

Pre-Crime™ Targeted Attack Defence

Pre-emptive defence against the most sophisticated Business Email Compromise (BEC) attacks against you, your suppliers and clients.



Contents

Overview - Why Pre-Crime?	3
What are Business Email Compromise 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	11
Anatomy of Targeted Attack-in-Progress	13
Conclusion	22
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	28

Overview: What is Pre-Crime

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 (and often AI-generated) scams target businesses conducting legitimate fund transfers, aiming at diverting payment to fraudulent bank accounts.

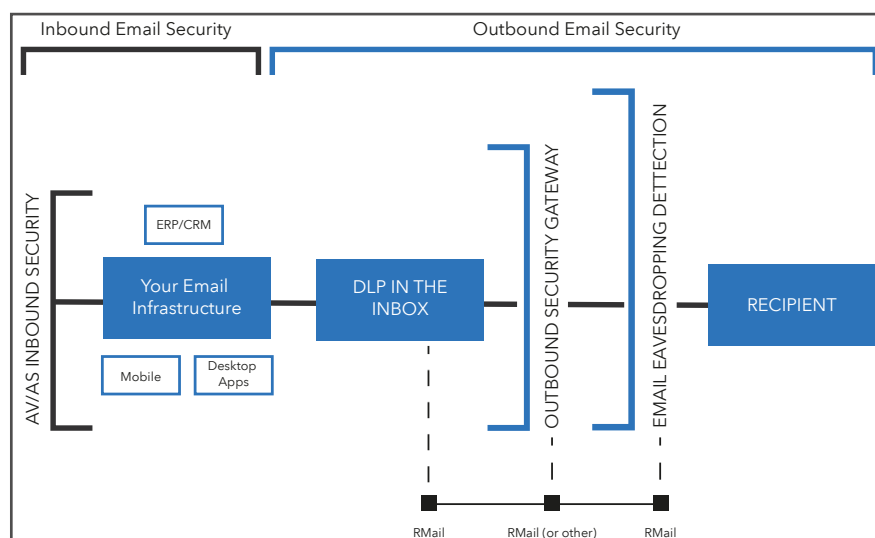
The latest figures from FinanceUK show a worrying trend. In the first 6 months of 2023, a staggering £530 million was stolen from UK businesses via fraud. This represents a 43% increase from the same period in 2022. There were more than 116,000 cases in this time frame, all of which has prompted FinanceUK to state that **‘the level of fraud in the UK has now reached a point where it must be considered a threat to national security.’**

Both FinanceUK and the Financial Conduct Authority (FCA) have noted trends within the cybercrime and online fraud environment that are moving criminals’ focus away from the companies and onto the clients themselves.

According to FinanceUK, ‘firms must now ‘undertake continual analysis...to understand what constitutes effective warnings against fraud for customers, looking for impactful ways to highlight the risks, increases protections, and encourage preventative actions through the customer journey.’

According to the FCA, ‘firms must strengthen anti-fraud systems...there is not enough focus on delivering good customer outcomes.’

It is clear that avoiding fraud and preventing crime must now be the primary focus of any UK business. Identifying the causes and taking proactive action is the responsibility of every organisation.



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

Frama RMail is already well known for its Registered Email™ and Registered Encryption™ features that mitigate risk by providing proof of who said what when, as well as audit-ready proof of fact of privacy compliance. Frama RMail has and continues to evolve, and now includes more than e-security risk mitigation. A unique AI performs Pre-Crime detection in-built into your email infrastructure - stopping the crime before it materializes.

Frama RMail's elegantly easy email encryption services provide a comprehensive foundation for email security, risk management and compliance. Our newest innovation for Pre-Crime 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 fraud is happening inside the sender's organisation or if the recipient's email account is being eavesdropped on.

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

Encrypting email is a central protector to minimise overall risk. Using Frama RMail's message level encryption which can be configured to remain encrypted inside the recipient inbox, can protect sensitive content from becoming attractive to cybercriminals. A Pre-Crime service focus thwarting attacks after the criminal has identified targets and has begun to act.

This technology paper discusses Frama RMail email security services focusing on targeted attacks often referred to as **Business Email Compromise (BEC)**. Within this category, cybercriminal tactics include **Phishing, Spearphishing, and Whaling**, as well as **Email Account Compromise, Supplier Account Compromise and Client Account Compromise.**

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 organisations. Attackers seek 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.

This type of fraud rose by a staggering 43% in the first half of 2023, resulting in a total of £530 million being stolen in the UK alone.

BEC attacks are among the fastest growing and most concerning cybercrimes against organisations and, according to a recent Research report, "many organisations are ill-prepared to address the threat of BEC and lack sufficient protections across people, process, and technology factors." Also cited in the same report is a startling finding that 80% of organisations 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. Frama RMail specializes in email security, while also offering a unique approach to specific threat vectors.

- **Prevention:** email encryption is a mainstay of the many Frama services and has traditionally been one of the methods to prevent cybercriminal activities from gaining a foothold within an organisation or within a business transaction. Unique to **Frama RMail Encryption** is its innovative AI which can determine the best method of delivery to each recipient based on security concerns, privacy compliance, and need for recipient simplicity. 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.
- **Defence:** once a cybercriminal sets their sights on a target, whether that target is within your organisation or an external party, it's time for defensive technology that can diffuse the crime-in-progress pro-actively. This is the focus of Frama 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 that require a level of privacy to protect consumer information (such as financial institutions), **Registered Email™** encryption returns a **Registered Receipt™** email record (available stand-alone or part of Frama 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.

Frama RMail's Pre-Crime intelligence provides email vector **targeted attack defense**. With specialty in addressing today's most sophisticated organized cybercriminal gang tactics.

Business Email Compromise (BEC) 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, the process of sending payments (e.g. invoice payments or payroll payments).

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 payer's account, or email stream is actively being eavesdropped on).

These tactics have proven successful. The estimated cost to the UK economy in 2022 was more than £2.5 billion. In most situations the criminal is not accessing the bank account of the sender, they are deceiving the sender 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 whom 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, starts the process to cause the individual or business to direct funds to the cybercriminal's account.

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) with (today more and more) well written emails that have often been copied from the original sender's own email string to appear authentically written. 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.

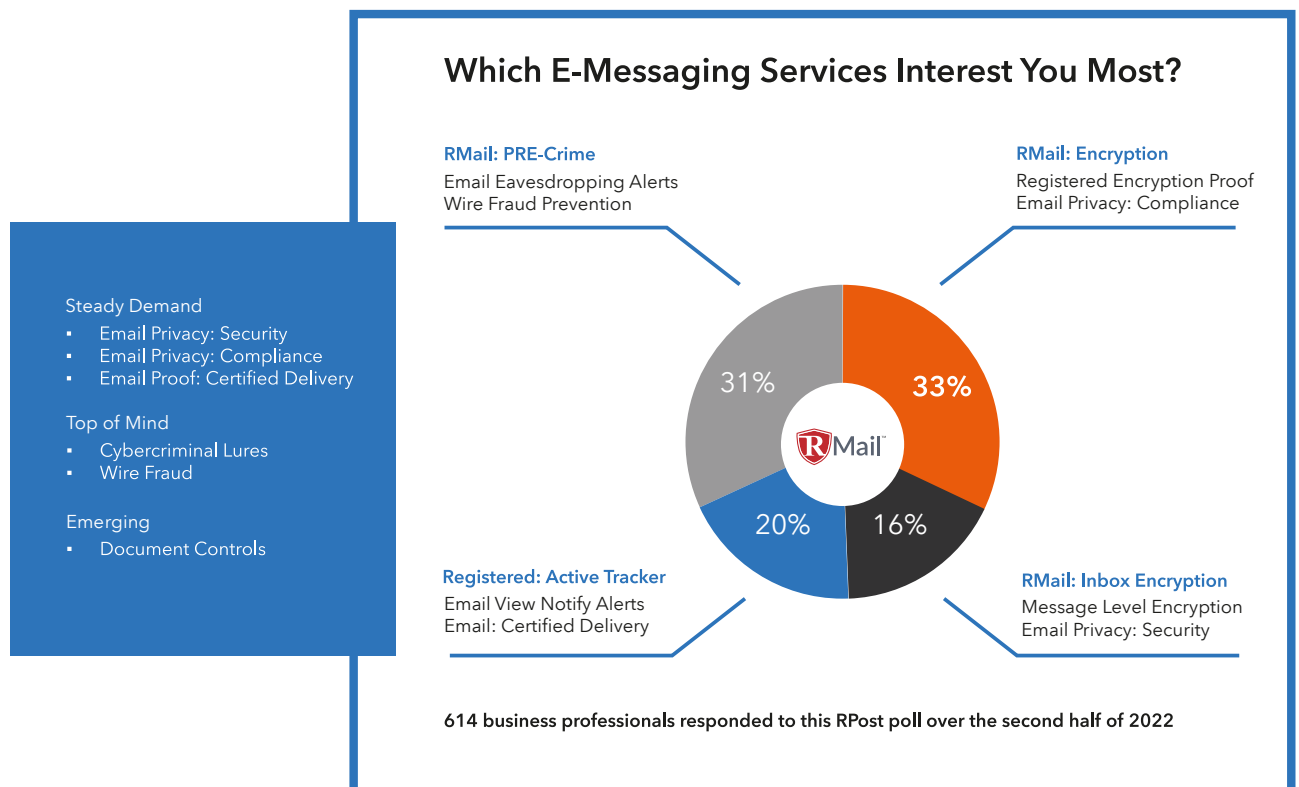
Enter Frama's Pre-Crime™ targeted attack defence.

While Frama RMail has a broad range of email security services, it specialises in its unique approach to what is transpiring with important email, inbound in the inbox, outbound to the recipient.

Whilst there are other secure email gateway services, most specialise on inbound protection from broad-based threats like virus-, spam-, and malware-ridden email. Where Frama RMail adds the most value is working in harmony with whatever a company currently has in place for these broad based threats.

Services like Frama 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, you can count on Frama’s services to have taken a unique approach where other security software and secure email gateway services do not.

R1 Meets More of E-Security Landscape



Targeted Attack Defense

A Pre-Crime scenario means 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 recipient; and / or (c) sent a fake email from the lookalike domain to the target aiming at diverting payment to a fraudulent bank account. Frama's Pre-Crime technology is designed to swoop in and stop this with specific alerts and awareness after the hook is in, before the fraud takes place.

RMail's Pre-Crime service covers both **inbound and outbound** protection.

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 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 back to the cybercriminal rather than the original sender. If the sender organisation 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 such as invoices that are attractive to the cyberthieves, 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 cease to be effective when a recipient forwards an email onward to others. RMail Digital Seal® technology is durable and verifiable even if forwarded.
4. **Right Recipient™ Lookalike Domain™ Detector.** An often-used trick in email fraud is a sender address with a domain that looks just like the familiar email address and domain of your long-time supplier or client. RMail's Lookalike Domain™ alert; running within the Microsoft Outlook email program, identifies this type of attack in action.

In-the-Inbox Inbound Email Security

- 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 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 organisation forwards the impostor email, once forwarded it becomes even more challenging to tell that the email came from an impostor. The content of the email gains a sense of legitimacy since it appears to be 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.

RMail's Pre-Crime™ e-security services run invisibly in the background of an 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.

"Today's email security needs to be humanised, and Frama'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

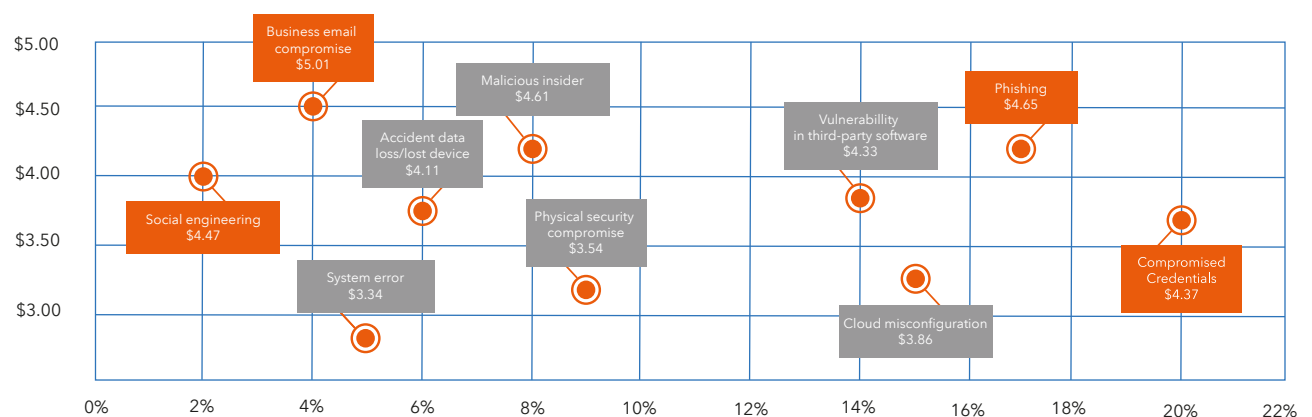
Threat Categories and Consequence

While there are many types of cybercrimes, 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 fraud.

The more sophisticated organised cybercriminal gangs use all of these in the same attack - producing lucrative benefits that often generate tens to hundreds of thousands of pounds every time. It is this high success rate that has been dubbed 'a threat to national security' by FinanceUK.

Main Cybersecurity Threat Vectors

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



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 organised crime rings that are sophisticated and composed of multiple teams.

The below is a real example, described by the West Midlands Cybercrime Unit:

1. The cybercriminal logs into LinkedIn and looks at all the employees for a targeted company. They find Emily, who works in accounts.
2. Emily's LinkedIn profile explains that Emily handles incoming and outgoing payments to clients.
3. A quick search online (or sometimes a quick phone call to the targeted company) identifies one or more of the targeted companies' clients.
4. The cybercriminal contacts one of these clients posing as a potential customer. They request an email confirmation. They now have the official email footer of the client.
5. The criminal creates a dummy domain, that is similar to that of the client (for example, @nothwestassociates.com instead of @northwestassociates.com).
6. They send Emily an email asking for an invoice payment, including the official email footer, a professional looking invoice, and a link to a payment gateway. The email comes from the dummy account, but as far as Emily is concerned it looks legitimate.
7. Emily clicks on the payment gateway to make a payment. Whilst the payment screen also looks legitimate, it is not - it has been created by the cyberthieves.
8. The payment gateway requires Emily to log in with her email and password, which she does, with no idea that the payment screen is anything but real.
9. Her first login returns an error message saying that her password was wrong. So she tries a different password. The second password is accepted.
10. She enters the card details to make the payment. She receives a message saying that the card was declined. Emily believes she must have made an error, so she tries again. On the second attempt, the payment is accepted.
11. The cybercriminals now have:
 - The credit card details of the company
 - Both payments that Emily made
 - Emily's two most-used passwords, which they can sell on the Dark Web

12. Emily carries on with another task, with no idea what has happened. It is not until days or weeks later that the payments come to light, by which time the cyberthieves have vanished without a trace.
13. Emily's bank accounts and personal email are hacked as her passwords have been sold and her personal details distributed to other parts of the same team, or to another criminal enterprise.

According to the West Midlands Cybercrime Unit, what makes the above process even more terrifying is that many of these schemes are not conducted by a single person, or even a gang, but by AI.

This allows criminals to perform the entire action at scale, over and over again, hundreds of times a week. And they only need it to work a handful of times before it becomes incredibly profitable.

If your company had the RMail Pre-Crime services with Email Eavesdropping™ alerts on, Emily would know that the email she received did not come from her client, and would not make any payments or divulge her or the company's details.

For your clients, you should certainly recommend they install Frama 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.

Further, if you make it part of your standard procedures to send all your company emails with RMail Digital Seal® email authentication technology, you then extend peace of mind beyond your organisation to your entire network. Another suggested best practice is to send important messages (like invoices) with Frama 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, Frama RMail is designed to enable your company (and your clients) to conduct transactions digitally with peace of mind, accelerating business securely in an era where pitfalls and uncertainty have unfortunately become the new normal.

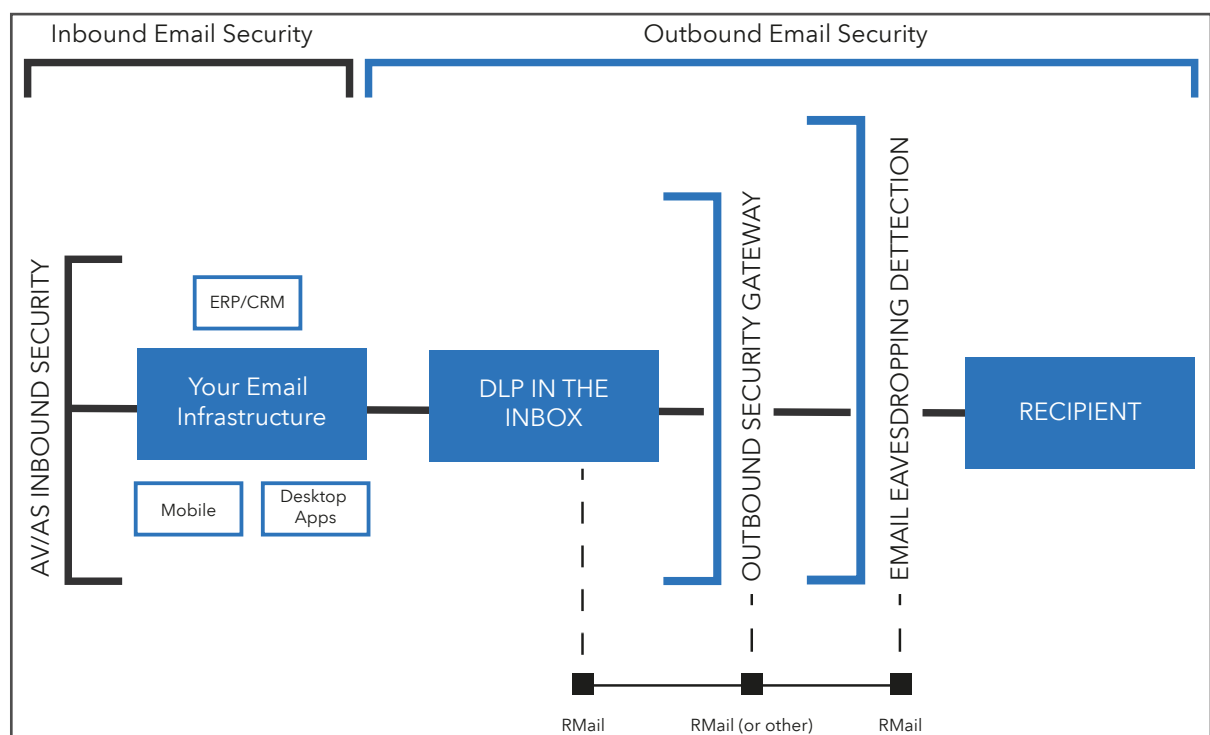
With Frama RMail Pre-Crime features, (a) you will get alerts if an email to a client is being unknowingly read by a nefarious party. If an email someone sends is being eavesdropped on due to an unknown security issue with the recipient's email account, you will be alerted; (b) you and they (if they use Frama 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 **whilst** raising e-security awareness at the user level.

Anatomy of Targeted Attack-in-Progress

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

Whilst some cybersecurity software protects companies against some elements of BEC attacks where they would otherwise be at risk, 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 organisation's clients' email accounts being compromised**. Both the FCA and FinanceUK have recognized the trend in targeting clients rather than companies, most notably in the amendments made to the FCA's Consumer Duty guidelines in November 2023. In the cases where the organisation 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. Frama RMail Pre-Crime services are specifically designed to protect organizations **and** their clients with 100% BEC and wire-fraud protection.

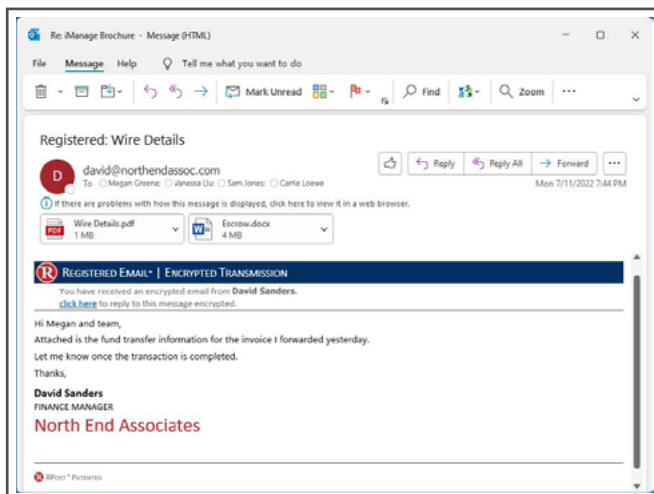
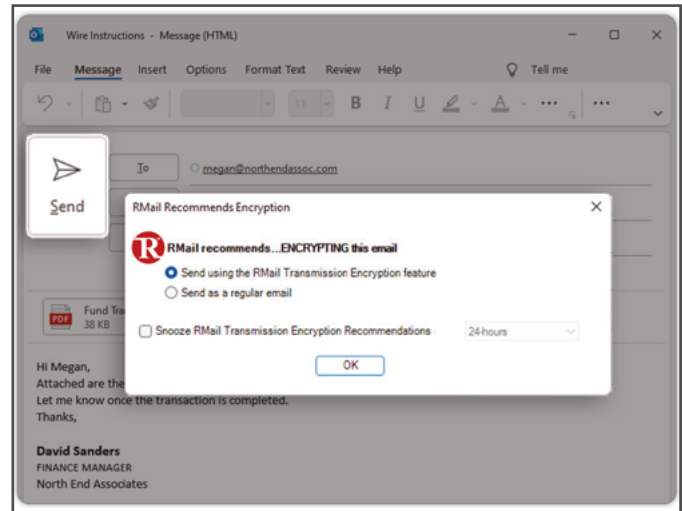
As an IT professional you might ask where does RMail Pre-Crime targeted attack defence fit within your organisation, without overlapping existing tools? Put another way, if one has the top-of-the-line email security gateway and all it has to offer, for what scenarios does Frama RMail add value (and security)?



Outbound Email Security

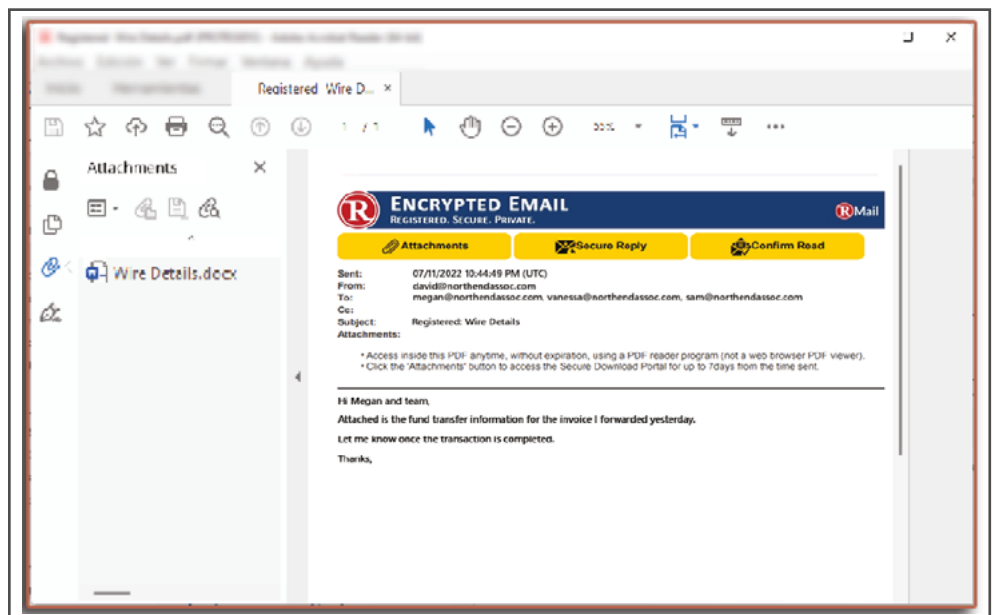
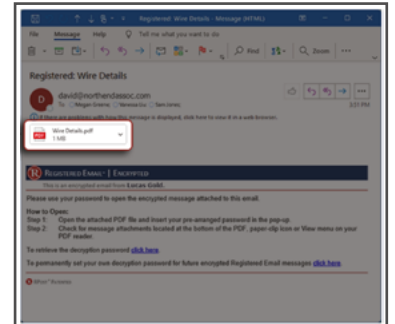
1. Registered Encryption™ privacy.

For email encryption to add value, it must be used, and be 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 technology on the intended recipient's end.

Further, if there is a future breach of a recipient email account, ideally the encrypted message, whilst inside the recipient's inbox, the data 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 route all, select, or policy trigger outbound email via RMail email encryption.

The 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).

Original Sender	Internal Msg ID	Security Details	Time	Encryption Method	End Recipient	Security Details	Time	Expiration
megan@northendassoc.com	07112022-104449-PM-11C1	RSA-AES256 TLSv1.2	07/11/2022 10:44:49 PM (UTC)	Best	megan@northendassoc.com	TLSv1.2	07/11/2022 10:44:49 PM (UTC)	Best
megan@northendassoc.com	07112022-104449-PM-11C1	RSA-AES256 TLSv1.2	07/11/2022 10:44:49 PM (UTC)	Best	megan@northendassoc.com	TLSv1.2	07/11/2022 10:44:49 PM (UTC)	Best
megan@northendassoc.com	07112022-104449-PM-11C1	RSA-AES256 TLSv1.2	07/11/2022 10:44:49 PM (UTC)	Best	megan@northendassoc.com	TLSv1.2	07/11/2022 10:44:49 PM (UTC)	Best

Original Sender	Original Recipient	Overall Encryption Status	Status Description
megan@northendassoc.com	wanda.megyer@northendassoc.net	★★★★★	Best encryption from sender device, best to recipient gateway
megan@northendassoc.com	jruell@northendassoc.net	★★★★☆	Best encryption from sender device, acceptable to recipient
megan@northendassoc.com	stuart.clark@associationsolutions.net	★★★★★	Best encryption from sender device, best to recipient

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

DeliveryReceipt.xml 17 KB
HtmlReceiptLhtm 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)
drlucasiones@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.mail.com/resources/coordinated-universal-time/>

Message Envelope	
From:	tom@northendassoc.com <tom@northendassoc.com>
Subject:	Insurance Policy Review
To:	<drlucasiones@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:	F95542A9A2EEEEBB4509C10C04569371335F2C815
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 >>> EHLO mta21.r1.rpost.net 4/6/2020 2:40:18 AM >>> 250 HE1EUR01FT033.mail.protection.outlook.com Hello

Other email security gateway or email privacy/encryption providers do not have the same dynamic adaptation of the method of encrypted delivery based on type of message, risk, or recipient, and does 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 attacks, target their victims by eavesdropping on email from sender to recipient. They then siphon off the email, analyse it, copy it with slight modifications related to payment instructions, and then pivot replies back to the cybercriminal rather than the original sender. For invoice delivery, for example, the supplier sends an invoice to the client. 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.

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.**

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: A48D52862EE9862A5FDD8BF336A99E2D69FEF54A

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/LGy25hw0Z65CNlyOLyZCLCuMKdk95gm4vir26b8CMDIx.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/LGy25hw0Z65CNlyOLyZCLCuMKdk95gm4vir26b8CMDIx.gif 192.168.10.153 192.168.10.153 46808 GET /open/images/LGy25hw0Z65CNlyOLyZCLCuMKdk95gm4vir26b8CMDIx-Dlx.gif open.r1.rpost.net 443 1 HTTP/1.1 Microsoft-InternetExplorer/8.5 /open/images/LGy25hw0Z65CNlyOLyZCLCuMKdk95gm4vir26b8CMDIx.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 sender organisation has an email security gateway, it may flag certain inbound email threats, or even prevent traditional outbound data leaks, but it likely does not identify email security breaches after an email has left its environment or when the email is at the recipient. **RMail does.**

3. **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.


Email Activity Report Active Tracker™ Intelligence

Original Recipient: jim@insurancegrp.com

Security: Green

Opens: 3

Locations: 2



Risk Details

Time	Activity	Detail	Locale	Location: Country	Location (IP)	Network	Risk
09/15/2022 08:12:46 UTC	Open	M	Frankfurt, Hesse	Germany	52.72.5.168	T-Mobile	Green
09/13/2022 12:54:18 UTC	Open		Boston, MA	USA	94.92.53.178	Verizon	Green
09/12/2022 02:15:17 UTC	Open		Boston, MA	USA	94.52.53.178	Verizon	Green

Original Message Details

Original Send Time: 09/12/2022 1:33:52 UTC
Transaction ID: E64B9039C2CE5914F42EE61BCADAB09C55894832

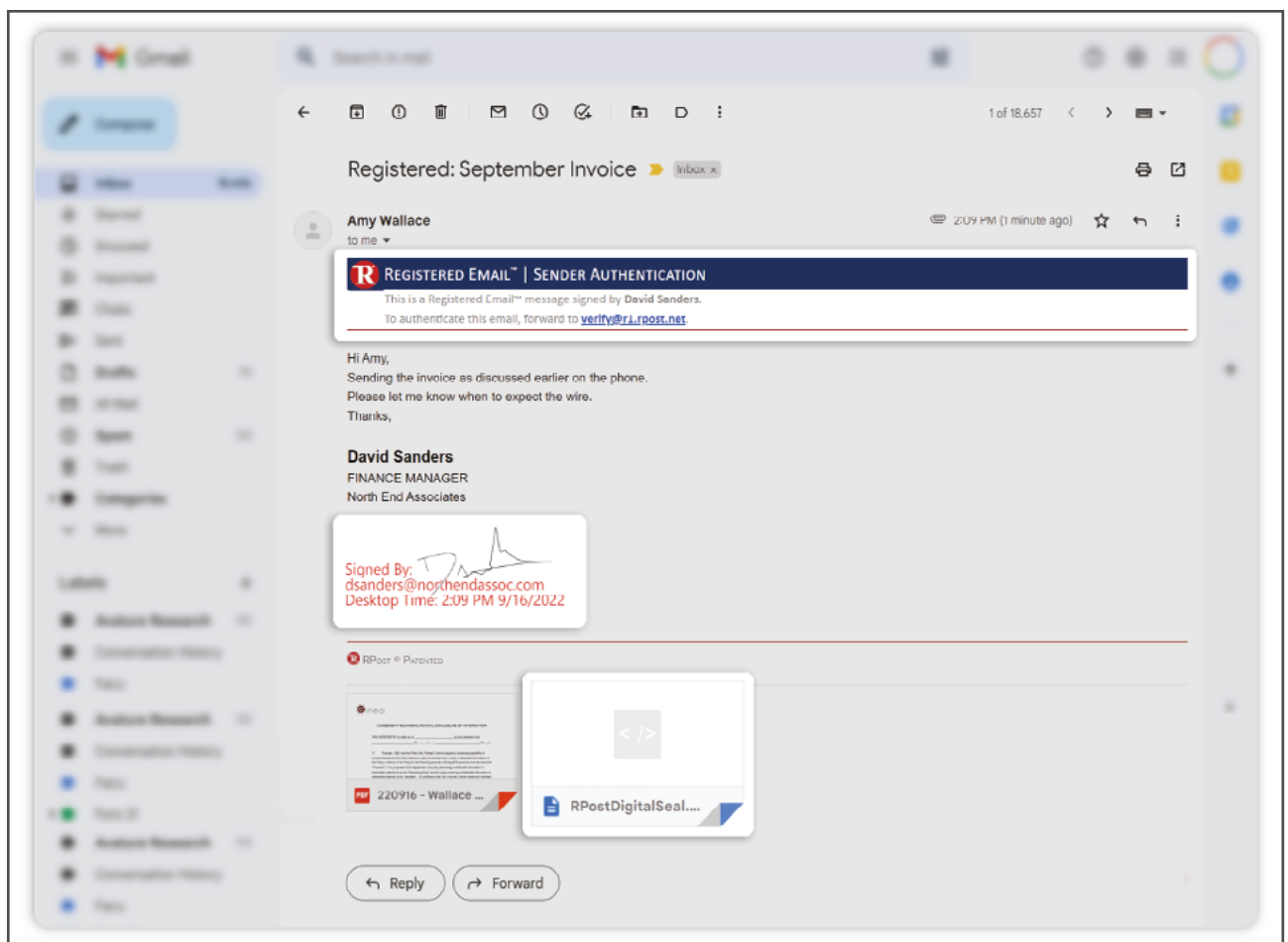
Metadata:

```
[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/LGy25hw0Z65CNlyOLYzCLCuMKdk95gm4vir26b8CMDlx.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/LGy25hw0Z65CNlyOLYzCLCuMKdk95gm4vir26b8CMDlx.gif 192.168.10.153 192.168.10.153 46808 GET /open/images/LGy25hw0Z65CNlyOLYzCLCuMKdk95gm4vir26b8CMDlx.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.

- 4. 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 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).



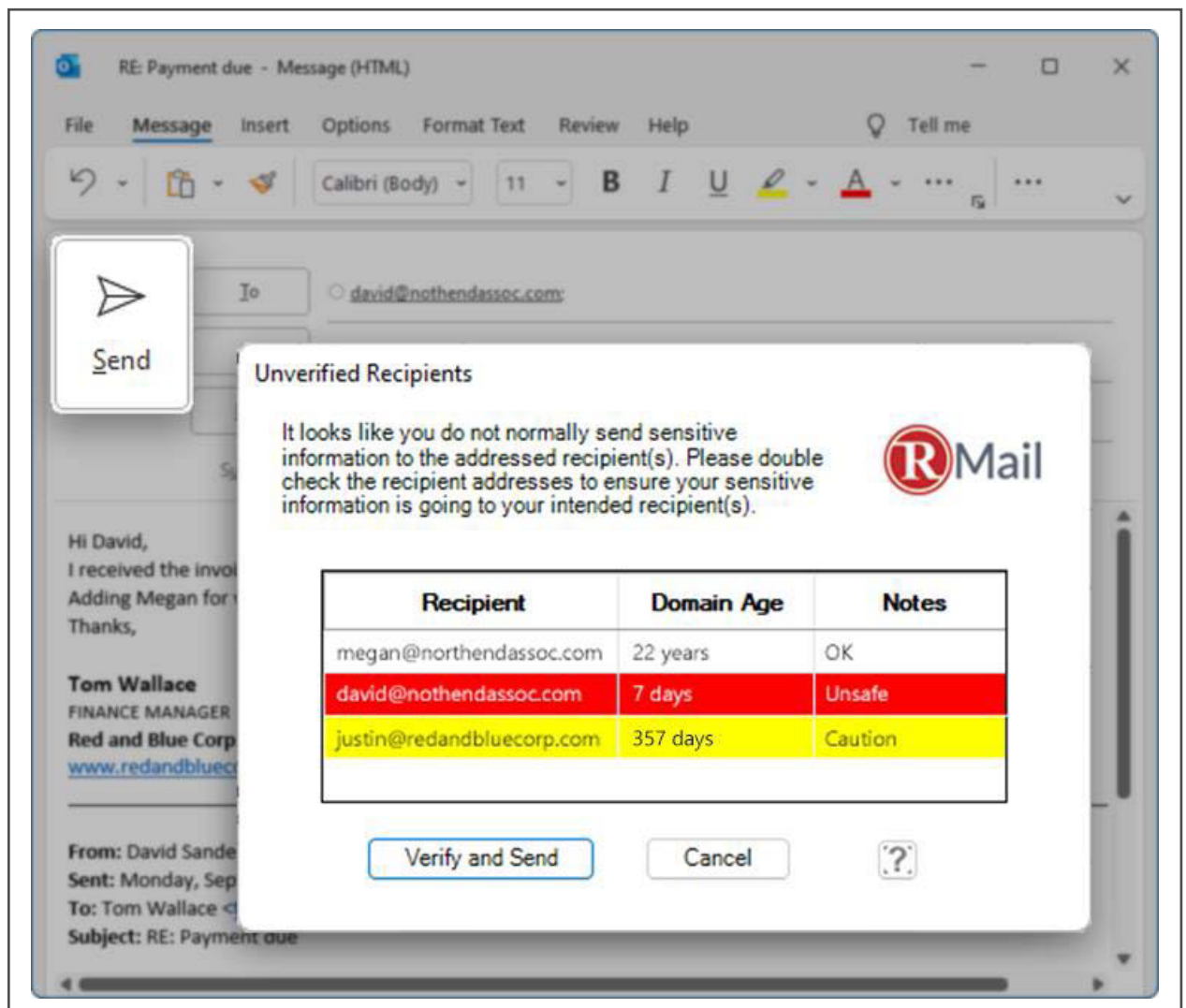
Whilst applying PKI digital signatures to email, while providing a form of sender authentication of email for a recipient, provides some value, these 'signatures' cease to be effective if the email is forwarded and are not visible if the recipient views the email in certain email programs.

If you applying DKIM and other (SPF, DMARC) sender authentication of email for a receiving server, you may flag certain inbound email threats. For this to be effective, these must be employed at both the sender email system and the recipient server. Even if this is configured correctly, it will not thwart lookalike domain fraud when sent from valid domains purchased to deceive 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™ email Lookalike Domain™ alert.** If an email was intercepted - for example, an invoice or other payment request - and the sender's email account has been compromised, the email en route to you as the recipient may be altered. The alteration ultimately (often after some back and forth) may have different payment coordinates, luring unsuspecting 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 similar and difficult for the human eye to see the difference.



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 **before the reply is sent** that the domain of the email address that they are about to reply to has been newly created with a red alert.

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.

6. **Right Recipient™ email 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.

Alternatively, 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. 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 end can look for DKIM, SPF, or DMARC sender authentication failures. If, however, the sender sends from a lookalike or plausibly alternative email address, these will generally pass DKIM, SPF and DMARC sender authentication policies. Email security gateways at the recipient end can also look for mismatches in the header of inbound email (mismatch in the from and reply-to headers). There are, however, 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 type of attack is also known as a “Whaling” type of “Spearphishing” or a “reply-to pivot”.

7. **Fake Forward™ email detector.** Following on the Reply-Hijack, if forwarded, depending on how the email was sent and composed, once the email has been forwarded, there is no way to tell that the email came from an impostor, and the content of the email gains a sense of legitimacy. 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 employs will not protect the recipient from this type of cybercrime. Email security gateways at the recipient end can block 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. Not all recipients, however, have this enabled (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 to alert when emails from impostor senders are being forwarded on by the first recipient.

Each of these RMail technologies are layers that either add to the email security gateway systems that companies employ, do not address, or do not address well (the Outbound Email Services). 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 features are essential to support your very own Pre-Crime-measures. Frama technology, in tandem with our team of elite customer support personnel, 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 additional information and intelligence to identify of e-crimes in progress at the recipient.

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.

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.

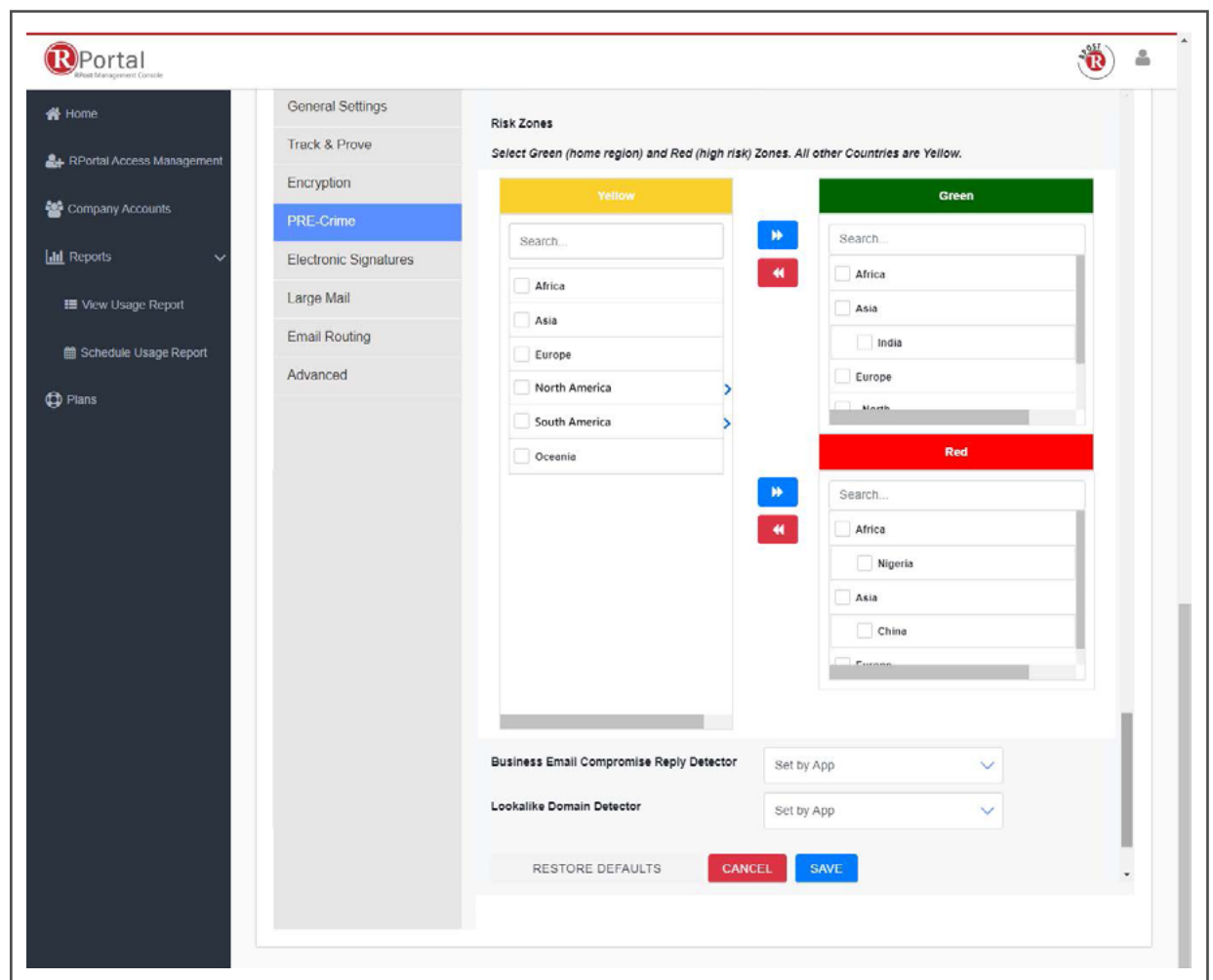
Contact us to discuss how you can get started preventing, detecting and disarming cybercrime with RMail Pre-Crime™ services.

Appendix: Technology Spotlights

Email Eavesdropping™ Alerts

Eavesdropping Alerts can be configured for administrators and senders. They provide insight into a potential cybercrime in progress at the recipient's end - before the cybercriminal cuts you (the sender) out of the communication.

There are many options for the administrator to adapt the threat thermometer and alert sensitivity. Admins can define green and red zones depending on where it would be expected/unexpected that the company's business emails are opened. By default, any country that is not manually set to green or red will be yellow. Put simply, if a company has no business whatsoever in China, they can flag the country as red and choose to be immediately notified if one of their business emails is opened in that geographic location. Admins can also choose to be notified on every open, only the first one, and more. The same configurations are available at the user level.



Admins can set the security throttle to low, medium, or high to adjust the level of sensitivity to outgoing email activities and the level and quantity of authentication techniques that the RMail system employs.

The alerts are designed to provide maximum forensic insights while also including information for “green” zone (low risk) insights about the lifecycle of your messages sent.

The Frama RMail activity report clearly indicates the security level (red, yellow or green) of the email open zone that triggered the notification, the number of opens, number of locations where your company’s email was viewed, and a world map highlighting the geographic location where the suspicious open took place.

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 such as 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 further investigate a particular message.

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 (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: A48D52862EE9862A5FDD88F336A99E2D69FEF54A

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_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/W35VC/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/W35VC/5 192.168.10.106 /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 httpc 443
Root=1-632d2601-68f7d3e527e10ac35f151b35 AMD64
```

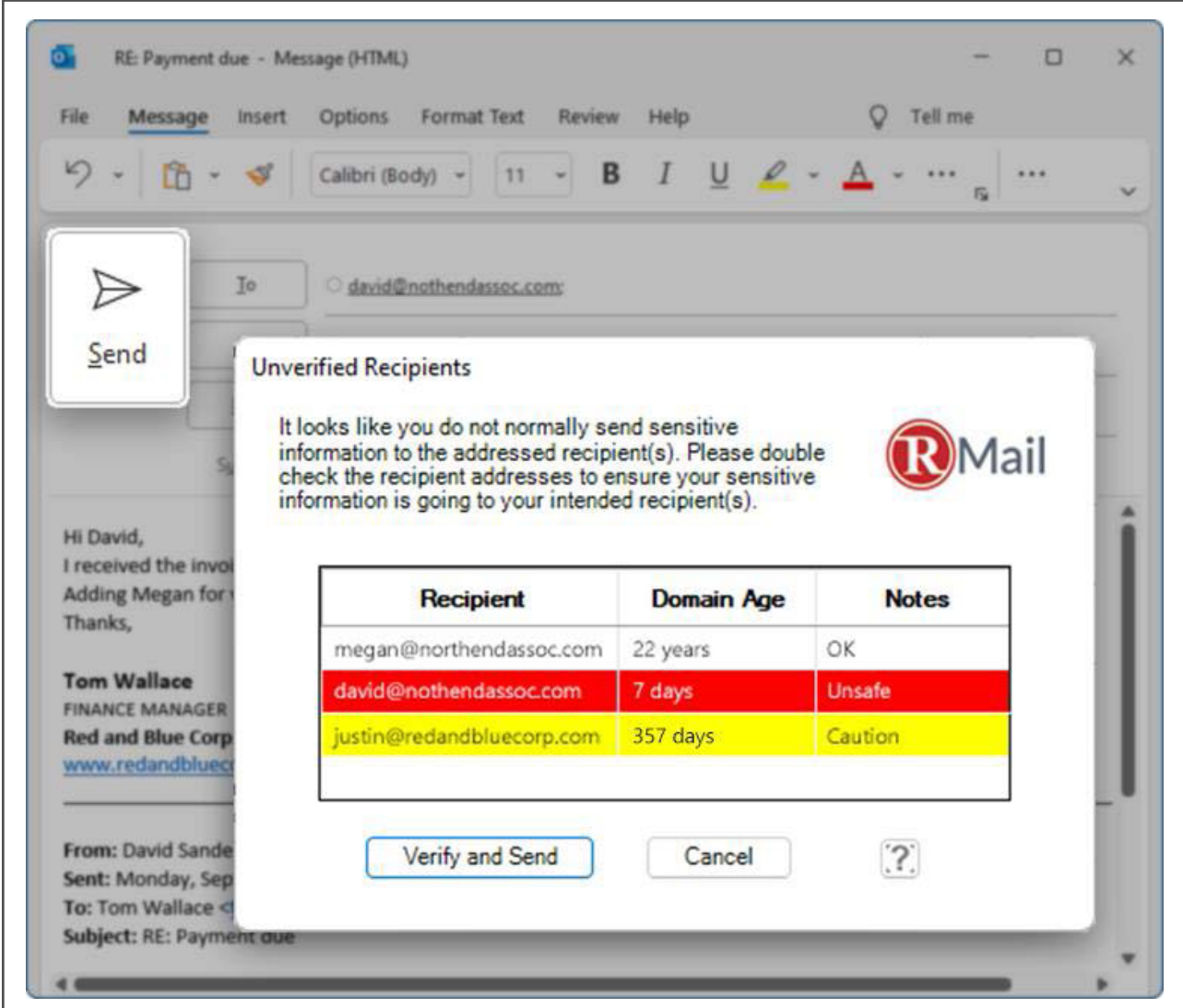
RPost patented (rpost.com/patents) including US patent applications 17663425, 63/201,857, 63/366,685, 63/366,661 and other applications.

(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.

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), 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 past 90 days or within the year).



RE: Payment due - Message (HTML)

File Message Insert Options Format Text Review Help


Calibri (Body) 11 B I U   ...

To: david@nothendassoc.com


Send

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

Verify and Send Cancel 

Hi David,
I received the invoice for
Adding Megan for
Thanks,
Tom Wallace
FINANCE MANAGER
Red and Blue Corp
www.redandbluecorp.com

From: David Sande
Sent: Monday, Sep
To: Tom Wallace
Subject: RE: Payment due

Enabling RMail Services

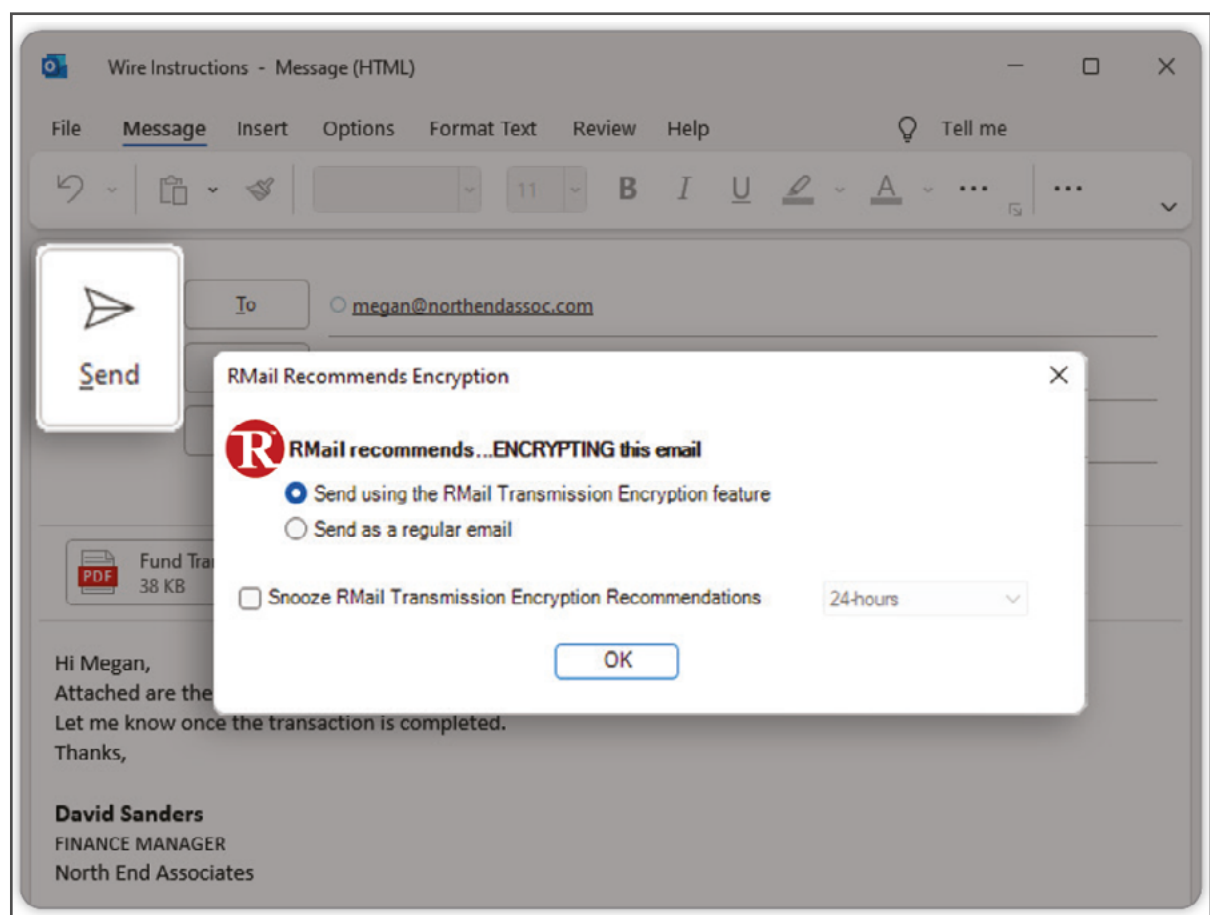
The RMail Lookalike Domain detector technology is included within RMail for Outlook. The hidden header detection occurs on all email replied or forwarded (before sent) and the domain age detector occurs on email that has been indicated to be important (by RMail AI - RMail Recommends™ or by using the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

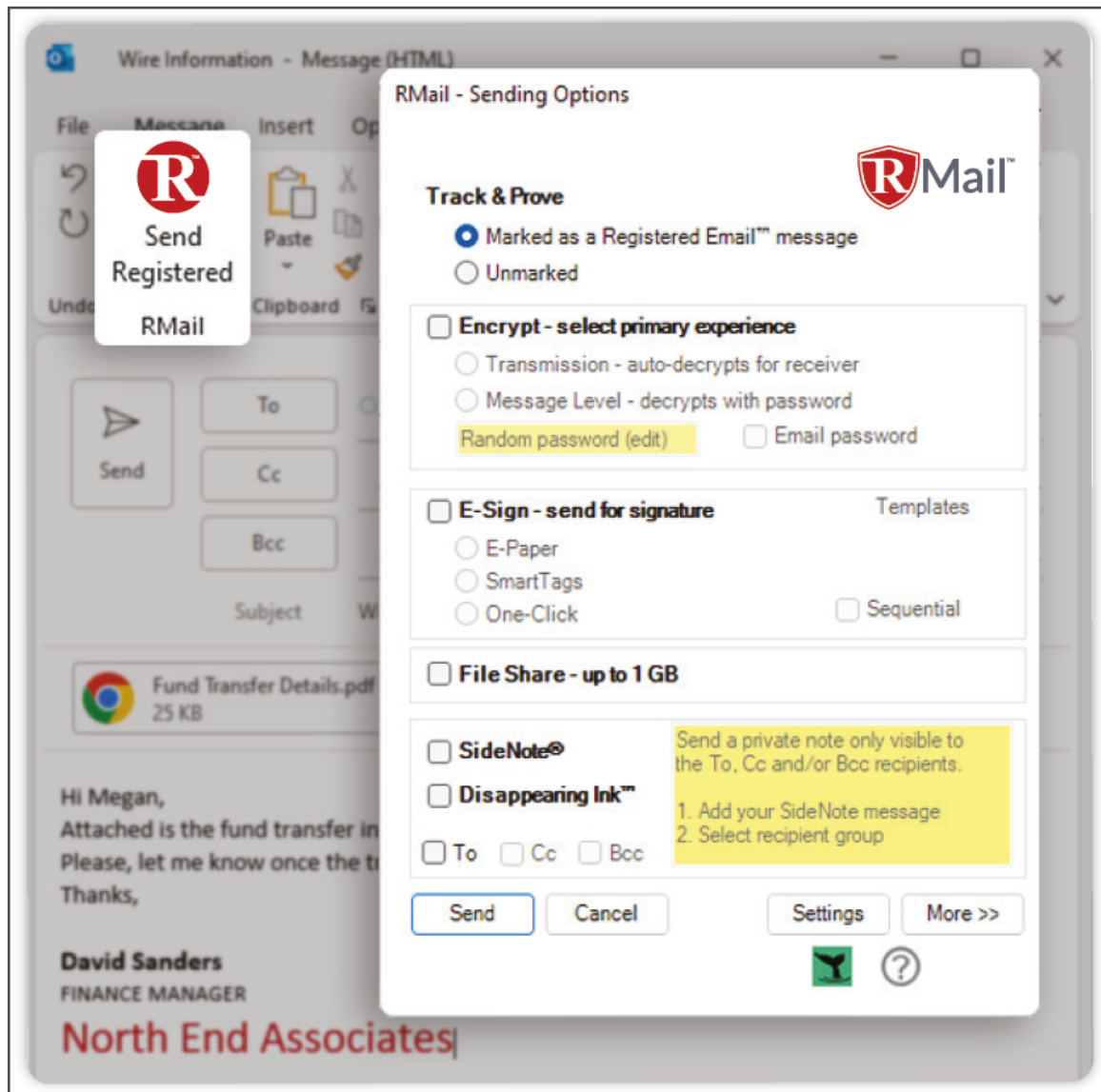
Microsoft Outlook 365

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

1. **RMail Recommends™**: AI-infused, data loss prevention service that sensitises 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.



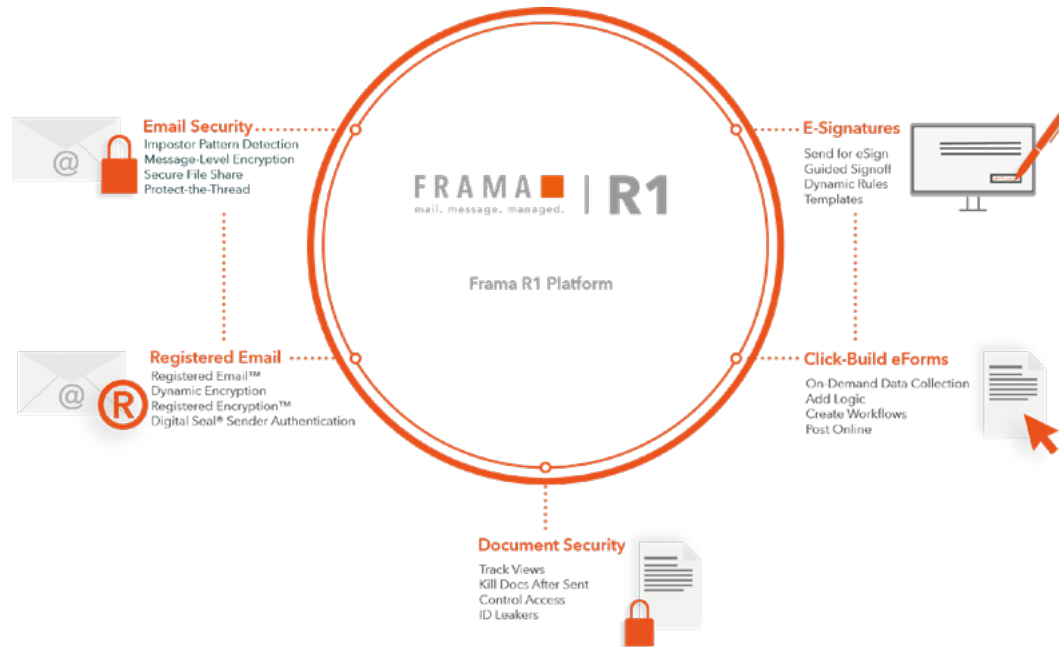
Security Gateway, Gmail, Salesforce and other apps

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

Frama 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.

About Frama Communications



mail. message. managed. - We have more than 50 years of experience in written business communication technologies.

We help companies realise their full potential in B2B and B2C document workflows and digitalisation.

Reach your customers!

Why Frama - Four reasons

Genuine customer satisfaction

We focus on individual customer needs. And unlike other technology companies, our team is always at the end of the phone.

Local presence worldwide

Wherever you are: Our sales partners are there for you worldwide!

Certified and audited quality

Our products and services meet international standards. This is guaranteed by our ISO certifications.

Individual system solutions

We listen and create exactly the solutions that move you forward. From API connections to system integrations - get in touch with us!



Frama Communications AG, a company of the Frama Group . Dorfstrasse 6 . CH-3438 Lauperswil
Offices in: Austria, Germany, Switzerland, United Kingdom
www.frama.com . Contact: www.frama.com/en-gb/contact/

integrity in communication.