INKY™

✧ Intelligent Defense Powered by INKY

INKY sees, reads, and stops email threats with unprecedented precision.

GenAI is redefining the future of email security. With billions of dollars lost each year to phishing attacks and data breaches, email security continues to be a critical concern for Managed Service Providers (MSPs) and their clients. Traditional methods of threat detection, which rely on pattern-based detection, often fall short in keeping up with the ever-evolving tactics of cybercriminals.

However, with the integration of Generative AI, INKY can now understand the meaning and intent behind every email, regardless of how cleverly it is worded or disguised. This revolutionary new capability takes email security to a whole new level.

INKY's GenAI detects an "unsubscribe" option, triggering further threat investigation.

Subject: Michel York | William Goodsell ✧

From: William Goodsell <wgoodsell@internetwebintel.com> ✧

To: <michel@polvocapital.com>

January 20th, 2025 8:40:54 AM

UNSUBSCRIBE

Caution! This message is potentially suspicious.
Graymail, First-Time Sender

Hi Michel,

I just was reviewing your company website and was impressed with your portfolio of services. How do you protect your clients' sensitive data?

We recently helped a SAAS company implement a new security framework, which galvanized their security posture and boosted client confidence.

Would you be interested in a quick chat to explore how we can strengthen your security practices?
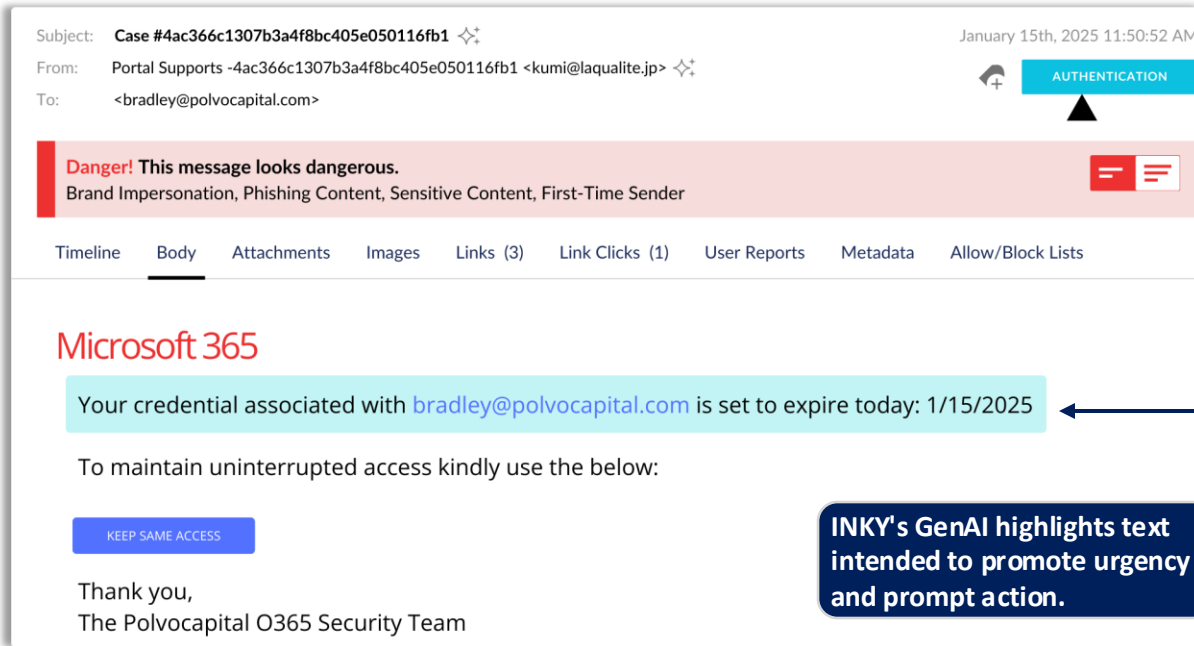
Best Regards,
William Goodsell

Cleverly disguised unsubscribe message is highlighted.

P.S. If you're not into this chat, reply with 'beans' and I'll gracefully exit!

INKY understands language like a human.

INKY's Computer Vision AI has been able to review email and understand its visual meaning for many years. Now, with Generative AI, INKY can read and understand the text of each email. INKY's deep understanding of language anticipates every way a request, threat, or scam could be worded. This capability ensures proactive, zero-day protection against phishing attacks.

INKY™

Subject: **Case #4ac366c1307b3a4f8bc405e050116fb1**

From: Portal Supports -4ac366c1307b3a4f8bc405e050116fb1 <kumi@laqualite.jp>

To: <bradley@polvocapital.com>

January 15th, 2025 11:50:52 AM

AUTHENTICATION

Danger! This message looks dangerous.
Brand Impersonation, Phishing Content, Sensitive Content, First-Time Sender

Timeline | **Body** | Attachments | Images | Links (3) | Link Clicks (1) | User Reports | Metadata | Allow/Block Lists

Microsoft 365

Your credential associated with bradley@polvocapital.com is set to expire today: 1/15/2025

To maintain uninterrupted access kindly use the below:

KEEP SAME ACCESS

Thank you,
The Polvocapital O365 Security Team

> **INKY'S GenAI detects an authentication request.**

> **INKY's GenAI highlights text intended to promote urgency and prompt action.**

Key Benefits of INKY Generative AI

Human-Level Language Understanding
INKY GenAI processes email content much like advanced chatbots, interpreting meaning and intent regardless of phrasing. This enables superior detection of zero-day attacks, thwarting even the most cleverly worded attempts to evade pattern-based detection systems.

Integrated Obfuscation Countermeasures
Combining Generative AI with INKY's existing countermeasures for cloaked text (e.g., zero font, Unicode, and homograph techniques), the platform transforms obfuscated email content into clean text for precise analysis.

Explainable Results
The INKY Dashboard highlights specific sections of an email that contribute to its assessment, giving administrators actionable insights and confidence in the AI's decision-making process.

Enhanced Graymail Detection
INKY's popular graymail filter is now even more accurate and effective, providing greater productivity and inbox organization for users.

Broad System Integration
Generative AI is infused into all aspects of INKY's platform, including the analysis of website content linked in emails and third-party cloud services.

Privacy-First Approach
INKY's Generative AI operates entirely within the company's infrastructure, ensuring that no company data or personally identifiable information (PII) is exposed to third parties.

INKY™

Seeing is believing.

GenAI optimizes the INKY Email Assistant by providing end users with specific, actionable advice. For administrators, the INKY dashboard offers a visual breakdown of what INKY GenAI detected, making it simple to track and understand email threats.

"Generative AI represents a major leap forward in email security. We think it fundamentally changes the game, making things harder for attackers, and enables us to provide our partners with the best information security protection on the market."

Dave Baggett
CEO and Founder

INKY's GenAI scans every email without exception.

Generative AI is seamlessly integrated into every step of our email analysis pipeline. When enabled, it analyzes 100% of incoming emails that pass initial reputational and spam checks. This is in stark contrast to the practices of other email security vendors who only analyze a fraction of the emails entrusted to their care. INKY's thorough approach ensures that no threat goes undetected. Additionally, our system can convert obfuscated email content into clean text, making it easier to analyze and understand the true intent of the sender.

INKY EMAIL SECURITY PLATFORM

Standard

Inbound Email Protection
Internal Email Protection
NextGen AI Detection
Advanced Computer Vision
QR Code Defense
Anomaly Detection
Standard Attachment Analysis
URL Time-of-Click Protection
Geo-Blocking
Spam Filtering

Pro

Everything in Standard plus:
GenAI Intent Analysis
Zero-Day Malware Protection
Advanced Attachment Analysis
Advanced Graymail Detection
Customer Graymail Delivery-Locations
End User-Managed Graymail
DMARC Monitoring

Advanced

Everything in Pro Plus:
Outbound DLP Detection
Custom Outbound Rules Engine
Advanced Approval Workflows
Encryption Portal

Add On Products:

Security Awareness Training

Email Signatures

Archiving