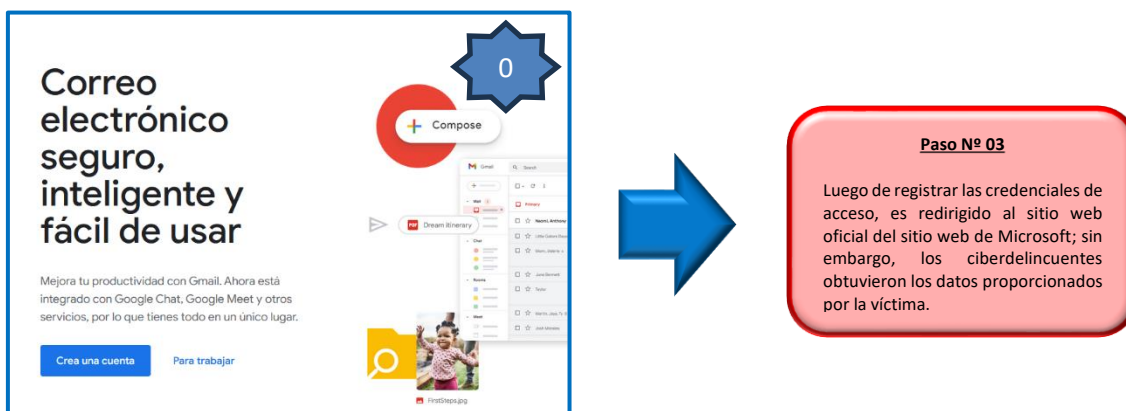
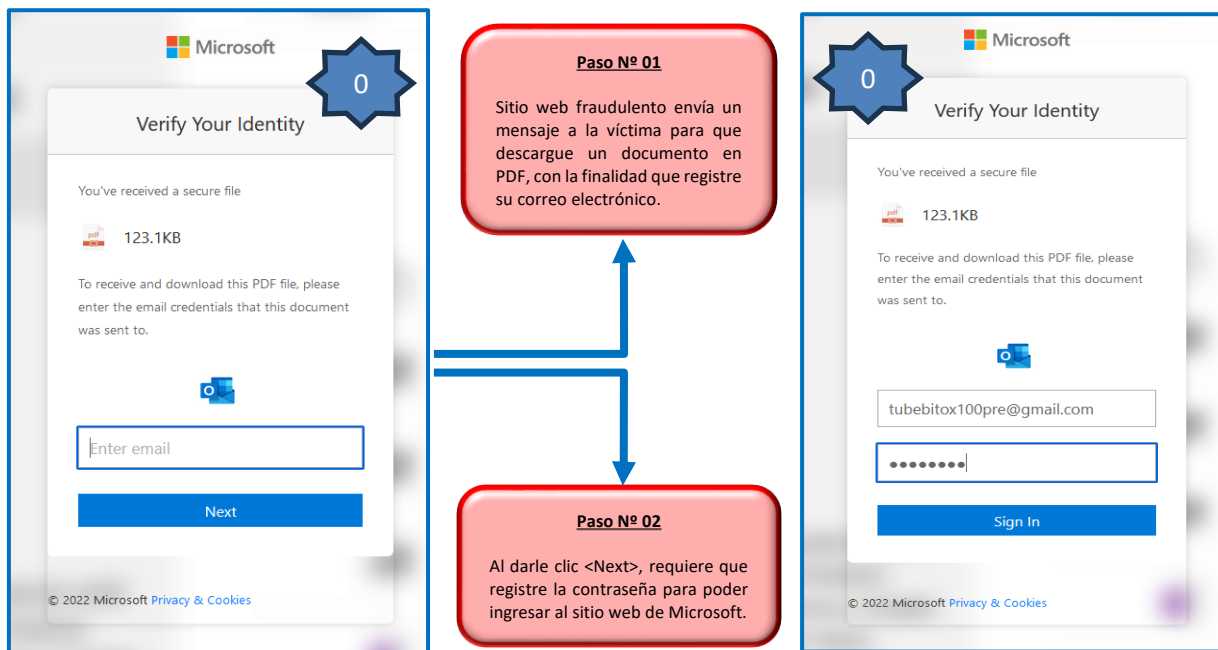
	<b>ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°234</b>		<b>Fecha: 04-10-2023</b>
			<b>Página: 10 de 13</b>
Componente que reporta	<b>DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ</b>		
Nombre de la alerta	Nueva campaña de Phishing que suplanta la identidad de Outlook		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

**Descripción**

**1. ANTECEDENTES:**

A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes se encuentran desarrollando una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad del sitio oficial de "Outlook"; con el objetivo de acceder u obtener credenciales de inicio de sesión de las posibles víctimas.

**2. DETALLES:**



A. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD**:

a) **Indicadores de compromisos:**

I. **URL:** <https://www.portaldelaestancia.com/wp-content/uploads/2023/rshMicro365/officeonline/cgi-bin/1/>



Site	<a href="https://www.portaldelaestancia.com">https://www.portaldelaestancia.com</a>
Netblock Owner	GoDaddy.com, LLC
Hosting company	GoDaddy
Hosting country	US

II. **SHA-256:** f6d10687c66251584a4efbc9cf07eec1b04701a8d686774b14a1b5cb12293af4



RecoveryStore__F9581B99-62B6-11EE-9D5F-0800277F2901_dat f2f90adeae5a7fe96c7d73d59b215e908defdf0b84b56fbbf3bd4d59aa98755f	sospechoso
arranque.min.js 56c12a125b021d21a69e61d7190cefa168d6c28ce715265ceal3b0112d169c4	ninguna amenaza especifica
RecoveryStore__88B090CO-D917-11E7-B67B-080027A49DD6_dat e5156152b1188a94f6f96a6b79b120f2ef9fad7058280cb261b9dbc6727354	sospechoso

III. **IP:** 107[.]180[.]44[.]125



IP range	Country	Name	Description
::ffff:0:0:0:0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
↳ 107.0.0.0-107.255.255.255	United States	NET107	American Registry for Internet Numbers
↳ 107.180.0.0-107.180.127.255	United States	GO-DADDY-COM-LLC	GoDaddy.com, LLC
↳ 107.180.44.125	United States	GO-DADDY-COM-LLC	GoDaddy.com, LLC

IV. **DOMINIO:** portaldelaestancia[.]com



Domain	<a href="https://www.portaldelaestancia.com">portaldelaestancia.com</a>
Nameserver	ns13.domaincontrol.com
Domain registrar	Unknown
Nameserver organisation	whois.wildwestdomains.com

B. **Otras detecciones:**

**MALICIOSO**

[https://www.portaldelaestancia...](https://www.portaldelaestancia.com)

Analizado en: 04/10/2023 15:04:55 (...)


Ambiente: Windows 7 de 32 bits

Puntuación de amenaza: 100/100

Detección AV: 7% Sitio de phishing

Indicadores: 1 2 11

Red:





**malicioso**

Puntuación de amenaza: 100/100

Detección AV: 60%

**#suplantación de identidad**

**C. Cómo funciona el Phishing:**

- Los correos electrónicos incluyen enlaces a sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
- Medios de propagación del Phishing: WhatsApp, Telegram, redes sociales, SMS entre otros.
- Los ciberdelincuentes intentan suplantar a una entidad legítima (organismo público o privado, entidad financiera, servicio técnico, etc.)

**D. Referencia:**

- Phishing o suplantación de identidad: Es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.

**3. RECOMENDACIONES:**

- Evitar acceder a enlaces que llegan inesperadamente por correo electrónico u otros medios.
- No proporcionar datos personales (contraseñas, tarjetas, cuentas bancarias, etc.) por correo, teléfono o SMS.
- No introducir datos confidenciales en sitios web sospechosas o de dudosa procedencia.
- Verificar la fuente de información de tus correos entrantes.
- Introducir tus datos únicamente en webs seguras.
- Tener siempre actualizado el sistema operativo y el antivirus. En el caso del antivirus, comprobar que está activo.

Fuente de Información:

Análisis propio de redes sociales y fuente abierta.