Engenharia Social

Cassiano Peres

DIO Tech Education Analyst

cassiano-dio

peres-cassiano

Objetivo Geral

Neste curso vamos falar sobre a engenharia social e a arte de manipular pessoas para obter vantagens, e como se proteger dela.

Pré-requisitos

Para este curso não há pré-requisitos técnicos, porém o conteúdo dos cursos anteriores facilitam a assimilação dos novos conteúdos.

Percurso

Etapa 1 O que é a engenharia social?

Etapa 2 Tipos de ataques

Etapa 3 Phishing

Percurso

Etapa 4 Como se proteger?

Etapa 1

O que é engenharia social?

Introdução

Nesta aula vamos falar de um tipo de ameaça importante, a **Engenharia Social**.

Engenharia social

Resumidamente, é persuadir alguém a fazer algo, sem que seja percebida a real intenção.

Engenharia social

É uma técnica empregada para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados.

[9]

Engenharia social

Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).

Deceiving the victim(s) to gain a foothold:

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Closing the interaction,
ideally without arousing suspicion:

- Removing all traces of malware.
- Covering tracks.
- Bringing the charade to a natural end.

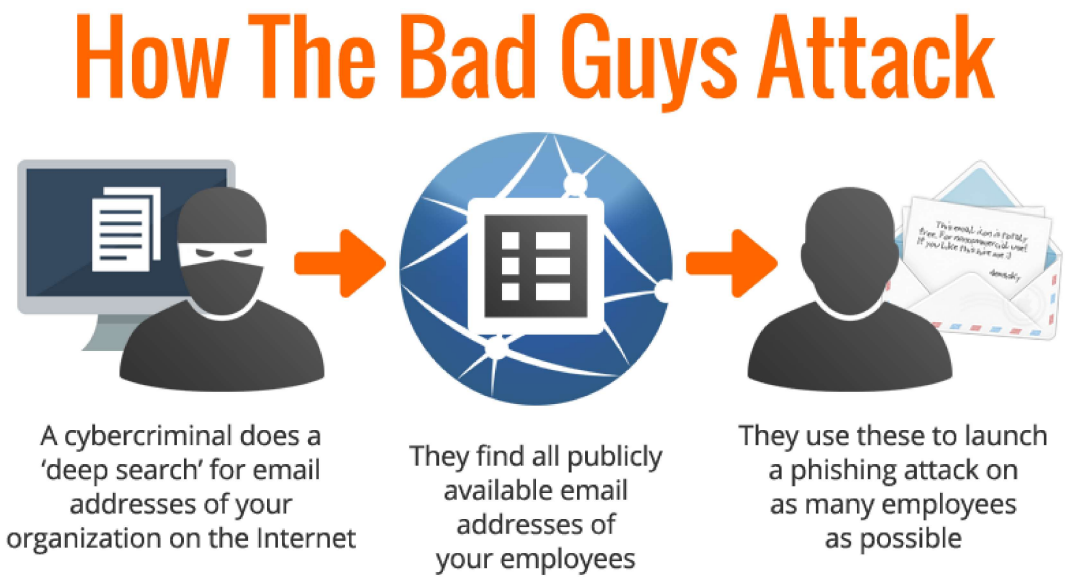
Etapa 2

Tipos de ataques

Introdução

Nesta aula vamos falar sobre os tipos de ataques que utilizam a engenharia social.

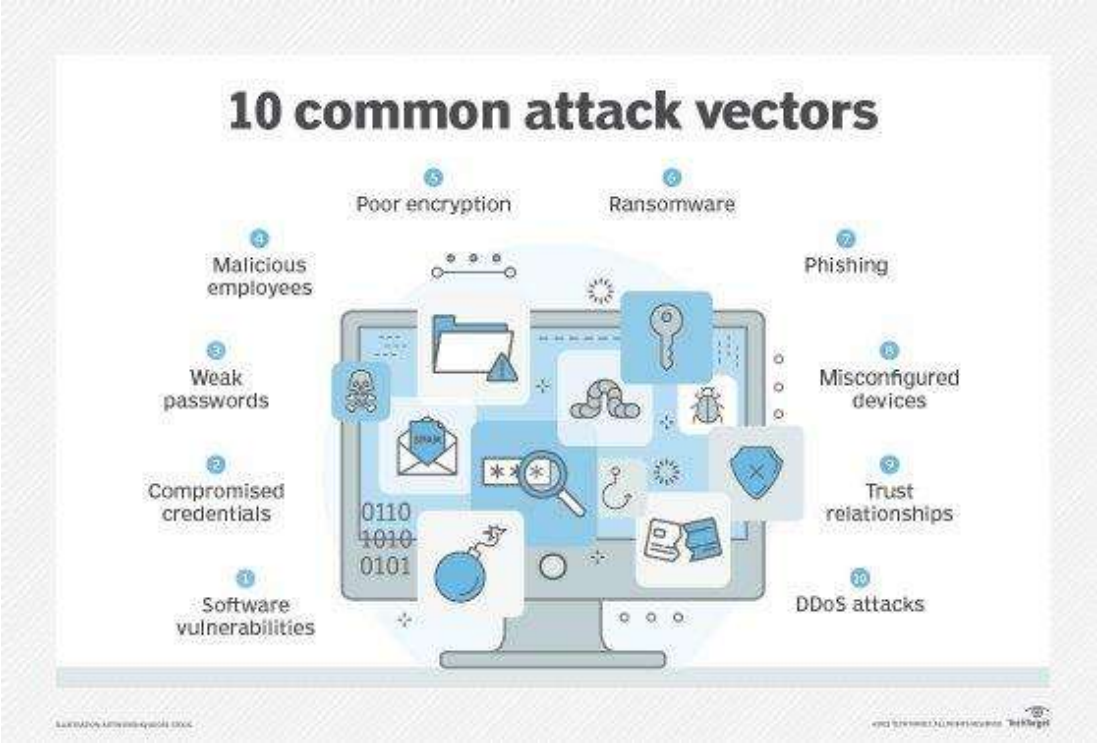
Tipos de ataques



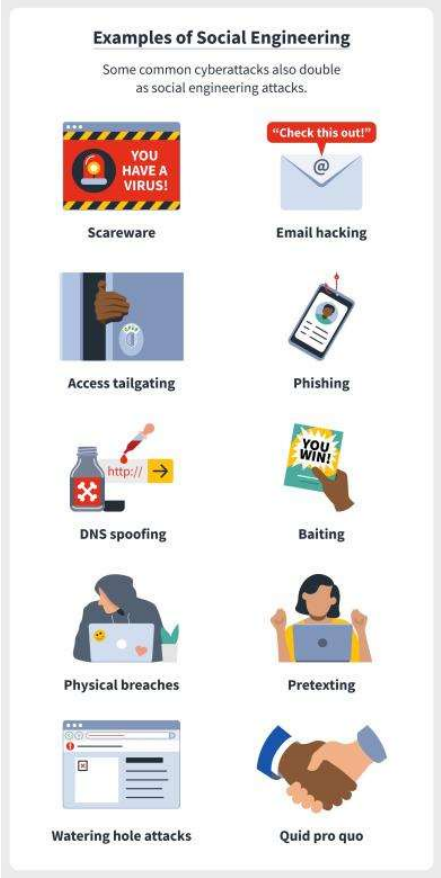
Tipos de ataques

Todos os ataques cibernéticos de certa forma utilizam um nível mesmo que mínimo de engenharia social.

Tipos de ataques



Tipos de engenharia social



Conclusão

Nesta aula vamos falar sobre os tipos de ataques que utilizam a engenharia social.

Etapa 3

Phishing

Introdução

Nesta aula vamos dar atenção a um tipo de ataque muito comum, o *phishing*.

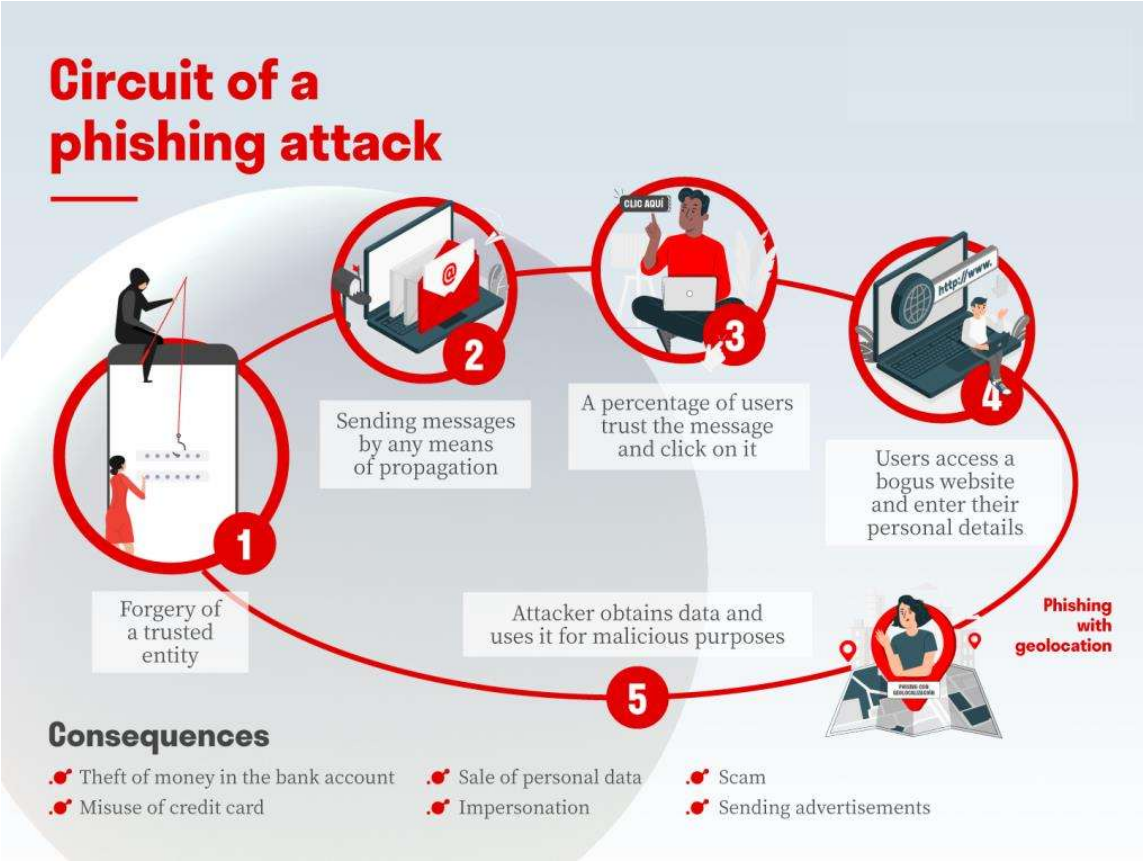
Phishing

Phishing é um crime cibernético em que um alvo ou alvos são contatados por e-mail, telefone ou mensagem de texto por alguém se passando por uma instituição legítima

Phishing

Busca atrair indivíduos a fornecer dados confidenciais, como informações de identificação pessoal, detalhes bancários e de cartão de crédito e senhas.

Phishing


Circuit of a phishing attack
1
Forgery of a trusted entity
2
Sending messages by any means of propagation
3
A percentage of users trust the message and click on it
4
Users access a bogus website and enter their personal details
5
Attacker obtains data and uses it for malicious purposes
Phishing with geolocation
Consequences
Theft of money in the bank account
Misuse of credit card
Sale of personal data
Impersonation
Scam
Sending advertisements

[22]

Phishing


What kind of information a phisher steals
Mailing addresses
ID number
Location and contact details
Personal data
Credit card number
Number of accounts
E-commerce information
Financial information
Social media
Email accounts
Access credentials
Main means of propagation
Malware infection
Social media
Telephone calls
SMS/ MMS
E-mail address

[23]

Social Engineering Red Flags

FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

Conclusão

- Tem foco em emoções e medos das pessoas;
- Se camuflam atrás de pessoas e instituições legítimas;
- Os cibercriminosos continuam inovando;
- Um ataque bem sucedido basta para comprometer.

Etapa 4

Como se proteger?

Introdução

Nesta aula vamos ver como se proteger de ataques de engenharia social

Proteção

Nessa fase é extremamente importante cuidar dos comportamentos das pessoas envolvidas.

Proteção


Social Engineering Tactics to Watch For
Knowing the red flags can help you avoid becoming a victim.
Your 'friend' sends you a strange message.
Your emotions are heightened.
The request is urgent.
YOU WIN!
$1,000,000
The offer feels too good to be true.
You're receiving help you didn't ask for.
The sender can't prove their identity.

Proteção


What To Do if You Get a Phishing Email
Don't respond
Don't open any links or attachments
Report the email as phishing
Delete the message

Como se proteger

- Não abrir emails de fontes suspeitas;
- Usar autenticação de múltiplos fatores;
- Cuidado com ofertas mirabolantes;
- Mantenha o antivirus atualizado.

Conclusão

Nesta aula tivemos uma noção do quão abertos são os sistemas e o perigo que isso representa.

Dúvidas?

> Fórum/Artigos

> Comunidade Online (Discord)

SCAN ME