



PRE-Crime™ Targeted Attack Defense

Preemptive defense against the most sophisticated Business Email Compromise (BEC) wire fraud attacks targeting you, your suppliers and clients.

RMail.com

Contents

Why PRE-Crime™ security?	3
What Are Business Email Compromise (BEC) Attacks?	5
Threat Vectors.....	5
Targeted Attack Defense	8
Outbound Email Security	8
In-the-Inbox Inbound Email Security	9
Anatomy of Targeted Attack-in-Progress	10
Threat Categories and Consequence	10
Living a Sophisticated Targeted BEC Attack.....	10
PRE-Crime™ Defense Meets Your E-Security Stack	12
Outbound Email Security	13
Registered Encryption™	13
Email Eavesdropping™ Account Compromise Alerts	16
Aggregate Eavesdropping™ Heartbeat Monitor	17
Digital Seal® Email Origin and Authorship Verification for Recipient	18
Inbound Email Security	19
Right Recipient™ Lookalike Domain™ Alert.....	19
Right Recipient™ Reply Hijack™ Detector.....	20
Fake Forward™ Detector	20
Conclusion.....	21
RPost is About Continuous Innovation	21
Appendix: Technology Spotlights.....	23
Email Eavesdropping™ Alerts.....	23
Right Recipient™ email Lookalike Domain™ Alerts	25
Enabling RMail Services	26
Microsoft Outlook 365.....	26
Security Gateway, Gmail, Salesforce and other apps	27
Eavesdropping Heartbeat Service	27

Overview: Why PRE-Crime™ security?

Cybercrimes often referred to as Business Email Compromise (BEC), Email Account Compromise (EAC), Client Account Compromise (CAC), often leading to wire fraud, are one of the most financially damaging vectors of cybercrime. These sophisticated, socially engineered scams target businesses conducting legitimate fund transfers, aiming at diverting payment to fraudulent bank accounts.

According to the FBI, between July 2019 and December 2021, there was a 65% increase in global exposed losses (meaning the monetary loss including both actual and attempted loss) in the US attributed to BEC attacks, resulting in more than 2 billion US dollars being irrecoverably mis-wired annually in recent years. Following this alarming statistic, the 2023 report highlights another 17% increase in global exposed losses from 2021 to 2022. From October 2013 to December 2022, there have been 277,918 domestic and international *reported* incidents (many go unreported to the FBI), with an exposed dollar loss of approximately \$50.87 billion. This includes both U.S. and non-U.S. victims. With today's work-from-home environment, where more workplaces across all industries and nations are forced to conduct routine business virtually overnight, this trend is, unfortunately, only expected to grow.

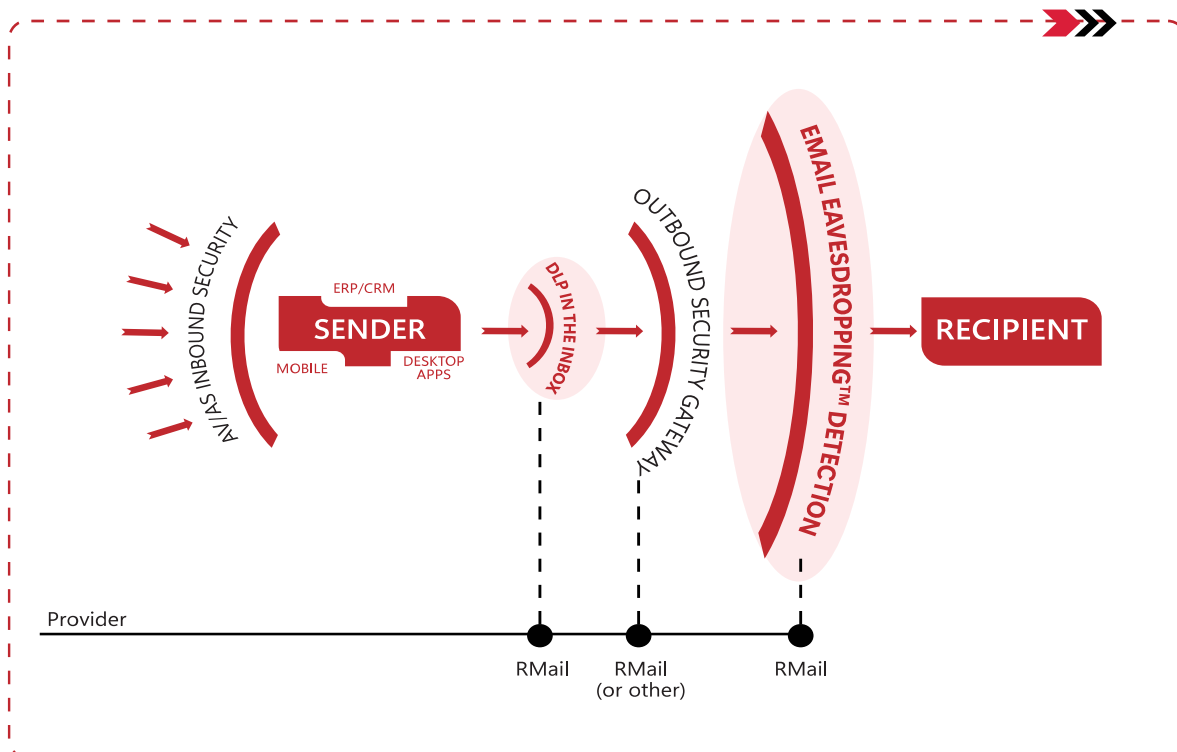


Fig 1: RMail Secure Email Services harmoniously extend your email security stack.

While recent years have witnessed the emergence of cybersecurity solutions that help protect companies from miswiring their own funds, companies remain exposed to scenarios where it's their clients falling for these scams - more often than not resulting in damaged business relationships, delayed payments, or even litigation to determine who was responsible for the vulnerability that led to the attack in the first place.

RMail, RPost's comprehensive email security suite, now includes its newest innovation, its PRE-Crime™ targeted attack defense cybersecurity services. Now, any RMail user or their administrators have visibility into whether the latest cyber trickery is currently in progress **not only within their environment, but also at the recipient of their business email.**

Well known for its Registered Email™ and Registered Encryption™ features that mitigate risk by providing proof of who said what when, or audit-ready proof of fact of privacy compliance, RMail AI has and continues to evolve, and now includes more than e-security risk mitigation; enter PRE-Crime™ detection. Put more simply, this means stopping the e-crime after the hook is in, but before the steal (crime) completes.

***Fun Fact:** RMail's PRE-Crime™ targeted attack defense for email, is similar to "Precrime" futuristic policing; infamous from Philip Dick's 1956 sci-fi short story, "The Minority Report" and the 2002 Tom Cruise movie based on it. Precrime, in science fiction, is the name of a future police agency tasked with identifying people who will commit crimes in the very near future.*

RMail's elegantly easy email encryption services provide a foundation of email security – for risk management and compliance. PRE-Crime™ security is different. It has components designed to alert the sender and their administrator of a potential e-crime in progress, before it is too late; whether that cyber trickery is happening inside the sender's organization or if their recipient's email account is being eavesdropped on.

These services generally aim to thwart cybercriminal man-in-the-middle email interception, recipient email account compromise, business email compromise, spear-phishing and phishing using impostor names and email addresses of known colleagues --- including the most sophisticated versions operated by organized cybercrime syndicates.

While encrypting email is a central protector to minimize overall risk; and using RMail's message level encryption which can be configured to remain encrypted inside the recipient inbox, can protect certain content from becoming attractive to cybercriminals, these PRE-Crime™ services focus thwarting attacks after the criminal has identified its targets and has begun to act.

This technology paper discusses RMail email security services that focus on defense against cybercriminal targeted attacks often referred to as **Business Email Compromise (BEC)**. Within this category, cybercriminal tactics include **Phishing, Spear-phishing, and Whaling**, as well as **Email Account Compromise, Supplier Account Compromise** and **Client Account Compromise**. The result, if cybercriminals are successful, is referred to as **Wire Fraud**.

What Are Business Email Compromise (BEC) Attacks?

Business Email Compromise (BEC) attacks are a specific type of “phishing” attack that relies on targeting specific people within organizations. Attackers seek monetary payment as a direct outcome, and types of BEC attacks include (but are not limited to) diverting payment on a valid invoice to a fraudulent bank account, submitting a fake invoice for payment, diverting employee payroll to a fraudulent bank account, and using impersonation of senior executives to lend credibility to plausible but irregular requests. A report by Osterman Research predicts that threat actors are likely to step up the frequency and cost of BEC attacks in the coming year, and they note that employees at all levels of an organization are targeted by BEC attacks.

BEC attacks are among the fastest growing and most concerning cybercrimes against organizations and, according to the Osterman Research report, “many organizations are ill-prepared to address the threat of BEC and lack sufficient protections across people, process, and technology factors.” Also cited in the report is a startling finding that 80% of organizations have experienced BEC attacks over the last year.

Threat Vectors

While most e-security threats begin with email, the marketplace boasts a broad scope of services that are designed to mitigate risk and thwart cybercriminal activities in action.

RMail specializes in email security, while also offering a unique approach to specific threat vectors.

- **Prevention:** Email encryption is a mainstay of the many RMail services and has traditionally been one of the methods to prevent cybercriminal activities from gaining a foothold within an organization or within a business transaction. Unique to **RMail Encryption** is its AI automation to determine the best method of delivery to each recipient based on security concerns, privacy compliance, and need for recipient simplicity. However, with some of the newest cybercriminal tactics of eavesdropping on email accounts, after the email has been securely delivered while sitting in the recipient’s inbox, email encryption alone may simply not be enough today.
- **Defense:** Once a cybercriminal sets their sights on a target, whether that target is within your organization or part of a transaction as an external party associated with your organization, it’s time for defensive technology that can diffuse the crime-in-progress before there is a loss. This is the focus of RMail’s **PRE-Crime™** targeted attack defense service, with its centerpiece patented and patent pending **Email Eavesdropping™** and **Right Recipient™** email **Lookalike Domain™** detection.
- **Compliance:** Further to risk mitigation, for those regulated industries or communications that require a level of privacy to protect consumer information, **Registered Email™** encryption returns a **Registered Receipt™** email record (available stand-alone or part of RMail), that can provide proof of fact of content delivered, and proof as to whether or not that content was

delivered encrypted end-to-end. This proof of encrypted delivery becomes an audit-ready record in case of any claim of a breach or any privacy compliance audit.

This paper focuses on RMail as a defensive technology. RMail's PRE-Crime™ intelligence provides email vector **targeted attack defense**. And, with specialty in addressing today's most sophisticated organized cybercriminal gang tactics.

The FBI refers to this category of targeted attack as **Business Email Compromise (BEC)** induced **wire fraud**. It often includes an Email Account Compromise, at the sender or recipient side (mail client or server-level) and focuses on targeting those individuals within companies that are involved in some manner of business transaction or tangentially, the process of sending payments (purchases or escrow, invoice payments, payroll payments, or otherwise).

Email Compromise Attacks Targeting Businesses: These attacks often involve targeting suppliers sending invoices to customers and tricking the customer into paying the invoice to the cybercriminal account without the supplier's awareness. This approach can be termed, Supplier Account Compromise (if the supplier's email account or email stream is actively being eavesdropped on), or Client Account Compromise (if the client, the payor's account, or email stream is actively being eavesdropped on).

These tactics have proven successful; over the last few years cybercriminals have enjoyed a lottery windfall of success. The FBI reports \$2.4 billion has been mis-wired to cybercriminals last year alone. These mis-wires are referred to as Wire Fraud crimes but uniquely in most situations the criminal is not accessing the bank account of the wire transmitter, they are tricking the wire transmitter into sending funds to the wrong person (to the cybercriminal posing as a legitimate party to the transaction).

Email Compromise Attacks Targeting Individuals: These attacks often involve cybercriminals targeting those who they have determined are more likely to direct money (for investments or major purchases such as real estate or homes) and eavesdrop on the individual's email account. The cybercriminal patiently waits for a transaction to be in progress, and at the right time, begins trickery aimed at causing the individual or an escrow or other business advisor, to mis-wire money and direct it to the cybercriminal's account accidentally.

What makes these types of attacks challenging to detect and thwart, is that they often involve security breaches outside of the firewall of the company that may employ all the e-security technology, training, and best practices. They use legitimate email accounts to successfully bypass email security filters and leverage AI to prepare emails that are not only grammatically correct and well written, but also mimic the writing style of the impersonated sender. For these and other reasons, companies (and individuals) need to employ unique technical approaches in addition to their standard email security gateway, filter, firewall and encryption technologies.

Enter RMail's PRE-Crime™ Targeted Attack Defense.

While RMail has a broad range of email security services, it specializes in its unique approach to what is transpiring with important email, inbound-in-the-inbox, outbound-to-the-recipient, and even at the recipient. Furthermore, RMail AI can instantly auto-lock any transaction (whether that be access to a shared file or an eSign request, and more) if it detects a risk of eavesdropping or any hazardous activity. This way, RMail provides an added layer of protection and peace of mind around sensitive content like invoices, patient records, Real Estate closing information, and more, and can even record court-admissible forensic evidence that although a file might have been leaked, the content was not accessed, meaning that the content remains secure and therefore the scenario does not constitute a reportable breach.

While there are other secure email gateway services, most specialize on inbound protection from broad-based threats like virus-, spam-, and malware-ridden inbound email. RMail has partners that provide security in these areas alongside RMail products, for those customers in need. But, where RMail adds the most value is working in harmony with whatever a company currently has selected for these broad-based threats. RMail focuses on specialized needs related to targeted attacks, privacy compliance, or certified proof.

R1Meets More of E-Security Landscape E-Security en Vogue

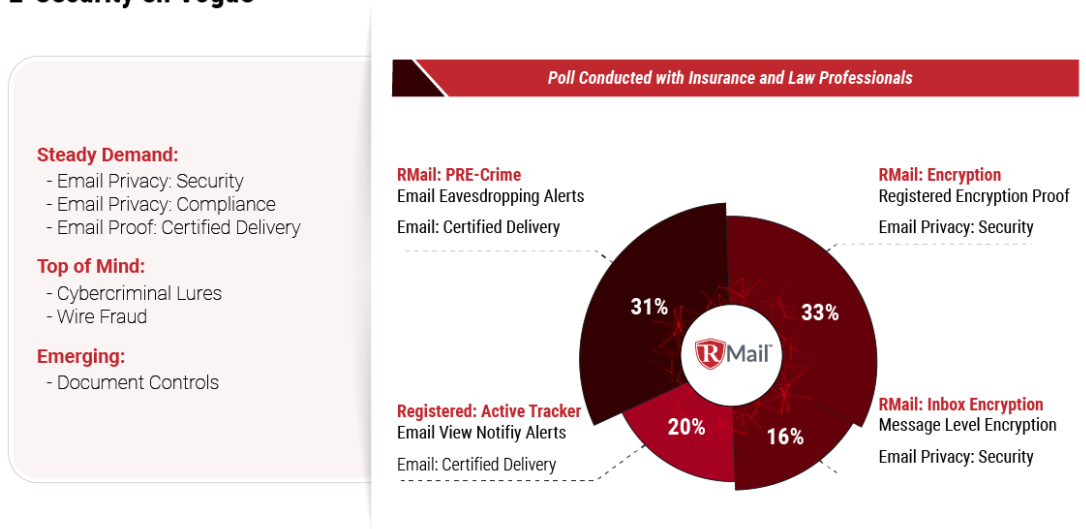


Fig 2: What's most interesting to you today?

614 business professionals responded to this RPost poll over the second half of 2022.

Services like RMail's Registered Email™ proof, Registered Encryption™ privacy proof, PRE-Crime™ targeted attack defense, Email Eavesdropping™ alerts, and Right Recipient Lookalike Domain™ alerts are

truly unique patented technologies. While the industry is laden with buzzwords, with confidence, you can count on RMail services to have taken a unique approach that where other security software and secure email gateway services do not.

Targeted Attack Defense

A PRE-Crime™ detection scenario is stopping the crime after the cybercriminal has (a) identified who to target in the sender's company and what normal recipient domain to fake; (b) purchased a lookalike domain of that normal recipient; and finally, (c) sent a fake email from the lookalike domain to the target in the original sender's company aiming at diverting payment to a fraudulent bank account. RPost's PRE-Crime™ technology is designed to swoop in and stop this with specific alerts and awareness after the hook is in, before the steal.

RMail's PRE-Crime™ service covers both **inbound and outbound** protection, with its main components being as follows.

Outbound Email Security

1. Registered Encryption™ privacy. For email encryption to add value, it must be used --- and easy to use --- for all important email leading up to a transaction. Other email security gateway or email privacy/encryption providers do not dynamically adapt the method of encrypted delivery based on type of message, risk, or recipient, and further, do not return insights or proof of fact of encrypted delivery.

RMail does.

2. Email Eavesdropping™ account compromise alerts. The most successful cybercriminals, with regards to Business Email Compromise wire fraud attacks, target their victims by eavesdropping on email from sender to recipient, to siphon off email, analyze it, copy it with slight modifications related to payment instructions, and then pivot replies so the route in a loop back to the cybercriminal rather than the original sender. If the sender organization has an email security gateway, it may flag certain inbound email threats, or even prevent traditional outbound data leaks, but it certainly does not identify email security breaches after an email has left its environment or when the email is at the recipient. **RMail does.**

3. Digital Seal® email origin and authorship verification for recipient for invoices and more. When delivering messages like invoices that are susceptible to be the type of messages a "man-in-the-middle" may try to intercept, alter, and continue the delivery, or send a near replica follow-up email, the RMail Digital Seal® impostor defense makes it easy for a recipient to verify origin and authorship of an email (for example, an email with an invoice attached). Other attempts at sender authentication for the recipient, like PKI cryptographically digitally signing, and pre-authenticated DKIM messages, can break when a recipient forwards an email onward to others. RMail Digital Seal® technology is durable and verifiable even if forwarded.

In-the-Inbox Inbound Email Security

4. Right Recipient™ Lookalike Domain™ Detector. If on the receiving side of an email that was intercepted at the sender --- for example, an invoice or other payment request --- and the sender, or supplier email account has been compromised, the email en route to you the recipient may have been sent to you with from a sender address with a domain that looks just like the familiar email address and domain of your longtime supplier or client. RMail's Lookalike Domain™ alert; running within the Microsoft Outlook email program, identifies this type of trickery in action.

5. Right Recipient™ Reply Hijack™ Alert. Sophisticated internet criminals may place the newly created lookalike email domain within the hidden-to-recipient "reply-to" header of the message that they send to the target recipient. RMail's Reply-Hijack™ alert; running within the Microsoft Outlook email program catches these reply-to pivots before your reply routes to the cybercriminal.

6. Fake Forward™ email detector. Following on the Reply-Hijack, if someone in your organization forwards the impostor email, depending on how the email was sent and composed, once forwarded, one cannot tell that the email came from an impostor of the sender, and the content of the email gains a sense of legitimacy – since forwarded from a source known to the new (forwarded to) recipient. RMail will detect and alert that a fake email that was part of a Reply-Hijack reply-to pivot scheme is about to be forwarded, unknowingly creating a sense of legitimacy to the impostor email content.

RMail's PRE-Crime™ e-security services run invisibly in the background of one's email program (e.g., Microsoft Outlook, Gmail, or any email security gateway) and comes to life to alert staff when a potential cybercrime targeting a staff member OR external client has been initiated but before it concludes. This RMail technology includes real-time notifications if a recipient's email is being eavesdropped on, user alerts to stop your staff from replying to a potential lookalike email address, and more.

These crimes most often lure companies into sending money to the cybercriminals through trickery or as a ransomware bounty.

"Today's email security needs to be humanized, and RPost's latest RMail e-security services that run inside Microsoft Outlook do just that. Their triple play with AI-triggered encryption and wire fraud protection, in-the-flow email security user training, and their suite of anti-whaling BEC protections (recipient verification, domain age, impostor alerts, Double Blind CC™, and Disappearing Ink™) add essential layers critical to not only protect externally facing business executives and their organizations but also those newfound [human] targets in HR and finance teams. Traditional email security plus RMail for Outlook is a winning combination," states Michael Sampson, Senior Analyst at Osterman Research, one of the world's leading e-security and messaging technology analysts.

Anatomy of Targeted Attack-in-Progress

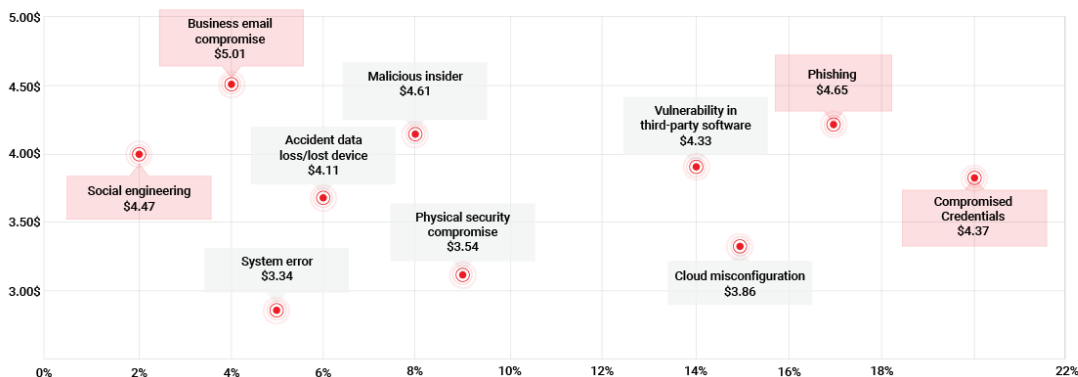
Threat Categories and Consequence

While there are many types of cybercrimes and cybercriminal lures these days, the main threat vectors that PRE-Crime™ services work to thwart are those social engineering attacks that involve compromised credentials or different forms of phishing and spyware that lead to email account compromise and, ultimately, business email compromise-induced wire fraud.

The more sophisticated organized cybercriminal gangs use all of these in the same attack --- and with lucrative benefits that often generate tens to hundreds of thousands of dollars per success. With this trend growing, one could consider this a cybercriminal pandemic in that the cybercriminals are well versed in many languages and are conducting these in all regions of the world.

Main Cybersecurity Threat Vectors

Trend: most frequent and damaging cyber attacks exploit the human factor. Therefore, cybersecurity needs to be humanized



IBM Security, Cost of a Data Breach Report 2021.

Living a Sophisticated Targeted BEC Attack

There are lazy cybercriminals that send sloppy phishing emails, and then organized crime rings that are quite sophisticated and put a team on the task once they get their hooks in. Here is a brief rundown of a sophisticated email crime in progress that could be foiled with the RMail PRE-Crime™ services.

1. You send an email to a client or recipient about a payment due to you (invoice, purchase order, etc.).
2. Your recipient's email account is being unknowingly eavesdropped on by a cybercriminal (using a discovered reused password and IMAP or POP protocol at their server, for example).

3. Within hours of your email going to your recipient, the cybercriminal copies that email content (often including PDF payment details for a wire or ACH) and changes only one thing—the account where the money is to be sent!

Note that these cybercriminals often have bank accounts at the same major banks that many of us use. So, if you usually have payments going to your Bank of America account, they will use that same bank, same routing number, but they will use their own account number.

4. This email will arrive in your recipient's inbox from what appears to be your email address (or it will come from a lookalike address – your name with a newly purchased domain one letter off from your domain), so the recipient only sees your original request and then a second one. To most people it would appear as if you sent the email twice, and the recipient usually opens the newer one, which is the one from the cybercriminal.

The email is configured so when the recipient replied, thinking it is coming to you, the reply actually routes the cybercriminal, and essentially your email thread back-and-forth with your recipient is hijacked. This is where there can be several or a week's worth of back-and-forth email between the cybercriminal (posing as you) and your recipient – without your knowledge! And just like that, you are cut out of the loop of your own originated transaction.

5. The cybercriminal then has someone follow-up by phone with your unwitting recipient stating that they are your assistant (or some other yarn), and they are following up to see when the invoice or purchase payment will be sent.

6. Your recipient sends the payment to the cybercriminal's bank account (thinking it was your account) and replies to the fake email address from the fake you with confirmation.

7. The cybercriminal immediately moves the funds from the bank to an offshore account. The money is now, for all intents, gone forever.

8. Meanwhile, a week or so later, the real you follows up to find out when payment will be made. The recipient replies that it was already sent, and then panic ensues when account numbers are found to be wrong, and the funds are gone.

The above scheme and its iterations have been so successful that the FBI recently reported more than \$2 billion of funds have been mis-wired and unrecoverable in the last year alone with similar amounts in the prior several years – and that is only what is reported to the FBI. Because all email schemes are done at scale, a cybercriminal can send out hundreds of these fake emails at a low cost needing only one of the messages to 'hit' to be a profitable enterprise.

If you had the RMail PRE-Crime™ services with Email Eavesdropping™ alerts on, you would know when your clients are being drawn into the above scheme before you are cut out of the loop!

For your clients, you should certainly recommend they install the RMail for Outlook with its Lookalike Domain™ detector – their use will protect you in that they will be alerted **before** replying to the cybercriminal posing as you. These would be able to protect funds from not being mis-sent.

Further, if you make it part of your standard procedures to send all your company invoices with RMail Digital Seal® email authentication technology, you then extend peace of mind beyond your organization to your entire network with the ability to authenticate the sender by a trusted third-party: RPost. Another suggested best practice is to send important messages (like invoices) with RMail Message Level Encryption, which wraps the email content and attachments inside a 256-bit password-protected PDF, and allows your recipient to set their own decryption password for all encrypted transactions with you. This way, you continue to minimize the chances that a nefarious party is able to successfully impersonate you.

Importantly, your email content and all attachments can be set to even remain encrypted inside the recipient's inbox. This protects you in case of a future breach at the recipient; your past content sent will not be exposed.

In summary, RMail is designed to enable your company (and your clients) to transact digitally with peace of mind, accelerating business securely in an era where pitfalls and uncertainty have unfortunately become the new normal.

With RMail PRE-Crime™ security features, (a) you will get alerts if an email to a client is being unknowingly read by a nefarious party. Put another way: if an email someone sends is being eavesdropped on due to an unknown security issue with the recipient's email account, you will be alerted. And (b) you and they (if they use RMail), will get alerts after they click SEND, before the message is sent, that they are about to correspond with a cybercriminal unknowingly, preventing the cybercrime **while** raising e-security awareness at the user level.

PRE-Crime™ Defense Meets Your E-Security Stack

Most IT security professionals have come to rely on – and for good reason, trust – their existing email security services and technology vendors. Most also realize that e-security requires a stacked security approach, multi-pronged, to deal with the variety of threat vectors and human factors.

While some cybersecurity software protects companies against some elements of BEC attacks where they would otherwise be at risk of miswiring funds, at best, this only means that these companies are protected against **50% of the risk scenarios**. The other 50% is comprised by the set of cyberattacks where it's the organization's clients' email accounts being compromised. In these cases where the organization is unknowingly cut out from an email thread with a client, and superseded by an impostor, inbound BEC protection is of no help. As a result, a client may end up paying a valid invoice to a fraudulent account, and the authentic organization would then need to initiate actions to demand their client to re-schedule the wire to the real bank account. RMail PRE-Crime™ services are specifically designed to protect organizations **and** their clients with 100% BEC and wire-fraud protection.

There is not any one provider that specializes in defending for all the threat areas. So, as an IT professional, you might ask, where does RMail PRE-Crime™ targeted attack defense fit within within your organization, without overlapping existing tools? Put another way, if one has the top-of-the-line email security gateway and all it has to offer, for what scenarios does RMail add value (and security)?

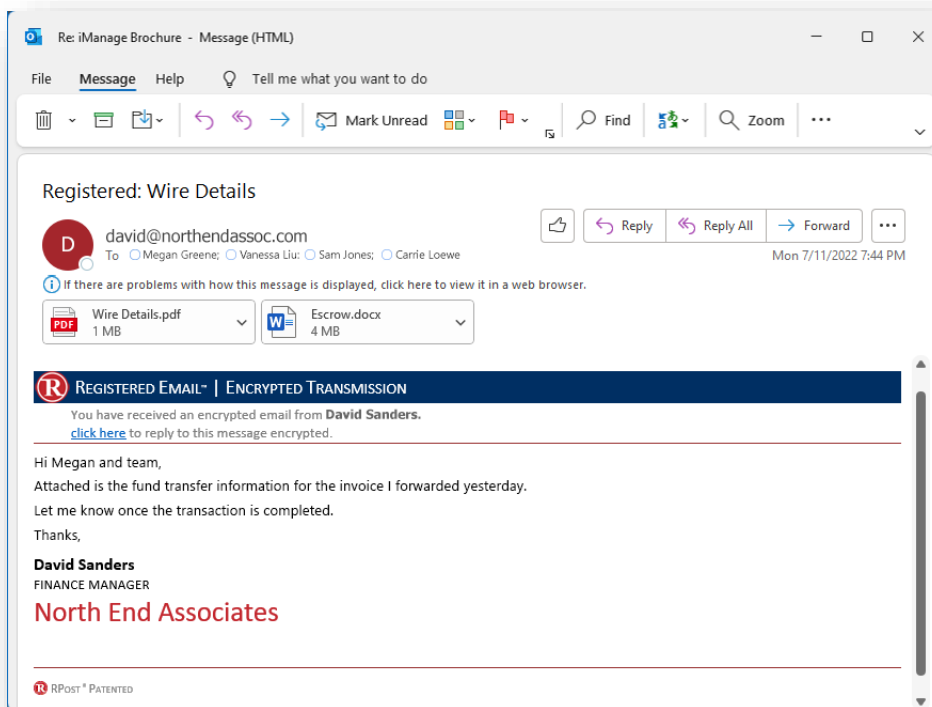
Outbound Email Security Registered Encryption™

For email encryption to add value, it must be used, and easy to use, for all important email leading up to a transaction (back-and-forth purchase order discussions, invoice delivery, transmission of funding instructions, payment confirmations, funding follow-up, etc.).

Ideally, the encryption service adapts to the type of message and risk of the transaction --- and the sophistication of the intended recipient.

Further, if there is a future breach of a recipient email account, ideally the encrypted message, while inside the recipient's inbox, remains private even to an inbox (cybercriminal) eavesdropper.

This is where RMail encryption excels; and regardless of your inbound email security gateway policies, you can easily, and harmoniously route all, select, or policy triggered outbound email via RMail email encryption.



It's return Registered Receipt™ proof record even adds proof of fact of end-to-end encryption for each message (for security peace-of-mind) and proof of privacy compliance for each message (for compliance audits).

REGISTERED ENCRYPTION™
CERTIFICATE EVIDENCING END-TO-END SECURITY

The 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 date 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 10895125

Message Overview

Message ID: C47F796C716184332CA46408B7F42C932844

From: mjames@newinsurance.com

Subject: Policy Update

To: wanda.mcgrath@holdingsusa.net; jonathan.ogden@holdingsusa.net; richard.clark@associatesolutions.net

Cc:

Outbound Details: Sender to RMail Cloud					Inbound Details: RMail Cloud to Recipient					
Original Sender	Internet Hop ID	Security Details		Time Inducted	Encryption Status	End Recipient	Security Details		Time Received	Encryption Status
		Message Level	Transmission				Message Level	Transmission		
mjames@newinsurance.com	smtp13.relay.iad3a.emailsrvr.com (Authenticated sender: mjames@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@holdingsusa.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

Wire Instructions - Message (HTML)

To: megan@northendassoc.com

Send

RMail Recommends Encryption

RMail recommends...ENCRYPTING this email

Send using the RMail Transmission Encryption feature

Send as a regular email

Send using a different RMail feature

Snooze RMail Transmission Encryption Recommendations 24-hours

OK

Hi Megan,
Attached are the...
Let me know once the transaction is completed.
Thanks,
David Sanders
FINANCE MANAGER
North End Associates

Other email security gateway or email privacy/encryption providers do not have the dynamic adaptation of the method of encrypted delivery based on type of message, risk, or recipient, and further, does not return insights or proof of fact of encrypted delivery. **RMail does.**

To tom@northendassoc.com
Sun 4/5/2020 9:40 PM

DeliveryReceipt.xml
17 KB

HtmlReceipt.htm
960 KB

REGISTERED RECEIPT

EVIDENCE OF DELIVERY, CONTENT & TIME

This receipt contains verifiable proof of your RPost transaction.
The holder of this receipt has proof of delivery, message and attachment content, and official time of sending and receipt. Depending on services selected, the holder also may have proof of encrypted transmission and/or electronic signature.

To authenticate this receipt, forward this email with its attachment to 'verify@r1.rpost.net'

Delivery Status					
Address	Status	Details	Delivered (UTC*)	Delivered (local)	Opened (local)
drlucasjones@outlook.com	Delivered and Opened	MUA+HTTP-IP:76.118.20.145	4/6/2020 2:40:19 AM (UTC)	4/5/2020 10:40:19 PM (-4.0)	4/5/2020 10:40:37 PM (-4.0)
bobdavisinsurance@gmail.com	Delivered and Opened	HTTP-IP:74.125.151.18	4/6/2020 2:40:20 AM (UTC)	4/5/2020 10:40:20 PM (-4.0)	4/5/2020 10:40:23 PM (-4.0)
alice@northendassoc.com	Delivered to Mail Server	relayed,mx-biz.mail.am0.yahoodns.net (67.195.228.75)	4/6/2020 2:40:22 AM (UTC)	4/5/2020 10:40:22 PM (-4.0)	
mark@northendassoc.com	Delivery Failed	5.1.2 (bad destination system: no such domain)	***	***	

*UTC represents Coordinated Universal Time: <https://www.rmail.com/resources/coordinated-universal-time/>

Message Envelope

From: tom@northendassoc.com <tom@northendassoc.com>

Subject: Insurance Policy Review

To: <drlucasjones@outlook.com> <bobdavisinsurance@gmail.com>

Cc: <alice@northendassoc.com> <mark@northendassoc.com>

Bcc:

Network ID: <0bfd01d60bbc\$b093ed10\$11bbc730\$@northendassoc.com>

Received by RMail System: 4/6/2020 2:40:18 AM (UTC)

Client Code:

Message Statistics

Tracking Number: F95542A9A2EEE4509C10C04569371335F2C815

Message Size: 638204

Features Used:

File Size (bytes): 460330 **File Name:** Insurance Policy Review.pdf

Delivery Audit Trail

4/6/2020 2:40:18 AM starting outlook.com/mta-tls in 4/6/2020 2:40:18 AM connecting from mta21.r1.rpost.net (0.0.0.0) to outlook.com.olc.protection.outlook.com (104.47.0.33) in 4/6/2020 2:40:18 AM connected from 192.168.10.11:54337 in 4/6/2020 2:40:18 AM >>> 220 HE1EUR01FT033.mail.protection.outlook.com Microsoft ESMTMP MAIL Service ready at Mon, 6 Apr 2020 02:40:18 +0000 in 4/6/2020 2:40:18 AM >>> EUIQ mta21.r1.rpost.net in 4/6/2020 2:40:18 AM >>> 250 HE1EUR01FT033.mail.protection.outlook.com Hello

Email Eavesdropping™ Account Compromise Alerts

The most successful cybercriminals, with regards to Business Email Compromise wire fraud attacks, target their victims by eavesdropping on email from sender to recipient, to siphon off email, analyze it, copy it with slight

modifications related to payment instructions, and then pivot replies so the route in a loop back to the cybercriminal rather than the original sender. For invoice delivery, for example, the supplier sends an invoice to the client. En route (supplier account compromise) or at the client (client account compromise), if the invoice-by-email delivery is being eavesdropped on, the RMail system will in-real-time, return a red alert to the sender and/or their administrator indicating which email to whom has been reviewed by an unauthorized third party (cybercriminal) in which location with a full forensic record of the cybercriminal internet record.

If the sender organization has an email security gateway, it may flag certain inbound email threats, or even prevent traditional outbound data leaks, but it certainly does not identify email security breaches after an email has left its environment or when the email is at the recipient. RMail does.

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

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

Risk Details: All Activities

Time (UTC)	Activity	Location	Country	Network Addr.	Network	Risk
09/15/2022 08:12:48	Open (VFW)	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: A48D52862EE9862AFDD88F336A99E2D69EF54A

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/LGy25hw0Z65CNlyOlyzCLCuMkdk95gm4vir26bBCMDix.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_ID: PORT443 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/S/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/LGy25hw0Z65CNlyOlyzCLCuMkdk95gm4vir26bBCMDix.gif 192.168.10.153 192.168.10.153 46808 GET /open/images/LGy25hw0Z65CNlyOlyzCLCuMkdk95gm4vir26bBCMDix.gif open.r1.rpost.net 443 1 HTTP/1.1 Microsoft-InternetExplorer/8.0 /open/images/LGy25hw0Z65CNlyOlyzCLCuMkdk95gm4vir26bBCMDix.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 17883425, 63201857, 633966165, 633966161 and other applications.

(M) = activity determined to be on a mobile device.
(N) = content delivery network delivered email data to viewer via webmail client.
(V) = activity was detected at an anonymizing VPN endpoint location.
(S) = activity determined to be caused by a server.
(E) = activity determined to be an expert user.
(D) = activity determined to be related to a Russian-centric device.
(K) = activity determined to be related to nefarious behavior of masking data.
(B) = activity determined to be related to automation scripts or bots.
Location = registered location of the detected network.
Network = registered network associated with the internet protocol.
IP Addresses: The "*" are replaced with "." to convert them to a valid IP, change these symbols back.

Aggregate Eavesdropping™ Heartbeat Monitor

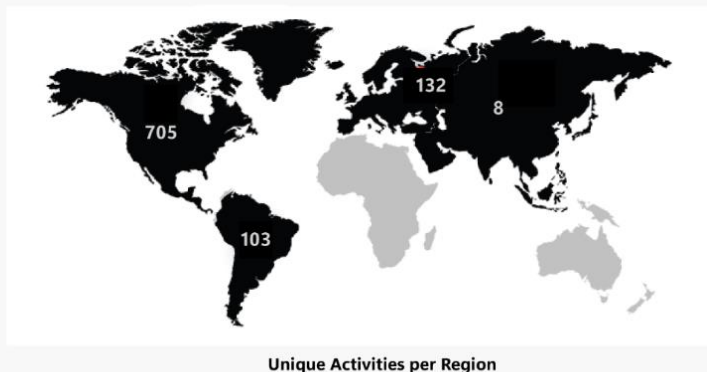
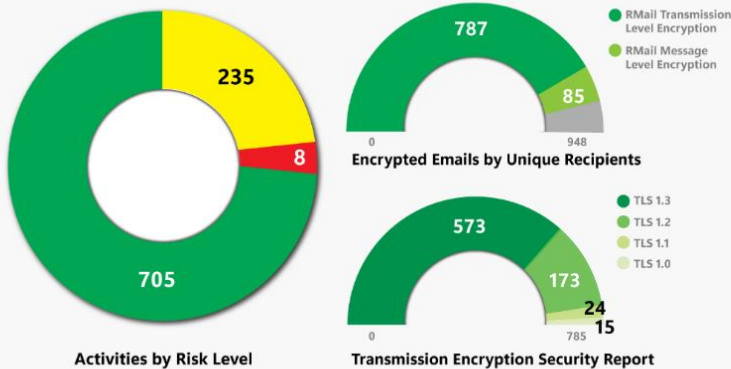
The Aggregate Eavesdropping Heartbeat™ Monitor offers a daily snapshot of eavesdropping risks for MSPs or IT admins. This aggregate report provides peace of mind by forensically monitoring the journey of all outbound messages to the recipient and beyond. IT Admins or MSPs can swiftly investigate further if they see any high alerts or unusual activity across all users, all domains, and all companies that they manage or monitor security for.

AGGREGATE EAVESDROPPING HEARTBEAT™ MONITOR

Date: 11-01-2022

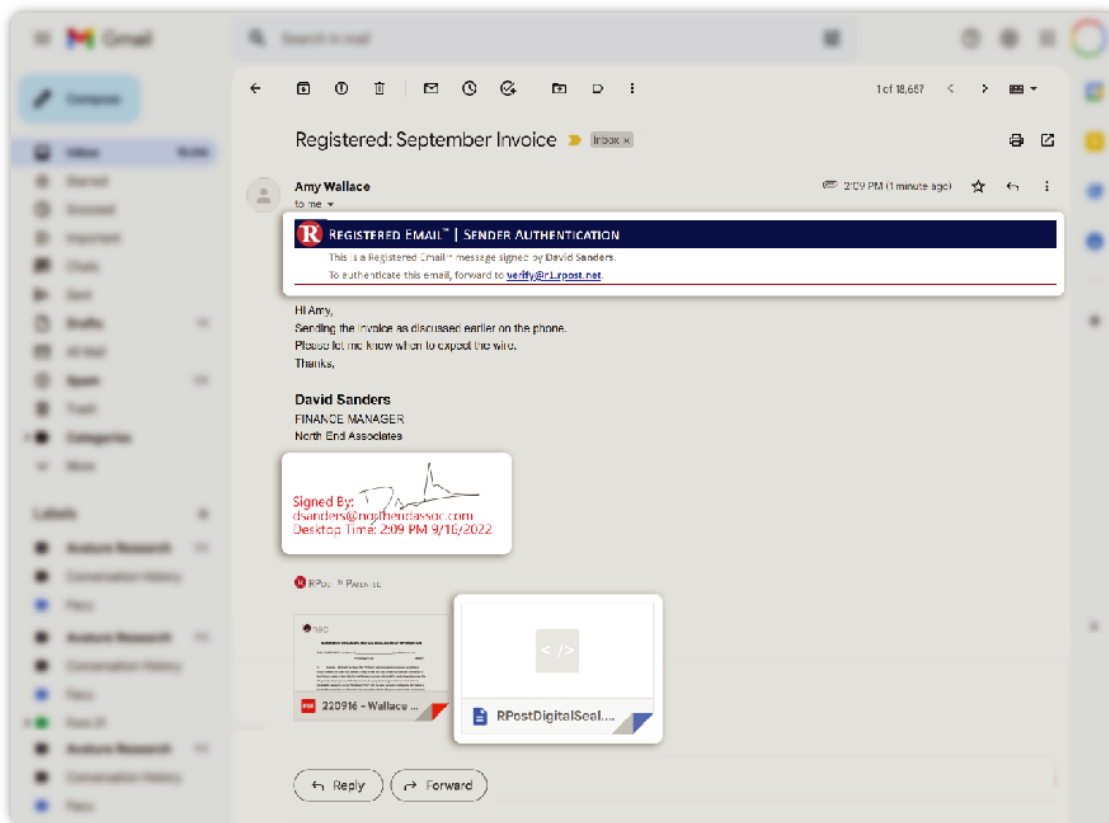
Sender Domains: northendassoc.com, northendassoc.co.uk

Red Alerts: 8



Digital Seal® Email Origin and Authorship Verification for Recipient

When delivering messages that are susceptible to be the type of messages a “man-in-the-middle” may try to intercept, alter, and continue the delivery, or send a near replica follow-up email, the RMail Digital Seal® impostor defense makes it easy for a recipient to verify origin and authorship of an email (for example, an email with an invoice attached). This is technology that the sender employs that protects the recipient from being fooled; providing the sender, value with assurance that funds requested will get sent from the recipient to the authentic sender (versus an impostor of the sender).



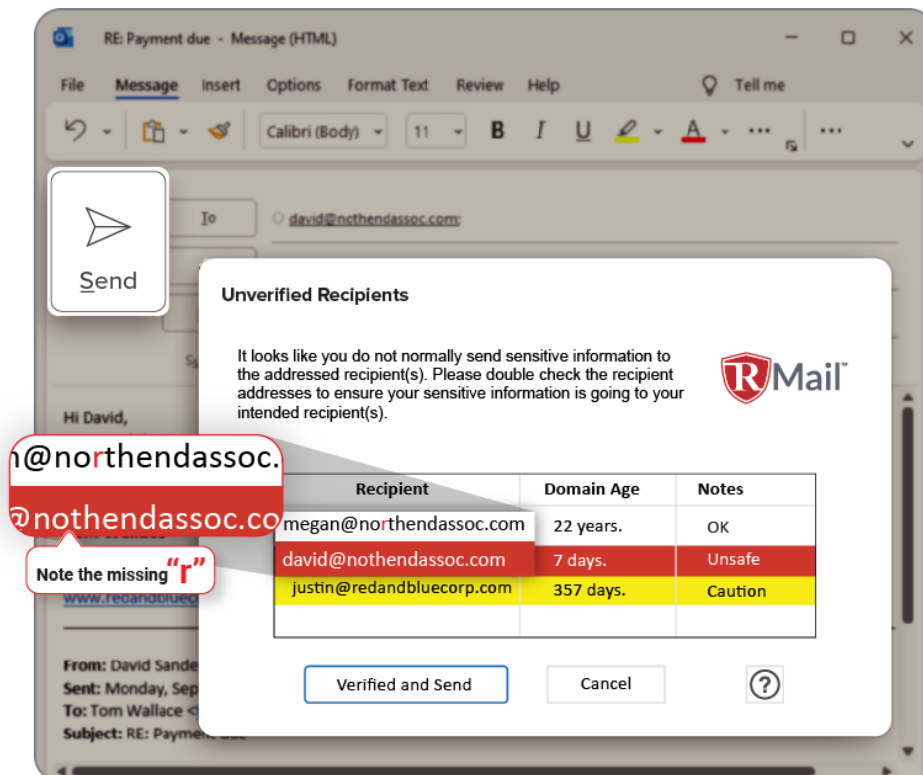
Applying PKI digital signatures to email, while providing a form of sender authentication of email for a recipient, provides some value, these “signatures” technically break if the email is forwarded onward and are not visible if the recipient views the email in certain email programs.

Applying DKIM and other (SPF, DMARC) sender authentication of email for a receiving server may flag certain inbound email threats, they must be employed at the sender email system and the recipient server and even if so, will not thwart lookalike domain trickery when sent from valid domains purchased to trick a recipient by visual similarity even though the email sender is a technically sending from a legitimately configured email account. More on this below.

Inbound Email Security Right Recipient™ Lookalike Domain™ Alert

If on the receiving side of an email that was intercepted at the sender --- for example, an invoice or other payment request --- and the sender, or supplier, email account has been compromised, the email en route to you the recipient may be altered. The alteration ultimately (often after some back and forth) may have different payment coordinates, luring unsuspecting payment staff into sending funds to the cybercriminal.

When the cybercriminal creates the impostor email to send to you (the recipient), so that they can bypass sophisticated inbound email security gateway and firewall security (e.g., DKIM, SPF, DMARC, phishing detectors, malicious link detectors), the cybercriminal will purchase a legitimate domain that is one letter off and difficult for the human eye to see the difference and send from that lookalike domain.



With the Right Recipient email Lookalike Domain alert, if the recipient replies to one of these newly purchased legitimate email addresses (technically legitimate but created with criminal intent), the RMail system will alert the user in milliseconds after they click send, before the reply is sent, that the domain of the email address that they are about to reply to has been newly created --- red alert --- likely with the intent to circumvent back-and-forth correspondence between recipient and legitimate sender. This generally leads to impostor wire or funding instructions being sent to the recipient by this impostor supplier/sender, and if successful, ends in a mis-wire of money (sending to the cybercriminal).

Email security systems that the sender or supplier employs will not protect the recipient of invoices they send from these types of domain trickery attacks. Email security gateways at the recipient cannot block traffic for newly created domains as there are legitimate reasons a new domain may be sending legitimate email. This is best automated with adaptive AI, at the email program of the recipient. This is where RMail employs its Lookalike Domain™ alert running within the Microsoft Outlook email program.

Right Recipient™ Reply Hijack™ Detector

Sophisticated internet criminals may place the newly created lookalike email domain within the hidden-to-recipient “reply-to” header of the message that they send to the target recipient.

Or, they may place another seemingly plausible email address that poses as a legitimate sender, in the hidden-to-recipient “reply-to” header. In both cases, they may put the actual email of the legitimate sender in the email “from” field – and send it to the recipient to make it appear as though the legitimate sender sent the email. The goal of this type of trickery is to have the recipient continue unwittingly a back-and-forth email exchange with the impostor, thinking it is a trusted sender (supplier, or otherwise); ultimately making a payment to the impostor’s bank account to pay an invoice or consummate a purchase. Sometimes they are successful in convincing the payor to update recurring payment systems and even payroll systems.

Email security systems that the sender or supplier employs will not protect the recipient from this type of cybercrime. Email security gateways at the recipient can look for DKIM, SPF, or DMARC sender authentication failures – which can block some of these based on the method that the sender employed. However, if the sender sends from legitimate lookalike or plausibly alternative email address, these will generally pass DKIM, SPF and DMARC sender authentication policies. Email security gateways at the recipient can also look for mismatches in the header of inbound email (mismatch in the from and reply-to headers) however there are legitimate reasons for such mismatches to occur and blocking this traffic can block legitimate email. This is best automated at the email program of the recipient. This is where RMail employs its Reply-Hijack™ alert running within the Microsoft Outlook email program. This is also known as a “Whaling” type of “spear phishing” or a “reply-to pivot”.

Fake Forward™ Detector

Following on the Reply-Hijack, if forwarded, depending on how the email was sent and composed, once forwarded, one cannot tell that the email came from an impostor of the sender, and the content of the email gains a sense of legitimacy – since forwarded from a source known to the new (forwarded to) recipient. RMail will detect and alert that a fake email that was part of a Reply-Hijack reply-to pivot scheme is about to be forwarded, unknowingly creating a sense of legitimacy to the impostor email content.

Email security systems that the sender or supplier employs will not protect the recipient from this type of cybercrime. Email security gateways at the recipient can block for email that was sent by an impostor appearing as if they were a legitimate sender known to the recipient if they have sender authentication policies like DKIM set up. However not all recipients do (because not all senders legitimately employ these at the point of sending). RMail employs its Fake Forward™ alert running within the Microsoft

Outlook email program that can alert on some forms of email from impostor senders being forwarded on by the first recipient.

Each of these RMail technologies are additive layers that either the email security gateway systems that companies employ do not address or do not address well (the Outbound Email Services), or the most sophisticated email gateway servers do provide some protection at the gateway level but not in as focused a manner as the RMail inbound security services that run within Microsoft Outlook (with the RMail full install).

Regardless of existing email systems in place within a company, these RMail technologies focus outside the boundaries of normal email security server filtering capabilities and can thwart a crime in progress, after the spearphishing hook is in, before the steal.

Conclusion

RMail AI now features are essentially turning RPost (makers of RMail) into a customer's very own PRE-Crime™ fighting agency. RPost technology, in tandem with our team of elite customer agents, now and in the near future, will alert customers of a crime related to email cybercriminal hook-and-steal lures that have not yet occurred but are in the process of occurring — with enough warning so that users and IT admins can take action to eliminate the crime right before it happens. These crimes most often lure companies into sending money to the cybercriminals through trickery or as a ransomware bounty.

Essentially, we've extended the sender's ability to secure email to include the identity of e-crimes in progress at the recipient. How is this possible? **20+ years of singular focus on email security!**

Imagine that every time you email your client, you are (with RMail) essentially learning if their account is at risk so you can save yourself and your trusted client. This is really a must-have for any businessperson sending important email to clients.

Contact us to discuss how you can get started preventing, detecting and disarming cybercrime with RMail PRE-Crime™ services.

RPost is About Continuous Innovation

We're the global leader in premium, feature-rich and more affordable e-signature, email compliance and cybersecurity services, and we've been continuously innovating for our customers the world over since 2000. From within our three main platforms, RMail e-security, RSign eSignatures, and Registered™ e-compliance, we're everything our customers need when it comes to email, document and form security, compliance, and workplace acceleration — track, prove, eSign, encrypt, share, certify, control. We do what no other company does — all in one.

We thrive on ensuring that we are artisans and experts in everything we do: secure and certified email encryption for privacy and compliance; eSignatures and web forms to ease digitization of workflows; e-delivery tracking to prove important communications; managed file transfer to simplify secure sharing of large documents and sets of files; document-level digital rights management to empower control of document access even after transmission; and AI-infused apps to prevent data leaks by minimizing human e-security errors. This is why more than 25 million users have enjoyed our RMail, RSign, and Registered services for over two decades across 193 countries.

RPost was recognized as Hot Vendor and Most Innovative Vendor in Digital Transaction Management by Aragon Research in 2022.

“This recognition validates RPost commitment to providing organizations with the tools they need to embrace digital transformation, enhance customer experiences, and ensure the security and privacy of their digital interactions, not only for the ‘today’ but for organizations’ journey of continuous digital transformation into their future.”

Jim Lundy, CEO, Aragon Research

Learn more at the [RPost website](#).



Identifies **RPost** as

Most Innovative Software Provider

In Aragon Research Globe[™]

For Digital Transaction Management



Leader in eSign & e-Security

was viewed, and a world map highlighting the geographic location where the suspicious open took place.

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 Send Time: 09/13/2022 05:20:00 UTC
 Transaction ID: A4BD52B62EE9862A5FDD88F336A99E2D69FEF54A

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/LGy25hw0Z65CNlyOLyZCLCuMKdk95gm4vir26bBCMDlx.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.
 (N) = content delivery network delivered email data to viewer via webmail client.
 (V) = activity was detected at an anonymizing VPN endpoint location.
 (S) = activity determined to be caused by a server.
 (E) = activity determined to be an expert user.
 (R) = activity determined to be related to a Russian-centric device.
 (K) = activity determined to be related to nefarious behavior of masking data.
 (B) = activity determined to be related to automation scripts or bots.
 Location = registered location of the detected network.
 Network = registered network associated with the internet protocol.
 IP Addresses: The "*" are replaced with "", to convert them to a valid IP, change these symbols back.

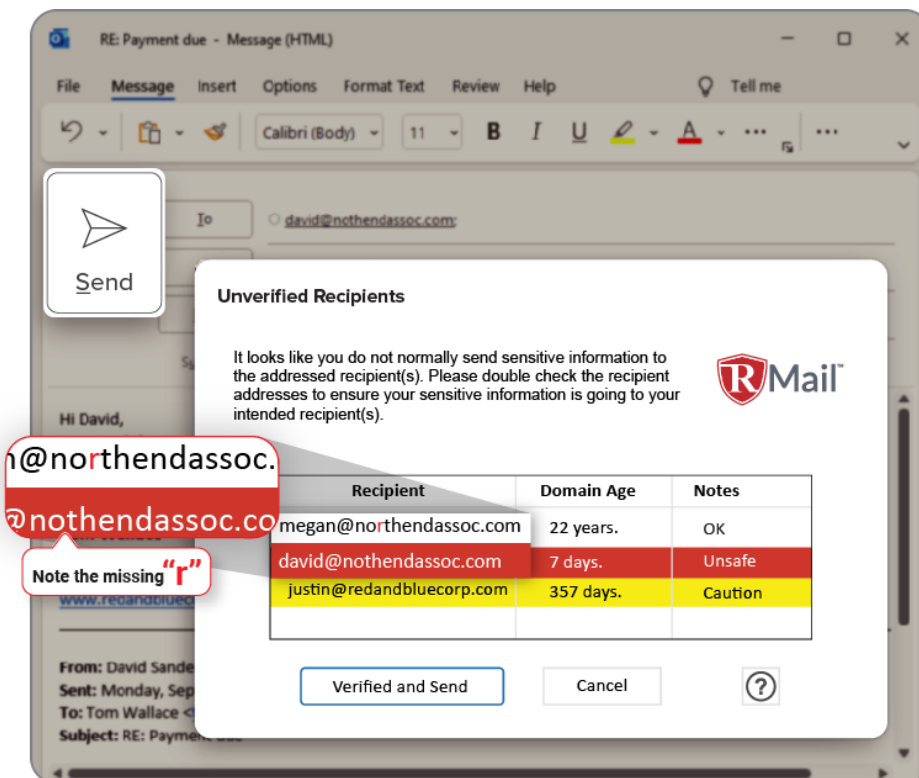
The report then lists all activities with your email, timestamped, per geo location and IP address, plus the geo location risk level.

Lastly, the email provides the original message details like original recipient, original sender (in the admin report), sent time and transaction ID, and includes a deep forensic meta data record in case IT security needs to do further investigation on a particular message.

Right Recipient™ email Lookalike Domain™ Alerts

Higher level of cybercriminal efforts include purchasing clever lookalike domains of authentic recipient addresses.

If the message structure does not trigger the “Reply Hijack” alerts, and the domain looks like another recognizable domain to the recipient (e.g.: **user@amazon.com** vs. **user@amazon.com**) created for the purpose of trickery, upon clicking reply and send (Send Registered, or otherwise triggering RMail service sending as an important email), the RMail service will provide a red or yellow alert if it determines the domain of the recipients in the to/cc/bcc lines are likely a lookalike domain created within the recent past 90 days or within the year) with intent to fool.



Enabling RMail Services

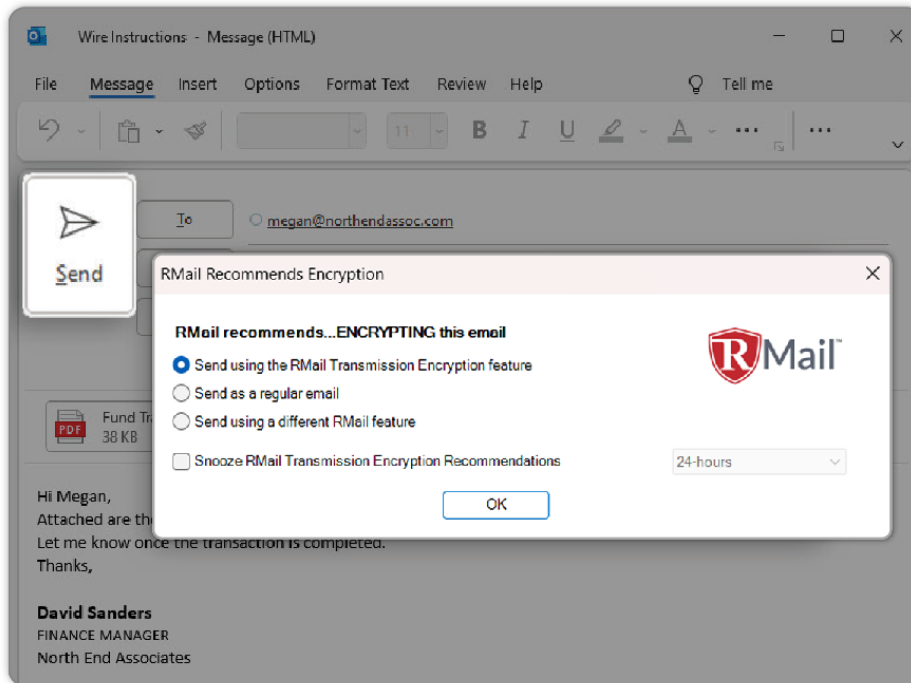
The RMail Lookalike Domain detector technology is included within RMail for Outlook. The hidden header detection occurs on all email replied or forwarded (before sent) and the domain age detector occurs on email that has been indicated to be important (by RMail AI – RMail Recommends™ or by using the RMail Send Registered button).

The Eavesdropping Alerts can be set for any message routed via the RMail Gateway outbound email security server, or sent as an encrypted, e-sign, or Registered Email message from any RMail app (Outlook, Office365, Gmail, Salesforce, etc.).

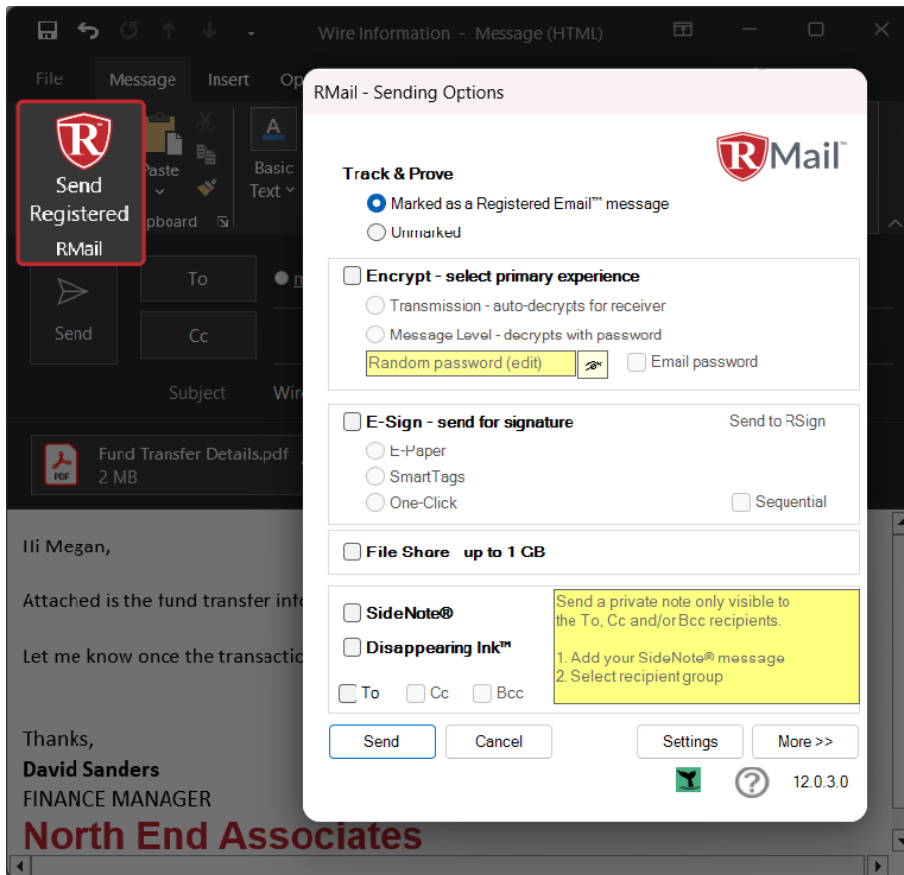
Microsoft Outlook 365

In Microsoft Outlook (full install, Office 365), there are two modes:

1. **RMail Recommends™**: AI-infused, data loss prevention service that sensitizes users of their need to treat certain messages differently (e.g., encrypt, track and prove delivery and open, and more), based on the content of the message. RMail Recommends™ not only protects your organization's data, but also trains users in the moment of sending.



2. **RMail Send Registered™**: Senders can click the Send Registered button, seamlessly embedded in the Microsoft Outlook interface, to leverage the full extent of RMail features: track and prove email content delivery and open, transmission and message level encryption, sending email and attachments for eSignature, secure large file share, and more.



Security Gateway, Gmail, Salesforce and other apps

For Gmail, Salesforce and any other apps, it is recommended to install the dedicated RMail app, which allows to secure email transactions with both Transmission and Message Level encryption (and many more security, compliance and productivity tools), and configure RMail Gateway secure email gateway service or server to enable Email Eavesdropping™ alerts and automate email security and compliance company-wide.

Eavesdropping Heartbeat Service

RPost teams can also be engaged to send your approved fake transaction message to your staff to try to lure any cybercriminals into engaging in their cybercrime, identifying accounts where there is a cybercriminal patiently waiting for a transaction to then act. This can uncover compromised accounts before users are lured into costly cybercriminal schemes.



Contact us to get started!
www.RMail.com

US: +1-866-468-3315

UK: +44 203 6333505