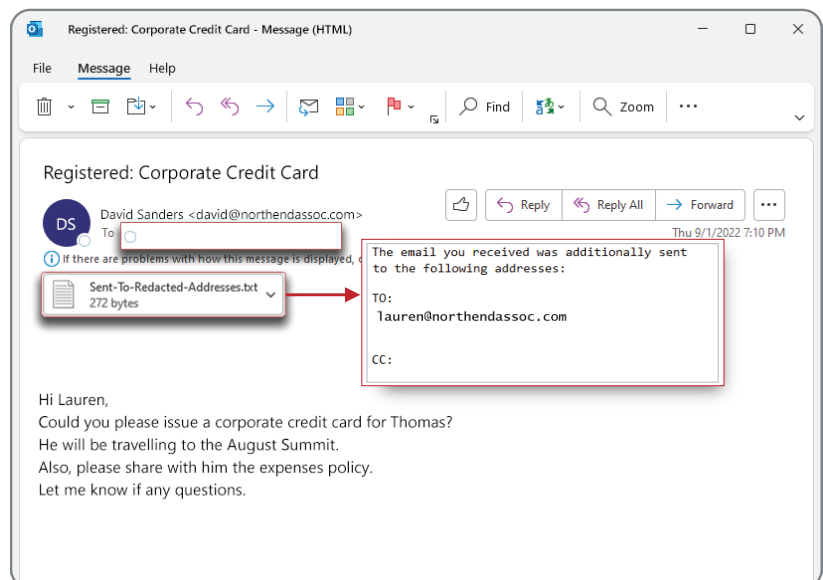
Email Eavesdropping™ Alerts for Wire-Fraud Pre-Emption

Email Activity Report

Email Eavesdropping™ Alert

Original Recipient: David.Smith@northwestinsurance.com

Security:	Red
Opens:	3
Locations:	2

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

Email Age: 15 days 1 hour 4 minutes

Risk Details: All Activities

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: A4BD52B62EE9862A5FDDB8F336A99E2D69FEF54A

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/LGy25hw0Z65CNLyOLYzCLCuMKdk95gm4vir26bBCM-Dlx.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.

If the RMail **active threat hunting** technology identifies unusual activity patterns, RMail generates an Email Eavesdropping™ instant alert, and notifies in real-time IT admins (and optionally senders) with forensic details.

BEC lures start with cybercriminals targeting their victims by eavesdropping on email from sender to recipient, to siphon off email, analyze it, copy it with slight modifications (e.g., payment instructions), and then pivot replies so they route in a loop back to the cybercriminal.

With Email Eavesdropping™ alerts, every email sent out of the organization has every activity associated with it analyzed forensically, for a period of time. 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.**

RMail By **RPost**

Email Security

Security Breach Locator™ Report

REGISTERED ENCRYPTION™
CERTIFICATE EVIDENCING END-TO-END SECURITY

RMail

This privacy certificate provides proof of the privacy status of the associated email, from the original sender through to each recipient. Together with the Registered Receipt™ it is attached to, a user may authenticate the data in this certificate along with the original message content and all of the delivery history and timestamp details. To authenticate the information in this certificate, follow the instructions on the associated receipt. Patented and Pending US 16866135.

Message Envelope

Message ID:	C8737FB9CF1519A2053C44E0056FDF5C39DDB645
From:	MelanieJames <mjames@newinsurance.com>
Subject:	Policy Updates
To:	<wanda.mcgrath@holdingsusa.net> <jonathan.ogden@holdingsusa.net> <richard.clark@associatesolutions.net>
Cc:	
Bcc:	-
Received by RMail System:	05/26/2022 07:39:38 PM (UTC)
Client Code:	-

Outbound Details: Sender to RMail Cloud / Inbound Details: RMail Cloud to Recipient

Outbound Details: Sender to RMail Cloud		Security Details				Inbound Details: RMail Cloud to Recipient		Security Details			
Original Sender	Internet Hop ID	Message Level	Transmission	Time Inducted	Encryption Status	End Recipient		Message Level	Transmission	Time Received	Encryption Status
mjames@newinsurance.com	smtp13.relay.iad3a.emailsrvr.com (Authenticated sender: mjames-AT-newinsurance.com)	RSA-AES256	TLSv1.2*	05/26/2022 07:39:34 PM (UTC)	Best+	wanda.mcgrath@holdingsusa.net			TLSv1.2	05/26/2022 07:39:38 PM (UTC)	Best
mjames@newinsurance.com	smtp13.relay.iad3a.emailsrvr.com (Authenticated sender: mjames-AT-newinsurance.com)	RSA-AES256	TLSv1.2*	05/26/2022 07:39:34 PM (UTC)	Best+	jonathan.ogden@holdingsusa.net			TLSv1.1	05/26/2022 07:39:38 PM (UTC)	Acceptable
mjames@newinsurance.com	smtp13.relay.iad3a.emailsrvr.com (Authenticated sender: mjames-AT-newinsurance.com)	RSA-AES256	TLSv1.2*	05/26/2022 07:39:34 PM (UTC)	Best+	richard.clark@associatesolutions.net		PDF-AES256	TLSv1.0	05/26/2022 07:39:38 PM (UTC)	Best+

End-to-End Security Summary

Original Sender	Original Recipient	Overall Encryption Status	Status Description
mjames@newinsurance.com	wanda.mcgrath@holdingsusa.net	★★★★☆	Best encryption from sender device, best to recipient gateway
mjames@newinsurance.com	jonathan.ogden@holdinsusa.net	★★★☆☆	Best encryption from sender device, acceptable to recipient.
mjames@newinsurance.com	richard.clark@associatesolutions.net	★★★★★	Best encryption from sender device, best+ to recipient.

For more information about RMail® services, visit www.rmail.com.

An RPost® Technology

If an email is identified as being eavesdropped on, the Registered Encryption™ report identifies the most likely security gaps; **and/or provides audit-ready proof that the security gap must have been after the recipient forwarded the message onward --- and not a fault of the sender.**

The security forensics provided by RMail are fact, and allow IT admins to easily justify and demonstrate their hypothesis about where cybercriminals may have accessed an email in the path from sender to recipient, even if the breach occurred at the recipient's end.
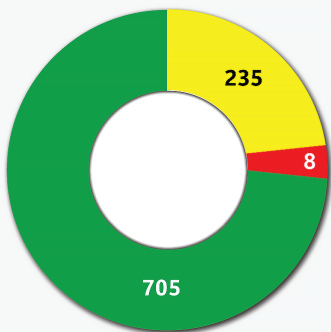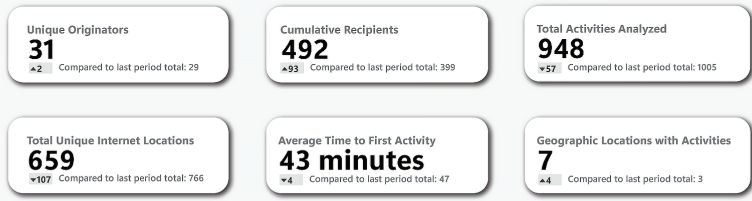
Aggregate Eavesdropping Heartbeat™ Monitor

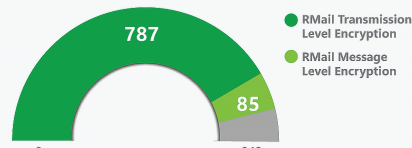## AGGREGATE EAVESDROPPING HEARTBEAT™ MONITOR

Date: 11-01-2022
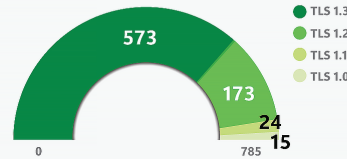
Sender Domains: northendassoc.com, northendassoc.co.uk

Red Alerts: 8

Unique Originators	Cumulative Recipients	Total Activities Analyzed
31	**492**	**948**
▲2 Compared to last period total: 29	▲93 Compared to last period total: 399	▼57 Compared to last period total: 1005

Total Unique Internet Locations	Average Time to First Activity	Geographic Locations with Activities
659	**43 minutes**	**7**
▼107 Compared to last period total: 766	▼4 Compared to last period total: 47	▲4 Compared to last period total: 3

Activities by Risk Level

235
8
705

Encrypted Emails by Unique Recipients

787
85
0   948

- 🟢 RMail Transmission Level Encryption
- 🟢 RMail Message Level Encryption

Transmission Encryption Security Report

573
173
24
15
0   785

- 🟢 TLS 1.3
- 🟢 TLS 1.2
- 🟢 TLS 1.1
- 🟢 TLS 1.0

132
8
705
103
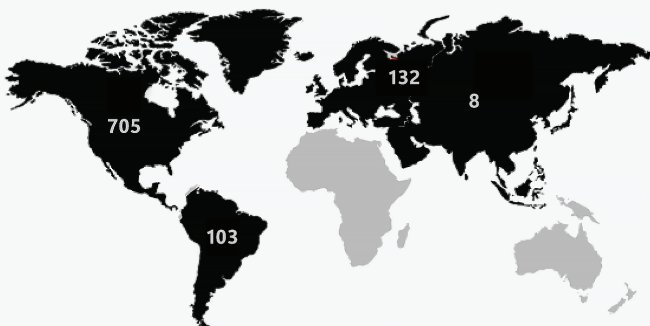
Unique Activities per Region

The Aggregate Eavesdropping Heartbeat™ Monitor offers a daily snapshot of eavesdropping risks for MSPs or IT admins. This aggregate report provides peace of mind by forensically monitoring the journey of all outbound messages to the recipient and beyond.

IT Admins or MSPs can swiftly investigate further if they see any high alerts or unusual activity across all users, all domains, and all companies that they manage or monitor security for.

RMail By RPost

RMail Outbound Security Cloud

In-the-Inbox Integrated Security
- Sender Auto-Training & Security Recommendations
- In-the-Inbox DLP
- Lookalike Domain™ Detection
- Reply Hijack™ Detection

Secure Web Portal Send Option for Recipients

SENDER

Desktop Apps

Mobile Apps

CRM/ERP

ADMIN

NORMAL ROUTE

FILTER

HIGH VALUE ROUTE

RMail AI Brain

Encrypted Reply & Secure File Share Reply
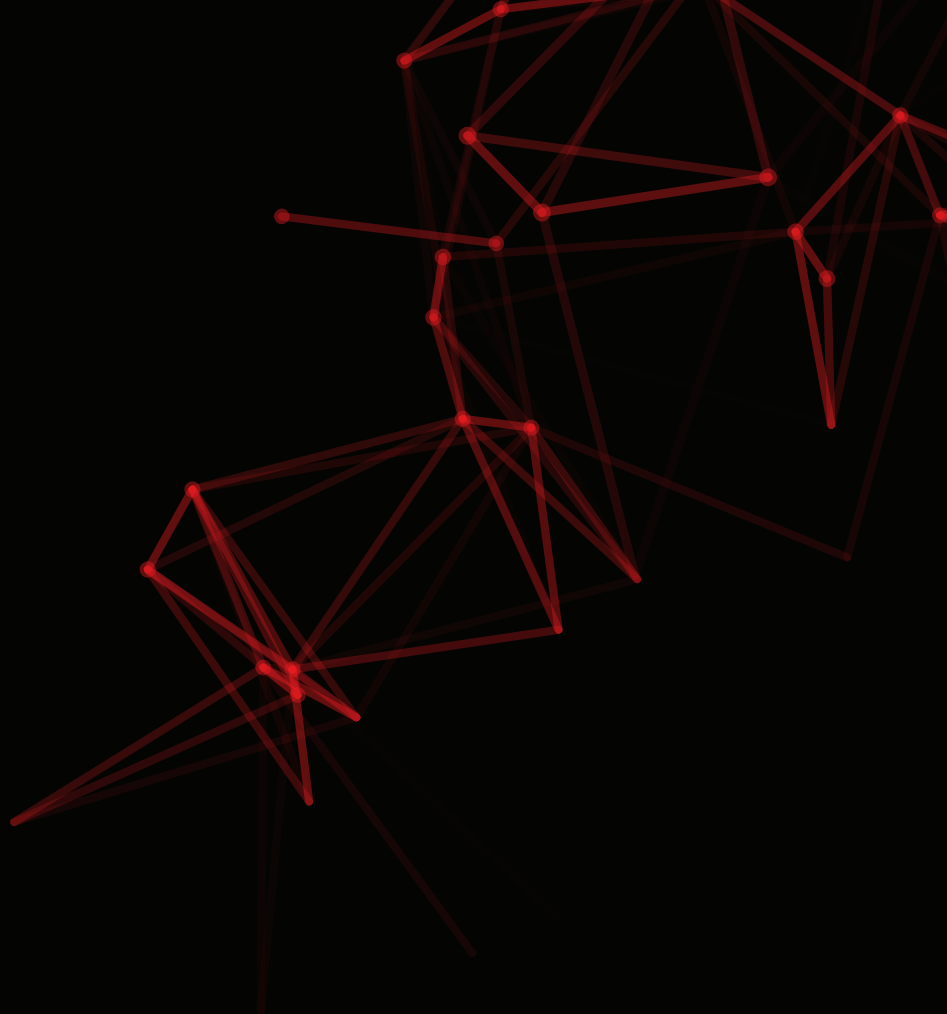
MESSAGE TRANSFORMATION FOR RECIPIENT

INTERNET FORENSICS

INTERNET DATA

RECIPIENT

Outbound DLP Email Security
- Email Encryption Automation
- Email Eavesdropping Detection
- Email Tracking & Certification

ENTERPRISE SECURITY INTELLIGENCE

EVIDENCE TO SENDER

- Email Eavesdropping™ Sender Alerts
- Active Tracker™ Email Journey Report
- Registered Receipt™ Certified Proof
- Email Open & Timestamp Tracking

SMARTR™ Encryption
Dynamic Transmission and Message Level Encryption

Digital Seal®
Email Authorship Verification

Protect-the-Thread™
Reply Content Redaction

Disappearing Ink™
Self-Purging Content

MSP & IT ADMIN INSIGHTS/ALERTS

- Email Eavesdropping™ Admin Alerts
- Security Breach Locator Report
- Aggregate Eavesdropping Heartbeat™ Monitor
- Custom Security Analytics

Perfect Harmony, Enhance the Outbound
Keep your existing inbound email security – and even your outbound DLP if you so choose. Add RMail outbound security gateway, in-the-inbox integrated cloud email security, and in-the-ether e-security content controls: all, some or one. RMail harmoniously extends your existing email security systems, adding elegantly-easy encryption user experiences, unique BEC targeted attack detection, and more, with AI DLP automation.