

Phishing: cómo reconocer un correo falso y qué hacer

El **phishing** (suplantación de identidad) es un mensaje que se hace pasar por la Universidad, un banco, Google, Microsoft o una persona conocida para que entregues tu contraseña, descargues un archivo dañino o hagas un pago. Llega por correo, pero también por WhatsApp, SMS o llamadas.

Toda la comunidad UBB

5 minutos

Correo institucional

La regla de oro

El DSC nunca te pedirá tu contraseña: ni por correo, ni por WhatsApp, ni por teléfono. Tampoco te pedirá códigos de verificación ni que «valides» o «actualices» tu cuenta en un enlace.

Si un mensaje te pide eso, aunque parezca venir de la Universidad, es falso.

Cómo reconocer un correo de phishing

1 Mira quién lo envía de verdad

El nombre que se muestra puede decir «Soporte UBB» o el nombre de tu jefatura, pero lo que importa es la **dirección de correo**. Haz clic en el nombre del remitente para verla completa.

Desconfía de direcciones parecidas a las reales (ubiobio-soporte.com, ubioblo.cl) o de cuentas personales (@gmail.com, @outlook.com) que dicen ser de la Universidad.

2 Desconfía de la urgencia y las amenazas

«Tu cuenta será bloqueada hoy», «tu buzón está lleno», «último aviso», «pago rechazado». El objetivo es que actúes rápido sin pensar. Un aviso real del DSC no te exige hacer clic en minutos.

3 Revisa los enlaces antes de abrirlos

En el computador, **pasa el mouse sobre el enlace sin hacer clic**: abajo del navegador o del correo aparece la dirección real. En el celular, **mantén presionado** el enlace para verla.

Si el texto dice una cosa y la dirección otra, o la dirección no termina en el sitio que dice ser (por ejemplo, ubiobio.cl), no lo abras.

4

Cuidado con los archivos adjuntos

No abras adjuntos que no esperabas, aunque vengan de alguien conocido. Son especialmente peligrosos los archivos .zip, .html, .exe y los documentos que piden «Habilitar contenido» o «Habilitar macros».

5

Si pide datos, es sospechoso

Contraseñas, códigos que te llegan por SMS, datos bancarios o de tu tarjeta, o que compres tarjetas de regalo «para una urgencia». Ninguna unidad de la Universidad pide eso por correo.

Otras pistas: saludos genéricos («Estimado usuario»), errores de redacción y logos mal recortados. Pero ojo: muchos correos falsos están bien escritos, así que no te fíes solo de eso.

Un ejemplo

Así se ve un correo típico de phishing. Las partes marcadas son las señales de alerta:

De

Mesa de Ayuda UBB <soporte@ubiobio-cuentas.com>

Asunto

URGENTE: su cuenta institucional será desactivada

Mensaje

Estimado usuario, detectamos actividad irregular. Para evitar el cierre de su cuenta en las próximas 24 horas, valide su contraseña en el siguiente enlace: Validar cuenta.

Remitente que no es de la Universidad, urgencia, saludo genérico y un enlace que pide la contraseña: es phishing.

Si te llega un correo sospechoso

1

No hagas clic, no respondas y no lo reenvíes

No abras los enlaces ni los adjuntos, no contestes (confirmarías que tu correo está activo) y no se lo reenvíes a colegas «para preguntar».

2

Denúncialo en Gmail

Con el correo abierto en Gmail, haz clic en **Más** (los tres puntos ⋮, arriba a la derecha del mensaje) y elige **Denunciar suplantación de identidad (phishing)**. El correo se elimina y ayudas a que Google lo bloquee para todos.

3

Avisa a la Universidad

Si el correo suplanta a la Universidad, a una autoridad o a un servicio institucional, o si llegó a muchas personas, avísanos:

- Escribe a sec@ubiobio.cl indicando el **remitente, el asunto y la hora** en que llegó, o
- usa el Formulario de Notificación de Incidentes de Ciberseguridad de la sección Ciberseguridad del portal.

Si tienes dudas, llama a Soporte: anexo 1547 o 1541.

Si ya hiciste clic o entregaste tu contraseña

No te preocupes: le pasa a mucha gente y actuar rápido evita la mayor parte del daño.

1

Cambia tu contraseña de inmediato

- **Funcionarios y académicos:** idubb.ubiobio.cl/pwm
- **Estudiantes y egresados:** idubb.ubiobio.cl/apwm

Dentro de la página, elige **Cambiar contraseña**. Si usas esa misma contraseña en otros sitios (banco, redes sociales), cámbiala también allí.

2

Si abriste un adjunto, desconecta el equipo

Desconecta el cable de red o apaga el WiFi del equipo, no lo apagues y llama a Soporte: anexo 1547 o 1541.

3

Cuéntanos qué pasó

Escribe a sec@ubiobio.cl contando qué hiciste (hiciste clic, escribiste tu contraseña o abriste un archivo) y a qué hora, o llama a Soporte al anexo 1547 o 1541. Así podemos revisar tu cuenta y avisar a otras personas.

Preguntas frecuentes

¿Y si el correo viene de una cuenta @ubiobio.cl?

Puede ser igual de falso: si una cuenta institucional fue robada, desde ella se envían correos de phishing. Aplica las mismas señales y, ante la duda, confirma con esa persona por otra vía (teléfono o en persona), no respondiendo el correo.

¿Pasa también por WhatsApp o SMS?

Sí. Mensajes de «paquete retenido», «premio», «tu banco» o de un número desconocido que dice ser tu jefatura funcionan igual. No abras sus enlaces ni entregues códigos que te lleguen por SMS.

Denuncié un correo que era real, ¿qué hago?

Nada grave. Si lo necesitas, búscalo en la carpeta **Spam** o **Papelera** de Gmail y márcalo como «No es spam».

¿Cómo sé si un aviso del DSC es real?

Los avisos reales se publican también en este portal (Novedades y estado de los servicios) y nunca piden tu contraseña. Si dudas, escríbenos desde Contáctanos antes de hacer nada.

Incidentes de seguridad: sec@ubiobio.cl. Soporte técnico: anexos 1547 · 1541.

Departamento de Servicios Computacionales · Universidad del Bío-Bío · Guía web actualizada en octubre de 2026. Versión web siempre actualizada: servicios.dmz.ubiobio.cl/help/guias/phishing.html.