# Opção A - Em que *Phishing* cairia eu?

Neste trabalho pretende-se refletir um pouco sobre como é que alguém da área de TI, mais especificamente de cibersegurança, poderia ser vítima de um ataque de *phishing*.

Apesar de profissionais e estudantes de TI terem, em média, maior consciencialização em cibersegurança, vários estudos demonstram que nenhum grupo está completamente imune a este ataque de engenharia social, sobretudo quando estes são altamente personalizados ou contextualizados.

Um estudo conduzido por Daengsi et al. (2021) analisou o impacto da consciencialização em cibersegurança através de simulações de phishing numa organização financeira. Os autores compararam funcionários de departamentos técnicos (como TI) com departamentos de natureza social (como Recursos Humanos). Os resultados mostraram que, embora os colaboradores de TI apresentassem inicialmente maior capacidade de deteção de phishing, ambos os grupos eram vulneráveis. Após ações de formação e simulações, verificou-se uma melhoria significativa nos dois grupos, especialmente nos colaboradores não técnicos. Este estudo evidencia que a formação contínua e a exposição a cenários realistas são fundamentais para reduzir o sucesso de ataques de phishing, independentemente do perfil técnico do utilizador.

De forma complementar, Meyers et al. (2018) estudaram a formação de estudantes de cibersegurança na criação de ataques de spear phishing através de um processo estruturado denominado SiEVE (Social Engineering Vulnerability Evaluation). O estudo demonstrou que alunos que seguiram este processo conseguiram criar emails de spear phishing mais convincentes e eficazes. Estes resultados mostram que ataques bem-sucedidos dependem fortemente do contexto e da personalização da mensagem, reforçando a ideia de que utilizadores, mesmo com formação técnica, podem ser enganados quando confrontados com mensagens altamente credíveis.

Em conjunto, estes trabalhos reforçam a importância da consciencialização contínua em cibersegurança e demonstram que o phishing, especialmente o spear phishing, continua a ser uma ameaça relevante e eficaz.

Antes de elaborar em que tipos de phishing que poderia cair, convidava o professor a fazer um pequeno quiz para testar as suas capacidades, disponível em https://phishingquiz.withgoogle.com/. Eu obtive o seguinte resultado:

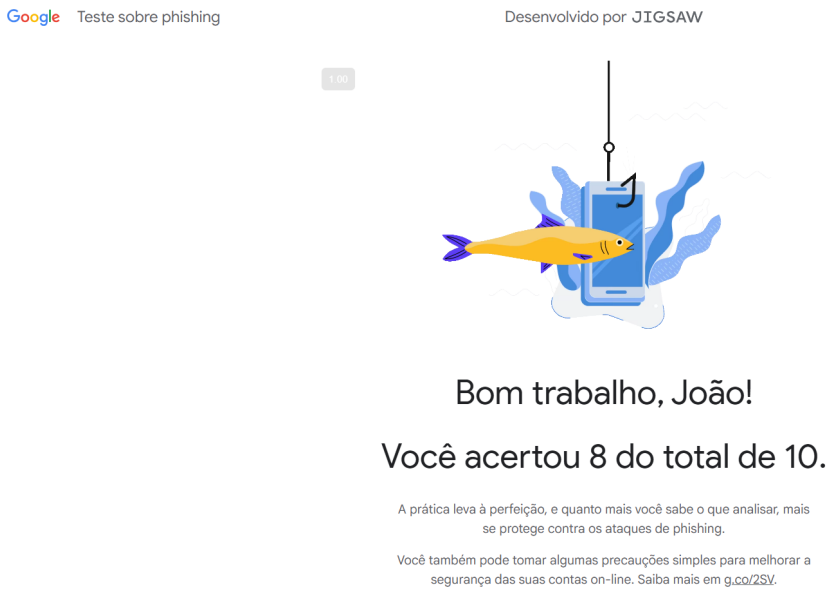


Figura 1: Resultados do questionário de phishing

Como é possível ver, não acertei em todas as perguntas devido a um dos aspetos mais importantes no phishing na minha visão: **o contexto**, já que em ambas as perguntas erradas é importante perceber se de facto existia algum processo de compra/encomenda em curso.

No entanto, com base neste questionário, é possível identificar algumas técnicas comuns utilizadas por atacantes de phishing:

- Uso de domínios muito semelhantes aos legítimos, com pequenas alterações (ex:substituição de caracteres);
- Criação de um sentido de urgência ou escassez de tempo para icentivar uma ação imediata;
- Exploração de temas relevantes para o utilizador, como atualizações de *software* ou problemas de armazenamento.

Adicionalmente, verifica-se que o uso de dispositivos móveis aumenta a vulnerabilidade ao phishing, uma vez que o utilizador tende a clicar diretamente nos links e não a copiá-lo para um separador novo, sem analisar o endereço de destino, ao contrário do que acontece num computador.

Tendo em conta os tipos de phishing abordados na Unidade Curricular, o ataque ao qual considero estar mais vulnerável é o spear phishing, mais especificamente o whaling. Neste cenário, o atacante faria passar-se, não pelo Reitor da UA, mas pelo meu orientador de bolsa e tese, o Professor Doutor João Paulo Barraca.

Um exemplo plausível seria um convite falso para uma reunião no Microsoft Teams,que é bastante comum em ambos os trabalhos desenvolvidos. Outra possibilidade seria um email relacionado com a plataforma NextCloud, utilizada para armazenamento e partilha de ficheiros no âmbito da bolsa. Neste segundo caso, o fator de urgência poderia ser explorado através da proximidade de prazos para entrega de indicadores de progresso, aumentando a probabilidade de uma ação impulsiva.

TODO: Print do mail do teams a convidar para reunião de tese mas com link falso Inventar mail para os indicadores do Nextcloud que teria link para o NC.