Nro. Alerta:	AL-2026-004	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **Aviso de seguridad**	ecucert
TLP:	TLP:CLEAR		
Fecha:	30-ene-2026	**Campaña de Phishing mediante suplantación de identidad de Microsoft**	V 1.1

I. DATOS GENERALES:

Clase de alerta: Phishing.

Tipo de incidente: Suplantación de identidad.

Nivel de riesgo: Alto

II. INTRODUCCIÓN

El fraude mediante correo electrónico, comúnmente asociado a técnicas de *phishing*, consiste en el envío de mensajes electrónicos que suplantan la identidad de entidades legítimas e incorporan URLs maliciosas. Dichos enlaces redirigen a sitios web fraudulentos diseñados para capturar credenciales de autenticación, información sensible o ejecutar código malicioso, comprometiendo la confidencialidad, integridad y disponibilidad de los sistemas de información de los usuarios afectados.

III. VECTOR DE ATAQUE:

- El usuario recibe un correo electrónico fraudulento, alertando sobre un problema, verificación urgente de su cuenta o actualización de datos.
- El mensaje incluye un enlace con una URL engañosa que no pertenece a un dominio oficial.
- Al hacer clic, el enlace redirige a un portal de inicio de sesión falso que imita visualmente el sitio legítimo de Microsoft.
- El usuario ingresa sus credenciales, las cuales son capturadas inmediatamente por el atacante.
- Posteriormente, la página solicita una falsa verificación adicional (por ejemplo, tomarse una foto) y queda detenida, mientras el robo de credenciales ya se ha concretado.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

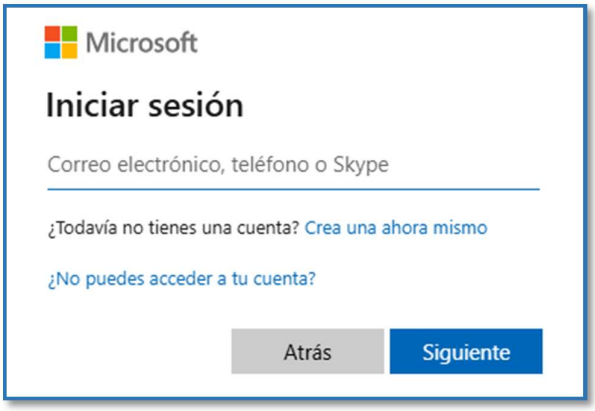
Nro. Alerta:	AL-2026-004	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **Aviso de seguridad**	ecucert
TLP:	TLP:CLEAR		
Fecha:	30-ene-2026	**Campaña de Phishing mediante suplantación de identidad de Microsoft**	V 1.1

- **MODUS OPERANDI**

CASO 1

- Llega un correo fraudulento donde se menciona que la cuenta podría estar vinculada a un dispositivo diferente y que se debe ingresar en el enlace.

- A continuación, aparece un portal que visiblemente parece oficial de Microsoft, pero no lo es, se solicita el ingreso de un usuario y una contraseña.



- Luego, solicita una selfie para confirmar la identidad del propietario de la cuenta de correo electrónico.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	AL-2026-004	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **Aviso de seguridad**	ecucert
TLP:	TLP:CLEAR		
Fecha:	30-ene-2026	**Campaña de Phishing mediante suplantación de identidad de Microsoft**	V 1.1

Nota: Valida que no tiene una cámara conectada al computador:

- Posteriormente, el robo de credenciales se concreta.

CASO 2

- Llega un correo fraudulento donde se menciona que la cuenta podría estar vinculada a un dispositivo diferente y que se debe ingresar en la siguiente opción.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	AL-2026-004	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **Aviso de seguridad**	ecucert
TLP:	TLP:CLEAR		
Fecha:	30-ene-2026	**Campaña de Phishing mediante suplantación de identidad de Microsoft**	V 1.1

- A continuación, solicita el consentimiento para el tratamiento de los datos personales del propietario de la cuenta de correo electrónico, para hacerlo parecer más real.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	AL-2026-004	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	ecucert
TLP:	TLP:CLEAR	**Aviso de seguridad**	
Fecha:	30-ene-2026	**Campaña de Phishing mediante suplantación de identidad de Microsoft**	V 1.1

- Luego aparece un portal que visiblemente parece oficial de Microsoft, pero no lo es, y solicita el ingreso del correo electrónico y la contraseña.

- A continuación, solicita se realice una selfie por parte del propietario de la cuenta de correo electrónico con el fin de hacerlo parecer real o con una seguridad adicional.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	AL-2026-004	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	ecucert
TLP:	TLP:CLEAR	**Aviso de seguridad**	
Fecha:	30-ene-2026	**Campaña de Phishing mediante suplantación de identidad de Microsoft**	V 1.1

- Después, solicita dar un click en el botón. (Capturar foto).

- Inicia con la carga de la supuesta selfie y se mantiene la página en verificando, se despliega el siguiente texto: Microsoft > Enviando…

- Posteriormente, el robo de credenciales se concreta.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	AL-2026-004	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR	
TLP:	TLP:CLEAR	**Aviso de seguridad**	ecucert
Fecha:	30-ene-2026	**Campaña de Phishing mediante suplantación de identidad de Microsoft**	V 1.1

IV. INDICADORES DE COMPROMISO:

El indicador de compromiso reportado y asociado a la campaña maliciosa son los enlaces que dirigen a los sitios web fraudulentos:

- ***Sitios web:***

https[:]//validar2026.webcindario.com/

https[:]//hotmailahoras.z20.web.core.windows.net/index3.html?email=cnfkdkskskksk%40hotmail.com

V. RECOMENDACIONES:

El EcuCERT recomienda a su comunidad objetivo tomar en consideración lo siguiente:

- Validar si los sitios web en los que se navega son seguros (se utiliza el puerto https) y oficiales (el dominio corresponde al nombre de la empresa, no tiene errores ortográficos).
- Hacer caso omiso a correos, links o mensajes de dudosa procedencia y márcalos como spam o bloquearlos y comunicar a su departamento técnico.
- Ante cualquier duda contactarse directamente con la persona o empresa suplantada para su comprobación y/o denuncia.
- Habilita el MFA para todas tus cuentas Microsoft,
- preferentemente con la aplicación authenticator.
- En caso de haber ingresado los datos personales en el sitio web fraudulento, cambiar la contraseña de las cuentas y comunicarse inmediatamente con la empresa suplantada para la toma de acciones de remediación.
- Nunca entregue los usuarios y contraseñas solicitados a través de correos electrónicos, redes sociales o llamadas telefónicas.
- Instalar y mantener actualizado una solución Antivirus.
- Bloquear los sitios web o direcciones de correo electrónicos indicados en la sección indicadores de compromisos.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec

Nro. Alerta:	AL-2026-004	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **Aviso de seguridad**	ecucert
TLP:	TLP:CLEAR		
Fecha:	30-ene-2026	**Campaña de Phishing mediante suplantación de identidad de Microsoft**	V 1.1

- Mantenerse informado continuamente sobre tipos de amenazas en el internet.
- Instalar archivos .apk en su dispositivo descargarlo sólo de fuentes confiables como Google Play Store, AppGallery, Galaxy Store u otras tiendas oficiales.

Dirección: Av. 9 de Octubre N27-75 y Berlín.
Código postal: 170513 / Quito - Ecuador.
Teléfono: +593-02 2946400 / 02 2947800 Ext.: 2001 / 2002 / 1173 / 2004 / 2048
www.arcotel.gob.ec