



Presentación

El Lado Oscuro del Correo Electrónico





EMAIL SECURITY

**El Lado Oscuro del Correo Electrónico:
Proteja sus Correos Electrónicos con
Seguridad Impulsada por AI**

El Panorama del Correo Electrónico

El número de correos electrónicos enviados y recibidos a nivel mundial ha aumentado cada año desde 2017¹

El correo electrónico es el vector de ataque más importante que los atacantes explotan para obtener acceso a empresas e individuos²

Trabajar desde la casa ha aumentado en más del 55%³ en los últimos años y, como resultado, las amenazas de seguridad cibernética también han aumentado específicamente a través de los correos electrónicos a una tasa del 32% interanual⁴

65% de las empresas globalmente se enfrento a un ataque de compromiso de correo electrónico empresarial en 2020⁵

El 91 % de todos los ataques dirigidos comienzan con el correo electrónico⁶

1- Statista

2- Information Age

3- The economist

4- IT pro

5- Kaseya

6- Knowbe4

Algunos Desafíos de las Empresas

Independientemente del tamaño de la empresa, todas las organizaciones enfrentan problemas de seguridad de correo electrónico

- ❖ Las empresas en industrias altamente reguladas (seguros, finanzas, atención médica) deben enviar miles de correos electrónicos cifrados con datos confidenciales a sus clientes a diario. Sin embargo, los destinatarios no abren la mayoría de esos correos electrónicos debido a la complejidad de las soluciones de cifrado actuales.
- ❖ Las empresas tienen recursos de TI y seguridad cibernética muy limitados. Se enfrentan a muchas prioridades en competencia y luchan por administrar muchos proveedores diferentes, por lo que a menudo quedan vulnerables.
- ❖ La seguridad del correo electrónico es una parte esencial de cualquier infraestructura empresarial. Sin embargo, para obtener una solución de seguridad holística, a menudo una organización necesita hasta 3 proveedores diferentes o más, lo que los deja con seguridad inadecuada o con demandas administrativas adicionales.

Compromiso de correo electrónico

¿Qué es un ataque BEC?

- ✉ Los ataques de compromiso de correo electrónico empresarial (BEC) son una forma de delito cibernético que utiliza el fraude por correo electrónico para atacar a las organizaciones para lograr un resultado específico que afecta negativamente a la organización objetivo.
- ✉ Un ataque BEC comienza con un ciberdelincuente que piratea y falsifica correos electrónicos para hacerse pasar por los supervisores, el CEO o los proveedores de su empresa.
- ✉ Los ciberdelincuentes utilizarán estas técnicas para filtrar datos confidenciales de PII, interceptar transferencias bancarias y robar credenciales.

Compromiso de correo electrónico

¿Cómo ocurre un ataque BEC?



¿Qué aspecto tiene un ataque BEC?

Suspended account

PayPal Support <service@login-paypal.com>
To: Zack Schwartz

Reply Reply All Forward

Tue 10/23/2018 2:15

We could not verify the identity of the sender. Click here to learn more.

Confirm Your Identity

Your account has been suspended due malicious activity, please confirm your identity to recover your account and secure it with Paypal

Confirm My Identity

Pay With Confidence

Threat Detection

Malicious

- The sender is not authorized to use this domain and appears to be spoofed.
- No malicious links detected.
- No attachments to scan.

I trust this email ✓
confirm Malicious ✓
Show analysis ✓

Trustifi

Ataques de Phishing



El 91% de las violaciones de datos exitosas comienzan con un solo correo electrónico de phishing



Office 365 es la plataforma número uno dirigida con campañas de phishing, con estafas comunes en torno a páginas de destino y facturas falsas.



Los atacantes monitorearán su tráfico en tiempo real, identificando cuándo es más alto el tráfico y es más probable que un empleado responda a un correo electrónico de phishing porque está ocupado.

The screenshot shows an email from Maor Dahan to Zack Schwartz. A blue warning banner from Inbound Shield™ states: "Inbound Shield™ has detected suspicious elements in this email. You are advised to be cautious when clicking on links or opening attachments." Below the banner are buttons for "I trust this email" and "Report as malicious". The email body contains a request for an Amazon Gift card. On the right, a "Threat Detection" sidebar shows a "Suspicious" classification with a warning icon. The detection details include: "The message has been classified as a potential Business Email Compromise attack by the AI.", "No malicious links detected.", and "No attachments to scan." Below this, a "Headers" section lists verification status for DKIM, SPF, DMARC, ARC, and CompAuth, all with green checkmarks. The message ID is CAHOBFxW-D2hzEaYFNlv3sQa1ZOz5EQIT-E0h...@mail.ema.

Ataques Previos al Vishing

- ✉ Los ataques previos a Vishing solicitan al destinatario que llame al número proporcionado para proporcionar a la persona información personal o confidencial.
- ✉ Es posible que el correo electrónico en sí no tenga contenido malicioso incrustado, pero cuando el usuario llama al número, cree que es seguro porque hizo la llamada.

Example #3 – Pre-Vishing Attack

Subject: Payment Successfully Updated

🚩 Phishing 🚩 Phishing Metrics

Threats detected (Pre-Voice Phishing)

Summary

- 👤 The message has been classified as a potential Pre-Vishing attack.
- 🔗 No malicious links detected.
- 📎 No malicious attachments detected.

Trustifi proprietary metrics identified the email's goal as Vishing (phishing by phone call) and quarantined the email. The email was flagged as malicious, despite having no obvious malicious payload (links/files).

||GEEK||SQUAD||

Renewal Notice

Renewal Amount: \$ 615.97

Thank You For Renewing Family-PC Protection Plan. Your Account is set for Auto Renewal so we have Auto Renewed Your Account. And from today onward you can enjoy More Amazing Features This Transaction Will Appear on your Next Statement For More Please Login to client Area.

(Please keep a copy of this receipt for your records.)

Amount: \$ 615.97

Subscription Details: 4 Users total Protection Antivirus 3TB-Cloud

Payment Mode: Online

Unless otherwise noted by the product or offer, any Products/Services purchased on the Geek Squad Store is eligible for refund within 48 Hours of purchase. For More see our refund policy for details.

For Return Refund or upgrade in current plan Please Call Help Desk

[+ 1 888 849 4492](tel:+18888494492)

Best Regards

Jennifer M Help Desk Team

Adquisición de Cuentas

- ✉ Los ataques de adquisición de cuentas han aumentado un 307% desde el inicio de la pandemia
- ✉ Los ataques de adquisición de cuentas solicitarán al usuario que proporcione sus credenciales a un enlace malicioso. Una vez completado, el actor malicioso cambiará su contraseña bloqueando el acceso del usuario a su cuenta.

Suspended account

PayPal Support <service@login-paypal.com>
To: Zack Schwartz

We could not verify the identity of the sender. Click here to learn more.

Confirm Your Identity

Your account has been suspended due malicious activity, please confirm your identity to recover your account and secure it with Paypal

Confirm My Identity

Pay With Confidence

Trustifi

Threat Intelligence

Malicious

The sender is suspicious and appears to be spoofing

No malicious links detected

No attachments to scan

I trust this email

confirm Malicious

Show analysis

Ataque de Fuente Cero



El ataque de fuente cero implica insertar palabras ocultas con un tamaño de fuente de cero que es invisible para el destinatario.

Self-Service: Release Messages

Malicious | This email is quarantined | Mailbox: `alice@trustifitest.com`

Summary

- The message has been classified as a ZeroFont phishing attack.
- A link has been flagged by multiple anti-malware engines.
- No malicious attachments detected.

Email Actions

Release | Trust Links | Set Category | Set not handled

Sender Actions

Allowlist | Blocklist | Authenticate

Message Analysis **ZeroFont**

Sender Identities

Sender	emdr@trustifsimulation.com	✓
Relationship	0%	?
Reply To	emdr@trustifsimulation.com	✓
Return Path	emdr@trustifsimulation.com	✓
Message ID	166686210523.37776.738831572583997974.2.emdr@trustifsimulation.com	✓
MTA Domain	sgmmsa23.alpha-prm.jp	✓
IP Addresses	157.205.202.218, 60.113.238.1, 157.205.203.52	✗

AI Confidence

AI Decision	Internal Metrics Decision	?
- BEC AI	26%	
- Spam AI	26%	
- Graymail AI	13%	

Authentication Standards

SPF	Validated client identified.	✓
ARC	No ARC chain to validate.	!
DKIM	Message was not signed.	!
DMARC	Message passed the authentication.	✓
CompAuth	Message passed explicit authentication.	✓
TLS	The message passed between 11 servers. 8 of them exposed the message in plain-text.	✗

Links Analysis (1) **Multi-Engine Links**

Name: Review My Messages

URL: `https://jgcmumbai.in/htali/ht.php`

Malware Type: HTML/PhishingKit

Attachments Analysis ✓

No attachments in email

Email Content

NOTE: Email content is not fully displayed here since some elements are missing from this view, like CSS. To view the original email content you can [download the EML file](#).

From: Microsoft Activation (emdr@trustifsimulation.com)
To: alice@trustifitest.com
Subject: Self-Service: Release Messages

Self-Service: Release Messages

Microsoft

Hello

Here's your 9AM email review for Monday, August 15th. **3 messages** were held since your last review **1 day ago**.

[Review My Messages](#)

Contact your email administrator if you have any questions about this service.

Personificación de Marca



La personificación de marca es un ataque que se hace pasar por una empresa de confianza o una marca para engañar a las víctimas para que respondan y divulguen información personal o confidencial.

Password Expiration Notice

Malicious | This email is quarantined | Mailbox: alice@trustfittest.com

Summary

- Perhaps the sender is impersonating a known brand. If you trust this sender then click on "Allowlist"
- Brand:** Microsoft
- A link has been flagged by multiple anti-malware engines.
- No malicious attachments detected.

Email Actions

Release Trust Links

Set Category Set not handled

Sender Actions

Allowlist Blocklist

Authenticate

Message Analysis **Brand Impersonation**

Sender Identities

Sender	emdr@trustfittestsimulation.com	✓
Relationship	0%	ⓘ
Reply To	emdr@trustfittestsimulation.com	✓
Return Path	emdr@trustfittestsimulation.com	✓
Message ID	acJnBG-NKNtrWifAHQifluKTHKSybkuHIHCib ea4K6kHZMONEqtJ4erxqQJlz1x2EqXc3_M 8DZkOmOhpMMjDDVVqSCUDACKSI3yrRY=@t rustfittestsimulation.com	✓
MTA Domain	mail-4027.trustfittestsimulation.com	✓
IP Addresses	185.70.40.27	✓

AI Confidence

AI Decision Tagged By Microsoft ⓘ

- BEC AI 47%
- Spam AI 38%
- Graymail AI 60%

Authentication Standards

SPF	Validated client identified.	✓
ARC	No ARC chain to validate.	ⓘ
DKIM	Message is verified.	✓
DMARC	Message passed the authentication.	✓
CompAuth	Message passed explicit authentication.	✓
TLS	The message passed between 3 servers.	✓

Links Analysis (1) **Multi-Engine Links**

Name: <https://jgcmumbai.in/htali/ht.php>

URL: <https://jgcmumbai.in/htali/ht.php>

Malware Type: HTML/PhishingKit

Attachments Analysis ✓

No attachments in email

Email Content

NOTE: Email content is not fully displayed here since some elements are missing from this view, like CSS and JS. To view the original email content you can [download the EML file](#).

From: Microsoft (emdr@trustfittestsimulation.com)
To: alice@trustfittest.com
Subject: Password Expiration Notice

Hi,

Please update your password before our ISO27001 review via the following link: <https://jgcmumbai.in/htali/ht.php>

Trustfittest.com - Service Support

¿Qué se puede hacer para prevenir un ataque BEC?



Desarrollar una estrategia sólida de prevención de pérdida de datos



Cree una defensa de entrada en capas utilizando herramientas de IA / ML para detectar ataques sin archivos o enlaces maliciosos



Analizar datos para comprender mejor si una cuenta se ha visto comprometida por un ataque BEC



Capacitar a los empleados sobre las mejores prácticas al usar el correo electrónico corporativo



technologies

2023
CELAES
Congreso Latinoamericano
de Seguridad Bancaria

Why Isn't O365 Secure?

**Almost 50% of
organizations use third
party security tools with
Office 365. Why?**

- ✔ Deployment can be complex, and many of O365's best security features are not configured by default
- ✔ Email is the most common attack vector; but O365 on it's own has a lack of advanced email security controls
- ✔ Skills gap: there is a lot of O365 features and functionality that is complex, and many admins do not configure it
- ✔ O365 is very accessible to cybercriminals: you can very easily grab a domain and test out phishing campaigns on the cheap

La seguridad del correo electrónico de Microsoft carece de



Guía de mercado de Gartner

Para la seguridad del correo electrónico

"La capacidad de seguridad de correo electrónico predeterminada de Microsoft (Protección de Intercambio En línea (EOP)) carece de capacidades avanzadas de protección contra phishing y otras amenazas. ...

"La ausencia de una capa adicional de protección, sistemas de correo electrónico heredados o puertas de enlace de correo electrónico seguras a menudo no pueden evitar ataques sofisticados de ingeniería social y correos electrónicos maliciosos".

O365 users are targeted with phishing in email and instant messaging

Phishing Attacks

27%

O365 accounts are compromised and used in high-level scams

Account Takeover

20%

O365 users are at risk of data loss and exfiltration

Data Loss & Exfiltration

39%

La Solución---AI & ML

Correos de salida:

- ✓ Cifrado de correo electrónico y autenticación multifactor de destinatarios
- ✓ Prevención de pérdida de datos y exfiltración de datos por correo electrónico
- ✓ Cumplimiento™ con un solo clic

Correos de entrada:

- ✓ Motores de IA para mantener limpia la bandeja de entrada
- ✓ Protección avanzada contra amenazas
- ✓ Protección contra Phishing y BEC
- ✓ Detenga el SPAM y el correo gris

Detección de compromiso de cuenta:

- ✓ Identifique instantáneamente las cuentas que se han visto comprometidas
- ✓ Bloquea automáticamente el acceso a cuentas comprometidas

Indexación inteligente Archivado en la nube:

- ✓ Comparta fácilmente datos, casos y consultas con destinatarios específicos
- ✓ Autenticación inteligente y acceso de monitoreo en tiempo real

Resumen

Dolor

El 91 % de todos los ciberataques dirigidos comienzan con el correo electrónico¹. Las grandes empresas estadounidenses **pierden en promedio \$ 14.8M anualmente por ataques de phishing**². El costo promedio de la violación de datos **en 2021 fue de \$ 4.2M con un aumento anual del 10%**³.

Problema

Los SEG heredados son difíciles de implementar, administrar y no pueden abordar los ataques más sofisticados y avanzados que se utilizan. Los hackers están utilizando herramientas y estrategias de vanguardia para eludir las soluciones existentes, como Phishing, Pre-Vishing, Zero Font Attacks, BEC, Ransomware, Malware y están comprometiendo a terceros previamente aprobados y monitorearán su tráfico esperando el momento adecuado para cambiar la información bancaria o interceptar el tráfico.

Solución

Utilizando una solución avanzada de seguridad de correo electrónico que está diseñada para defenderse contra los ataques modernos y monitorea todos los aspectos de su tráfico de correo electrónico. Capacitación continua de concientización sobre seguridad que mantiene a su personal actualizado sobre los tipos de ataques más recientes.



PREGUNTAS

&

RESPUESTAS



IG TECHNOLOGIES

Simplifying Cybersecurity Solutions

Gracias



technologies