LET'S GO PHISHING

Comece a travar o phishing

Um guia prático da Knowledge Inside para todas as empresas

KNOWLEDGE INSIDE

ÍNDICE

01 Introdução

02 Compreender o Phishing
Descubra o que é o phishing, os tipos de ataque mais comuns e por que certos perfis são os principais alvos.

03 9 sinais de Phishing
Aprenda a identificar os sinais de alerta mais frequentes em mensagens fraudulentas e ensine a sua equipa a agir com segurança.

04 Defesas por camadas
Uma defesa eficaz combina tecnologia e comportamento humano, veja como proteger a organização em várias frentes e reduzir o impacto de ataques.

05 Passo a Passo para Implementar um Programa Anti-Phishing
Siga um plano estruturado em seis etapas para criar uma estratégia sólida, prática e sustentável contra o phishing.

06 Plano de Resposta a Incidentes
Saiba o que fazer quando um ataque acontece: como reagir rapidamente, mitigar danos e tirar lições de cada incidente.

07 A Solução Let's Go Phishing
Conheça o programa desenvolvido pela Knowledge Inside para capacitar equipas, reduzir riscos e fortalecer a cultura de segurança.

08 Conclusão

INTRODUÇÃO

O phishing continua a ser uma das principais portas de entrada para incidentes de segurança: roubo de credenciais, acesso inicial em ataques sofisticados, e vetor de ransomware. Um programa de formação e simulação bem desenhado reduz substancialmente a probabilidade de sucesso de um ataque e torna a organização mais resiliente. A maior parte dos incidentes envolve um componente humano, confiar numa mensagem, seguir instruções urgentes ou clicar num link aparentemente legítimo.

Este guia foi criado para gestores, responsáveis de IT e colaboradores: prático, direto e com um plano acionável para reduzir significativamente o risco de phishing na sua organização.

Compreender o Phishing
O inimigo invisível da cibersegurança

01 | O QUE É PHISHING

É uma técnica de engenharia social em que o atacante se faz passar por uma entidade de confiança para levar a vítima a revelar informação sensível (credenciais, cartões) ou a executar ações (transferências, instalação de ficheiros). Um ataque costuma incluir: mensagem de comunicação eletrónica (email/SMS/voz), falsificação da identidade do remetente e um objetivo claro (roubar credenciais, extorquir, instalar malware).

02 | TIPOS DE ATAQUE

1. **Phishing em massa:** envios amplos com linguagem genérica.
2. **Spear-phishing:** mensagens dirigidas e personalizadas para alvos específicos.
3. **Business Email Compromise (BEC):** Variante do spear-phishing recorrendo a comprometimento de contas empresariais para instruir transferências financeiras.
4. **Smishing:** phishing por SMS.
5. **Vishing:** phishing por voz/telefone

COMPONENTES TÍPICOS DE UM ATAQUE DE PHISHING

Vetor: e-mail, SMS, redes sociais, ligação telefónica.

Isco: link, anexo ou pedido urgente.

Objetivo: credenciais, dinheiro, instalação de malware.

03 | POR QUE ISTO ACONTECE E QUEM SÃO OS ALVOS

Ataques de phishing são rentáveis: muitas campanhas geram ganhos financeiros imediatos ou permitem acesso a sistemas que depois serão monetizados. Os alvos mais frequentes dentro de organizações: finanças, gestão, IT e RH, colaboradores com poder para autorizar pagamentos, aceder a dados sensíveis ou executar comandos administrativos.

9 SINAIS DE PHISHING
(O QUE ENSINAR AOS COLABORADORES)

MENSAGENS COM URGÊNCIA

Sinal: Linguagem alarmista que pressiona a agir rapidamente.

Exemplo: "A sua conta será suspensa nas próximas 24 horas. Clique aqui para confirmar os seus dados e evitar o bloqueio."

REMETENTE SUSPEITO

Sinal: O domínio do e-mail é parecido, mas não idêntico ao oficial.

Exemplo: Remetente: "suporte@microsof-support.com" (em vez de "support@microsoft.com

ERROS ORTOGRÁFICOS E GRAMATICAIS

Sinal: Mensagens mal traduzidas ou com erros evidentes.

Exemplo: "Caro cliente, o seu conta foi detetado com atividade sospeita. Para evitar suspenção, faça login no portal."

SAUDAÇÕES GENÉRICAS

Sinal: A mensagem não usa o seu nome verdadeiro.

Exemplo: "Caro utilizador, verifique a sua fatura pendente."

LINKS DISFARÇADOS

Sinal: O texto do link parece legítimo, mas o endereço é falso.

Exemplo: "Aceda à sua conta: www.novobanco.pt"

PEDIDOS DE DADOS PESSOAIS OU DE ACESSO

Sinal: Pedidos de dados pessoais ou de acesso

Exemplo: "Por motivos de segurança, envie-nos o seu código MFA para confirmar a identidade."

ANEXOS INESPERADOS

Sinal: Um ficheiro suspeito acompanha o e-mail, mesmo sem contexto.

Exemplo: Assunto: "Fatura pendente nº 4821" Anexo: "fatura.zip" (que contém "fatura.exe")

ALTERAÇÃO DE CONTAS BANCÁRIAS OU INSTRUÇÕES DE PAGAMENTO

Sinal: Um fornecedor ou colega informa nova conta bancária sem aviso prévio.

Exemplo: "Devido a auditoria interna, pedimos que transfira os próximos pagamentos para o IBAN PT50 9999... Obrigado."

OFERTAS TENTADORAS

Sinal: Promessas exageradas ou prémios inesperados.

Exemplo: "Parabéns! Ganhou um iPhone 16! Preencha este formulário para receber o seu prémio."

DEFESAS POR CAMADAS
TECNOLOGIA + PESSOAS

Antes da entrega (parar no gateway)

- **Secure Email Gateway:** filtragem de spam, reputação de remetente, bloqueio de domínios maliciosos.
- **Autenticação de remetente:** SPF, DKIM e DMARC para reduzir spoofing.
- **Reputação IP e heurísticas de conteúdo** (detetar padrões conhecidos).

Estas medidas reduzem muito o volume de phishing que chega às caixas dos colaboradores.

Após a entrega (se passou pelo gateway)

- **Proteção de endpoint:** detecção por comportamento, anti-exploit, antimalware moderno.
- **Sandboxing:** abrir anexos suspeitos em ambiente isolado.
- **Bloqueio de URLs maliciosos** (real-time URL scanning).
- **Deteção por machine learning / deep learning** para ameaças desconhecidas.

Redução do risco humano

- **MFA (autenticação multifator):** reduz o impacto quando credenciais são comprometidas.
- **Simulações de phishing e formação contínua:** testar e treinar colaboradores regularmente.
- **Políticas e processos claros:** fluxos aprovados para pagamentos e verificações secundárias (call-back).
- **Report de phishing:** incentivar o reporte imediato de mensagens suspeitas, criar uma cultura ativa de reporte.

PASSO A PASSO PARA IMPLEMENTAR UM PROGRAMA ANTI-PHISHING

Implementar um programa anti-phishing exige método. Estes seis passos ajudam a estruturar uma estratégia eficaz que combina tecnologia, processos e pessoas, da avaliação inicial à melhoria contínua.

Avaliar riscos e mapear ativos

quem pode autorizar pagamentos, que sistemas são críticos

Inventariar pontos de exposição

contas de e-mail, formulários públicos, números de telefone

Implementar controles técnicos prioritários

Filtragem, SPF/DKIM/DMARC, MFA.

Definir políticas e processos de verificação

rotina de dupla validação para transferências.

Treinar e simular

campanhas de simulação, micro-learning e relatórios

Monitorizar, auditar e melhorar

métricas, KPIs e testes de recuperação

PLANO DE RESPOSTA A INCIDENTES

IMEDIATO

PASSO 1
Isolar a conta/dispositivo comprometido (reset de sessão).

PASSO 2
Forçar alteração de credenciais e revogar tokens/MFA se aplicável.

PASSO 3
Avaliar se houve transferência financeira, notificar banco.

INVESTIGAR

PASSO 4
Recolher headers do email, anexos, URLs e logs.

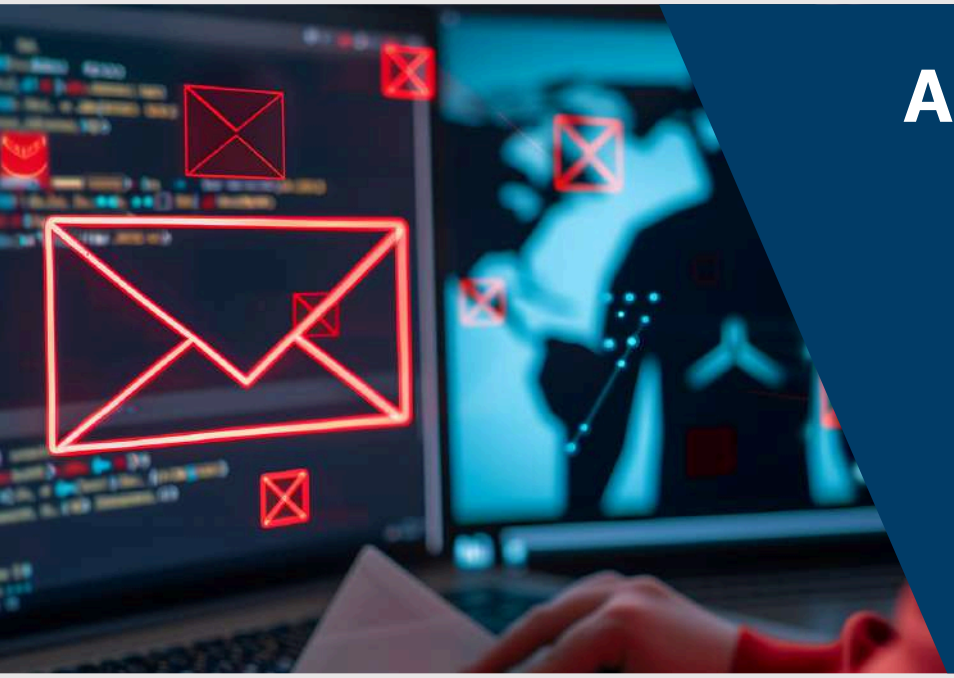
PASSO 5
Verificar movimento lateral na rede / acessos recentes.

REMEDIAR E COMUNICAR

PASSO 6
Restaurar a partir de backups se necessário, comunicar internamente e quando aplicável , às partes externas (clientes/parceiros)

PASSO 7
Atualizar formação com o caso concreto (lições aprendidas).

Inclua sempre uma checklist de contactos de emergência (IT, segurança, jurídico, financeiro) e prazos para execução das ações.



A SOLUÇÃO LETS GO PHISHING

A Knowledge Inside desenvolveu o programa Let's go phishing para ajudar as organizações a criar defesas eficazes contra ataques de engenharia social.

O que inclui:

1. **Campanhas de phishing simuladas :** Criação e envio de e-mails de phishing realistas para avaliar o comportamento dos colaboradores e medir o nível de risco.
2. **Master Class Interativa:** Sessão prática de 90 minutos para explicar o impacto do phishing, analisar os resultados da campanha e ensinar técnicas de identificação e prevenção.
3. **Análise de Mensagens Suspeitas:** Avaliação especializada das mensagens reportadas pelos colaboradores, com feedback claro para reforçar a segurança e confiança no processo de reporte.
4. **Formação e Sensibilização Contínua:** Envio recorrente de testes e conteúdos educativos, com relatórios de desempenho e incentivos para reforçar comportamentos seguros.

BENEFÍCIOS

Redução comprovada da taxa de cliques em e-mails fraudulentos

Aumento da consciência digital entre colaboradores

Fortalecimento da cultura de segurança e confiança interna

Cumprimento de políticas e normas de segurança da informação

CONCLUSÃO

A defesa contra phishing não é um projecto único, é um programa contínuo que combina tecnologia sólida, processos e, acima de tudo, pessoas bem treinadas. Uma estratégia de proteção eficaz contra phishing defende-o tanto de campanhas em larga escala quanto de ataques direcionados e tecnicamente avançados.

Comece por priorizar autenticação, filtragem e formação, depois evolua para simulações regulares e integração com um plano de resposta a incidentes testado.

O COLABORADOR É A PRIMEIRA LINHA DE DEFESA