

Experiência de simulação:

Desmascarando ataques de phishing e whaling

Visão geral

Ataques de phishing manipulam funcionários para que comprometam a segurança, explorando emoções como medo, boa vontade ou respeito pela autoridade. Esta atividade se concentra em uma forma específica e altamente direcionada de phishing conhecida como "Whaling" ou "Fraude do CEO". Nesses ataques, os criminosos se fazem passar por executivos de alto escalão, como o CEO ou o CFO, para explorar a figura de autoridade e desencadear uma resposta emocional urgente.

Os golpistas modernos usam frequentemente a inteligência artificial (IA) generativa para produzir e-mails de phishing com logotipos idênticos aos das organizações e sem erros gramaticais. Embora os participantes ainda devam ficar atentos a erros ortográficos óbvios ou desvios de identidade de marca, este exercício os desafia a entender que não podem mais confiar apenas nesses indícios superficiais de phishing.

Funções

Facilitador:

Controla o ritmo do exercício, orienta as discussões e garante a participação de todos.

Participantes:

Discutem abertamente seu raciocínio e respondem aos cenários de acordo com as regras do exercício.

Introdução

Apresente aos participantes este cenário: A Summit View Logistics está expandindo suas operações para a Europa. O CEO, Marcos Vieira, passou a semana inteira viajando pela Alemanha para garantir a locação de um grande armazém. Todos na organização sabem que esse negócio é prioridade máxima. A CFO, Helena Silva, está em um voo de 10 horas de volta à sede e, no momento, não pode ser contatada. Tânia Reis, Gerente de Contas a Pagar, recebe um e-mail suspeito.

Parte 1: Anotação dos sinais

Duração: 15 minutos

Materiais:

- Temporizador ou cronômetro
- Folhetos de cenários
- Canetas ou lápis

Instruções:

- Divida a sala em pequenos grupos.
- Distribua o e-mail impresso e as canetas ou lápis para cada grupo.
- Instrua os grupos a grifarem os elementos que constroem confiança falsa. Alguns exemplos são assinaturas de e-mail corretas, menções a projetos internos reais ou um tom executivo autêntico.
- Instrua os grupos a **circular**em sinais de alerta comportamentais. Exemplos incluem extrema urgência, exigências para manter o pedido em segredo ou instruções para contornar os portais de pagamento padrão.
- Dê aos grupos 15 minutos para ler o e-mail, discutir e fazer anotações.

Parte 2: Debate

 **Duração:** 10 minutos

Perguntas:

- Quais indicadores falsos de confiança você identificou e em que medida eles afetaram sua confiança no e-mail?
- Quais sinais de alerta comportamentais específicos denunciaram o golpe?
- Como esses gatilhos comportamentais são projetados para influenciar seus sentimentos ou reações?

Respostas possíveis/sugestões:

- Indicadores falsos de confiança: os golpistas de phishing coletam nomes de projetos reais do LinkedIn ou de sites corporativos para fazer com que o e-mail pareça autêntico.
- Sinais de alerta: o e-mail de phishing pede aos funcionários que desviem dos procedimentos padrão. O remetente exige sigilo do gerente direto do funcionário.
- A principal conclusão: os elementos de aparência autêntica são apenas uma cortina de fumaça. São os sinais de alerta comportamentais que representam o perigo real.

Conclusão

 **Duração:** 5 minutos

Para finalizar o exercício, conecte os conceitos diretamente à realidade da sua organização. Explique que identificar um sinal de alerta comportamental é apenas o primeiro passo da defesa; o segundo é tomar a atitude correta seguindo os procedimentos da organização.

Aproveite a oportunidade para responder a eventuais perguntas dos participantes sobre como denunciar esse tipo de golpe internamente e sobre as ferramentas, canais e documentação disponíveis para relatar esses incidentes.

Anexo – Folheto de cenário

 Redigir

-  Caixa de entrada
-  Rascunhos
-  Enviar
-  Com estrela
-  Spam
-  Lixeira
-  Arquivar
-  Todos os e-mails

 Arquivar  Spam  Excluir  Mais

 Responder  Encaminhar

De: Marcos Vieira <m.vieira@summitview-logistica-interna.com>
Para: Tânia Reis
Assunto: **URGENTE: Caução do armazém em Berlim**

Olá, Tânia,

Estou com os corretores em Berlim. Estamos prontos para assinar o contrato de locação do armazém que discutimos na reunião geral de segunda-feira.

Temos um grande problema. Outra empresa fez uma oferta para o estabelecimento. O corretor disse que, se não pagarmos o depósito de garantia de R\$ 50.000 na próxima hora, eles vão passar a locação para a outra empresa.

Helena Silva está em voo e eu não posso esperar pela aprovação dela. O corretor ainda não está no nosso portal de fornecedores, e isso levará muito tempo.

Preciso que você faça agora mesmo uma transferência bancária direta usando os dados anexados abaixo. Não mencione isso até Helena chegar, para que as pessoas não entrem em pânico com a possibilidade de o acordo não se concretizar. Me avise assim que a transferência for confirmada.

Atenciosamente,
Marcos

 Anexo: Dados_para_Transferência_Bancária.pdf

Indicadores falsos de confiança: Sabe a localização do suposto remetente (Berlim); menciona um projeto real (aluguel de armazém / reunião geral); sabe o nome e a situação da CFO (Helena está em um voo).
Sinais de alerta comportamentais: Urgência extrema (na próxima hora, senão outra empresa ficará com o aluguel); procedimentos incomuns (não está no portal do fornecedor); isolamento (manter segredo).