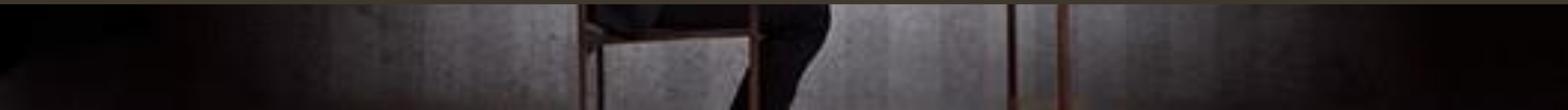
INTRODUÇÃO A ENGENHARIA SOCIAL PRÁTICA PT.1

PROF. JOAS ANTONIO



Sobre o Ebook

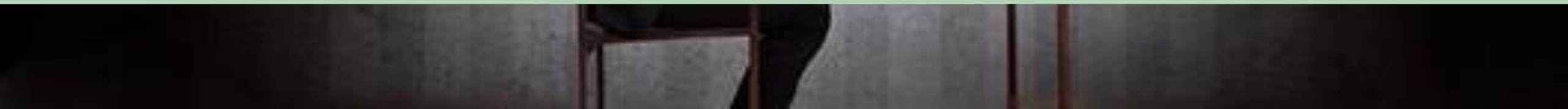
- Parte 1 do livro prático e introdutório sobre engenharia social
- Recomendado para iniciantes
- Pouco conceito e mais prática

OBS: Esse ebook não vai conter muitas imagens com utilização de ferramentas, pois o livro pode se tornar obsoleto, então como sugestão vou deixar links para a consulta e visualização.

Sobre o Autor

- Pesquisador de segurança da informação pela Experience Security
- Assistente de Professor pela Cybrary
- Owner e Founder da Cyber Security UP
- Bounty Hunter pela HackerOne
- Palestrante
- Professor de Redes, Informática e Segurança da Informação pela Udemy
- Desenvolvedor Web
- Acumulei mais de 180 cursos e 25 certificações

CONCEITOS DE ENGENHARIA SOCIAL



Engenharia Social

- A engenharia social usa a influência e a persuasão para enganar as pessoas e convencê-las de que o engenheiro social é alguém que na verdade ele não e, ou pela manipulação. Como resultado, o engenheiro social pode aproveitar-se das pessoas para obter as informações com ou sem o uso da tecnologia.

  Kevin Mitnick – A arte de enganar

Engenharia Social: Tipos

- Os tipos mais comuns de ataques de engenharia social incluem baiting, phishing, pretexting, quid pro quo, spear_phishing e tailgating.
- Vale ressaltar que um dispositivo de segurança como Firewall, Antivírus e relacionados, podem sim coibir esse tipo de ataque, porém a conscientização é essencial.

Engenharia Social: Tipos

Baiting

- Por meio dessa técnica, hackers deixam à disposição do usuário um dispositivo infectado com malware, como um pen-drive ou um CD. A intenção é despertar a curiosidade do indivíduo para que insira o dispositivo em uma máquina a fim de checar seu conteúdo.
- O sucesso dos ataques de baiting depende de três ações do indivíduo: **encontrar o dispositivo, abrir seu conteúdo e instalar o malware sem perceber**. Uma vez instalado, o malware permite que o hacker tenha acesso aos sistemas da vítima.

Engenharia Social: Tipos

Phishing

- O e-mail de phishing, apesar de já existir há anos, ainda é uma das técnicas mais comuns de engenharia social pelo alto nível de eficiência. O phishing ocorre quando um hacker **produz comunicações fraudulentas que podem ser interpretadas como legítimas pela vítima por alegarem vir de fontes confiáveis**.
- Em um ataque de phishing, os usuários podem ser coagidos a instalar um malware em seus dispositivos ou a compartilhar informações pessoais, financeiras ou de negócio.
- Apesar de o e-mail ser o modo mais tradicional para o envio de phishing, esse tipo de ataque também pode vir na forma de um contato telefônica ou de uma mensagem no Facebook, por exemplo.
- Os piores ataques de phishing se aproveitam de situações trágicas com o objetivo de explorar a boa vontade das pessoas, fazendo com que passem informações pessoais e de pagamento para realizar doações, por exemplo.

Engenharia Social: Tipos

Pretexting

- Por meio do pretexting, os hackers fabricam **falsas circunstâncias para coagir a vítima a oferecer acesso a informações e sistemas críticos**. Nesse caso, os hackers assumem uma nova identidade ou papel para fingir que são alguém de confiança da vítima.
- Tudo que o cibercriminoso precisa é dar uma olhada nos perfis da vítima nas redes sociais para descobrir informações como data e local de nascimento, empresa, cargo, nomes de parentes, colegas de trabalho, amigos, entre outros.
- Depois, basta enviar um e-mail (ou outro tipo de comunicação) à vítima fingindo a necessidade de confirmar dados para garantir seu acesso a algum sistema específico. Pode ser, por exemplo, um e-mail supostamente da equipe de TI coagindo a vítima a divulgar suas credenciais.

Engenharia Social: Tipos

Quid pro quo

- Um ataque de quid pro quo ocorre quando um hacker requer informações privadas de alguém em troca de algo. “Quid pro quo” basicamente significa “isso por aquilo”, em que o cibercriminoso **oferece algo à vítima em troca de informações sensíveis.**
- A tática mais comum envolve se passar por alguém da TI e abordar diversas vítimas encontrar alguém com um problema real de TI. Sob instruções do hacker, a vítima então dá acesso a códigos, desabilita programas vitais e instala malwares achando que conseguirá resolver seu problema.
- Outra tática bastante usada é a de simular uma pesquisa em que funcionários passam uma série de informações sensíveis em troca de brindes, como canetas e canecas.

Engenharia Social: Tipos

Spear phishing

- O spear-phishing é uma forma mais sofisticada de phishing que foca em indivíduos e organizações específicas. Nesse tipo de ataque, o hacker se passa por algum executivo ou outro membro chave da empresa e aborda funcionários com intuito de obter informações sensíveis.
- Os cibercriminosos podem obter, por meio das redes sociais, informações sobre o alvo e o quadro organizacional da empresa. Depois disso, basta enviar alguma comunicação fingindo ser, por exemplo, um dos executivos da empresa com uma demanda urgente que requer uma transação financeira imediata para uma conta específica.
- Esse tipo de ataque costuma ter altas taxas de sucesso no convencimento de funcionários para que executem ações específicas ou passem informações sensíveis.

Engenharia Social: Tipos

Tailgating

- O tailgating é uma **técnica física de engenharia social** que ocorre quando indivíduos não autorizados seguem indivíduos autorizados até localizações seguras. O objetivo é obter ativos valiosos e informações confidenciais.
- É o caso, por exemplo, de quando alguém pede para o outro “segurar a porta” porque esqueceu seu cartão de acesso, ou pede seu smartphone ou computador emprestado para fazer “algo rapidinho”, mas na verdade instala malwares e rouba dados da máquina.

Engenharia Social: Tipos

Dumpster Diving

- Dumpster Diving ou trashing é o termo usado para a ação de hackers que vasculhavam o lixo da empresa ou pessoal alvo para descobrir informações para invadir mais facilmente os sistemas, como nomes de contas, senhas, informações pessoais e confidenciais

Engenharia Social: Tipos

Shoulder Surfing

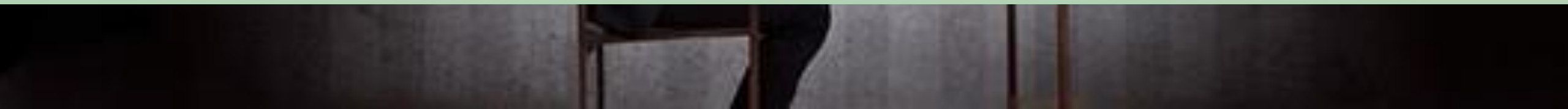
- Shoulder Surfing (espiar sobre os ombros) – Este tipo de ataque ocorre quando uma das partes é capaz de olhar sobre o ombro de outro ou espionar a tela do outro. Isso é comum em ambientes de todo tipo, porque quando você vê outras pessoas assistindo o que você está fazendo, você terá a curiosidade humana normal sem perceber.

Engenharia Social: Tipos

Eavesdropping

- Isso envolve em ouvir conversas, vídeos, telefonemas, e-mails e outras comunicações com a intenção de reunir informações que um atacante não seria autorizado teria.

PRÁTICA DOS TIPOS DE ENGENHARIA SOCIAL



Consideração

- Agora vamos realizar uma prática básica de pelo menos 4 ataques listado acima, assim para a compreensão de suas funcionalidades em prática
- Porém vamos simular uma situação vítima e atacante ;)

Prática: Baiting (Caso)

Caso:

- Uma empresa do ramo financeiro, com 200 funcionários, sempre tem uma rotina de limpeza das 08:00 as 10:00, depois as 10:30 as 14:30 e das 15:00 as 19:00
- O atacante sabendo disso, ele já prepara um meio de levar uma mídia física, seja um pendrive ou cd/dvd para dentro do prédio, para isso ele precisaria utilizar técnicas avançadas de engenharia social
- Então estudando o ambiente cada cronograma, nota-se que a equipe de limpeza vai para a portaria efetuar a limpeza, com isso ele precisaria persuadir tal funcionário ao ponto de ele acreditar em uma das suas mentiras, sendo elas:

1) Sou funcionário, mas esqueci meu cartão de acesso
2) Teria como levar essa mídia para tal pessoa?
3) Obter o cartão de acesso do funcionário, que seria mais arriscado

Eae? Qual utilizar? A 1? 2? 3? Ou outra alternativa? Pense em algo, use sua criatividade

Prática: Baiting (Caso 2)

Caso 2:

- Tal funcionário que está chegando para trabalhar na empresa do ramo de tecnologia é barrado por um suposto vendedor que está oferecendo pendrives e cds, mas para que ele convença ao ponto da pessoa comprar o seu produto é um trabalho difícil
- Então para isso o atacante precisaria preparar uma boa engenharia social para que consiga persuadir a pessoa a tal ponto, mas para isso é necessário criar uma história boa e convincente, talvez estuda r linguagem corporal e sentimentos é a melhor solução
- Caso a vítima compre, obviamente ela irá testar o produto, você pode utilizar da caridade como, dizer para a pessoa pagar depois na hora do almoço ou saída, a pessoa aceitando é torcer para que ela faça o plugin-in do pendrive na sua máquina

Prática: Baiting (Prática)

- Agora vamos criar um pendrive infectado?
- Porém não vou utilizar pendrives realmente, pois novas versões dos sistemas Windows, acabaram por deixar uma funcionalidade que é o autorun meio que inútil, até mesmo alguns antivírus estão barrando infelizmente
- Então para isso vou utilizar algum embarcado, no caso um Digispark para efetuar a exploração de um sistema Windows 10

O Digispark é uma placa de desenvolvimento baseada no microcontrolador Attiny85 semelhante à linha Arduino, só que mais barato, menor e um pouco menos potente.

OBS1: Você pode utilizar outros embarcados com suporte HID

OBS2: Consulte o material complementar para saber mais

Prática: Baiting (Shell Reverse with Digispark)

- Consulte: https://github.com/CedArctic/DigiSpark-Scripts/tree/master/Reverse_Shell
- Abra um ouvinte de netcat em uma porta (o script usa a porta 4444 por padrão): nc -lp 444
- Faça o download e modifique o Invoke-PowerShellTcpOneLine.ps1 removendo o comentário da primeira linha e alterando o endereço IP para o da máquina host e a porta para a que você escolheu anteriormente.
- Agora você precisa hospedar a carga útil em um servidor da Web para que possa ser baixada no computador Windows. Há muitas maneiras de fazer isso, mas para quem quiser uma solução rápida e fácil, você pode hospedar um servidor web php do terminal linux como este:sudo php -S 0.0.0.0:80 -t /directory/to/folder/of/powershellScript/ ou utilizando um apache2
- Faça o download e edite o Reverse_Shell.inoscript do DigiSpark para coincidir com o endereço onde o script ps1 powershell está hospedado e compile e carregue Reverse_Shell.inono seu DigiSpark.

Prática: Baiting (Shell Reverse with Rubber Ducky)

- Já imaginou utilizar um mouse fake para ganhar uma shell?
- Sim é possível utilizando o digispark + adaptadores USB, porém existe uma alternativa chamada “RUBBER DUCKY”
- Veja o seguinte vídeo feito por um profissional de segurança da informação: https://www.youtube.com/watch?v=9S58osEZZg8
- Conheça um pouco mais sobre Rubber Ducky: https://www.youtube.com/watch?v=QpuvarOYSsU
- Construindo um Mouse USB fake para invadir um Windows 10 ou outro sistema operacional: https://www.youtube.com/watch?v=57J59AactV8

Prática: Baiting (Shell Reverse with Teensy)

- Além do Rubber Ducky e Digispark existe uma alternativa chamada Teensy
- O **Teensy** é uma placa de desenvolvimento compacta e fácil de utilizar, que pode ser programada diretamente pelo computador utilizando a IDE do Arduino
- Ganhando Shell utilizando o Teensy:

https://github.com/KernelEquinox/Teensyterpreter

https://www.youtube.com/watch?v=FfRhKzbgmeU

Prática: Phishing

- Existe diversos meios de aplicar um Phishing, seja por SMS, E-mail ou um site falso
- No caso vamos ver esses 3 tipos de ataques, mas antes analise o seguinte caso

Prática: Phishing (Caso)

- Um usuário recebe um e-mail de um banco, ao qual contém um link que redireciona para uma página falsa desse banco, aonde ele precisaria digitar a sua conta e sua senha
- Como o usuário não tem conhecimentos em segurança, obviamente ele põe suas informações achando que é real, mas por consequências ele tem seu dinheiro roubado e uma dor de cabeça grande.

Como o atacante realizou esse ataque? Qual seria esse cenário?

Prática: Phishing (Caso 2)

- Um funcionário de uma empresa, recebe um e-mail contendo um pdf malicioso
- Por consequência esse funcionário baixou e clicou no pdf malicioso, com resultado o computador dele foi infectado

Qual seria esse cenário?

Prática: Phishing

- Agora vamos ver como fazer um e-mail spoofing, criar um site falso, preparar um phishing e criar um pdf malicioso

Prática: Phishing(E-mail Spoofing)

- Vamos aprender a mandar um e-mail falso?
- Existe algumas técnicas que vou listar logo abaixo, porém vamos analisar uma especifica que não precisa instalar nenhum tipo de software

https://www.youtube.com/watch?v=tqP2sZikO2w

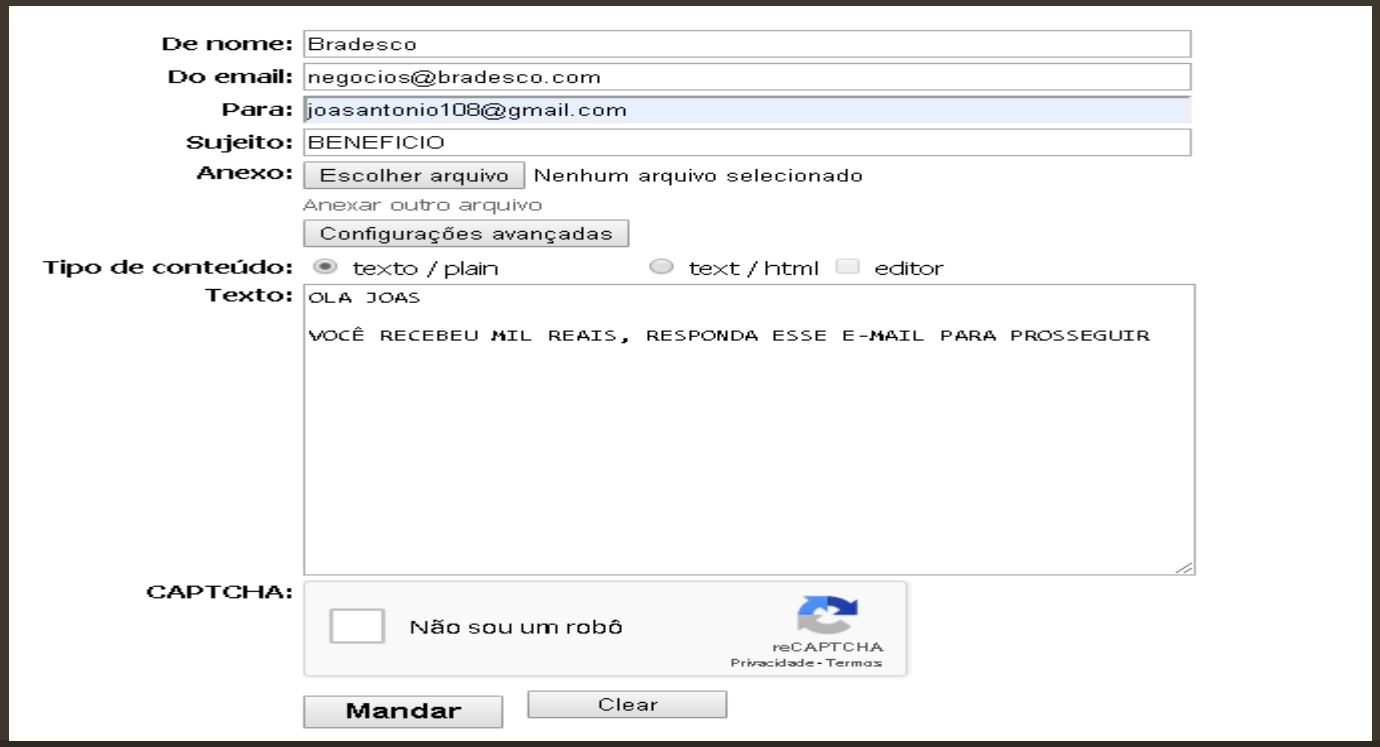
https://www.yeahhub.com/send-fake-mail-setoolkit-kali-linux/

https://null-byte.wonderhowto.com/forum/send-fake-emails-0164808/

https://www.allabouthack.com/2019/04/how-to-send-spoof-email-hacker.html

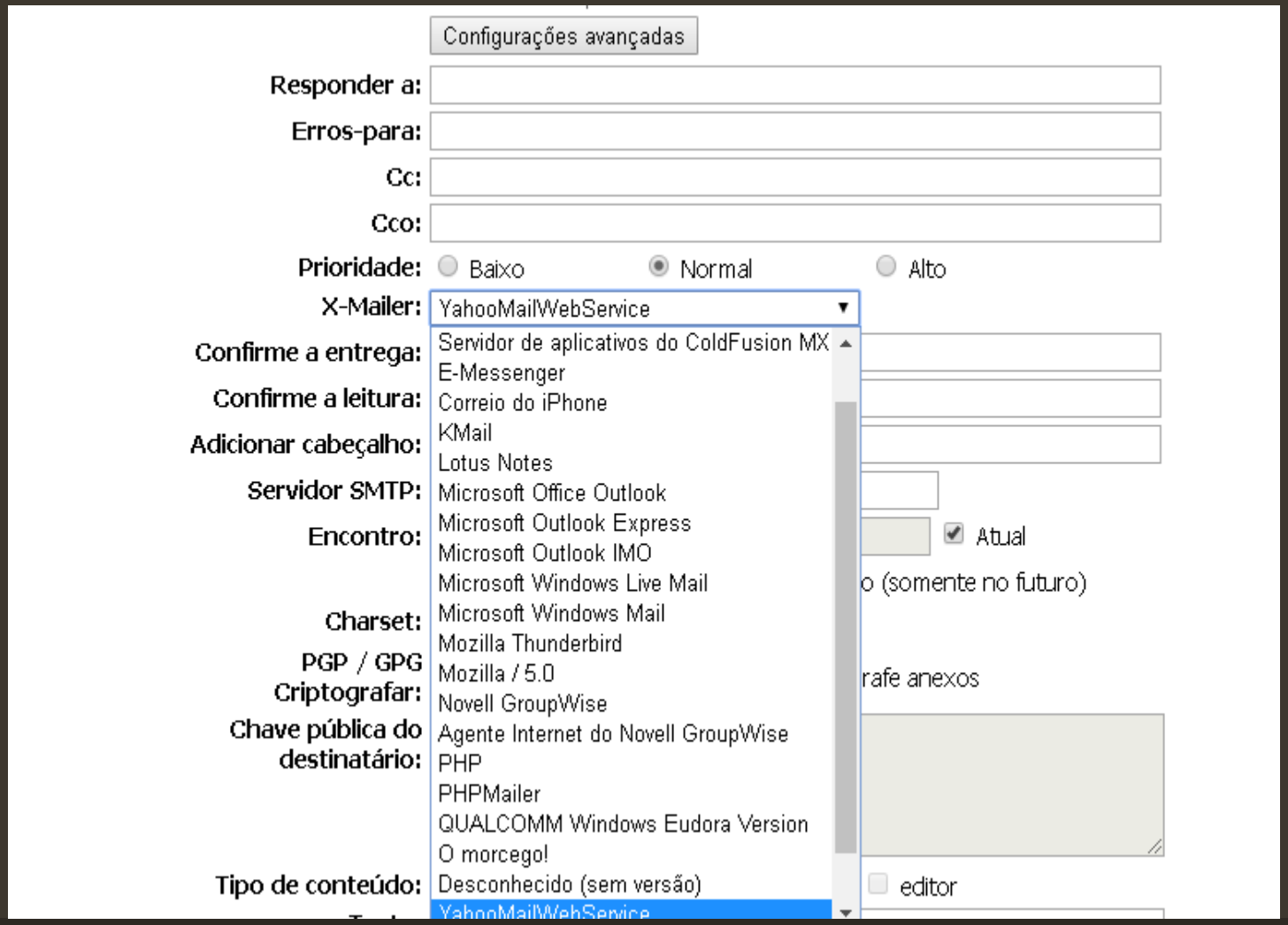
Prática: Phishing (E-mail Spoofing with Emkei)

- Envie e-mails falsos com anexos, criptografia e afins, site: https://emkei.cz/
- Vamos enviar um e-mail falso, vou utilizar o meu Gmail para isso, vou enviar no nome do Banco Bradesco, veja:



Para melhorar mais ainda, e ter certeza de que o e-mail chegou, vamos em opções avançadas para configurar algumas questões

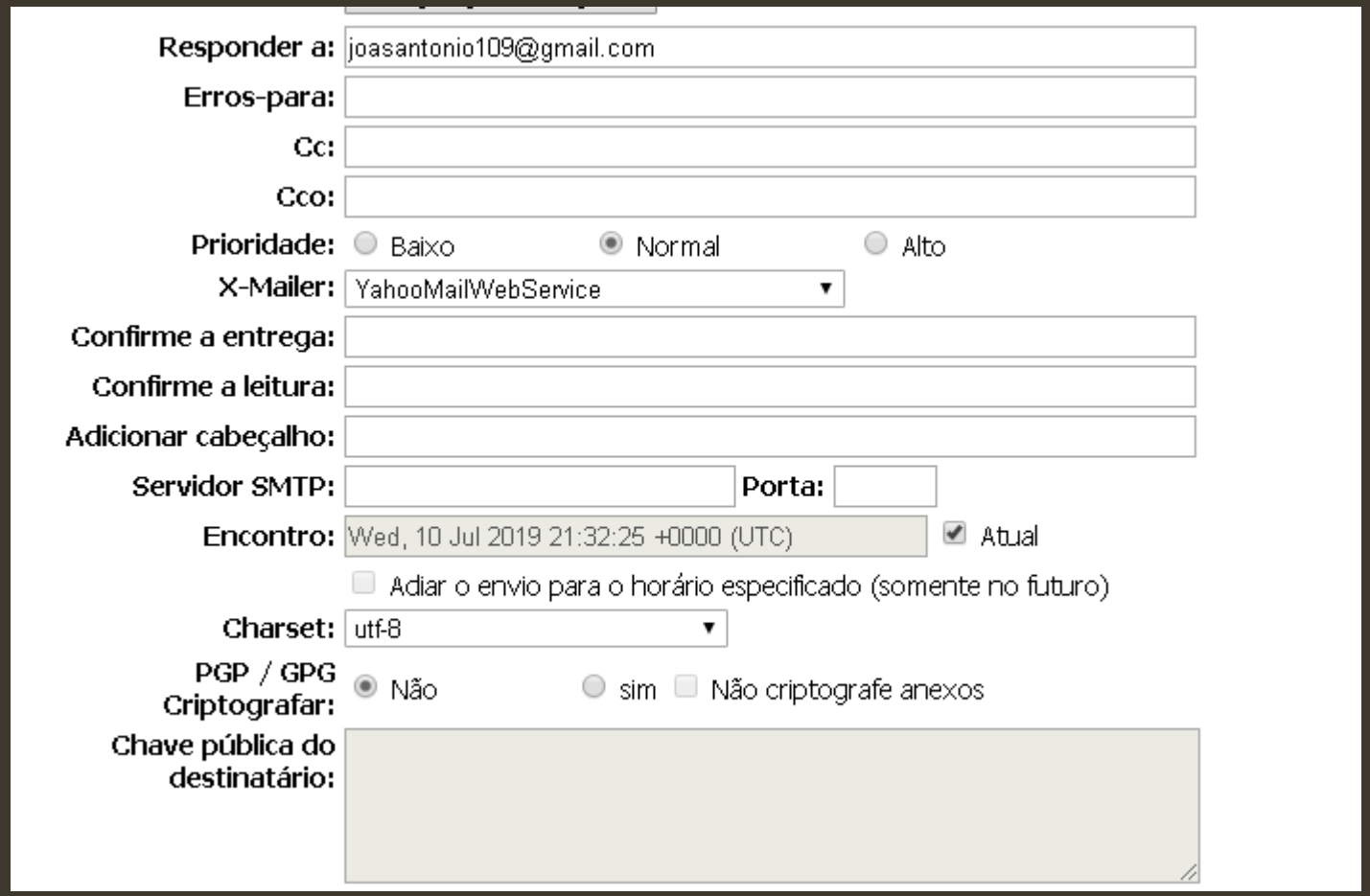
Prática: Phishing (E-mail Spoofing with Emkei)



As opções que vou alterar são, X-Mailer eu costumo colocar “YahooMail” e a prioridade eu vou deixar “Normal”, pois se ela for “Alto” pode cair no Spam.

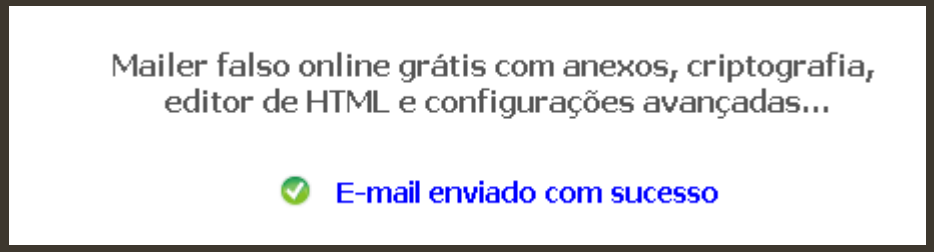
Além disso, vou colocar um e-mail para que quando ele for responder, não envie para esse e-mail do bradesco que não é de nosso domínio, mas sim um que seja nosso mesmo, para isso é só preencher o “Responder a:”

Prática: Phishing (E-mail Spoofing with Emkei)

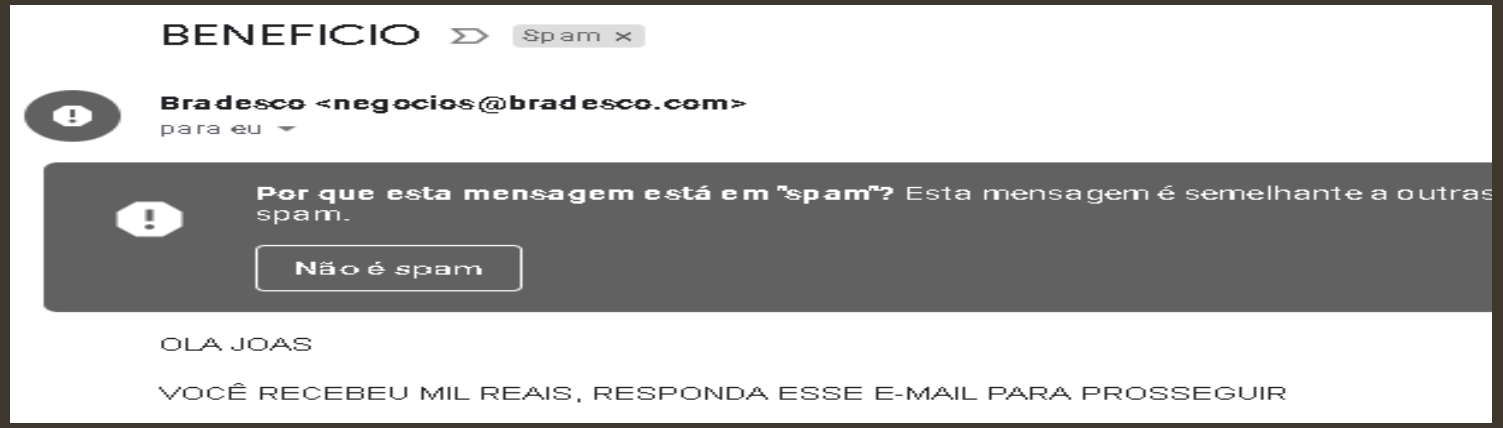


Então ficou essas opções, eu recomendo estudar as outras para que você possa mandar e-mails com mais confiabilidade, por exemplo: Confirmação de Entrega, Confirmação de Leitura, Cabeçalho e até mesmo um servidor SMTP seu próprio.

Prática: Phishing (E-mail Spoofing with Emkei)

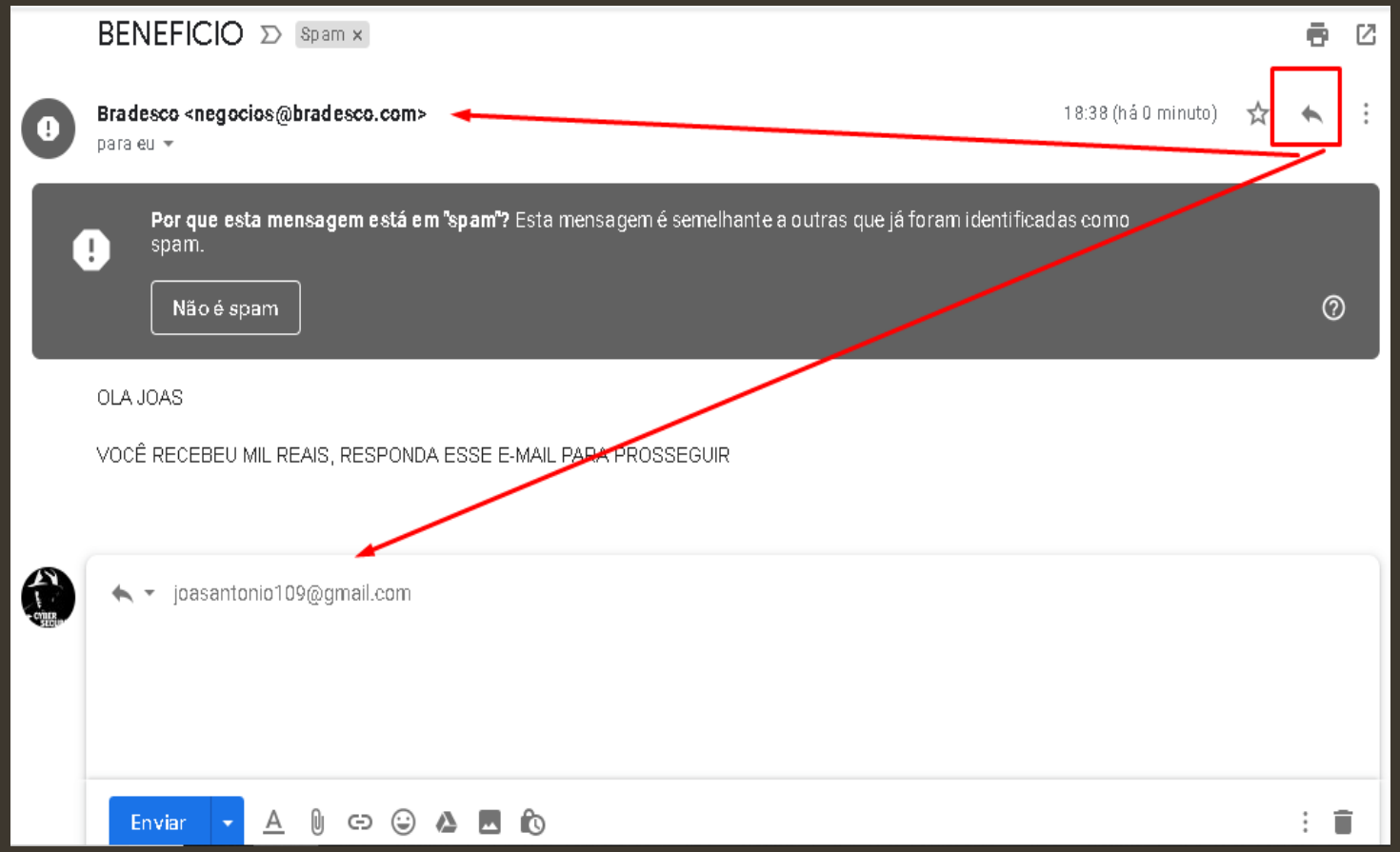


- E-mail mandado, vamos ver se foi mesmo?



- Infelizmente caiu no Spam, porém com alguns testes você consegue burlar essa questão

Prática: Phishing (E-mail Spoofing with Emkei)



Ao clicar para responder o e-mail os domínios são automaticamente mudados, perceba que a mensagem veio de “negócios@bradesco.com” e a resposta vai para “joasantonio109@gmail.com”

Prática: Phishing (Criando uma Página Web falsa)

- Agora vamos criar um site falso para capturar informações ou algo do gênero
- Para isso podemos utilizar algumas ferramentas como:

Setoolkit: https://www.trustedsec.com/social-engineer-toolkit-set/

Blackeye Phishing: https://github.com/thelinuxchoice/blackeye

SocialFish: https://github.com/UndeadSec/SocialFish

Gophish: https://github.com/gophish/gophish

- Essas são algumas ferramentas para você criar sua página falsa de algum serviço conhecido
- Para facilitar, vou postar alguns tutoriais sobre a utilização dessas ferramentas

Prática: Phishing (Criando uma Página Web falsa)

Setoolkit: https://www.youtube.com/watch?v=9Sb__83SriU

Blackeye Phishing: https://www.youtube.com/watch?v=Zf7Nf1zqJ80

SocialFish: https://www.youtube.com/watch?v=xkGsfd-_-a8

Gophish: https://www.youtube.com/watch?v=S6S5JF6Gou0

- Cada um desses vídeos vão dar uma base para a utilização da ferramenta, pois não é difícil
- Alguns erros que podem ocorrer seria com o Apache2, mas para isso é só reinstalar ele de novo ou reiniciar o serviço.

Prática: Phishing (Preparando um Phishing)

- Agora a questão é preparar um phishing para enviar a vítima e tentar extrair alguma informação ou até mesmo compromete-la
- Para isso é necessário conhecimentos em HTML e CSS, pois assim você pode extrair um HTML de algum e-mail original e modificar algumas coisinhas para reutilizar
- Vou mostrar um exemplo utilizando o ifood:

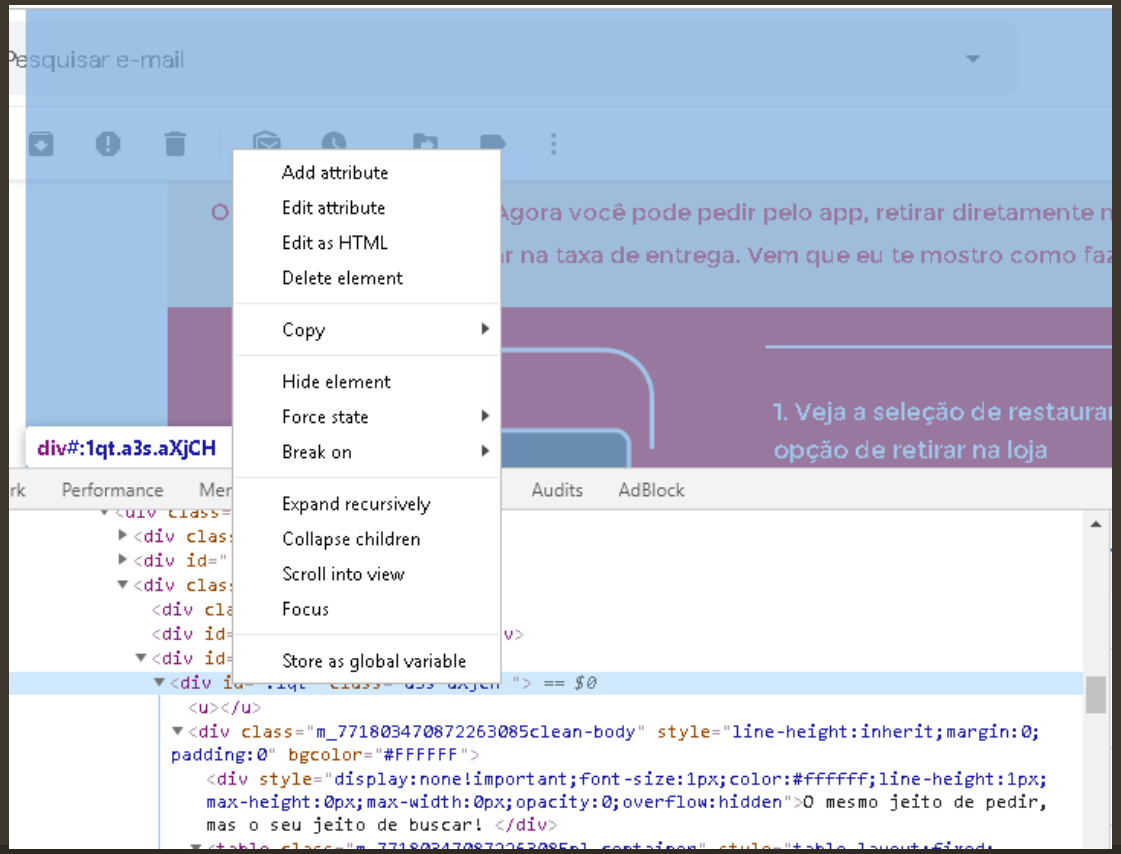
Prática: Phishing (Preparando um Phishing)

- Vou extrair o HTML desse e-mail do ifood para editar apenas um item, que seria esse abaixo

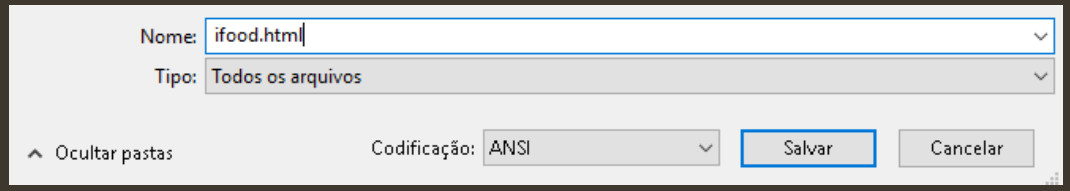
Para extrair, basicamente vou utilizar o “inspecionar elemento” para acessar essa opção é só clicar com botão direito do mouse e ir em “inspecionar elemento”

Prática: Phishing (Preparando um Phishing)

- Agora é só selecionar , apenas o código fonte daquele e-mail, para saber qual é o código correto é analisando e observando a marcação azul que fica na tela

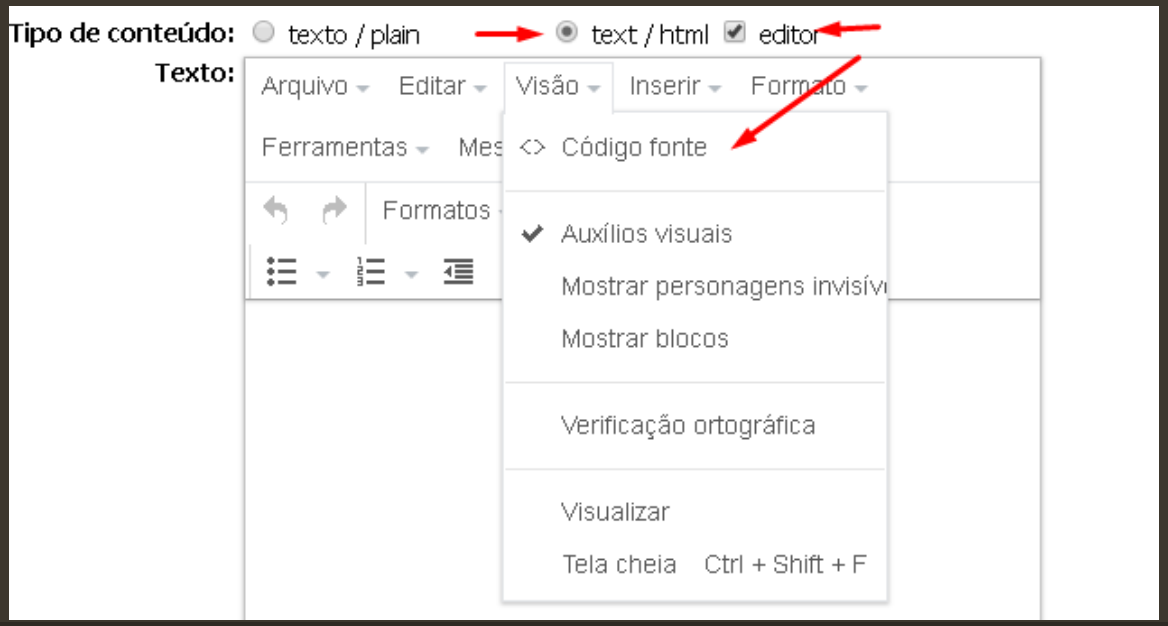


Depois disso é só clicar em “Edit as HTML” no inicio do código e “Copiar” ele e “Colar” em um editor de texto e salve com a extensão (.HTML)



Prática: Phishing (Preparando um Phishing)

- Agora vamos realizar o ataque, vou utilizar o “Emkei” para enviar um e-mail falso
- Para isso vou realizar o mesmo processo anterior, só que a diferença é que vou enviar esse HTML que editei
- Então selecione as seguintes opções:



Prática: Phishing (Preparando um Phishing)

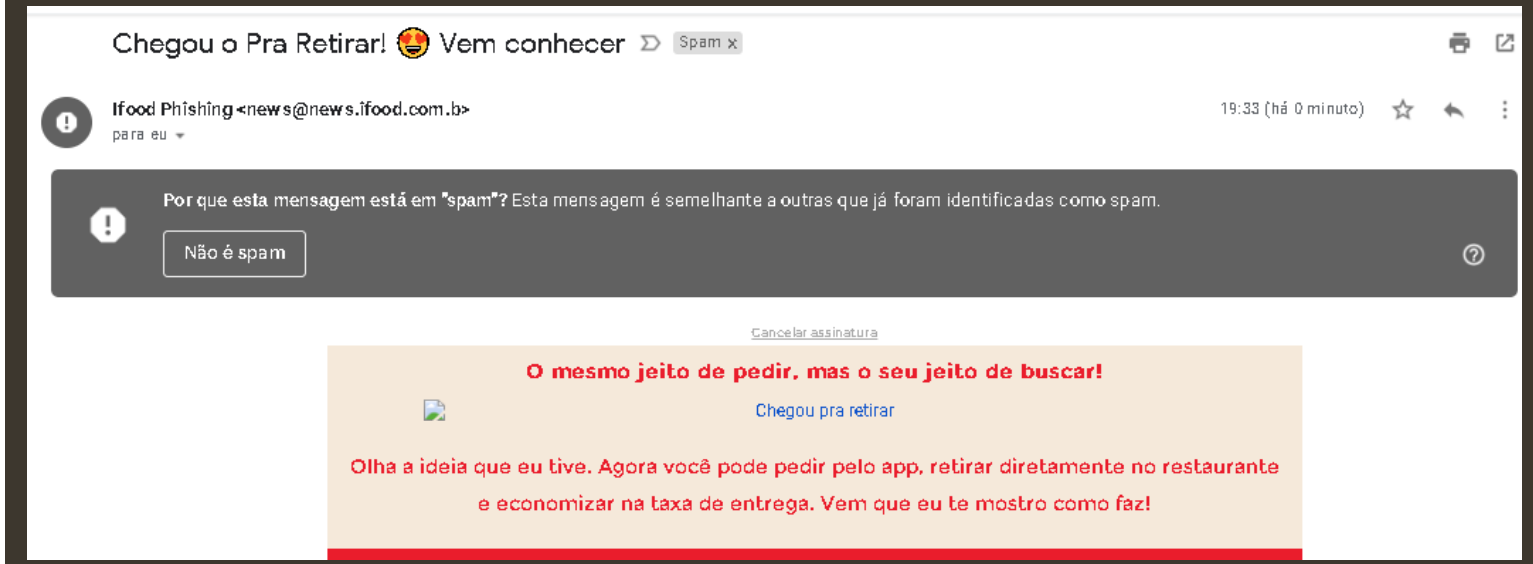
- Agora é só efetuar a edição do código
- No meu caso vou editar somente aquele botão para redirecionar para meu Phishing ou baixar algum arquivo, vai de sua criatividade

- Aqui eu só editei o redirecionamento para o meu website, poderia ser um Phishing ou algum download de um arquivo malicioso.

Prática: Phishing (Preparando um Phishing)

- Agora basta copiar o HTML editado e colar
- Com isso é só dar um "**okay**" e visualizar se está tudo nas conformidades

Após isso é só enviar



Infelizmente caiu no Spam e não ficou legal, porém ele está redirecionando para a página que eu desejava

Prática: Phishing (Criando um documento infectado)

- Vamos agora criar um pdf malicioso

https://www.youtube.com/watch?v=3RSn9JwnWlQ

https://www.youtube.com/watch?v=q0DdW13zMRk

https://linuxsecurityblog.com/2018/11/12/payload-in-pdf/

https://null-byte.wonderhowto.com/how-to/hack-like-pro-embed-backdoor-connection-innocent-looking-pdf-0140942/

Prática: Phishing (SMS SPOOFING ou SMISHING)

- É uma forma de ataque semelhante ao phishing mas através de SMS, onde geralmente a vítima recebe um SMS solicitando realizar uma ação “urgente”, como por exemplo uma troca de senha do banco.
- http://www.smsgang.com/
- https://www.spoofbox.com/en/app/spoof-sms
- https://globfone.com/send-text/
- http://www.spoofmytext.com/

Links de Casos

- https://www.researchgate.net/publication/301851712_Case_Study_On_Social_Engineering_Techniques_for_Persuasion
- https://opendatasecurity.io/the-most-famous-cases-of-social-engineering/
- https://www.dummies.com/programming/networking/a-case-study-in-how-hackers-use-social-engineering/
- https://gatefy.com/posts/7-real-and-famous-cases-social-engineering-attacks/
- https://subscription.packtpub.com/book/networking_and_servers/9781788837927/10
- https://www.bankinfosecurity.com/case-study-one-small-institution-fights-back-big-time-against-social-a-681
- https://www.7elements.co.uk/about-us/case-studies/social-engineering-drive-by-download-attack/

Fontes e Material complementar

https://www.proof.com.br/blog/ataques-de-engenharia-social/

https://www.diegomacedo.com.br/ameacas-comuns-de-engenharia-social/#more-6486

https://www.filipeflop.com/produto/placa-de-desenvolvimento-attiny85-digispark/

https://www.arduinoecia.com.br/2016/11/digispark-attiny85-ide-arduino.html

Invadindo Windows 10 com Digispark: https://www.youtube.com/watch?v=ZPuC2JZlemY

https://www.binance.com/en/support/articles/360020817051-Phishing-Email-Cases

https://www.inc.com/will-yakowicz/biggest-email-phishing-scams-2018.html

https://www.phishprotection.com/blog/the-top-5-phishing-scams-in-history-what-you-need-to-know/

https://hackersec.com/ataque-de-engenharia-social/