**Mitigaciones clave contra PHISHING**

1. **Prevención en la capa de correo / entrega**

* **Implementar y reforzar protocolos de** autenticación de correo electrónico que se implementan en el DNS para verificar la identidad del remitente, proteger contra el phishing y el spam, y mejorar la entregabilidad de los emails con políticas estrictas
* **Gateway de correo seguro (SEG)**/ATP: escaneo de attachments, rewriting/sanitización de links, detección de URLs maliciosas en tránsito.
* **Bloqueo a nivel de perímetro**: listas de bloqueo de dominios/IPs/URLs provenientes de feeds reputacionales.
* **Políticas de contenido**: bloquear tipos de attachment peligrosos o convertir/analizar (ej. desactivar macros en Office).
* **Protecciones de identidad**: forzar MFA (Multi-Factor Authentication) y autenticación resistente a phishing (FIDO2) para reducir impacto si credenciales se filtran.

1. **Educación y resistencia del usuario**

* **Programas regulares de awareness y formación** sobre phishing (cómo detectar enlaces/URLs, remitentes falsos, señales de ingeniería social).
* **Simulaciones de phishing periódicas** (campañas controladas) con feedback y medidas formativas para usuarios que fallan.
* **Botón/reportar-phish** integrado en el cliente de correo / app para que usuarios reporten correos sospechosos fácilmente, y se integre posteriormente en una base de datos para que quede un registro y se bloqueen en el futuro.
* **Política clara de gestión de credenciales** (no reutilizar contraseñas, no enviar credenciales por email).
* **Obligatorio cambio de contraseña** para todo el personal cada 2-3 meses de promedio.

1. **Detección y enriquecimiento (Data / AI)**

* **Clasificadores de correo (Machine learning + reglas)**: modelos Natural Language Processing para detectar texto phishing (urgencia, enlaces, llamadas a acción), combinados con reglas heurísticas (DomainKeys Identified Mail/Sender Policy Framework fail, suplantación del remitente).
* **Análisis de URLs**: features para Machine learning (longitud URL, no permitir punycode y solo usar caracteres ASCII, redirecciones, edad dominio, WHOIS, protocolo Transport Layer Security, coincidencia visual/homograph ejemplo g00gle en vez de google).
* **Sandboxing / detonation**: abrir archivos adjuntos y URLs en entorno controlado para observar comportamiento (formularios, robo de credenciales).
* **Enriquecimiento con Threat Intel**: PhishTank, MISP, feeds de dominio/IP; consultas a HaveIBeenPwned para credenciales comprometidas.
* **Reglas Sigma / SIEM**: correlaciones como “email con enlace a dominio nuevo + click desde usuario + login posterior” → alerta tomo de control de cuenta probable.

1. **Respuesta y mitigación automatizada**

* **Cuarentenar/aislar correos detectados** automáticamente y notificar al usuario.
* **Bloqueo/rewriting de URLs** en tiempo real (WAF/proxy o link-rewriting en gateway).
* **Remediación de credenciales comprometidas**: forzar reset de contraseña, revocar sesiones y aplicar Multi Factor Authentication si el usuario clicó y suministró datos.
* **Request takedown y coordinación:** se refiere a **solicitar oficialmente que se retire un contenido malicioso o fraudulento de Internet**. C**oordinar con terceros**: registradores de dominios, proveedores de hosting, plataformas de seguridad, etc.

1. **Herramientas, procesos y gobernanza**

* **Integración con MISP / PhishTank** para procesar y compartir Indicador de Compromiso.
* **Dashboard + métricas**: tasas de click en simulaciones, tiempo medio de detección, número de correos cuarentenados, dominios bloqueados.
* **Playbooks documentados** por tipo (credential harvesting, spear-phish, brand impersonation) y traducidos a TheHive/Cortex.
* **Retención de evidencia**: almacenar correos originales (headers + body), sandbox logs y actividad del usuario para forense.
* **Reentrenamiento**: usar los correos reales y simulaciones para reentrenar modelos y reducir falsos positivos/negativos.