TECNOLOGÍA QUE CONECTA

GUÍA PRÁCTICA · 2026

Guía contra phishing

15 señales y controles para frenar el fraude por correo

El phishing es un engaño por correo, mensaje o llamada para robar contraseñas, instalar programas maliciosos o desviar pagos. Es la puerta de entrada más común de los ataques a empresas. Usa esta guía para entrenar a tus colaboradores y revisar los controles de tu organización.

Cómo usar esta guía

1. Comparte la sección “Reconocer” con todos tus colaboradores: son las señales que cualquiera puede detectar.
2. Revisa con tu equipo de TI las secciones “Proteger” y “Responder”, y marca solo lo que se cumple por completo.
3. Cuenta las casillas marcadas y consulta el resultado en la última página.

> **Las tres etapas**
>
> **Reconocer:** que cada persona detecte el engaño. **Proteger:** que los controles técnicos lo bloqueen. **Responder:** actuar rápido si alguien cae.

RECONOCER

Señales de un correo fraudulento

- [ ] **Urgencia o amenaza** 01
  "Tu cuenta será bloqueada hoy", "pago vencido", "último aviso". La presión busca que actúes sin pensar.
- [ ] **Remitente que no coincide** 02
  El nombre parece conocido, pero la dirección real es distinta o tiene letras cambiadas (por ejemplo, "rnicrosoft" en lugar de "microsoft").
- [ ] **Enlaces engañosos** 03
  Antes de hacer clic, pasa el cursor sobre el enlace: la dirección real no coincide con la empresa que dice escribir.
- [ ] **Adjuntos inesperados** 04
  Facturas, documentos o archivos comprimidos que no esperabas, sobre todo si piden "habilitar contenido".
- [ ] **Piden contraseñas o códigos** 05
  Ninguna empresa seria pide tu contraseña ni el código de verificación por correo, mensaje o llamada.
- [ ] **Cambios de pago o cuenta bancaria** 06
  Solicitudes urgentes de transferencias o de nuevas cuentas bancarias, aunque parezcan venir de un directivo o un proveedor.
- [ ] **Algo no cuadra** 07
  Saludo genérico, errores, un tono distinto al habitual de esa persona o un horario poco usual.

PROTEGER

Controles técnicos que lo bloquean

- [ ] **Filtrado avanzado del correo** 08
  Los adjuntos y enlaces se analizan antes de llegar al usuario, y los correos sospechosos se bloquean o se ponen en cuarentena.
- [ ] **SPF, DKIM y DMARC configurados** 09
  El dominio de la empresa está protegido para que nadie pueda enviar correos haciéndose pasar por ella.

- [ ] **Autenticación multifactor** 10
  Activa en todas las cuentas de correo y de acceso remoto, de preferencia con aplicación o llave de seguridad.

- [ ] **Aviso de correo externo** 11
  Los correos que vienen de fuera de la organización muestran una etiqueta o advertencia visible.

- [ ] **Capacitación con simulaciones** 12
  Los colaboradores reciben entrenamiento periódico y simulaciones de phishing para practicar.

RESPONDER

Actúa rápido si alguien cae

- [ ] **Canal para reportar** 13
  Existe un botón o un correo para reportar mensajes sospechosos, y todos saben usarlo.

- [ ] **Procedimiento ante un clic** 14
  Está claro qué hacer si alguien abrió un enlace o un adjunto: a quién avisar y qué pasos seguir.

- [ ] **Verificación de pagos** 15
  Toda solicitud de pago o de cambio de cuenta se confirma por un segundo canal, como una llamada a un número conocido.

Tu resultado

Cuenta cuántas casillas marcaste:

13 a 15
POSTURA SÓLIDA
Tienes las bases. El reto es sostenerlas: revisa esta lista cada seis meses y mide la respuesta con simulacros.

8 a 12
CON BRECHAS
Un correo fraudulento podría pasar tus defensas. Prioriza la capacitación y los controles de la sección “Proteger”.

0 a 7
RIESGO ALTO
Tu empresa está muy expuesta al phishing. Conviene actuar de inmediato, empezando por MFA, filtrado del correo y capacitación.

Si alguien hizo clic: primeros pasos

01
Desconecta
Desconecta el equipo de la red si se descargó o abrió un archivo.

02
Cambia claves
Cambia la contraseña desde otro equipo y cierra las sesiones activas.

03
No borres
Conserva el correo: sirve para investigar y bloquear a otros.

04
Avisa
Informa de inmediato a TI o a especialistas en respuesta.

VIVA SOLUTIONS · NOC Y SOC 24/7 DESDE PANAMÁ

¿Quieres cerrar las brechas con especialistas?

viva
TECNOLOGÍA QUE CONECTA

Protegemos el correo con Vi-Mail & Web, entrenamos a tus colaboradores con Vi-Awareness y vigilamos 24/7 desde nuestro SOC. Conoce tu nivel con nuestra autoevaluación gratuita.

Autoevaluación: vivaconecta.com/autoevaluacion
¿Bajo un ataque?: vivaconecta.com/incidente
(507) 216-9004
webforms@vivaconecta.com

Guía orientativa de buenas prácticas. No sustituye una evaluación profesional de tu entorno.