UNIVERSIDADE PORTUCALENSE

ENGENHARIA SOCIAL

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Engenharia social

"You could spend a fortune purchasing technology and services...and your network infrastructure could still remain vulnerable to old-fashioned manipulation."

-Kevin Mitnick

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

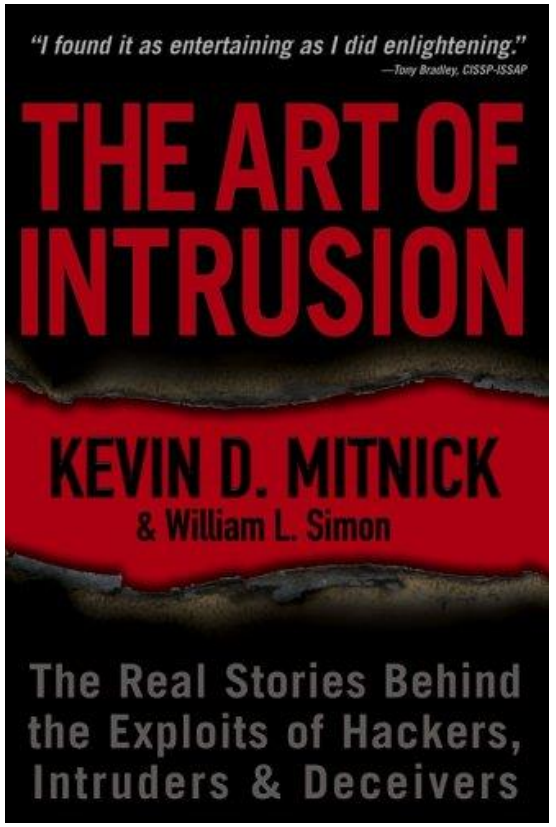
Engenharia social

- Engenharia Social é a arte de manipular pessoas de modo a que elas executem ações ou divulguem informações confidenciais;
- Este tipo de ataque não é técnico e depende fortemente de interação humana;
- Os hackers utilizam ataques de engenharia social para obter informações que lhes permitiram obter acesso não autorizado a um sistema e às informações que nele residem.

UNIVERSIDADE PORTUCALENSE

Engenharia social

- O termo engenharia social tornou-se popular pelo ex-criminoso Kevin Mitnick



DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Engenharia social

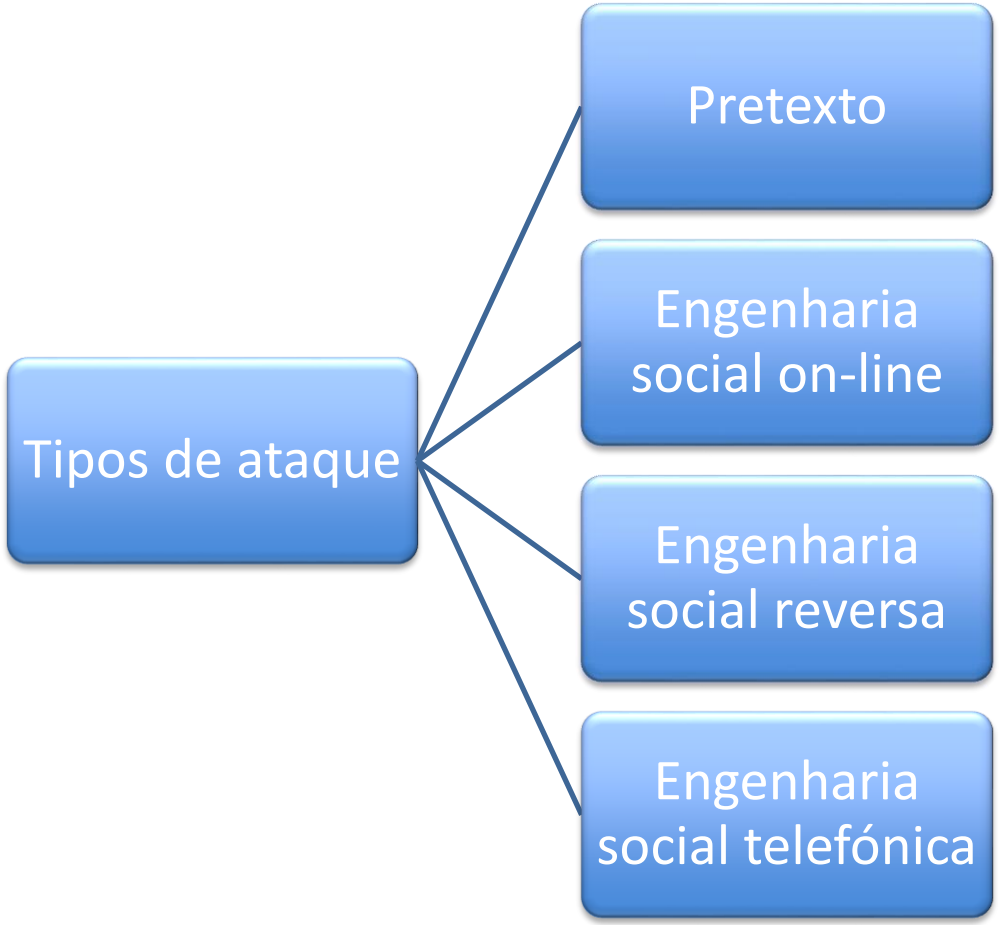
- Confessou ter acedido ilegalmente a redes privadas e possuir documentos falsos.
- Afirmou que usou apenas técnicas de engenharia social sem a ajuda de programas de software.

  “Testifying before Congress not long ago, I explained that I could often get passwords and other pieces of sensitive information from companies by pretending to be someone else and *just asking for it*.” - Kevin Mitnick

UNIVERSIDADE PORTUCALENSE

Engenharia social

Tipos de ataque



DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Engenharia social

Tipos de ataque - Pretexto

- O ato de criação e utilização de uma situação inventada a fim de convencer um alvo para divulgar informações ou conceder acesso a materiais sensíveis.

- Este tipo de ataque é normalmente implementado através do telefone e pode ser utilizado para obter informações de clientes, registos telefónicos, registros bancários e também é usado por investigadores privados.

UNIVERSIDADE PORTUCALENSE

Engenharia social

Tipos de ataque - Pretexto

- O hacker disfarça a sua identidade, a fim de poder colocar uma série de questões destinadas a obter a informação que necessita do seu alvo.

- Fazendo estas perguntas a vítima, sem saber, fornece ao atacante as informações que o hacker precisa para realizar o seu ataque.

UNIVERSIDADE PORTUCALENSE

Engenharia social

Tipos de ataque – On-line

- Este ataque explora o fato de que muitos utilizadores utilizarem a mesma senha para todas as suas contas online, como por exemplo, para o e-mail, serviços bancários, contas ou facebook.
- Portanto, uma vez que um atacante tem acesso a uma conta tem acesso a todas elas.
- Outro ataque on-line comum é quando um hacker finge ser um administrador de rede e envia e-mails a solicitar nomes de utilizadores e senhas.

UNIVERSIDADE PORTUCALENSE

Engenharia social

Tipos de ataque – On-line

Byod Maior evento Wireless em Portugal. - www.wirelessmeeting2013.com - 21 março. Veja aqui a programação!

Confirmar a sua identidade EMAIL Bin x

WEBMASTER HELP DESK <rdominguez5@mail.csuchico.edu> 8 Mar (2 days ago)

to bcc:

...

--

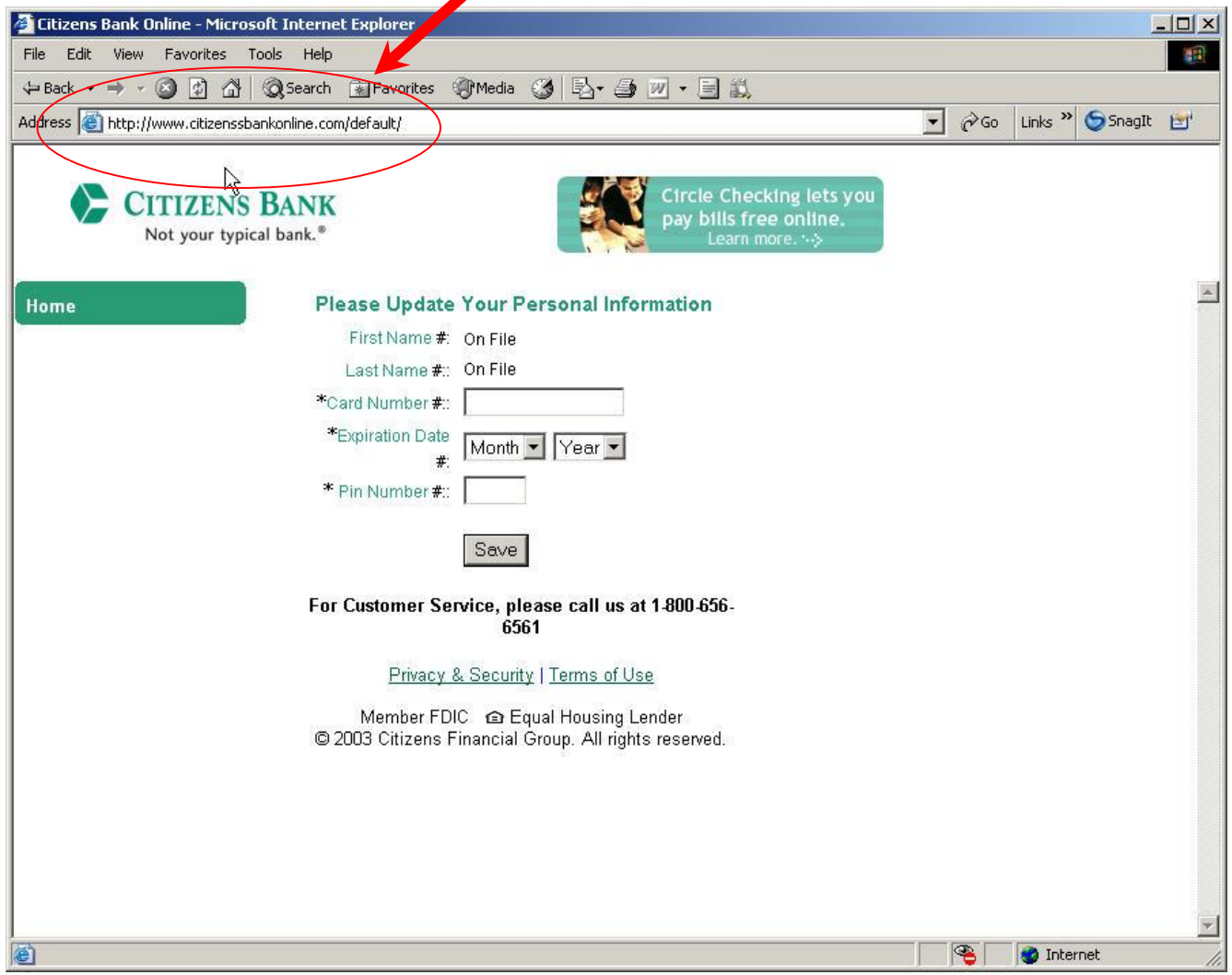
Sua caixa de correio excedeu o limite de 2GB estabelecida pelo nosso webmaster, você está executando no 2.30GB você não pode enviar ou receber novas mensagens até que você confirme sua caixa de entrada.
Clique no link para validar a sua conta
http://celebration.myccav.com/accupdate

obrigado
Administrador do Sistema

DICT DEPARTAMENTO **INOVAÇÃO CIÊNCIA E TECNOLOGIA**

UNIVERSIDADE PORTUCALENSE

Phishing



Site real: www.citizensbank.com

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Engenharia social

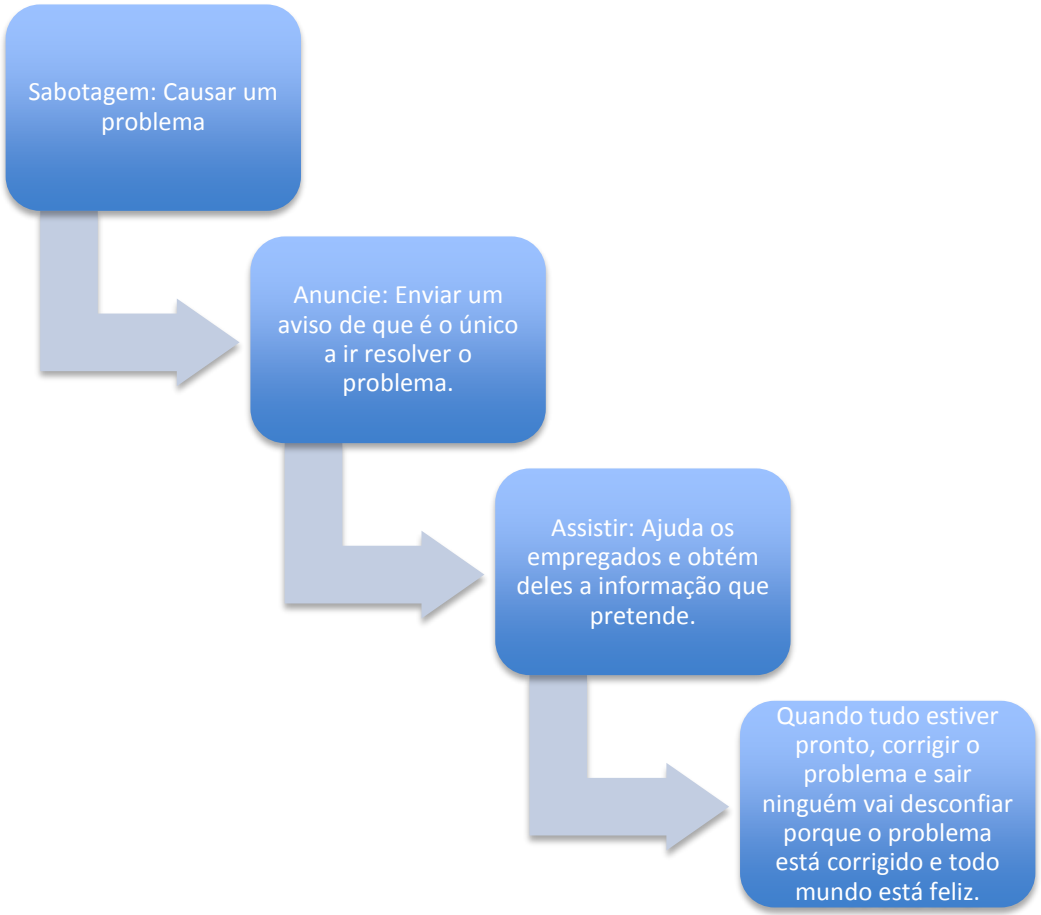
Tipos de ataque – Engenharia social reversa

- Provavelmente o menos utilizado dos ataques.
- Requere uma extensa pesquisa e planeamento.
- A chave é estabelecer-se numa posição de autoridade de forma a que os alvos venham até si.
- Dando-lhe uma melhor chance de recuperar informações.

UNIVERSIDADE PORTUCALENSE

Engenharia social

Tipos de ataque – Engenharia social reversa



DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Engenharia social

Tipos de ataque – Engenharia social telefónica

- A prática mais comum de engenharia social
- O hacker entra em contato, simulando ser uma pessoa de autoridade e, lentamente, obtém informações que necessita.
- Os serviços de help-hesk estão incrivelmente vulneráveis a este tipo de ataque.

UNIVERSIDADE PORTUCALENSE

Engenharia social

Aspetos dos ataques

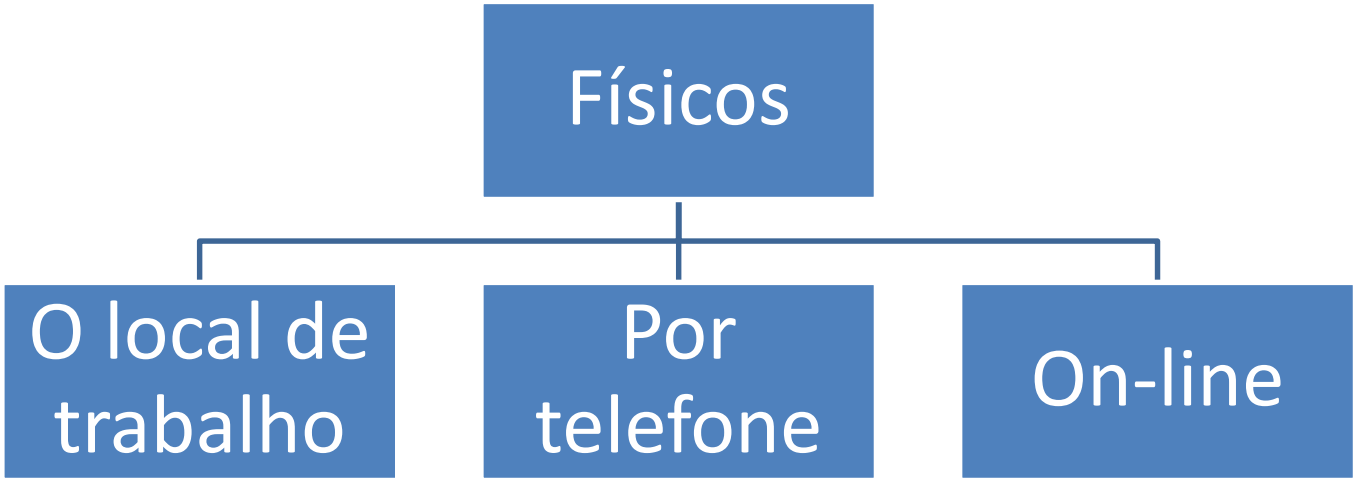
Os ataques de Engenharia Social podem ter dois aspetos diferentes:

- **Físico**: local de trabalho, por telefone, no lixo ou mesmo on-line.
- **Humano/psicológico**: refere-se à maneira como o ataque é executado.

UNIVERSIDADE PORTUCALENSE

Engenharia social

Aspetos dos ataques



UNIVERSIDADE PORTUCALENSE

Engenharia social

Aspetos dos ataques

UNIVERSIDADE PORTUCALENSE

Persuasão

- Na tentativa de convencer alguém a fazer algo. Há dois métodos que um persuasor pode utilizar:
  - Um caminho direto
  - Um caminho periférico

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Persuasão

- No caminho direto usa:
  - Argumentos sistemáticos;
  - Argumentos lógicos;
- Para:
  - Estimular uma resposta favorável;
  - Levar o destinatário a ação;

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Persuasão

- Um caminho periférico utiliza:
  - Atalhos mentais periféricos;
  - Pistas que deturpam seus objetivos;
- Para:
  - Aceitar sem pensar

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Representação

- Estudos de caso indicam que o help-desk é o alvo mais frequente de ataques de engenharia social.
  - Um engenheiro social chama o suporte técnico
  - Help-desk é útil
  - O engenheiro social muitas vezes vai saber nomes de funcionários

UNIVERSIDADE PORTUCALENSE

Utilizador importante

- Um truque comum é fingir ser não apenas um empregado, mas um vice-presidente.
  - O help-desk é menos provável de recusar um pedido vindo de um quadro de alto nível;
  - Engenheiro social pode ameaçar denunciar o empregado ao seu supervisor.

UNIVERSIDADE PORTUCALENSE

Autorização de terceiros

- O engenheiro social pode ter obtido o nome de alguém da organização que tem a autoridade para conceder acesso a informações.
  - Sra. Martinez deu o OK.
    - Antes de entrar de férias, a Sra. Martinez disse eu deveria chamá-lo para obter esta informação.

UNIVERSIDADE PORTUCALENSE

Suporte técnico

- O Engenheiro social finge ser alguém dos grupos de suporte de infraestrutura.
  - O sistema está com um problema – precisa deles para fazer logon para testar a ligação

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Engenharia social

Proteger contra estes ataques (físicos)

- Os ficheiros mais importantes devem ser guardados de forma segura;
- Destruir os papeis importantes antes de os eliminar;
- Apagar todos os meios de gravação magnética (discos duros, pens, etc.);
- Todas as máquinas na rede devem ser bem protegidas com palavras chave;
- Cuidado com o “lixo”.

UNIVERSIDADE PORTUCALENSE

Engenharia social

Proteger contra estes ataques (físicos)

- As instituições normalmente não se protegem do aspeto psicológico da engenharia social deixando-as desprotegidas para este tipo de ataques.
- O que procurar: recusa em fornecer informações de contato, apressar-se, intimidação, pequenos erros e solicitando informações protegidas.
- Coloque-se no lugar dos hackers. Pense como um hacker.

UNIVERSIDADE PORTUCALENSE

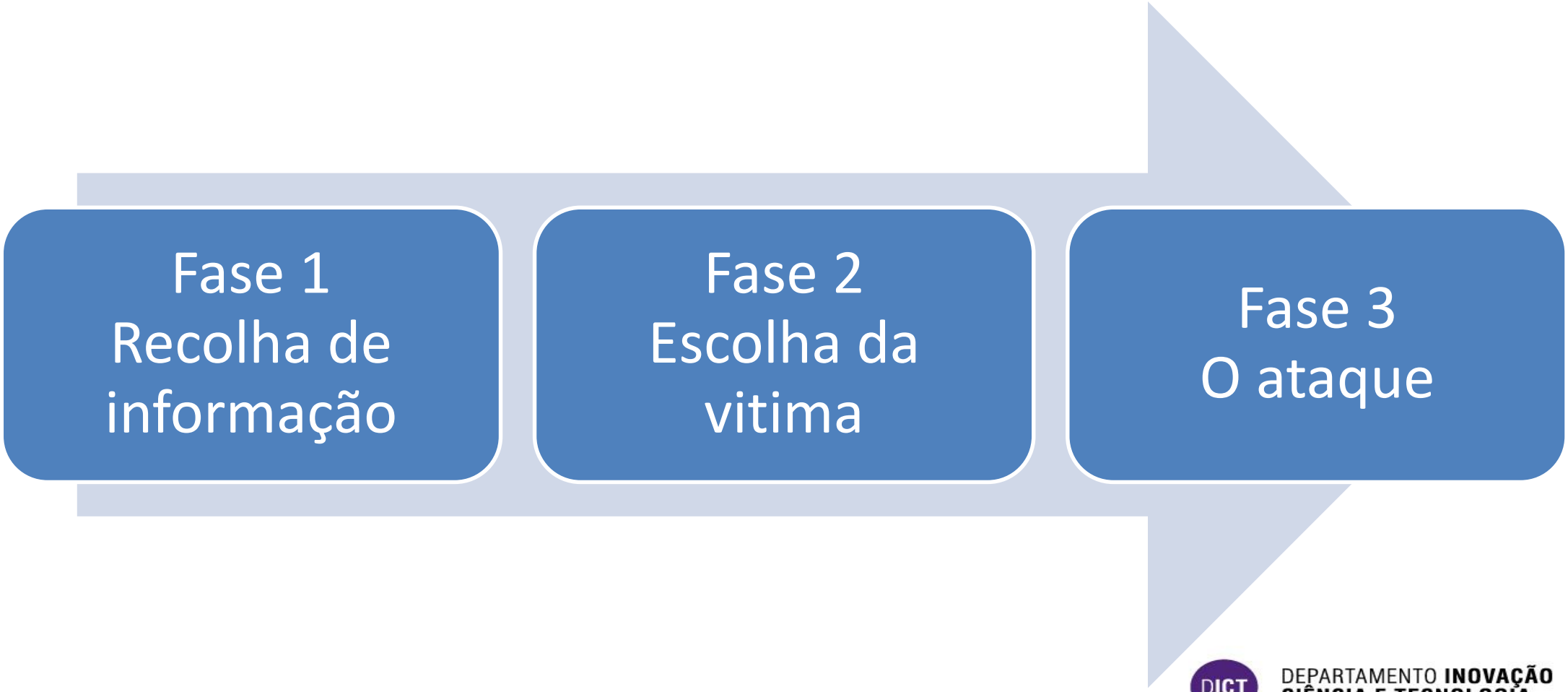
Anatomia de um ataque

ENGENHARIA SOCIAL

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

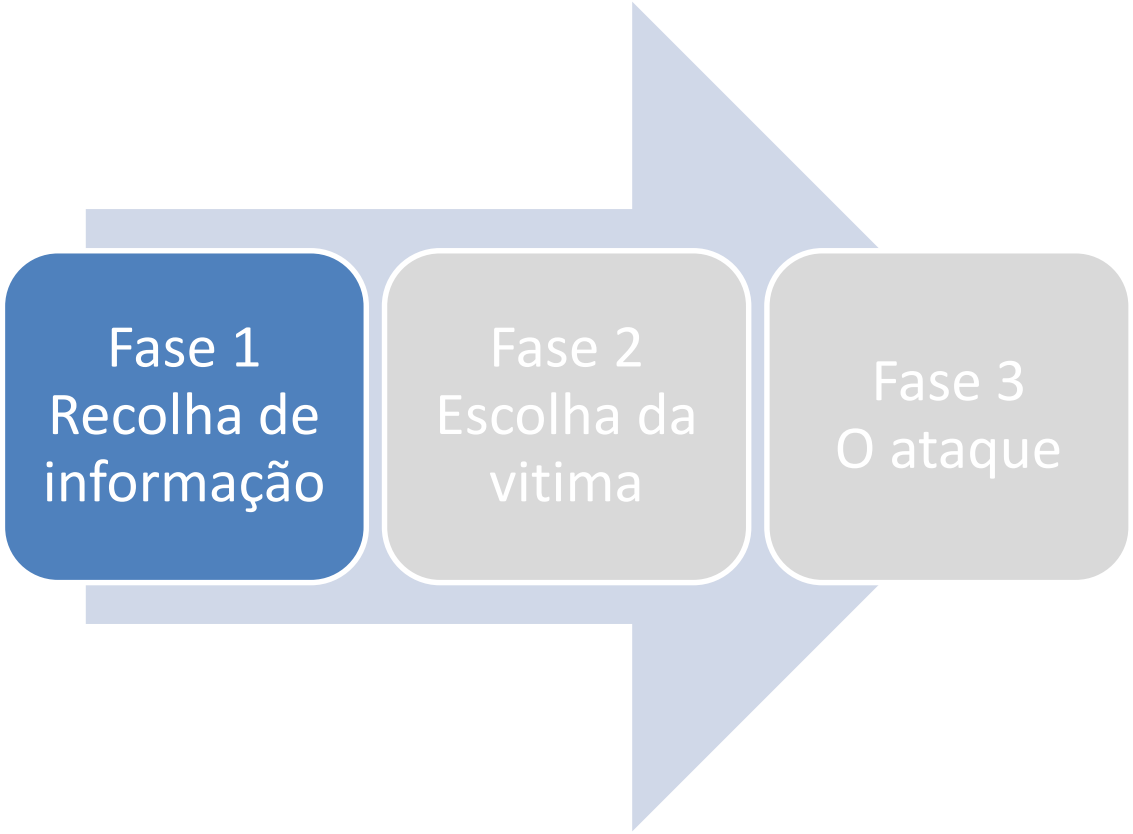
Anatomia de um ataque



DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Anatomia de um ataque



- Principalmente informações de fonte aberta
  - Análise do “lixo”
  - Páginas web
  - Ex-empregados
  - Prestadores de serviços
  - Fornecedores
  - Parceiros estratégicos

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

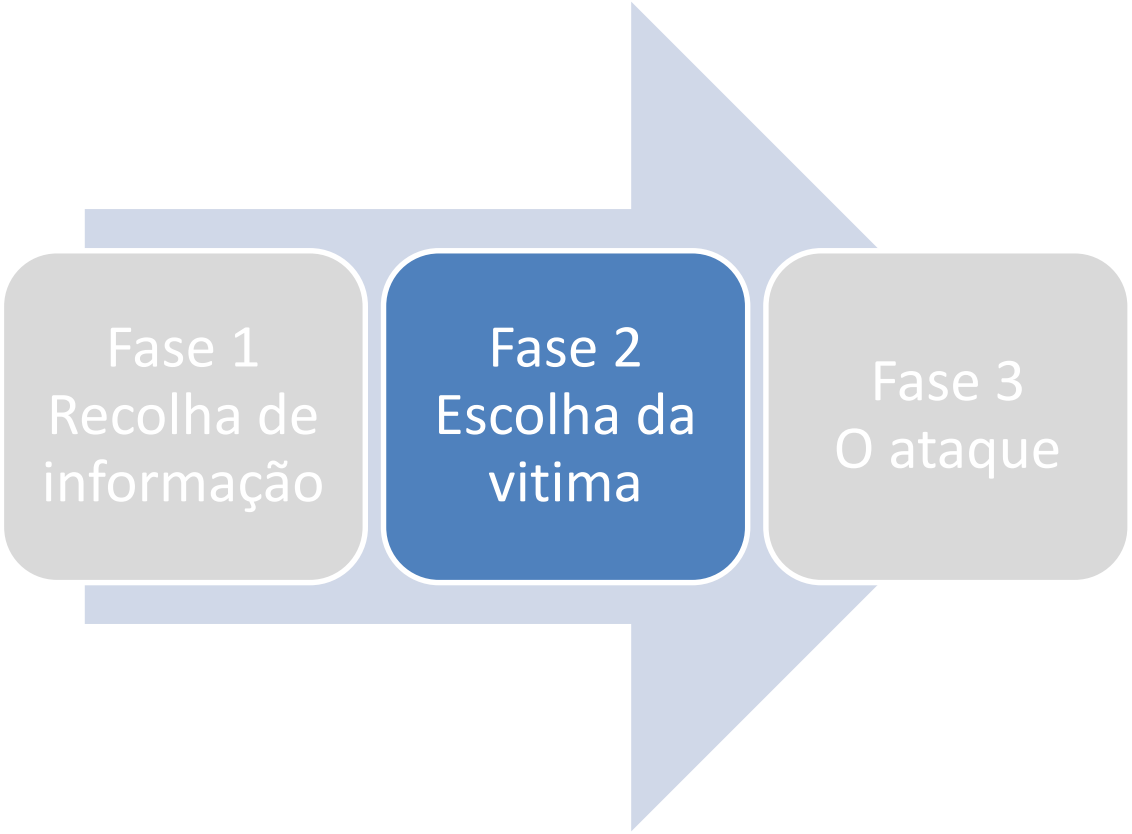
UNIVERSIDADE PORTUCALENSE

Anatomia de um ataque

- Análise do lixo:
  - Enorme quantidade de informações no lixo
  - A maior parte dele não parece ser uma ameaça
  - Quem, o quê e onde de uma organização
  - Conhecimento dos Sistemas internos
  - Materiais para maior autenticidade

UNIVERSIDADE PORTUCALENSE

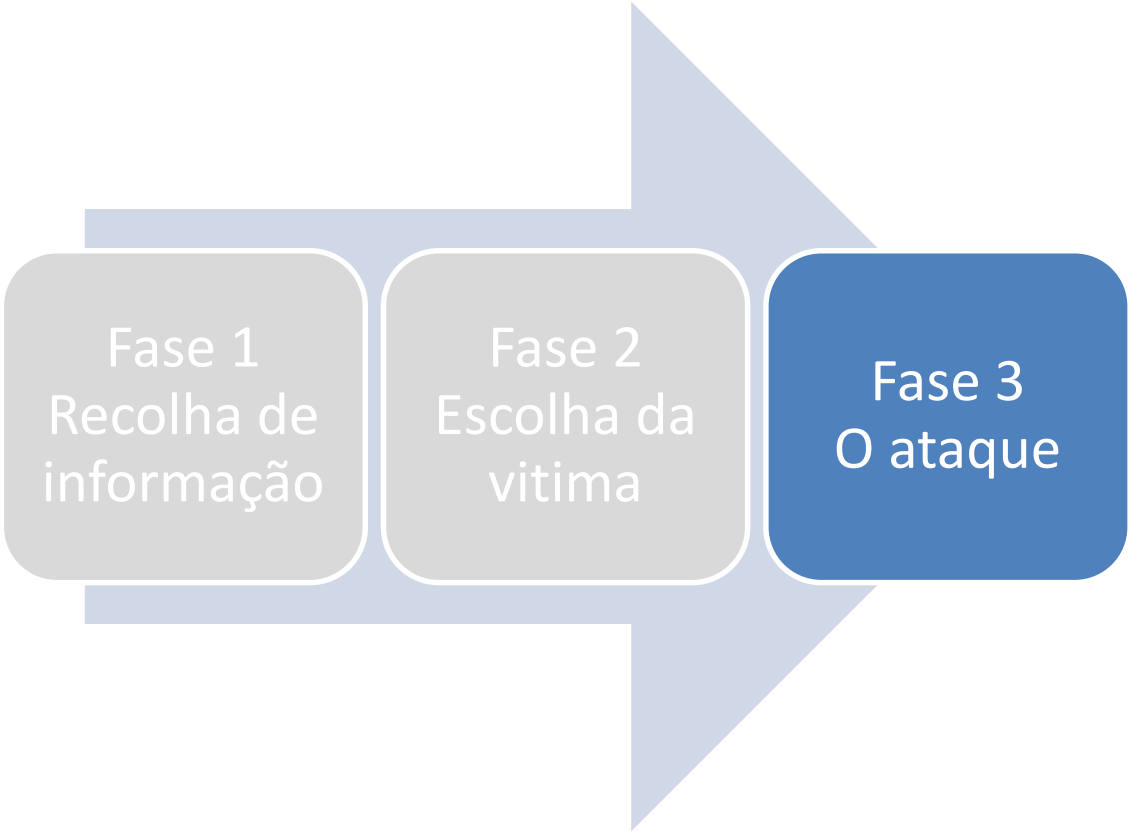
Anatomia de um ataque



- Procurando por pontos fracos no pessoal da organização
  - Help Desk
  - Suporte técnico
  - Receção
  - Pessoal administrativo
  - Etc…

UNIVERSIDADE PORTUCALENSE

Anatomia de um ataque



- Baseada principalmente em rotas "periféricas" a persuasão
  - Autoridade
  - Similaridade
  - Reciprocidade
  - Consistência & de compromisso
  - Usa a emoção como uma forma de distração

DICT DEPARTAMENTO **INOVAÇÃO CIÊNCIA E TECNOLOGIA**

UNIVERSIDADE PORTUCALENSE

Engenharia social

Exemplo

Um desconhecido liga para a sua casa e diz ser do suporte técnico do fornecedor de acesso à Internet e tenta estabelecer um contato com o utilizador dizendo que a conexão está lenta ou que tem apresentado problemas. No final acaba por pedir o seu login e a sua password para evitar interrupção do serviço. De posse do nome do utilizador e da palavra-chave o falso técnico pode efetuar fraudes e outras atividades em seu nome.

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA

UNIVERSIDADE PORTUCALENSE

Engenharia social

Exemplo

Mr. Smith: Hello?

Caller: Hello, Mr. Smith. This is Fred Jones in tech support. Due to some disk space constraints, we're going to be moving some user's home directories to another disk at 8:00 this evening. Your account will be part of this move, and will be unavailable temporarily.

Mr. Smith: Uh, okay. I'll be home by then, anyway.

Caller: Good. Be sure to log off before you leave. I just need to check a couple of things. What was your username again, smith?

Mr. Smith: Yes. It's smith. None of my files will be lost in the move, will they?

Caller: No sir. But I'll check your account just to make sure. What was the password on that account, so I can get in to check your files?

Mr. Smith: My password is tuesday, in lower case letters.

Caller: Okay, Mr. Smith, thank you for your help. I'll make sure to check you account and verify all the files are there.

Mr. Smith: Thank you. Bye.

UNIVERSIDADE PORTUCALENSE

Engenharia social

Conclusão

- Os ataques de ES são uma séria ameaça
- Os ataques de ES são fáceis e muito eficazes
- Não podemos esquecer a interação pessoa-máquina
- A garantia/segurança da informação é um problema de hardware, software, firmware e "peopleware"
- A melhor defesa é a educação adequada e o treino da consciência combinado com abordagens técnicas

DICT DEPARTAMENTO INOVAÇÃO CIÊNCIA E TECNOLOGIA