Engenharia Social

Licenciatura em Eng. Informática
Segurança Informática 2021-2022

UNIVERSIDADE DE ÉVORA
ESCOLA DE CIÊNCIAS E TECNOLOGIA
DEPARTAMENTO DE INFORMÁTICA

Ricardo Matono (44448), João Rouxinol (44451) e André Rato (45517)

Docente: Pedro Patinho

Trabalho desenvolvido no âmbito da disciplina de Segurança Informática da Licenciatura em Engenharia Informática.

Évora, 16 de junho de 2022

Conteúdo

1 Introdução

No âmbito da unidade curricular de Segurança Informática, foi proposta a realização de um trabalho teórico de investigação sobre um tema relacionado com a segurança informática.

O tema que será abordado neste trabalho será "Engenharia Social". Irão ser focados os mais variados tópicos relacionados com esta temática, tais como a sua definição e origem, os tipos de ataques praticados, os métodos de persuasão utilizados bem como o ciclo de vida de um ataque. Depois, serão apresentados um conjunto de números de impacto relacionados com a temática e um conjunto de exemplos de ataques a grandes organizações. Por fim, serão apresentadas as possíveis formas de evitar um ataque destes, quer seja em ambiente organizacional, quer seja em ambiente particular.

Espera-se que os leitores deste trabalho adquiram alguns conhecimentos sobre o tema abordado.

2 O que é a engenharia social?

A engenharia social, no contexto da segurança informática, refere-se à manipulação de algum indivíduo ou entidade, com vista a obter acesso a informações ou dados confidenciais. Por norma, estes ataques visam obter informações como credenciais de acesso, dados pessoais e, em alguns casos, a extorsão de quantias monetárias ou dados bancários [1] [2].

Este tipo de ataque continua a ter uma taxa de sucesso relativamente alta, pois muitas das vítimas são pessoas que, ou não estão informadas sobre os mesmos, ou não sabem o valor dos dados que possuem. Estes dois aspetos levam a que não sejam tomadas medidas de proteção e prevenção suficientes [3].

Apesar de ser um tema relacionado à informática, a engenharia social é uma ferramenta que tem origem em ambientes de cariz social. Este método passa pela utilização de meios sociais para manipular a vítima, de modo a influenciá-la e a mudar-lhe comportamentos [4].

Não é ousado afirmar que quase toda a população que tem acesso à Internet ou a um telemóvel já foi vítima de tentativas de ataque de engenharia social. Desde SMS com pedidos de pagamento de taxas alfandegárias inexistentes, até ao aparecimento de *popups* em *websites* afirmando que o computador do utilizador se encontra ameaçado, estes ataques estão presentes na vida de todos.

Figura 1: Exemplo de ataque de engenharia social através do Facebook

3 Perigos da engenharia social

As consequências de um ataque de engenharia social podem ser desastrosas. Sejam estes ataques a instituições para obter dados ou ganhar controlo sobre os seus sistemas, ou simplesmente ataques a indivíduos particulares visando obter dados bancários, os ataques de engenharia social representam um perigo iminente [5].

Alguns dos perigos dos ataques de engenharia social são os seguintes:

- roubo de dados confidenciais;
- potencial exposição de dados confidenciais publicamente;
- infeção de dispositivos com *malware* destrutivo, como *ransomware*;
- possibilidade do atacante tomar controlo de sistemas e dispositivos;
- perdas monetárias;
- perda de clientes por falta de confiança após ataques.

Dado que, contrariamente aos ataques que somente utilizam *malware* ou *hacking* (cuja taxa de sucesso se baseia na segurança dos sistemas alvo), os ataques de engenharia social têm a sua taxa de sucesso baseada na sua capacidade de manipular e enganar a vítima, um ser humano. Sendo que são criados sistemas cada vez mais resistentes a ataques de *malware* ou *hacking*, mas não é possível treinar um ser humano para detetar potenciais ataques de engenharia social, os ataques tornam-se cada vez mais perigosos, pois estão cada vez mais sofisticados e mais impercetíveis [6].

4 Métodos de persuasão

Visto que os ataques de engenharia social têm como base a desinformação e o erro humano, os atacantes devem recorrer a métodos de persuasão, de modo a manipularem as vítimas com sucesso [7] [8].

Sendo que a maioria deste tipo de ataques são feitos recorrendo à Internet ou a serviços como o telemóvel, não é possível que os atacantes analisem a linguagem corporal das vítimas, tendo de basear os seus ataques em outras características. Estas podem dividir-se em:

- **Reciprocidade**
  - consiste numa característica básica do ser humano, ou seja, quando alguém recebe algo sente necessidade de retribuir;
  - por exemplo, quando um restaurante oferece algo com a conta, como um digestivo, costuma receber uma gorjeta maior;
  - a reciprocidade é utilizada pelos atacantes quando prometem ofertas às vítimas, de modo a captar a sua atenção e interesse, manipulando-as com o intuito de obter os seus dados.
- **Escassez**
  - consiste na oferta de um produto ou serviço que seja exclusivo ou difícil de obter;
  - seguindo a lógica da expressão "o fruto proibido é o mais apetecido", o ser humano procura e deseja aquilo que não pode obter e, por norma, quanto mais exclusivo e restrito um produto é, mais desejado se torna;
  - por exemplo, a oferta de produtos de custo elevado, como *smartphones* topo de gama, em troca de algumas informações pessoais, ou até mesmo em troca do *download* de um *software*;
  - os atacantes recorrem à escassez, de modo a aliciar as vítimas com produtos ou serviços exclusivos, acabando por cativar a vítima com uma oferta "*to good to be true*".
- **Autoridade**
  - baseia-se na tendência em respeitar e seguir outros indivíduos com autoridade e poder;
  - por exemplo, chamadas telefónicas de atacantes, tentando fazer-se passar por colaboradores da Microsoft, ou emails de supostas entidades com ficheiros PDF infetados;
  - sendo provavelmente uma das características mais focada quando é planeado um ataque, os atacantes manipulam as vítimas, fazendo-as acreditar que estes são, na realidade, alguém com autoridade e poder.
- **Consenso**
  - também conhecido por prova social, baseia-se no facto de o ser humano gostar de tendências e funcionar em torno delas, seguindo a maioria destas, acabando, muitas vezes, por ter interesse em temas e conteúdos nos quais outros também tenham;
  - por exemplo, a criação de *websites* falsos para instituições, com um enorme número de avaliações positivas, também elas falsas;
  - o consenso é utilizado pelos atacantes de modo a que a vítima acredite que visualiza conteúdo que muitas outras pessoas tenham visualizado e gostado, de modo a tornar o mesmo mais credível.
- **Empatia**
  - baseia-se em criar empatia com a vítima, pois o ser humano tem tendência a confiar naquilo que é empático;
  - por exemplo, os ataques de *HoneyTrap*, ou até mesmo a criação de perfis falsos nas redes sociais.
- **Intimidação**
  - baseia-se na intimidação das vítimas, de modo a manipulá-las a realizar alguma ação;

- esta tática pode funcionar muito bem, pois a ameaça pode despertar sensações de ansiedade e urgência na vítima, obrigando-a a agir.

- **Urgência**
  - consiste em apresentar algo à vítima, de modo a que ela tenha um curto espaço de tempo para decidir e agir;
  - por exemplo, podem ser mostradas à vítima "ofertas de tempo limitado", ou "uma ameaça que irá danificar o computador se não for paga uma quantia rapidamente";
  - este método está de certa maneira relacionado com a escassez.

5 Ciclo de vida de um ataque de engenharia social

Visto que a engenharia social se aproveita de erros humanos, os atacantes devem orquestrar um plano que seja difícil de ser descoberto pelas vítimas. Então, de modo a realizar ataques com sucesso, os planos devem seguir o seguinte ciclo de vida [9]:

- ***Investigation***
  - nesta fase, os atacantes identificam o alvo ou os alvos do seu ataque;
  - após identificar os alvos do ataque, informações relevantes sobre as vítimas são recolhidas;
  - depois de obter essa informação, deve ser selecionado o melhor método para criar um ataque ao alvo ou aos alvos em questão.
- ***Hook***
  - nesta fase, a interação com a vítima começa;
  - o atacante começa por se relacionar com a vítima;
  - é nesta fase que o atacante deve manipular a vítima e controlar a interação para obter o que pretende;
  - as interações podem ser chamadas telefónicas, SMS, emails, etc. dependendo do plano definido na primeira fase.
- ***Play***
  - esta fase acontece após o atacante conseguir manipular a vítima;
  - nesta fase, o ataque é realizado e o atacante obtém os dados que desejava com o ataque.
- ***Exit***
  - nesta fase, o atacante deva dar uma conclusão natural à interação;
  - todos os vestígios do ataque realizado devem ser cobertos e todas as provas devem ser eliminadas.

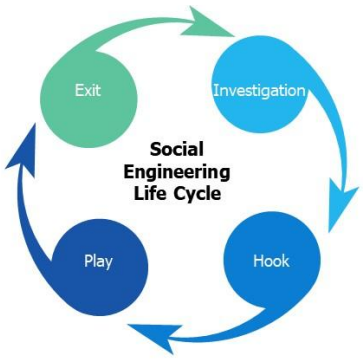


Figura 2: Ciclo de vida de um ataque de engenharia social

6 Tipos de ataques de engenharia social

De modo a atingir os seus objetivos, os atacantes recorrem a vários tipos de ataque de cariz social. Estes ataques podem ser realizados em qualquer sítio onde exista interação humana.

6.1 *Quid pro quo*

Quid pro quo, que significa "Something for something", é um ataque onde o atacante oferece algum benefício em troca de informações pessoais. Um simples ataque destes pode consistir apenas na oferta de uma pequena quantia monetária em troca de dados pessoais. Outro exemplo são os contactos com alegadas empresas que oferecem atualizações ao computador, fazendo com que as vítimas desativem os sistemas de segurança dos computados e permitindo que os atacantes tenham acesso aos seus dados [10].

Apesar de serem ataques simples e, muitas das vezes, facilmente detetáveis, muitos indivíduos estão dispostos a partilhar as suas informações pessoas em troca de simples ofertas.

6.2 *Baiting*

Baiting é um tipo de ataque semelhante ao *quid pro quo*, oferecendo às vítimas algo que desperte o seu interesse. Um exemplo deste ataque são os *websites* que oferecem *download* gratuito de conteúdos, como videojogos ou músicas. Ao descarregar esse conteúdo para o computador do utilizador, este contém um software malicioso que acaba por infetar o sistema.

6.3 *Phishing*

Phishing consiste na tentativa, por parte de atacantes, de obter informações confidenciais, como *passwords*, fazendo-se passar por entidades legítimas. Sendo este um dos ataques mais comuns, pode ser encontrado em diversos canais de comunicação, como emails, chamadas telefónicas, ou até mesmo *websites*. A taxa de sucesso destes ataques é muito alta pois, na maioria dos casos, os atacantes criam situações muito credíveis, como emails estruturados, endereços de remetente semelhantes aos das entidades reais, *websites* idênticos aos das entidades reais, entre outros [11].

O *phishing* pode então dividir-se em várias categorias, sendo elas:

6.3.1 *Spear phishing*

Este tipo de ataque é uma variação do *phishing* comum. Tem como alvo grupos específicos de indivíduos que podem variar, desde colaboradores de uma empresa com acesso a dados específicos, até grupos de empresas. Sendo este um ataque com um alvo em específico, requer um esforço maior e o ataque demora ainda mais tempo a ser planeado e realizado. Por norma estes são emails muitíssimo personalizados tendo em conta o alvo escolhido, para o qual o atacante investiga detalhadamente, tendo estes ataques, por norma, uma taxa de eficácia superior aos ataques de *phishing* comum, pois, apesar do volume de emails enviado ser, normalmente, muitíssimo baixo, como se trata de um ataque tão personalizado, é mais difícil de perceber [12].

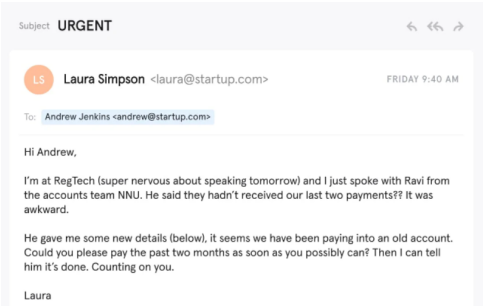
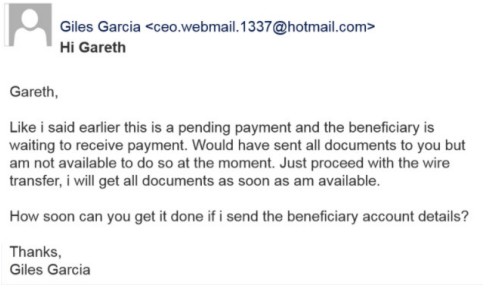


Figura 3: Exemplo de ataque de *spear phishing*

A figura apresenta um excelente exemplo de *spear phishing*, onde o atacante se faz passar por um colega de trabalho da vítima.

6.3.2 *Whaling*

Este ataque é também um tipo de *phishing*, sendo o ataque que possui alvos mais específicos. *Whaling* tem como alvos apenas pessoas com altos cargos em instituições, como cargos administrativos ou até CEOs de empresas.


Giles Garcia <ceo.webmail.1337@hotmail.com>
Hi Gareth

Gareth,

Like i said earlier this is a pending payment and the beneficiary is waiting to receive payment. Would have sent all documents to you but am not available to do so at the moment. Just proceed with the wire transfer, i will get all documents as soon as am available.

How soon can you get it done if i send the beneficiary account details?

Thanks,
Giles Garcia

Figura 4: Exemplo de um email de *whaling*

6.3.3 *Bulk phishing*

O *bulk phishing* é, provavelmente, o tipo de *phishing* mais utilizado. Neste caso, o atacante envia um enorme número de emails para um conjunto de indivíduos, como por exemplo colaboradores de uma instituição, de modo a que, em tantas possíveis vítimas, uma delas acesse um *link* e seja enganada pelo esquema. Este tipo de *phishing* é eficaz devido à abundância de possíveis vítimas geradas a partir do envio dos emails iniciais.

6.3.4 *Angler phishing*

Também considerado uma variante do *phishing* comum, o *angler phishing* tem como alvo os utilizadores de redes sociais. Os atacantes criam contas idênticas a contas de grandes entidades, tanto empresas como pessoas, e tentam enganar as vítimas, de modo a obter as suas informações pessoais. Muitas vezes, este processo tem ainda uma fase extra, onde o atacante promete benefícios à vítima, como por exemplo, vales monetários nas empresas em questão [13] [14].

6.3.5 *Smishing*

O *smishing* é outra variante do *phishing* comum. O seu nome deriva da junção de SMS (*Short Message Service*) e *phishing*. Estes ataques diferem do *phishing* tradicional por se realizarem através de SMS fraudulentos. Estes ataques tornaram-se muito comuns através de mensagens com pedidos de pagamento de taxas de saúde ou taxas alfandegárias [15].

6.3.6 *Vishing*

O *vishing* é uma variante do *phishing* comum semelhante ao *smishing*, onde o atacante tenta persuadir a vítima através de chamadas de voz, sendo que este nome deriva de *voice phishing*. Existem vários exemplos de ataques de *vishing*, tais como chamadas em que o atacante se faz passar por um representante bancário, ou até mesmo chamadas de *telemarketing*, onde o atacante tenta convencer a vítima que foi vencedora de um prémio [16].

6.4 *Diversion theft*

Os ataques de *diversion theft* são ataques em que os atacantes enganam empresas de transporte de mercadorias, fazendo-as acreditar que as suas encomendas devem ser entregues noutro local [17]. Por norma, estes ataques são feitos intercetando uma transação.

Existem vários exemplos de ataques deste tipo, como por exemplo:

- um atacante interceta uma compra de um computador, substitui o mesmo por um computador semelhante com *malware*, e envia-o para o comprador, ficando assim com acesso a tudo o que o comprador visualiza;

- um atacante pode intercetar todas as compras feitas de uma loja online, enviando aos compradores items falsos.

É também importante salientar que este tipo de ataques é extremamente perigoso pois pode ser usado em situações extremas como guerras, onde os atacantes deviam entregas importantes como medicamentos ou mantimentos.

6.5 *Watering hole*

Neste tipo de ataques que pode, ou não, ter um alvo especifico, o atacante tenta infetar um ou vários *websites* de modo a obter informações sobre os utilizadores do mesmo. No caso deste ataque ter alvos em específico, o atacante recorre a *websites* utilizados regularmente pelos mesmos [18]. Apesar deste tipo de ataques não ser muito comum, é bastante eficaz quando acontece, por serem muito impercetíveis.

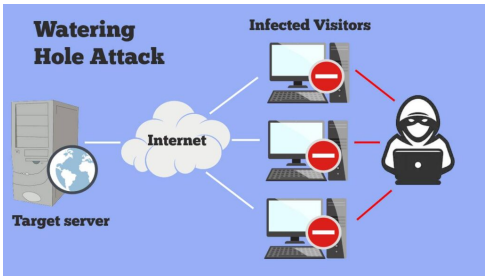


Figura 5: Como funciona o *watering hole*

6.6 *Pretexting*

Neste tipo de ataques, o atacante cria uma narrativa ou cenário fictício para convencer a vítima a partilhar informações importantes, como dados pessoais ou monetários. Um bom exemplo deste ataque são as chamadas telefónicas de pessoas que se fazem passar por trabalhadores de assistência técnica [19].

6.7 *Scareware*

Scareware é uma técnica de engenharia social que visa manipular as vítimas a pagarem por serviços falsos. Um destes exemplos é a tentativa de obter dinheiro através da remoção de suposto conteúdo malicioso do computador da vítima [20].

Estes ataques são feitos, na sua grande maioria, através de janelas *popup*. Assim que a vítima interage com o *popup*, é redirecionado para um *website* com conteúdo malicioso.

Figura 6: Exemplo de um *popup* de *scareware*

6.8 *HoneyTrap*

Este ataque tenta utilizar qualquer tipo de relacionamento entre o atacante e a vítima, de modo a obter acesso a dados e informações. Através de empatia e afeição, a vítima é facilmente enganada e fornece acesso aos seus dados confidenciais. Podem ser utilizados em vários contextos, como por exemplo *websites* e aplicações de encontros, onde o atacante tenta induzir a vítima a acreditar que existe uma relação entre ambos.

6.9 *Piggybacking*

Esta técnica é muitas vezes chamada *tailgating*, pois o atacante aproveita-se de utilizadores desinformados e pouco cautelosos para ter acesso aos seus dados confidenciais. Este tipo de ataque pode acontece através de vários meios, sendo que alguns deles podem nem ser pela via informática, podendo até o atacante se disfarçar de um colaborador de uma empresa de manutenção, aproveitando portas abertas por colaboradores da empresa, ou dispositivos, como computadores, que estejam desbloqueados, dando acesso ao atacante [21].

6.10 *Dumpster diving*

Este tipo de ataque baseia-se, não na interação entre o atacante e a vítima, mas sim na falta de cuidado da vítima. Os ataques de *dumpster diving* são ataques onde é feita uma busca nas imediações do alvo, procurando, por norma, em lixeiras ou caixotes do lixo por papéis ou notas que contenham informação ou dados importantes, como *passwords*, recibos, dados de cartões de crédito ou emails, que tenham sido deitados ao lixo de uma forma pouco cautelosa (riscar ou destruir os papéis) [22].

Este tipo de ataques pode ajudar na preparação de outros ataques de engenharia social, pois através de *dumpster diving*, o atacante pode obter informação importante sobre a vítima, que possa ajudá-lo a manipulá-la mais facilmente num outro ataque.

Figura 7: Funcionamento do *dumpster diving*

6.11 *Reverse social engineering*

A principal diferença entre este tipo de ataque e os restantes tipos de ataques de engenharia social é quem inicia a interação, sendo que, no caso da engenharia social reversa é, na maioria dos casos, a vítima a contactar o atacante, em busca de ajuda na resolução de um problema [23].

Na sua grande maioria, estes ataques iniciam-se após um problema, como *malware*, que chega ao computador da vítima, muitas vezes através de emails de *phishing* enviados pelo próprio atacante. Após ter o computador infetado, a vítima contacta o atacante, que pensa ser uma autoridade responsável pela resolução de problemas deste tipo, não sendo necessária a manipulação para o atacante obter os dados necessários (pois o facto da vítima contactar o atacante já significa que esta foi persuadida).

Como exemplo deste tipo de ataque é possível imaginar a seguinte situação:

1. O atacante envia um email com a descarga de um ficheiro que contém *malware*.
2. A vítima descarrega o ficheiro, ficando com o seu computador infetado e inutilizável.
3. Desesperada, a vítima procura algum contacto que resolva o seu problema, encontrando um contacto que pensa ser de assistência técnica, mas que se trata de um contacto do atacante.

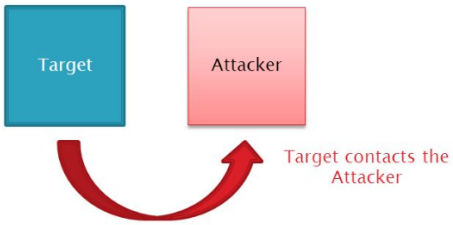


Figura 8: Imagem ilustrativa da engenharia reversa

4. A vítima contacta o atacante pensando que é alguém que irá resolver o seu problema, fornecendo todas as informações pedidas pelo mesmo.

Este tipo de ataque recorre a alguns métodos de persuasão, tais como a urgência ou a autoridade, de modo a manipular as vítimas [24].

7 Números de impacto

Dado que o número de ataques de engenharia social tem aumentado, novos estudos têm sido realizados e novos dados estatísticos têm surgido.

Nesta secção vão ser apresentados alguns estudos e dados estatísticos relevantes sobre o tema:

- entre 2013 e 2016, estima-se que, por ataques de engenharia social, tenham sido roubados cerca de 5 mil milhões de dólares em todo o mundo;
- de acordo com o FBI, as empresas vítimas destes ataques pagaram a atacantes cerca de 1.6 mil milhões de dólares, entre 2013 e 2017 [25].
- segundo a GlobalSign, mais de 70% de todas as falhas de segurança têm origem em ataques de engenharia social;
- em média, uma empresa é alvo de cerca de 700 ataques de engenharia social por ano;
- cerca de 71% dos profissionais da área das tecnologias afirmam que foram vítimas tentativas de ataques de engenharia social, sendo que 43% sofreram ataques no último ano.
- desde o início da pandemia de Covid-19, o número de ataques cibernéticos aumentou em cerca de 600% [26].

Segundo um estudo realizado pela CISCO, cerca de 80% de todos os ciberataques realizados em 2021 foram ataques de *phishing* ou de alguma das suas variantes [27]. Dada a enorme quantidade destes ataques, é também interessante apresentar alguns dados estatísticos sobre o *phishing*, em particular:

- de acordo com a Tessian, uma empresa de *software* sediada em Londres, cerca de 96% dos ataques de *phishing* recorrem à utilização de emails [28].
- segundo a Optimal Networks, *phishing* é o tipo de ataque que mais recorre à utilização de *ransomware* (em 2016, o número de ataques por *ransomware* era, em média, de 4 mil por dia);
- em 2020, o maior número de ataques e *phishing* foi registado na Mongólia;
- *spear phishing* é o método predominante no ataque a empresas, com 95% do número total de ataques;
- os *websites* do Facebook e da Microsoft são os mais replicados para utilização em ataques de *phishing*, sendo que representam 14% e 13% de todos os *websites* de *phishing*, respetivamente;
- 11% das empresas vítimas de ataques de *phishing* em 2021 foram multadas, devido ao incumprimento das medidas rígidas que existem relativas à segurança de dados;
- através de ataques de *phishing*, cerca de 15 mil dólares são roubados por minuto;
- estima-se que, anualmente um CEO é alvo de 57 ataques de *phishing*, em média;
- em 2020, a Google removeu cerca de 2.1 milhões de *websites* devido a denúncias de *phishing*;
- cerca de 84% dos *websites* de *phishing* utiliza SSL, dando uma aparência legítima e confiável aos mesmos;
- um ataque de *phishing* bem sucedido custa às instituições cerca de 5 milhões de dólares, em média [27];
- em 2021, cerca de 83% das empresas dos EUA foram vítimas de ataques de *phishing*. Este é uma aumento muito significativo, visto que, em 2020, apenas 37% das empresas foram vítima [29].

Analisando todos estes dados e resultados de estudos é possível perceber não só o quão frequentes e numerosos são os ataques deste tipo, mas também o abalo económico que estes trazem às empresas, bem como a enorme quantidade de dinheiro conseguida por parte dos atacantes.

8 Exemplos de ataques em grande instituições

O tema da engenharia social é um tema de alta relevância atualmente. São cada vez mais as notícias em jornais, revistas, rádio, Internet ou televisão sobre ataques e novas estratégias de *phishing* ou burla através de ataques de engenharia social. São às centenas os ataques a grandes instituições que utilizaram algum tipo de engenharia social, entre todos eles, podem destacar-se os seguintes:

- **2013, Target**
  - Em 2013, devido a uma falha de segurança causada por um ataque de segurança social, foram roubados dados de cerca de 40 milhões de clientes da Target.
  - Através de emails de *phishing*, os atacantes conseguiram inserir *malware* que lhes permitiu aceder à rede da empresa, roubando os dados de milhões de pessoas.
  - Este ataque torna-se realmente dedicado, pois entre os dados roubados de clientes, estavam as informações sobre cartões de crédito.
  - Foi estimado pela empresa que este ataque tenha resultado num prejuízo de cerca de 202 milhões de dólares[30].
- **2013, Sony Pictures**
  - Em 2013, a companhia Sony Pictures foi alvo de um ataque de *phishing* que conseguiu roubar milhares de documentos confidenciais com sucesso.
  - Neste ataque de *phishing*, os atacantes enviaram um email fazendo-se passar pela Apple.
  - Após investigação, foi revelado que o ataque teve como origem o governo da Coreia do Norte [31][30].
- **2013-2015, Google e Facebook**
  - Entre 2013 e 2015, um indivíduo da Lituânia, Evaldas Rimasauskas, criou um esquema de *spear phishing*, onde enviava vários emails a funcionários da Google e do Facebook, fazendo-se passar por um fabricante de computadores, pedindo-lhes dinheiro por serviços e equipamentos que as empresas tinham efetivamente comprado, mas esse dinheiro iria ser depositado em contas fraudulentas.
  - Este esquema roubou cerca de 100 milhões de dólares às duas empresas [32].
- **2013-2015, Crelan**
  - Entre 2013 e 2015, o banco belga Crelan foi alvo de um dos ataques de engenharia social com mais sucesso de sempre.
  - Foram enviados vários emails de *phishing* aos membros com cargos mais elevados das instituições, fornecendo dados de acesso aos atacantes, roubando ao banco cerca de 75 milhões de dólares [32].
- **2015-2016, FACC**
  - Entre 2015 e 2016, a empresa FACC, que fabrica componentes para aeronaves, foi alvo de um ataque que a fez perder cerca de 61 milhões de dólares.
  - Este ataque ficou conhecido como "fake president scam", pois o atacante enviou um email à empresa fazendo-se passar pelo CEO da mesma, utilizando um endereço de email, estrutura e composição de texto semelhantes, pedindo que fossem transferidos 61 milhões de euros para uma conta que estava na sua posse [32].
- **2016, Partido Democrata dos EUA**
  - Um dos casos mais icónicos de engenharia social aconteceu em 2016, quando foram partilhados emails e informações confidenciais sobre o partido republicano.
  - Neste ataque de *spear phishing*, foi enviado um email a vários membros do partido democrata a pedir que fosse alterada a sua palavra passe do email devido a atividade suspeita. As vítimas deste ataque acabaram por ter os seus emails comprometidos, o que levou a que

fossem expostas publicamente informações sobre o partido, bem como sobre a candidatura de Hilary Clinton à presidência do país.

  - Este ataque teve um valor incalculável, pois pode ter influenciado o resultado da eleição, onde o partido democrata saiu vencido [31][30].

- **2019, Companhia de Energia do Reino Unido**
  - Em março de 2019, o CEO de uma empresa de energia do Reino Unido recebeu uma chamada de um atacante que se fez passar pelo seu patrão, manipulando-o a transferir 243 mil dólares para uma conta que pertenceria a um fornecedor na Hungria, mas que, na realidade, era uma conta do atacante [32].
- **2019, Toyota**
  - Em 2019, a Toyota, uma das maiores produtoras automóveis de todo o mundo, foi vítima de um ataque com prejuízos de cerca de 37 milhões de dólares.
  - Neste ataque, os atacantes persuadiram um gestor financeiro a mudar as informações do recipiente de uma transferência [30].
- **2020, Júri do Shark Tank**
  - Em 2020, Barbara Corcoran, júri do Shark Tank, foi vítima de um ataque de *phishing* que a fez perder cerca de 400 mil dólares.
  - Neste ataque, o atacante fez-se passar pela assistente, criando um endereço de email semelhante ao da mesma, pedindo-lhe para transferir a quantia que seria referente ao investimento em propriedades [31][30].
- **2020, Twitter**
  - Em 2020, um grupo de *hackers* teve controlo de cerca de 150 contas de Twitter pertencentes a celebridades, como Barack Obama ou Kayne West.
  - Os atacantes utilizaram estas contas para criar publicações a pedir doações para uma carteira de Bitcoin, onde conseguiram cerca de 110 mil dólares.
  - Este ataque teve também como consequência uma redução em cerca de 7% do valor das ações da empresa [32].
- **2021, Sacramento County**
  - Em junho de 2021, cinco colaboradores de Sacramento County revelaram as suas credenciais de acesso após serem vítimas de ataques de *phishing* via email.
  - Este ataque resultou na partilha dos dados sobre o histórico de saúde de cerca de 2096 indivíduos, bem como 816 históricos sobre dados pessoais.
  - Este ataque resultou em prejuízo para o Sacramento County, visto que foi obrigado a oferecer a todas as vítimas serviços de proteção de roubo de identidade e monitorização bancária [32].
- **2021, Oversea Chinese Banking Corporation**
  - Em dezembro de 2021, clientes da Oversea Chinese Banking Corporation foram alvos de vários ataques de *phishing* e transações maliciosas, resultando em perdas de cerca de 8.5 milhões de dólares, distribuídos por cerca de 470 vítimas.
  - Estes ataques ocorreram, pois as vítimas foram bombardeadas por emails de *phishing*, levando-as a inserir os seus dados ou fazerem transferências para contas bancárias pertencentes a atacantes [32].
- **2022, Rússia vs Ucrânia**
  - Em fevereiro de 2022, a Microsoft lançou avisos sobre ataques de *spear phishing*.
  - Esses ataques tinham como alvos o governo ucraniano e algumas ONGs.
  - Este ataque foi realizado pelo grupo russo Gamaredon e consistia no envio de vários emails que continham *malware*.

- Este ataque é uma excelente prova que, com o avanço do tempo e tecnologia, ataques informáticos e de engenharia social são uma arma importantíssima [32].

Após analisar todos estes ataques, bem como o prejuízo que os mesmos causam às empresas, é possível afirmar que ser vítima de um ataque de engenharia social pode tornar-se muito dispendioso para uma empresa, podendo resultar, não só na perda de milhões de dólares, mas também na desvalorização da empresa, e possível perda de clientes, por medo ou falta de confiança. É também possível perceber que qualquer empresa pode ser alvo de um ataque, o que prova que é necessário que todas as instituições tomem medidas preventivas para evitar serem vítimas destes ataques.

9 Como evitar ataques de engenharia social

Como foi explicado nas secções anteriores, os ataques de engenharia social são realizados pelos mais variados meios, desde emails, SMS, chamadas telefónicas ou, até mesmo, através da procura de papéis em caixotes do lixo.

Para evitar que tais ataques aconteçam, é necessário que exista um elevado grau de prevenção em todos os setores para minimizar ao máximo a exposição a estes ataques.

Foi estimado que uma instituição demora em média 146 dias para detetar que existiu um ataque de engenharia social, o que se resume a, aproximadamente, cinco meses, sofrer um ataque deste tipo significa que durante, aproximadamente, cinco meses, um atacante pode ter acesso a toda a informação de uma instituição. Dado o perigo destes ataques e a necessidade de tomar medidas, algumas das formas de prevenção de ataques de engenharia social são:

9.1 Prevenção em instituições

Dado que este tipo de ataques tem muitas vezes como alvos grandes grupos de colaboradores em instituições, de modo a obter dados de acesso que providenciem, posteriormente, acesso a dados confidenciais das instituições, é importante que estas invistam em estratégias que forneçam ferramentas aos seus colaboradores, para estes conseguirem identificar este tipo de ataques. Algumas das estratégias que podem ser implementadas podem ser as seguintes [33]:

- **Utilização de certificação SSL**
  - A encriptação dos dados através de *Secure Socket Layer* minimiza os problemas causados pelo acesso aos dados por parte de atacantes.
- **Utilização de autenticação *multi-factor***
  - A utilização de algo mais do que apenas a *password* para autenticação obrigaria os atacantes a repensar na sua estratégia, de modo a conseguirem executar um ataque eficaz o suficiente para obter todos os fatores de autenticação.
- **Monitorização constante de sistemas críticos**
- **Implementação de políticas apropriadas para procedimentos chave**
  - Implementação de políticas que obriguem operações que envolvam dados confidenciais sejam realizadas apenas *face-to-face*, podendo reduzir a taxa destes ataques.
- **Implementação de políticas sobre o uso de redes sociais**
  - Dado que existe um elevado número de utilizadores que partilham demasiada informação nas suas redes sociais, limitar o que cada colaborador da instituição pode ou não postar pode reduzir o número de ataques.
- **Aumentar a filtragem de emails *spam***
  - Dado que se estima que cerca de 45% de todo o email a circular seja *spam*, a implementação de bons *email gateways* pode prevenir quase a totalidade do *spam*.

- **Formações de sensibilização de segurança**
  - Talvez a mais importante de todas as políticas de prevenção de ataques deste tipo, a formação de colaboradores para a identificação de ameaças pode ser essencial na prevenção destes ataques.
  - Um colaborador saber quando algo é, ou não, uma tentativa de *phishing* é suficiente para evitar um ataque por completo.
- **Simular ataques de engenharia social**
  - Após realizar formações de sensibilização de segurança, é útil que os colaboradores da instituição passem por situações de simulação de ataques periodicamente.

9.2 Prevenção individual

Diariamente, somos bombardeados com tentativas de ataques de engenharia social dos mais variados tipos, tornando essencial que todos tomem medidas para evitar ser vítimas de um ataque que possa pôr em risco os seus dados.

Alguns exemplos destas medidas são [34]:

- **Aumentar os filtros de *spam* do email**
  - Ao aumentar os filtros de *spam* resultaria numa redução da probabilidade de uma tentativa de ataque por email.
- **Não utilizar *passwords* semelhantes**
  - Ao utilizar a mesma *password* em várias contas, todos os dados do utilizador estarão comprometidos ao sofrer um ataque que dê ao atacante a *password*.
- **Alterar *passwords* regularmente**
- **Verificação de fontes**
  - Ao receber emails, contactos telefónicos ou SMS, verificar se o emissor é fidedigno pode ajudar a detetar ataques.
  - No caso de emails, verificar irregularidades como erros ortográficos ou linguagem genérica, muito comuns em emails de *phishing*.

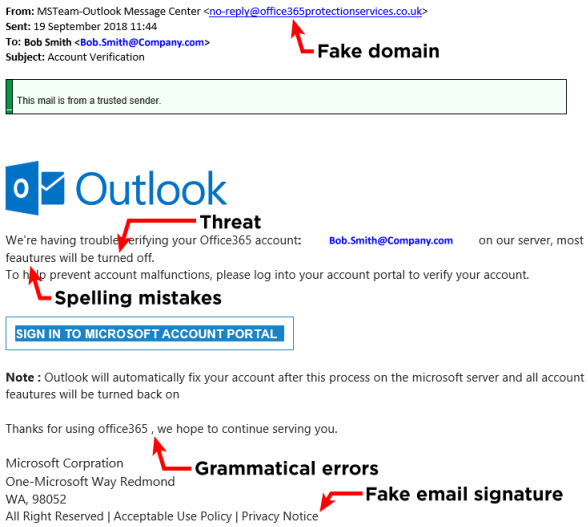


Figura 9: Alguns indicadores de que um email se trata de *phishing*

- **Ignorar pedidos de credenciais**
  - Entidades fidedignas não enviam pedidos de credenciais via email ou telefone, o que é, por norma, um sinal de tentativa de *phishing*.
- **Não realizar *downloads* de *websites* não confiáveis**
  - A não verificação de *downloads* da Internet pode significar o descarregamento de um ficheiro que contenha *malware* que permita a um atacante obter o acesso aos dados do sistema.
- **Privacidade nas redes sociais**
  - Muitos utilizadores de redes sociais expõem demasiados dados pessoais publicamente, tornando-os alvos fáceis.
  - É importante ter cuidado com a seleção dos dados colocados publicamente, de modo a não partilhar dados sensíveis.
- **Duvidar de situações de urgência**
  - Muitos ataques de engenharia social utilizam a urgência como tática para tentar persuadir as vítimas.
  - Um utilizador deve sempre duvidar de pedidos de ajuda monetária, informações, ou dados que tenham um carácter muito urgente.

Mesmo com um elevado número de estudos lançados sobre o impacto dos ataques de engenharia social em instituições, um estudo realizado pela GetApp estimou que, apenas cerca de 27% das empresas toma algum tipo de medidas, de modo a evitar ataques de engenharia de social, o que é um número baixíssimo sabendo que existem vários indicadores sobre como se proteger contra estes ataques, que podem originar vários milhões de euros em prejuízo.

10 Conclusão

Com a elaboração deste trabalho foi possível adquirir novos conhecimentos sobre a temática da engenharia social, chegando às seguintes conclusões:

- a engenharia social consiste em qualquer tipo de tentativa de manipulação de pessoas, com o objetivo de obter dados confidenciais;
- os ataques de engenharia social representam um enorme perigo na vida de todos, pois podem implicar a publicação de dados confidenciais roubados ou até perdas monetárias de grande escala;
- para aumentar a taxa de sucesso dos ataques, um atacante deve utilizar métodos de persuasão que facilitem a manipulação da vítima, tal como a criação de empatia, sensação de autoridade, intimidação da vítima ou criação de sensações de urgência;
- um ataque de engenharia social com sucesso segue um ciclo de vida específico, onde primeiro, o atacante deve identificar os alvos e reunir informação para escolher qual o tipo de ataque, para depois começar a interação, onde irá roubar os dados e eliminando, no final, todos os indícios que comprovem a existência do ataque;
- existe uma extensa lista de tipos de ataques de engenharia social, como *bulk phishing*, *watering hole* ou *dumpster diving*, sendo que o atacante deve escolher qual o mais indicado para cada situação;
- sendo que o tema da engenharia social é um tema atual e presente na vida de todos, existem vários estudos lançados que comprovam a frequência destes ataques e o prejuízo que estes podem causar em empresas;
- a lista de instituições que foram vítimas de ataques de engenharia social é bastante extensa, estando presentes grandes empresas como o *Facebook* ou a *Toyota*, o que mostra que qualquer pessoa pode ser vítima da engenharia social;
- para minimizar o risco de ataques deste tipo, é importante que as empresas tomem medidas como treinar os seus colaboradores, de modo a que estes saibam identificar estes ataques, ou simular ataques de engenharia social, para que os seus colaboradores sejam testados.

Referências

[1] Wikipedia. Engenharia social. https://pt.wikipedia.org/wiki/Engenharia_social_(seguran\unhbox\voidb@x\setbox\z@\hbox{c}\accent24ca). Accessed: 26-05-2022.

[2] Webroot. What is social engineering. https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering. Accessed: 26-05-2022.

[3] Kaspersky. What is social engineering. https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering. Accessed: 26-05-2022.

[4] Softwarelab. Engenharia social. https://softwarelab.org/pt/engenharia-social/. Accessed: 26-05-2022.

[5] Zbigniew Banach. The dangers of social engineering attacks. https://www.invicti.com/blog/web-security/social-hacking-social-engineering-attacks/. Accessed: 25-05-2022.

[6] Dale Shulmistra. Why social engineering is so dangerous. https://www.linkedin.com/pulse/why-social-engineering-so-dangerous-dale-shulmistra/. Accessed: 25-05-2022.

[7] Davide Andreoletti. What persuasion techniques are generally employed in phishing e-mails? https://www.dogana-project.eu/index.php/social-engineering-blog/11-social-engineering/42-persuasion-techniques. Accessed: 26-05-2022.

[8] Michael Kassner. 6 persuasion tactics used in social engineering attacks. https://www.techrepublic.com/article/6-persuasion-tactics-used-in-social-engineering-attacks/. Accessed: 26-05-2022.

[9] Imperva Team. What is social engineering. https://www.imperva.com/learn/application-security/social-engineering-attack/. Accessed: 27-05-2022.

[10] Mailfence Team. What is quid pro quo. https://medium.com/@Mailfence/social-engineering-quid-pro-quo-attacks-30d39ebdf5f7/. Accessed: 26-05-2022.

[11] Phishing.org. What is phishing. https://www.phishing.org/what-is-phishing/. Accessed: 26-05-2022.

[12] Tessian. Phishing vs spear phishing. https://www.tessian.com/blog/phishing-vs-spear-phishing//. Accessed: 26-05-2022.

[13] Amanda Hicks. What is angler phishing. https://www.clearviewfcu.org/Learn/about-financial-wellness/Blog/Angler-Phishing-What-is-it/. Accessed: 26-05-2022.

[14] Luke Irwing. Beware of angler phishing. https://www.itgovernance.co.uk/blog/beware-of-angler-phishing/. Accessed: 26-05-2022.

[15] Kaspersky. What is smishing. https://www.kaspersky.com.br/resource-center/threats/what-is-smishing-and-how-to-defend-against-it/. Accessed: 26-05-2022.

[16] TerraNova Security. What is vishing. https://terranovasecurity.com/what-is-vishing//. Accessed: 26-05-2022.

[17] Hasmik Khachunts. What is diversion theft? https://securityboulevard.com/2022/02/what-is-diversion-theft-attack-and-defense-strategies//. Accessed: 26-05-2022.

[18] Madelyn Bacon. What is a watering hole attack? https://www.techtarget.com/searchsecurity/definition/watering-hole-attack. Accessed: 26-05-2022.

[19] Thomas Wilhelm. What is pretexting. https://www.sciencedirect.com/topics/computer-science/pretexting/. Accessed: 26-05-2022.

[20] Fortinet. What is scareware. https://www.fortinet.com/resources/cyberglossary/scareware/. Accessed: 26-05-2022.

[21] Ty Mezquita. Piggibacking. https://cyberhoot.com/cybrary/piggybacking//. Accessed: 26-05-2022.

[22] Linda Rosencrance. social engineering. https://www.techtarget.com/searchsecurity/definition/social-engineering. Accessed: 26-05-2022.

[23] Ira S. Winkler. Social engineering and reverse social engineering. http://www.ittoday.info/AIMS/DSM/82-10-43.pdf. Accessed: 26-05-2022.

[24] Aware Team. What is reverse social engineering? and how does it work? https://aware.eccouncil.org/what-is-reverse-social-engineering.html. Accessed: 27-05-2022.

[25] Cynthia Lopez Olson. Social engineering attacks by the numbers: Prevalence, costs, impact. https://datafloq.com/read/social-engineering-attacks-numbers-cost/. Accessed: 26-05-2022.

[26] Purplesec Team. 2021 cyber security statistics the ultimate list of stats, data trends. https://purplesec.us/resources/cyber-security-statistics/. Accessed: 26-05-2022.

[27] SPANNING CLOUD APPS. Cyberattacks 2021: Phishing, ransomware data breach statistics from the last year. https://spanning.com/blog/cyberattacks-2021-phishing-ransomware-data-breach-statistics/. Accessed: 28-05-2022.

[28] Nick Galov. 17+ sinister social engineering statistics for 2022. https://webtribunal.net/blog/social-engineering-statistics/. Accessed: 26-05-2022.

[29] Catherine Reed. 21 social engineering statistics – 2022. https://firewalltimes.com/social-engineering-statistics/. Accessed: 26-05-2022.

[30] Gatefy. 10 real and famous cases of social engineering attacks. https://gatefy.com/blog/real-and-famous-cases-social-engineering-attacks/. Accessed: 25-05-2022.

[31] Clara Julio. Ataque de engenharia social: o que é, principais tipos e casos. https://backupgarantido.com.br/blog/ataque-de-engenharia-social/. Accessed: 25-05-2022.

[32] Gatefy. 10 real and famous cases of social engineering attacks. https://gatefy.com/blog/real-and-famous-cases-social-engineering-attacks/. Accessed: 25-05-2022.

[33] Stick Mancyber. 8 ways organisations prevent social engineering attacks. https://www.stickmancyber.com/cybersecurity-blog/8-ways-organisations-prevent-social-engineering-attacks. Accessed: 26-05-2022.

[34] Digital Hands. How to avoid social engineering attacks. https://www.digitalhands.com/guides/how-to-avoid-social-engineering-attacks. Accessed: 26-05-2022.