Respuesta a phishing

Versión 1.0 · Revisado el 11 oct 2026 · TLP:CLEAR · Para: Mesa de ayuda, responsables de TI y cualquier persona que administre correo.

Qué hacer cuando llega un correo, mensaje o sitio falso que busca robar credenciales o instalar malware. El objetivo es saber quién cayó, cortar el acceso del atacante y evitar que el mensaje siga circulando.

Señales de que está ocurriendo

- Correo que urge a iniciar sesión, pagar o descargar un archivo.
- Remitente con un dominio parecido al legítimo pero con una letra distinta.
- Enlace cuyo destino real no coincide con el texto que muestra.
- Usuarios que reportan haber ingresado su contraseña en una página extraña.
- Reglas de reenvío nuevas en un buzón o inicios de sesión desde otro país.

Qué tan grave es

Alta	Alguien ingresó credenciales o abrió un adjunto malicioso; cuentas con privilegios involucradas.
Media	Campaña dirigida a varios usuarios, sin evidencia de que alguien haya caído.
Baja	Correo genérico reportado y bloqueado antes de que alguien interactuara.

Primera hora

- [ ] **1.** Pide a quien lo reportó que no reenvíe el mensaje; que lo envíe como archivo adjunto.
- [ ] **2.** Busca en el servidor de correo cuántas personas recibieron el mismo mensaje.
- [ ] **3.** Elimina el mensaje de todos los buzones y bloquea remitente, dominio y enlace.
- [ ] **4.** Averigua quién hizo clic y quién ingresó datos: revisa registros de proxy y correo.
- [ ] **5.** Cambia la contraseña y cierra las sesiones de cada persona que ingresó credenciales.
- [ ] **6.** Avisa al resto del personal con una captura del mensaje para que lo reconozcan.

Preparación (antes del incidente)

- Configura SPF, DKIM y DMARC en tu dominio, con política de rechazo.
- Activa verificación en dos pasos en el correo de todo el personal.
- Habilita un botón o buzón para reportar correos sospechosos.
- Capacita al personal con ejemplos reales al menos dos veces al año.

Detección y análisis

- Revisa las cabeceras completas: remitente real, servidores y resultado de SPF/DKIM.
- Analiza enlaces y adjuntos en un entorno aislado, nunca en tu equipo de trabajo.
- Clasifica el objetivo: robo de credenciales, malware o fraude de pago.
- Extrae los indicadores: dominios, direcciones IP, hashes y asuntos.

Contención

- Bloquea los indicadores en correo, proxy, DNS y firewall.
- Revoca sesiones y tokens de las cuentas comprometidas.
- Elimina reglas de reenvío y delegaciones que no reconozca el dueño del buzón.
- Aísla el equipo de quien abrió un adjunto malicioso.

Erradicación

- Solicita la baja del sitio falso al proveedor de hosting y al registrador del dominio.
- Reporta el enlace a los navegadores (Google Safe Browsing, Microsoft SmartScreen).
- Analiza con antivirus los equipos de quienes interactuaron con el mensaje.

Recuperación

- Restablece el acceso de los usuarios con contraseñas nuevas y dos pasos activos.
- Revisa durante 30 días la actividad de las cuentas afectadas.
- Confirma que no se enviaron correos fraudulentos desde las cuentas comprometidas.

Lecciones aprendidas

- Mide cuántos recibieron, cuántos hicieron clic y cuánto tardó el primer reporte.
- Ajusta los filtros de correo con lo aprendido de esta campaña.
- Usa el caso, sin señalar a nadie, en la siguiente capacitación.

Evidencia que debes conservar

- El correo original en formato .eml o .msg, con cabeceras.
- Captura de pantalla de la página falsa y su dirección completa.
- Registros de correo y de navegación de los usuarios involucrados.
- Lista de destinatarios y de quienes interactuaron.

Qué no hacer

- Reenviar el correo sospechoso: propaga el enlace y borra cabeceras útiles.
- Abrir enlaces o adjuntos para “ver qué hacen” en un equipo de trabajo.
- Culpar a quien cayó: desalienta que la próxima persona reporte a tiempo.
- Cambiar la contraseña sin cerrar las sesiones abiertas.

A quién avisar

- Personal de la organización, con el ejemplo del mensaje.
- La marca suplantada, si es un banco o un proveedor.
- Clientes, si el correo fraudulento salió desde una cuenta de la organización.
- cert.gt, con los indicadores, para alertar a otras organizaciones.

Cuándo dar por cerrado el incidente

- El mensaje fue eliminado de todos los buzones.
- Todas las cuentas comprometidas tienen contraseña nueva y dos pasos.
- Los indicadores están bloqueados y el sitio falso reportado.
- No hay actividad anómala en las cuentas afectadas.

cert.gt es una iniciativa privada y comunitaria de Devel Group.

cert.gt · devel.group · Reporta un incidente en cert.gt/reportar o a incidentes@cert.gt

Guía general de buenas prácticas; no sustituye asesoría legal ni técnica especializada para tu caso. No es un documento de una entidad gubernamental. Puedes copiarla y adaptarla citando la fuente (CC BY 4.0).