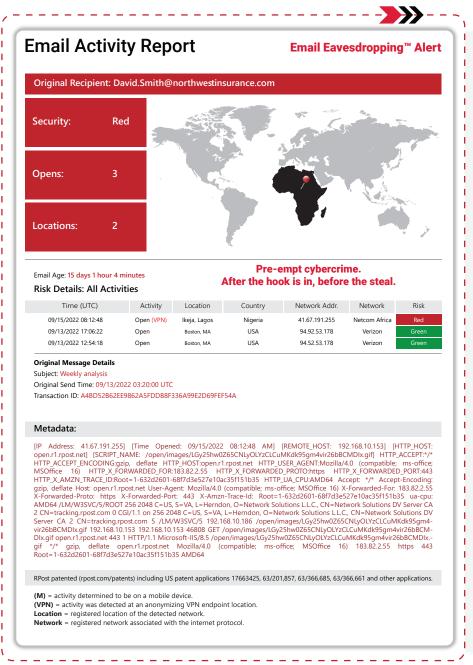


## **IT Admin Intelligence**

**Email Security** 

## **Email Eavesdropping<sup>™</sup> Alerts for Wire-Fraud Pre-Emption**



If the RMail **active threat hunting** technology identifies unusual activity patterns, RMail generates an Email Eavesdropping<sup>™</sup> 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<sup>™</sup> 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.** 

RPost patented (rpost.com/patents) including US patent applications 17304,305, 15469388, 17025955, 17659479, 16866135, 17653923, 17663425, 63/201,857, 63/366,685, 63/366,661 and other applications. RPost© Copyright 1999-2023. RPost trademarks are registered and unregistered.