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) [1] 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 e Jurídico). 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) [2] 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 incentivar 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 exposição ao *phishing*, uma vez que o utilizador tende a clicar diretamente nos *links* e não a copiá-los para um separador novo, sem analisar o endereço de destino, ao contrário do que acontece num computador em que basta dar *hover* sobre o mesmo.

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 que ocorrem mensalmente, aumentando a probabilidade de uma ação impulsiva.

De seguida, apresento um mail exemplo para o primeiro caso:

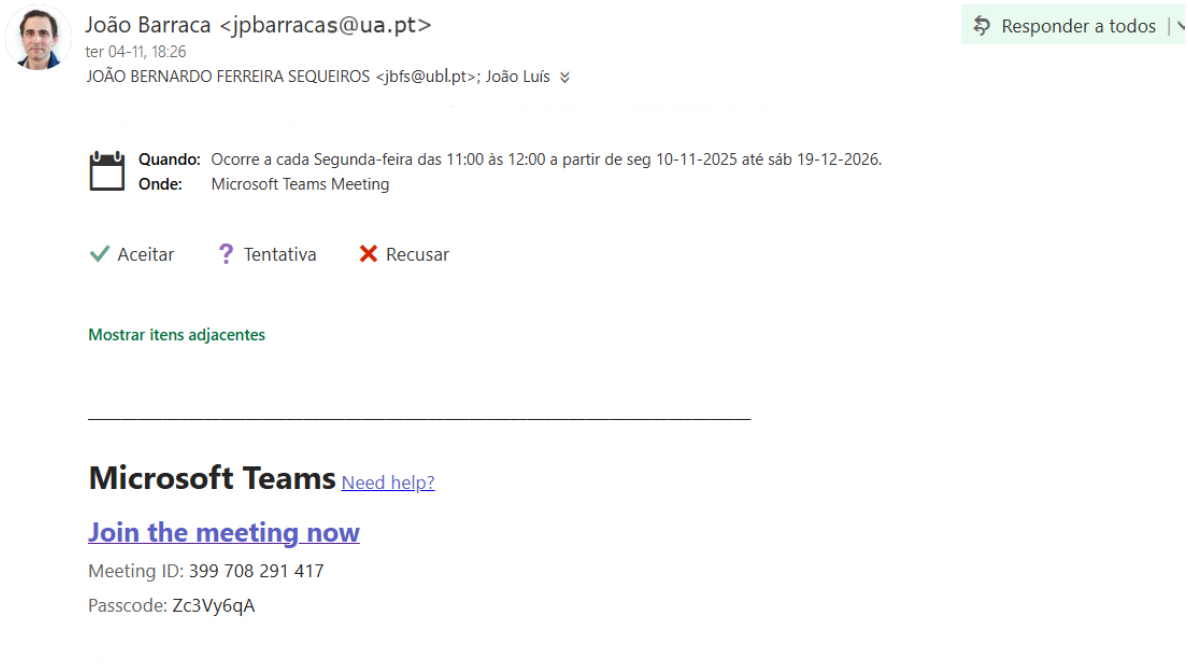

Figura 2: Exemplo de mail de phishing 1

Neste caso, o atacante faria-se passar pelo professor com um *mail* semelhante ao legítimo (jpbarracas@ua.pt), colocando em CC um mail semelhante ao do co-orientador. De resto, a complexidade estaria em replicar visualmente o convite que é enviado pelo Microsoft Teams.

Já para o segundo caso, o *mail* poderia ser da seguinte forma:

```
De: João Barraca (mail falso semelhante ao do Exemplo1)
Para info@ccc-centro.pt
Data: 30-10-2025

Assunto: C-Network \ Toolkit \ Validação de Indicadores CCC Centro \ Outubro 2025

Boa tarde,
Preciso de enviar os KPIs atualizados até amanhã. Por favor atualizem o Excel do
↪ NextCloud.
Cumprimentos,
```

```
João Paulo Barraca
Associate Professor
Cybersecurity Office
DETI / GCS / UNAVE / IT
University of Aveiro
tel. +351 927 036 039
ext. 90140
web. www.ua.pt/pt/p/10333322
```

Figura 3: Assinatura do email

Neste caso, para o *mail* ter maior probabilidade de ser clicado por mim, deveria haver um discurso informal e bastante direto, característico do professor. Além disso, a forma como os *mails* vêm assinados também é algo que costumo ter em atenção mas é fácil de fazer uma assinatura como a descrita na figura 3. Neste caso estou o info@ccc-centro.pt é uma *mailing list* legítima pela qual eu iria receber o ataque.

Assim, este trabalho evidencia que pessoas das área de cibersegurança permanecem vulneráveis a ataques de *spear phishing* altamente personalizados, especialmente quando exploram relações profissionais e contextos organizacionais familiares. A análise demonstra que a replicação de comunicações legítimas, aliada à criação de urgência temporal, constitui um vetor de ataque eficaz mesmo contra utilizadores tecnicamente preparados. A consciencialização contínua e a validação crítica de todas as comunicações são, portanto, essenciais para mitigar esta ameaça persistente.

Referências

[1] T. Daengsi, P. Wuttidittachotti, P. Pornpongtechavanich, e N. Utakrit, "A comparative study of cybersecurity awareness on phishing among employees from different departments in an organization," in *Proceedings of the 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE 2021)*, IEEE, 2021.

[2] J. J. Meyers, D. L. Hansen, J. S. Giboney, e D. C. Rowe, "Training future cybersecurity professionals in spear phishing using SiEVE," in *The 19th Annual Conference on Information Technology Education (SIGITE'18)*, 2018.