RMail By RPOST

IT Admin Intelligence »

Email Security

Email Eavesdropping™ Alerts for Wire-Fraud Pre-Emption

Email Activity Report

Email Eavesdropping™ Alert

Sender: Amy@TitleCompany.com

Original Recipient : James.Realtor@RealEstateBrokers.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
01/09/2026 08:12:48	Open (VPN)	Ikeja, Lagos	Nigeria	41.67.191.255	Netcom Africa	Red
01/09/2026 17:06:22	Open	Boston, MA	USA	94.92.53.178	Verizon	Green
01/09/2026 12:54:18	Open	Boston, MA	USA	94.52.53.178	Verizon	Green

Original Message Details

Subject: WIRE INSTRUCTIONS FOR CLOSING

Original Sender: Amy@TitleCompany.com

Original Send Time: 01/09/2026 03:20:00 UTC

Transaction ID: A4BD52B62EE9862A5FDDB8F336A99E2D69FEF54A

Metadata:

[IP Address: 41.67.191.255] [Time Opened: 01/09/2026 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 X-Forwarded-For: 183.82.2.55 X-Forwarde

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 distribution network activated email content.
(VN) = 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.
(C) = risk identified based on administrator defined Custom Risk Zones configuration.
(L) = user determined to be activating content in selected higher risk language.
(D) = activity determined to be on a desktop device.
(A) = activity determined to be related to airborne or roaming network.
(VS)= activity was detected at a VPS endpoint.
(T) = activity determined to be associated with the TOR anonymization network.
(CA) = activity associated with a common attack source.
(O) = activity associated with an automated scan.
(BP) = activity detected at a bulletproof hosting endpoint.
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.
Click-View: Open detection triggered from website access □: Indicates AI Auto Lock activated.

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

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

With Email Eavesdropping™ alerts, every email sent out of the organization has every activity associated with it analyzed forensically, for a period of time. These alerts include all the email forensics so that IT security specialists can validate and take immediate action, **before the cybercriminal lures users into mis-wiring money to the criminal's bank.**