



Tempest

ACADEMY

Conference
2023

~~Não~~ clique nesse
link

Palestra de conscientização



~# whoami

- Felipe Azevedo a.k.a. Milhous3
- 8 anos em segurança ofensiva



Phishing

 Tempest

ACADEMY

Conference



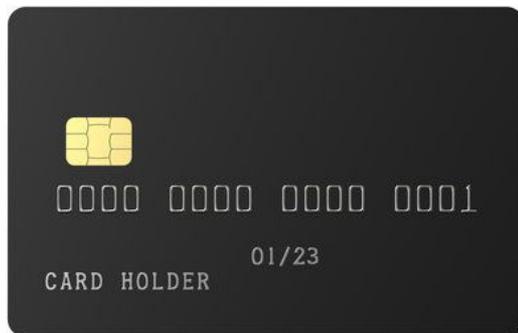
Phishing

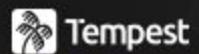
“Phishing is the process of attempting to acquire **sensitive information** such as usernames, passwords and credit card details by masquerading as a trustworthy entity using bulk email which tries to evade spam filters.”

KnowBe4 - <https://knowbe4.com/phishing>



E o que é Informação sensível?



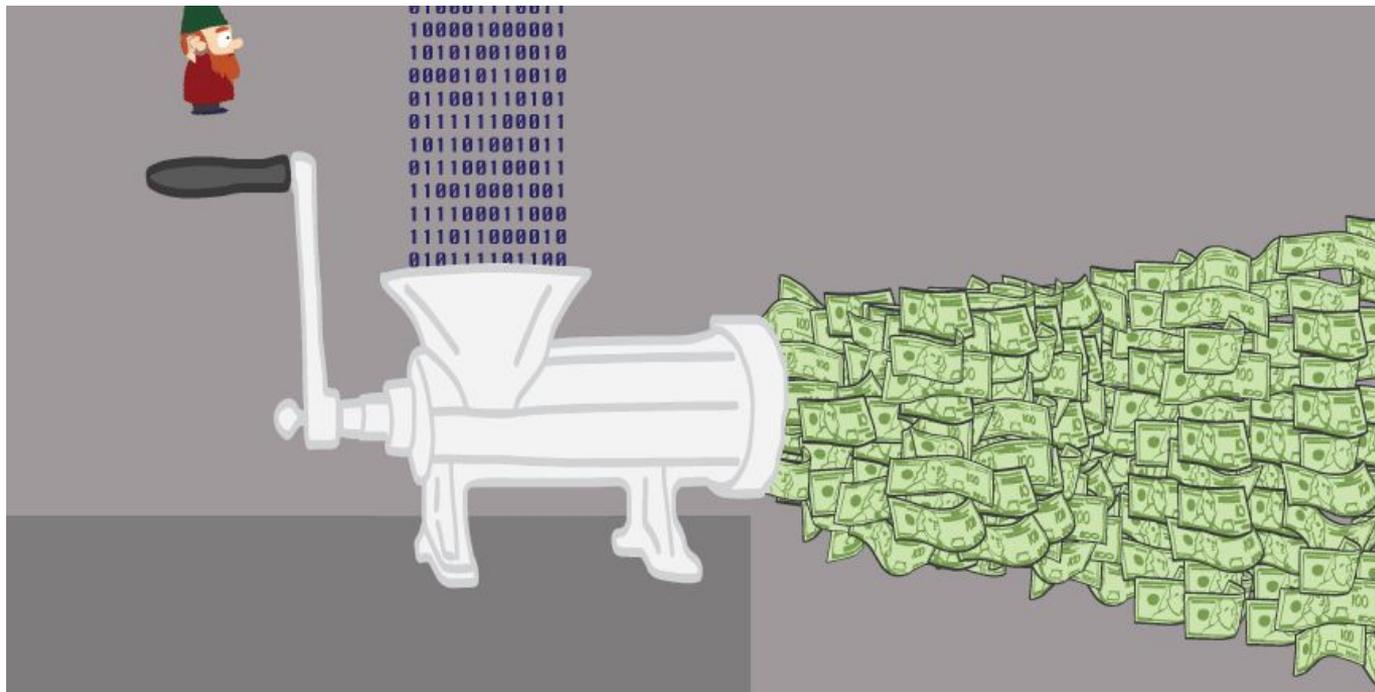


ACADEMY

Conference



~~TIME~~ DATA IS MONEEEEEEEY!!!!



 Tempest

ACADEMY

Conference

O que danado é Engenharia social?

Tempest
ACADEMY
Conference



O que danado é Engenharia social?

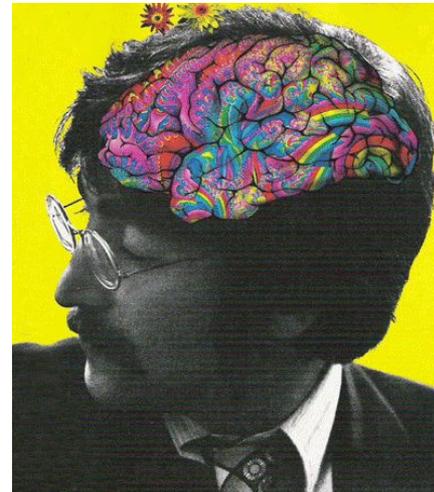
“Manipulação psicológica de pessoas para execução de ações ou para divulgação de informação sigilosa.”

[https://pt.wikipedia.org/wiki/Engenharia_social_\(seguran%C3%A7a\)](https://pt.wikipedia.org/wiki/Engenharia_social_(seguran%C3%A7a))

 Tempest

ACADEMY

Conference



O que danado é Engenharia social?

"The social engineer is able to take advantage of people to obtain information with or without the use of technology."

The Art of Deception - MITNICK, D. Kevin



Foto: KnowBe4/Divulgação

FREE KEVIN

 Tempest

ACADEMY

Conference

Como pode acontecer?

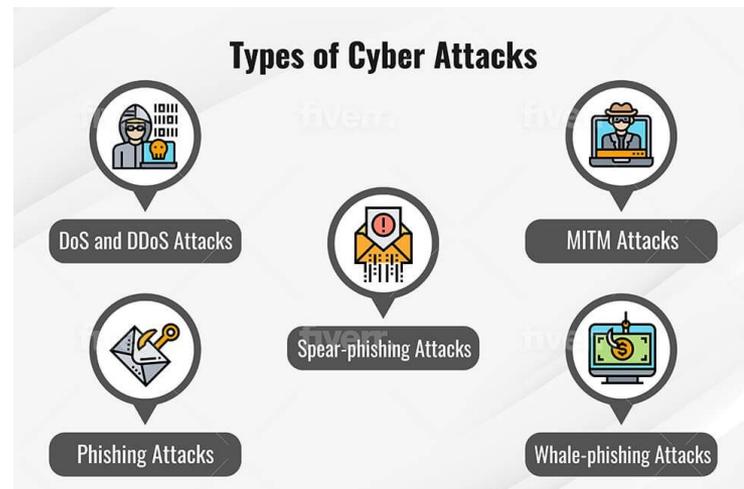
- Relação de confiança;
- *Links*;
- E-mails;
- Ligação;
- Mensagens por aplicativos;
- Entre outros.

Em resumo: qualquer interação com alguma pessoa.

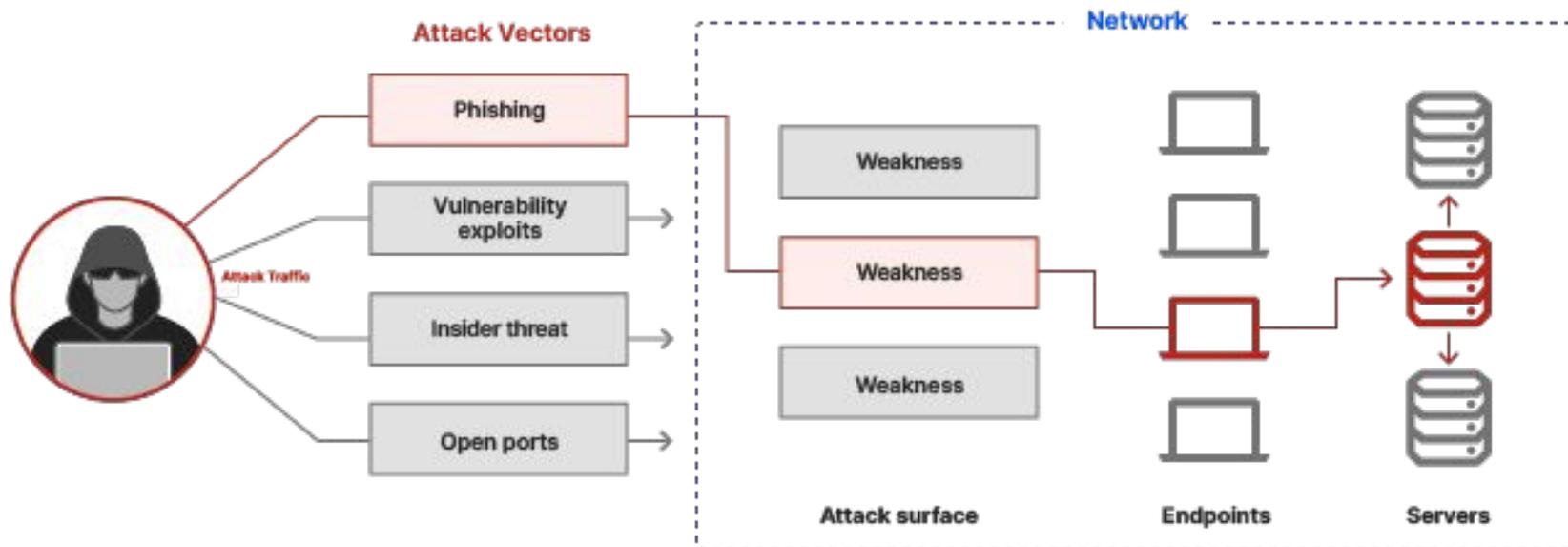


Tipos

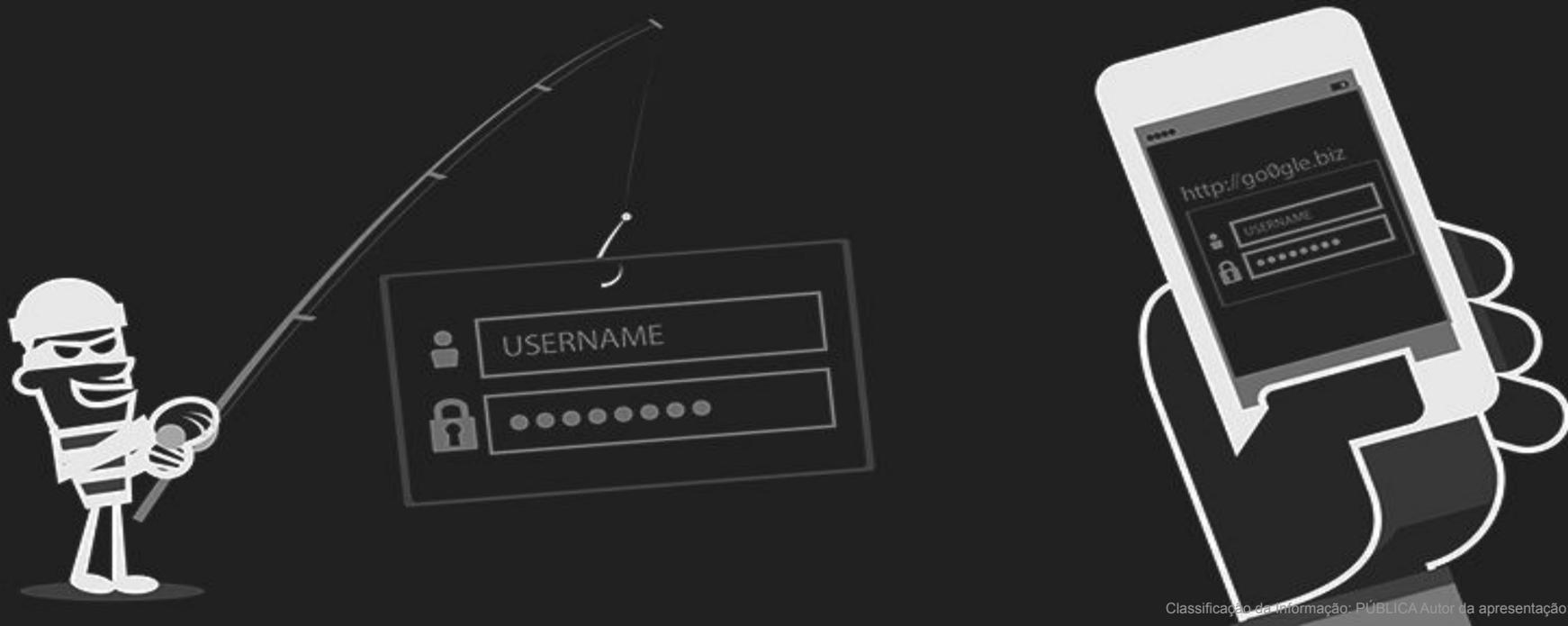
- “Golpes” em geral;
- *Phishing*;
- *Smishing*;
- *Vishing*;
- *Whaling*;
- *Candy drop*;
- Entre outros



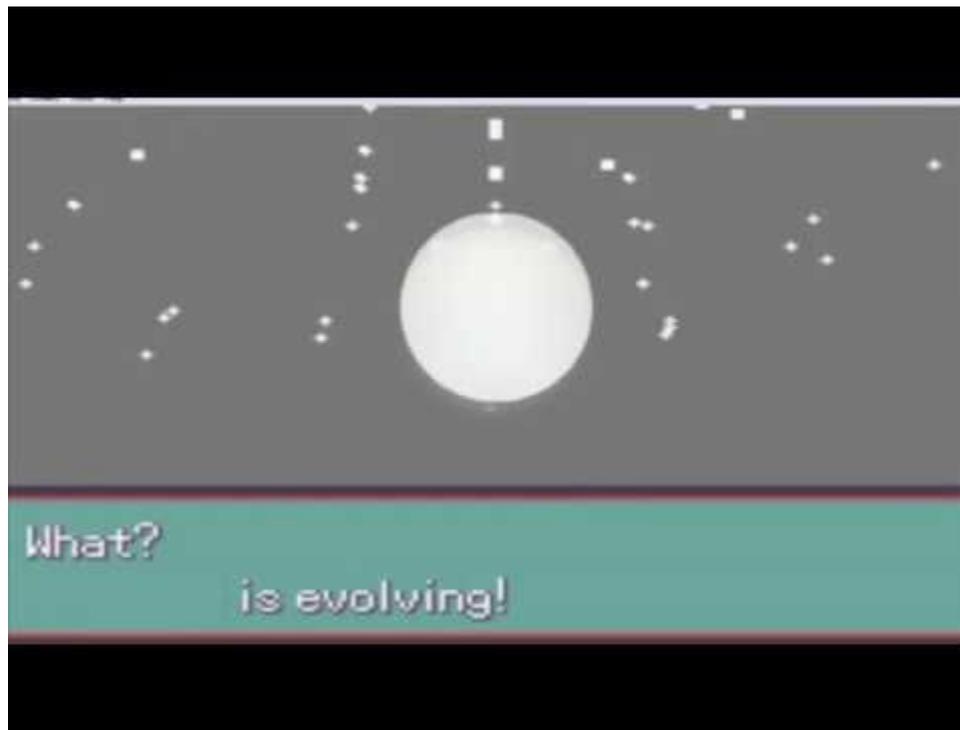
Elo mais fraco



Smishing



Smishing is evolving!

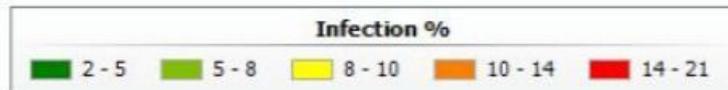
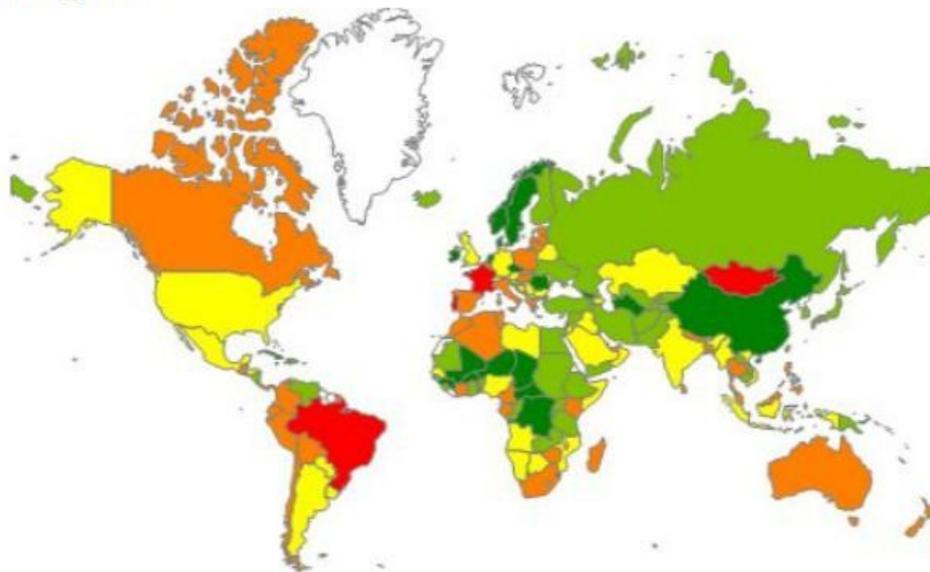


Aplicativos de mensagem instantânea



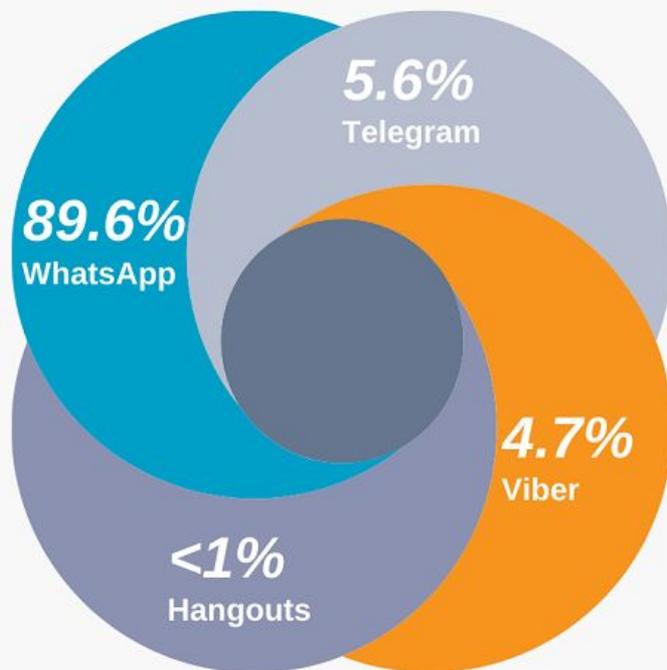
Aplicativos de mensagem instantânea

Phishing 2021



Aplicativos de mensagem instantânea

Percentage of detections by messenger



Aplicativos de mensagem instantânea



Netflix Grátis contra COVID-19

Ative sua conta grátis pelo PERÍODO DE ISOLAMENTO!

netflix.com

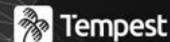
Devido a grande pandemia do CORONA VÍRUS no mundo todo, a Netflix está liberando o acesso a plataforma deles pelo período de isolamento. Corre no site que é só pra quem se cadastrar nos próximos 2 dias!

<https://netflix.com/periodo-de-isolamento-gratis>

13:33

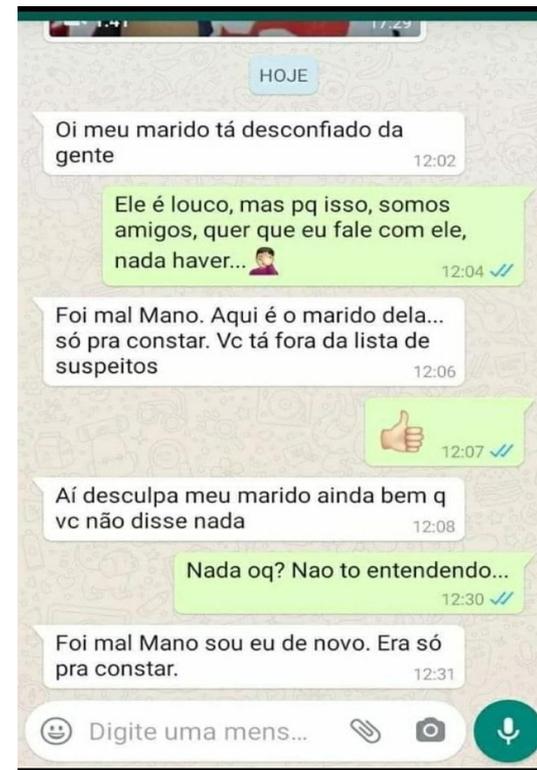
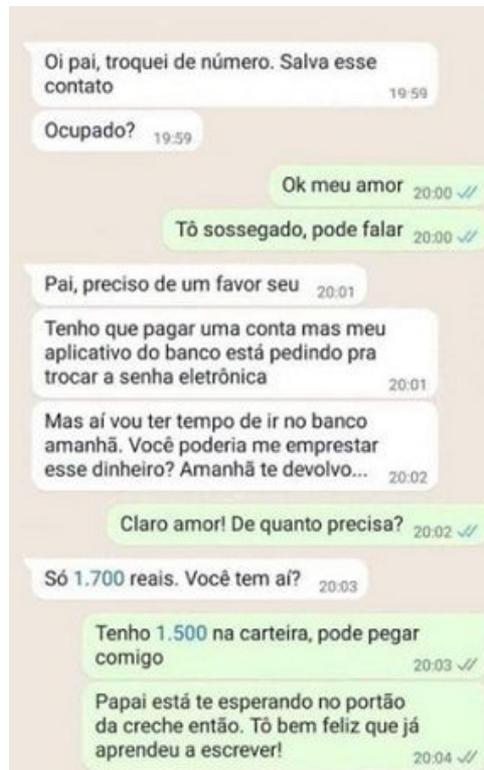
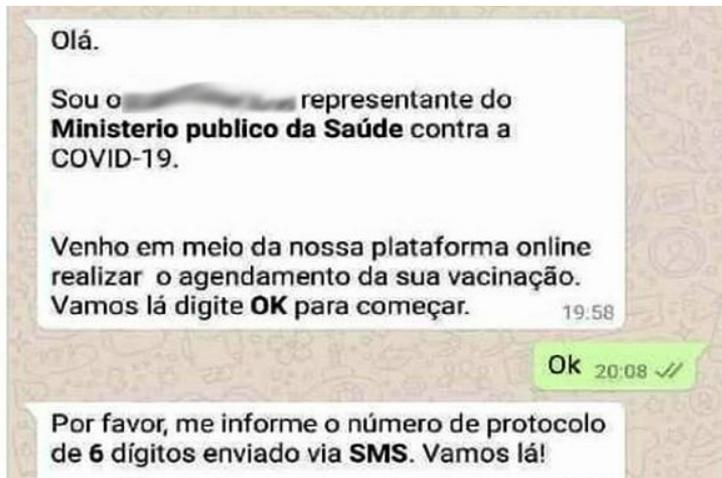


Aplicativos de mensagem instantânea



ACADEMY

Conference



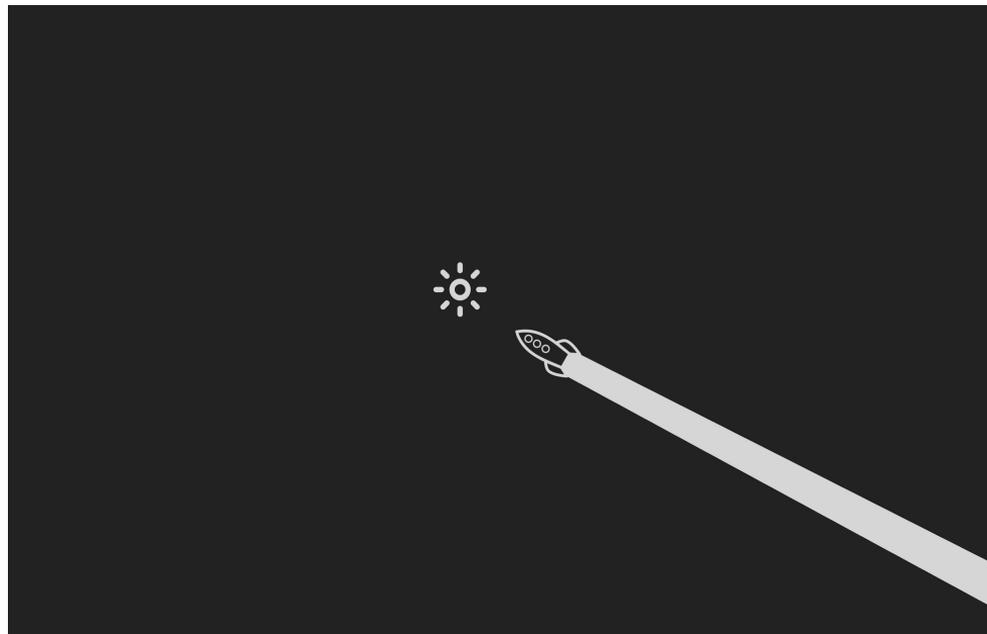
Vishing



Candy drop



Spear phishing



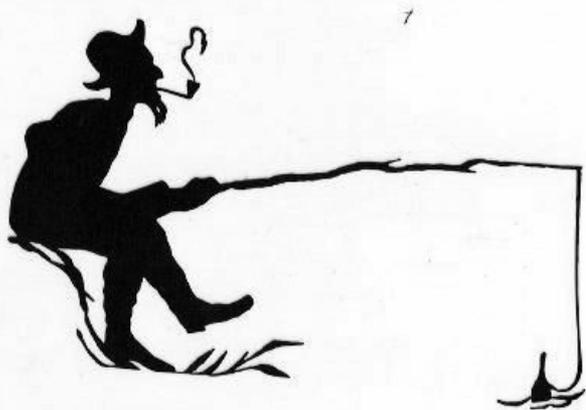
Clique para adicionar um título

Tempest

ACADEMY

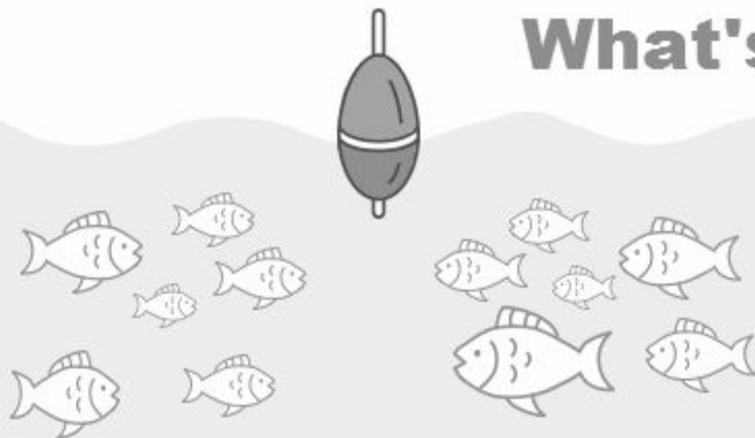
Conference

Clique para adicionar texto



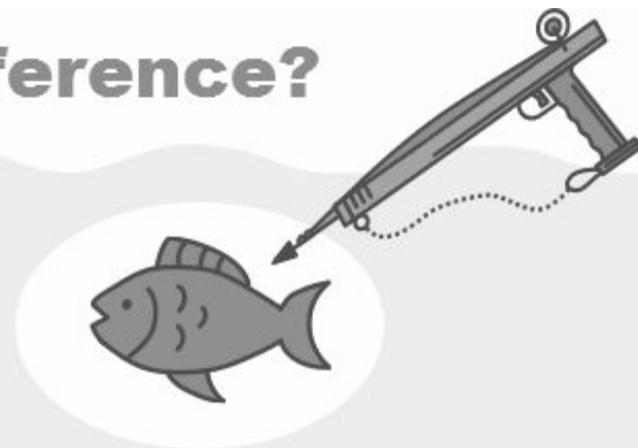
Phishing != Spear Phishing

What's The Difference?



PHISHING

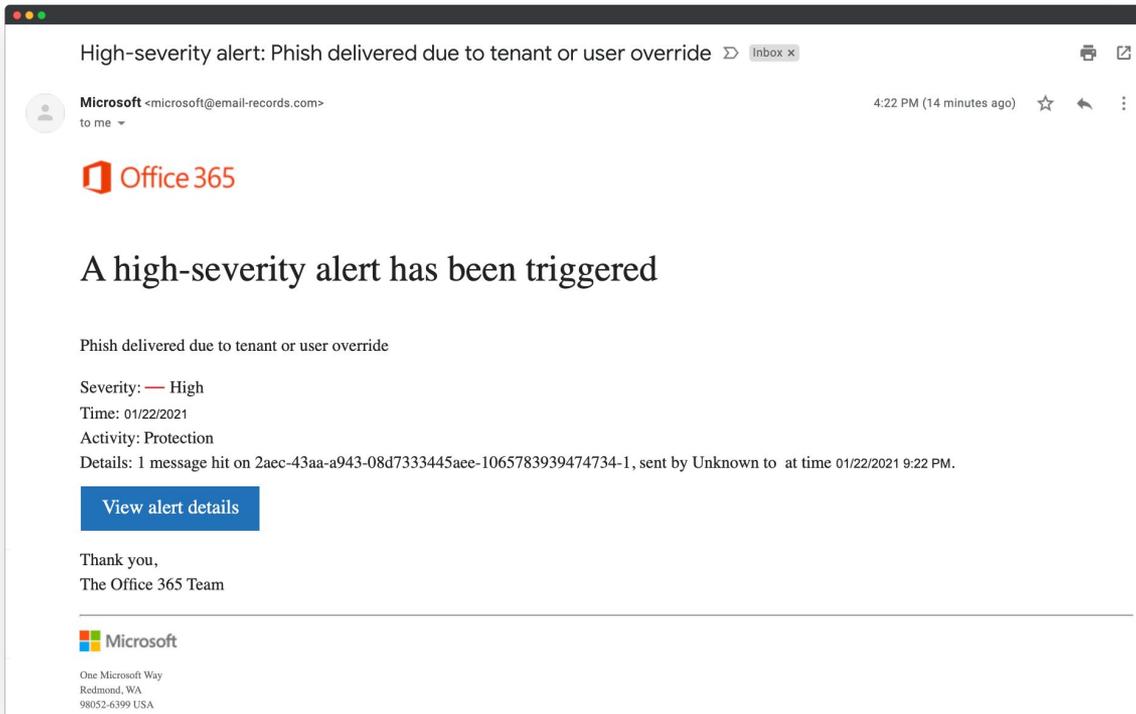
IS A BROAD, AUTOMATED ATTACK
THAT IS LESS SOPHISTICATED.



SPEAR-PHISHING

IS A CUSTOMIZED ATTACK ON A SPECIFIC
EMPLOYEE & COMPANY

Exemplos



High-severity alert: Phish delivered due to tenant or user override ↳ Inbox x 🖨 📧

 **Microsoft** <microsoft@email-records.com>
to me ▼ 4:22 PM (14 minutes ago) ☆ ↶ ⋮

 Office 365

A high-severity alert has been triggered

Phish delivered due to tenant or user override

Severity: — High
Time: 01/22/2021
Activity: Protection
Details: 1 message hit on 2aec-43aa-a943-08d7333445aee-1065783939474734-1, sent by Unknown to at time 01/22/2021 9:22 PM.

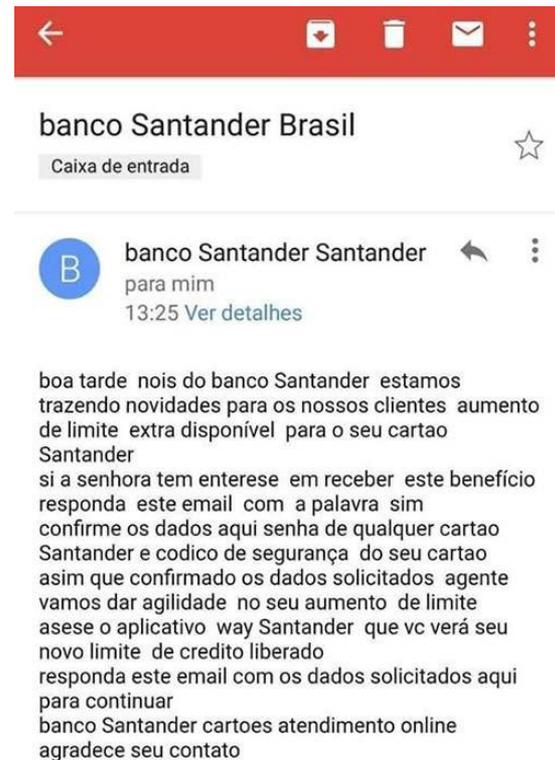
[View alert details](#)

Thank you,
The Office 365 Team

 Microsoft

One Microsoft Way
Redmond, WA
98052-6399 USA

Exemplos



Exemplos

A screenshot of a web browser showing the Netflix payment page. The browser's address bar displays 'netflix.com/signup/creditooption'. The page features the Netflix logo in red at the top left and a 'Sair' link at the top right. The main heading reads 'PASSO 3 DE 3 Informe os dados do seu cartão de crédito ou débito'. Below this, there are logos for VISA, Mastercard, American Express, and others. The form consists of several input fields: a large field for the card number, two smaller fields for the expiration date and CVV, a field for the cardholder's name, and a field for the surname. At the bottom, there are radio buttons to select the preferred payment method, with 'Crédito' selected.

Netflix

netflix.com/signup/creditooption

NETFLIX

Sair

PASSO 3 DE 3

Informe os dados do seu cartão de crédito ou débito

VISA Mastercard etc American Express

Número do cartão

Data de validade

CVV

Nome

Sobrenome

Escolha sua forma de pagamento preferida:

Crédito

Débito

Empresas vítimas



Breaking In

New information about the 2013 Yahoo hack triples the number of accounts affected in the largest data breach in history.

Selected data breaches by number of consumers/user accounts

| COMPANY | SIZE OF BREACH | YEAR DISCLOSED |
|------------------------|-------------------------------|----------------|
| | ┌ 2 billion newly disclosed ┐ | |
| Yahoo* | 3 billion | 2016-17 |
| Yahoo* | 500 million | 2016 |
| Equifax | 143 | 2017 |
| Heartland Payment Sys. | 130 | 2009 |
| LinkedIn | 117 | 2016 |
| Sony | 100 | 2011 |
| TJX | 90 | 2007 |
| Anthem | 80 | 2015 |
| J.P. Morgan | 76 [†] | 2014 |
| Target | 70 [‡] | 2013 |

*Believed to be separate incidents †Millions of households ‡Initial disclosure

Source: the companies

THE WALL STREET JOURNAL.

Empresas vítimas



Dúvidas?

Tempest

ACADEMY

Conference



<https://br.linkedin.com/in/felipe-gomes-74673598>

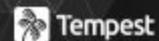




Obrigado



Hack the planet!



ACADEMY:

Conference





Tempest

ACADEMY

Conference

2023

