Cloud Email Security

Google Workspace

Microsoft 365

Microsoft Exchange (Online)

On-premises Email Security

Microsoft Exchange (On-premises)

Why CELLOPOINT

"Secure Your Email" is our mission and the driving force behind Cellopoint's commitment to combating cybercriminals and corporate espionage worldwide.

Statistics show that 85% of organizations are targeted by new forms of phishing emails, ransomware, and BEC scams. These advanced threats have shifted from large-scale attacks to targeted ones, designed to breach existing defenses.

In response to these new types of threats, Cellopoint employs cutting-edge artificial intelligence (AI), machine learning (ML), and deep learning (DL) algorithms to analyze the behavior, intentions, and patterns of attackers. This effectively distinguishes genuine emails from deceptive attacks, which is a key reason to choose Cellopoint.

Rated 4.7 on Gartner Peer Insights

Gartner peerinsights™

Cellopoint Reviews 4.7 ★★★★★

Three Email Threats That CIOs/CISOs Must Not Ignore

Phishing

Ransomware

Business Email Compromise

CELLOPOINT
Secure Your Email

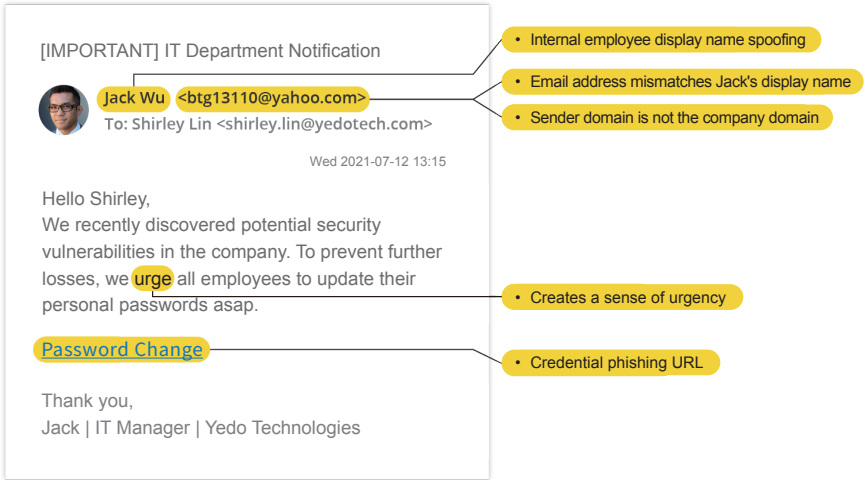
Cellopoint is a leader in next-generation email security solutions, using AI-based technology to protect users against advanced email attacks such as phishing, ransomware, and BEC scams.

Contact Us +886-2-89692558 | sales@cellopoint.com

Top 3 Email Attacks

AI based Email Security

1 Phishing



[IMPORTANT] IT Department Notification

Jack Wu <btg13110@yahoo.com>
To: Shirley Lin <shirley.lin@yedotech.com>

Wed 2021-07-12 13:15

Hello Shirley,
We recently discovered potential security vulnerabilities in the company. To prevent further losses, we urge all employees to update their personal passwords asap.

Password Change

Thank you,
Jack | IT Manager | Yedo Technologies

- Internal employee display name spoofing
- Email address mismatches Jack's display name
- Sender domain is not the company domain
- Creates a sense of urgency
- Credential phishing URL

Phishing attacks use social engineering techniques to lure recipients into clicking on phishing URLs, aiming to steal their account credentials, passwords, credit card information, or personal data. Phishing attacks may also contain malicious URLs designed to deceive recipients into triggering drive-by downloads that execute malware.

Cellopoint's phishing solution provides the following detection and protection mechanisms to block spear-phishing, credential phishing, and whaling attacks:

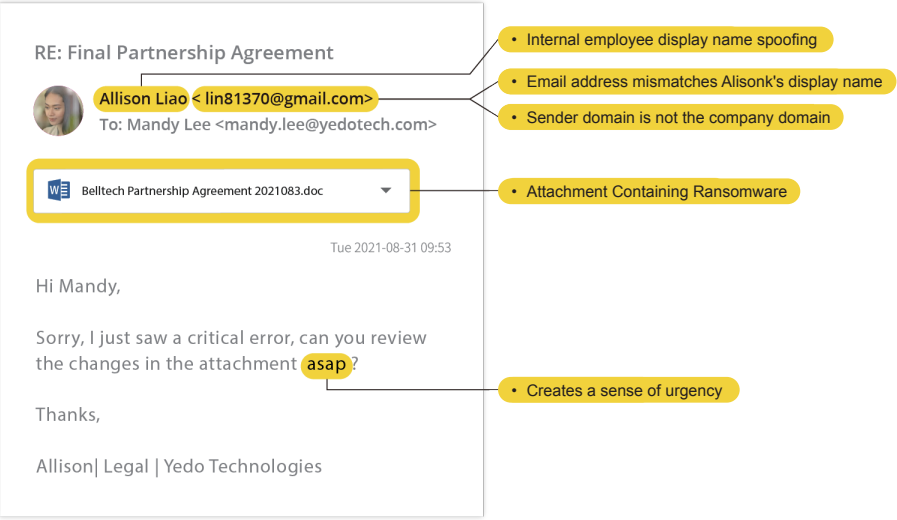
- Pre-click comparison with 100 types of URL threat intelligence.
- URL rewriting and real-time Time of Click (TOC) scanning.
- Retroactive scanning.
- Detection of URLs embedded in Microsoft Office files, PDFs, and ZIP archives.

2 Ransomware

Ransomware is a type of malware primarily spread through emails containing malicious attachments or URLs. Once ransomware is downloaded, the victim's computer system may be locked or files encrypted. To regain control of the system or obtain the decryption key, victims are often forced to pay a substantial ransom.

Cellopoint's ransomware solution provides the following detection and protection mechanisms to block ransomware attacks:

- Static code analysis.
- Detection of compressed files (e.g., ZIP, TAR, TBZ, TGZ, LZH, JAR, etc.)
- Detection of encrypted attachments.
- Detailed malware forensic reports.



RE: Final Partnership Agreement

Allison Liao < lin81370@gmail.com>
To: Mandy Lee <mandy.lee@yedotech.com>

Belltech Partnership Agreement 2021083.doc

Tue 2021-08-31 09:53

Hi Mandy,

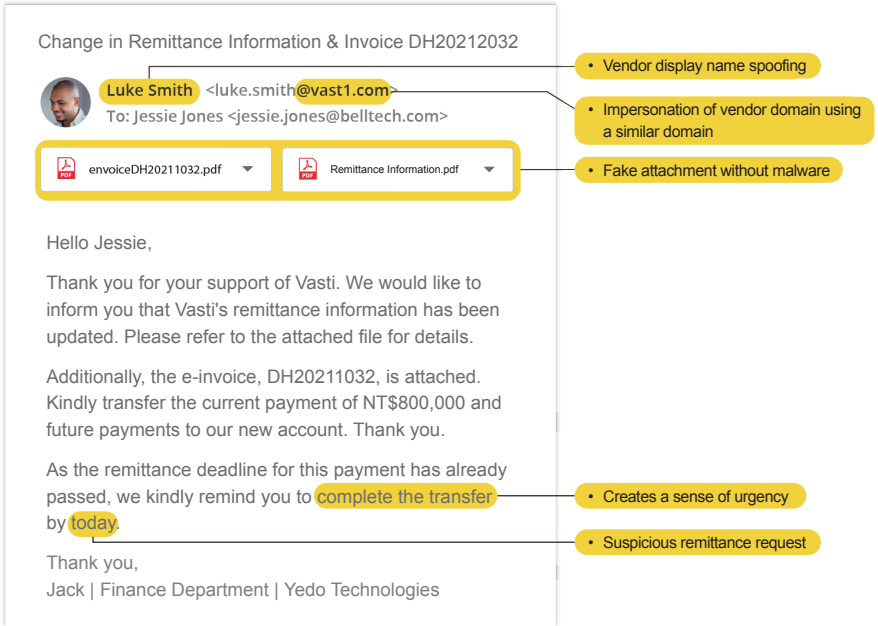
Sorry, I just saw a critical error, can you review the changes in the attachment asap?

Thanks,

Allison| Legal | Yedo Technologies

- Internal employee display name spoofing
- Email address mismatches Alisonk's display name
- Sender domain is not the company domain
- Attachment Containing Ransomware
- Creates a sense of urgency

3



Change in Remittance Information & Invoice DH20212032

Luke Smith <luke.smith@vast1.com>
To: Jessie Jones <jessie.jones@belltech.com>

envoiceDH20211032.pdf

Remittance Information.pdf

Hello Jessie,

Thank you for your support of Vasti. We would like to inform you that Vasti's remittance information has been updated. Please refer to the attached file for details.

Additionally, the e-invoice, DH20211032, is attached. Kindly transfer the current payment of NT$800,000 and future payments to our new account. Thank you.

As the remittance deadline for this payment has already passed, we kindly remind you to complete the transfer by today.

Thank you,
Jack | Finance Department | Yedo Technologies

- Vendor display name spoofing
- Impersonation of vendor domain using a similar domain
- Fake attachment without malware
- Creates a sense of urgency
- Suspicious remittance request

Business Email Compromise (BEC)

Business Email Compromise (BEC) is a type of email fraud that involves impersonating internal employees, executives, or external vendors to trick employees into making wire transfers or disclosing confidential information.

Cellopoint's BEC solution provides the following detection and protection mechanisms to block BEC attacks:

- DMARC authentication checks.
- Display name spoofing and cousin domain detection.
- Sender behavior modeling: Analyzing communication patterns between the sender and recipient to detect anomalous messages.
- Email content and intent analysis: Detecting specifically suspicious keywords in the email subject and body, such as "wire transfer", "urgent", or "request".

Next-generation AI-based Email Security

Cellopoint has launched a next-generation email security solution that utilizes artificial intelligence and machine learning algorithms to analyze cybercriminals' behavior, intentions, and patterns. By combining Cellopoint's global email threat intelligence, it can effectively analyze targeted attacks while blocking large-scale virus attacks in real time.

For Microsoft 365 cloud email, the solution integrates seamlessly through the Graph API without requiring changes to MX records or user habits, enhancing Microsoft email security effortlessly.

Additionally, the all-in-one email security platform provides outbound email DLP, email encryption, and email archiving, allowing you to effectively manage three critical issues: email threat protection, prevention against email data breaches, and compliance with regulations regarding the preservation of digital email assets.

All-in-one Solution:

Security					DLP		Archiving			Signature
Anti-Spam	Anti-Virus	Anti-APT	Anti-APT	Anti-BEC	Audit	Encryption	Archive	Grid Search	Case Management	
SPAM		URL	File	BEC						
AG	AV	URL	File	BEC	AUD	ENC	MA	GDS	CAS	SIG

CelloOS™

Azure, AWS, GCP / VMware, Hyper-V / x86 server, Appliance