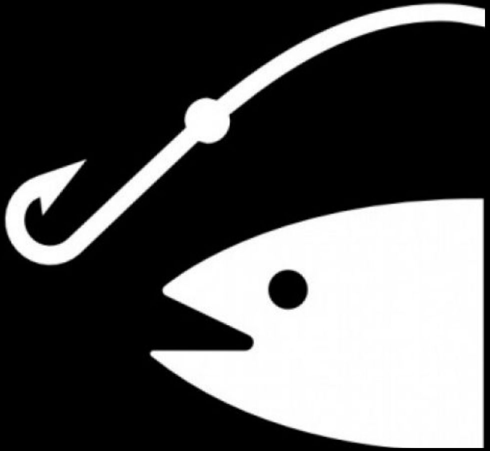


Phishing

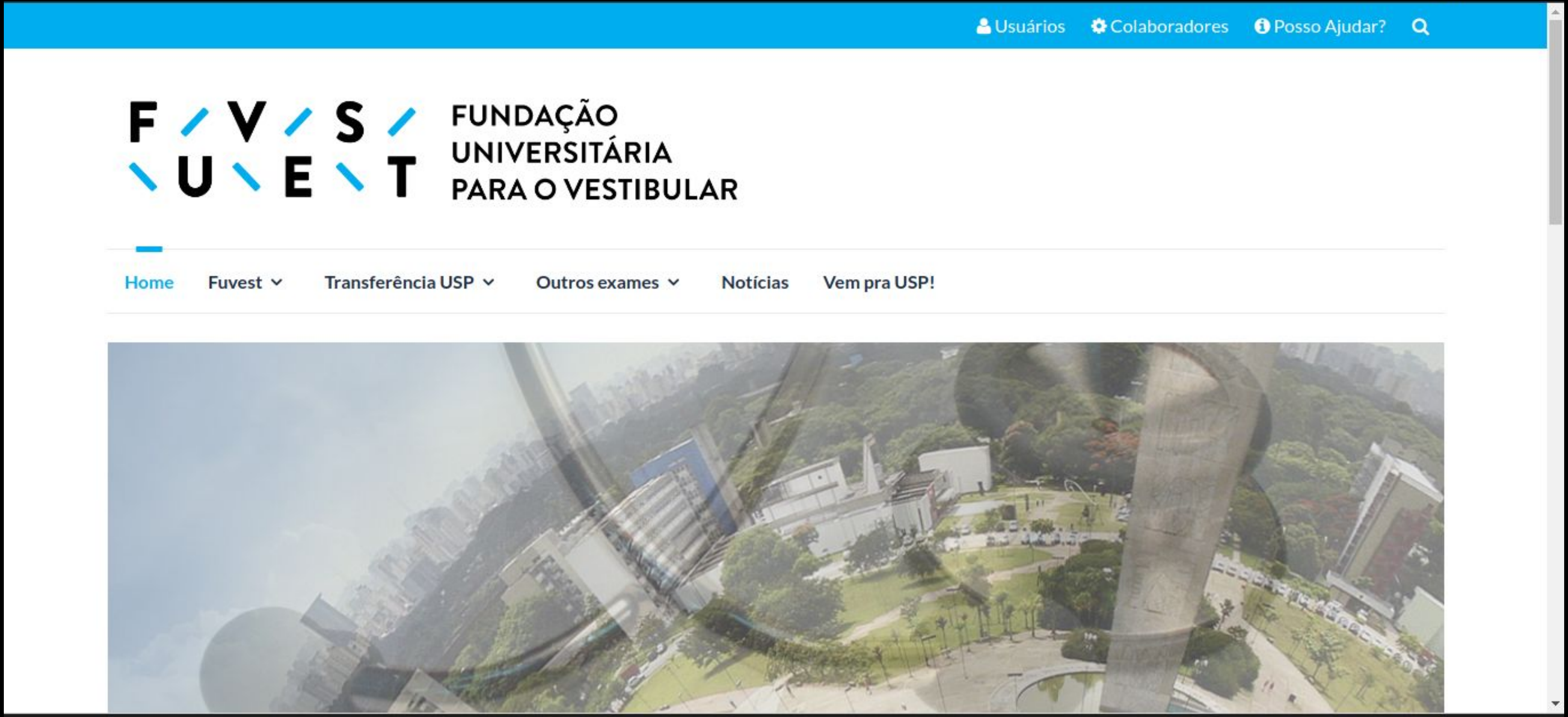
IMEsec

O que é?

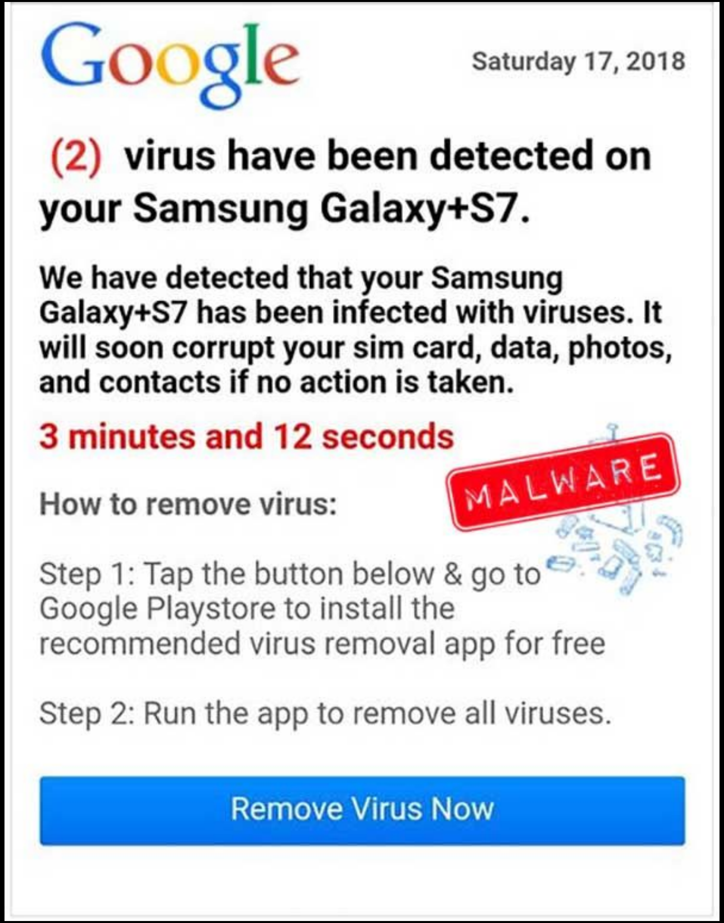
Tática de **engenharia social**

‘Pescaria’ de credenciais

Tática 1 - site convincente


Usuários
Colaboradores
Posso Ajudar?
FUVEST
FUNDAÇÃO UNIVERSITÁRIA PARA O VESTIBULAR
Home
Fuvest
Transferência USP
Outros exames
Notícias
Vem pra USP!

+ Ctrl-S



Google

Saturday 17, 2018

(2) virus have been detected on your Samsung Galaxy+S7.

We have detected that your Samsung Galaxy+S7 has been infected with viruses. It will soon corrupt your sim card, data, photos, and contacts if no action is taken.

3 minutes and 12 seconds

MALWARE

How to remove virus:

Step 1: Tap the button below & go to Google Playstore to install the recommended virus removal app for free

Step 2: Run the app to remove all viruses.

www.ltau.com.br ☺

www.ltau.com.br ☺

www.LTAU.com.br ☹

Tática 2 - Email customizado

exemplo: promoções exclusivas para funcionários de uma empresa exemplo: promoções exclusivas para funcionários de uma empresa

(spear phishing)

419 Scams:

https://www.hoax-slayer.net/category/scams/scam-catalogue/nigerian-scam-list/

Good Day,
My name is Dr William Monroe, a staff in the Private Clients Section of a well-known bank, here in London, England. One of our accounts, with holding balance of Â£15,000,000 (Fifteen Million Pounds Sterling) has been dormant and last operated three years ago. From my investigations and confirmation, the owner of the said account, a foreigner by name John Shumejda died on the 4th of January 2002 in a plane crash in Birmingham.

I have decided to find a reliable foreign partner to deal with. I therefore propose to do business with you, standing in as the next of kin of these funds from the deceased and funds released to you after necessary processes have been followed.

This transaction is totally free of risk and troubles as the fund is legitimate and does not originate from drug, money laundry, terrorism or any other illegal act.

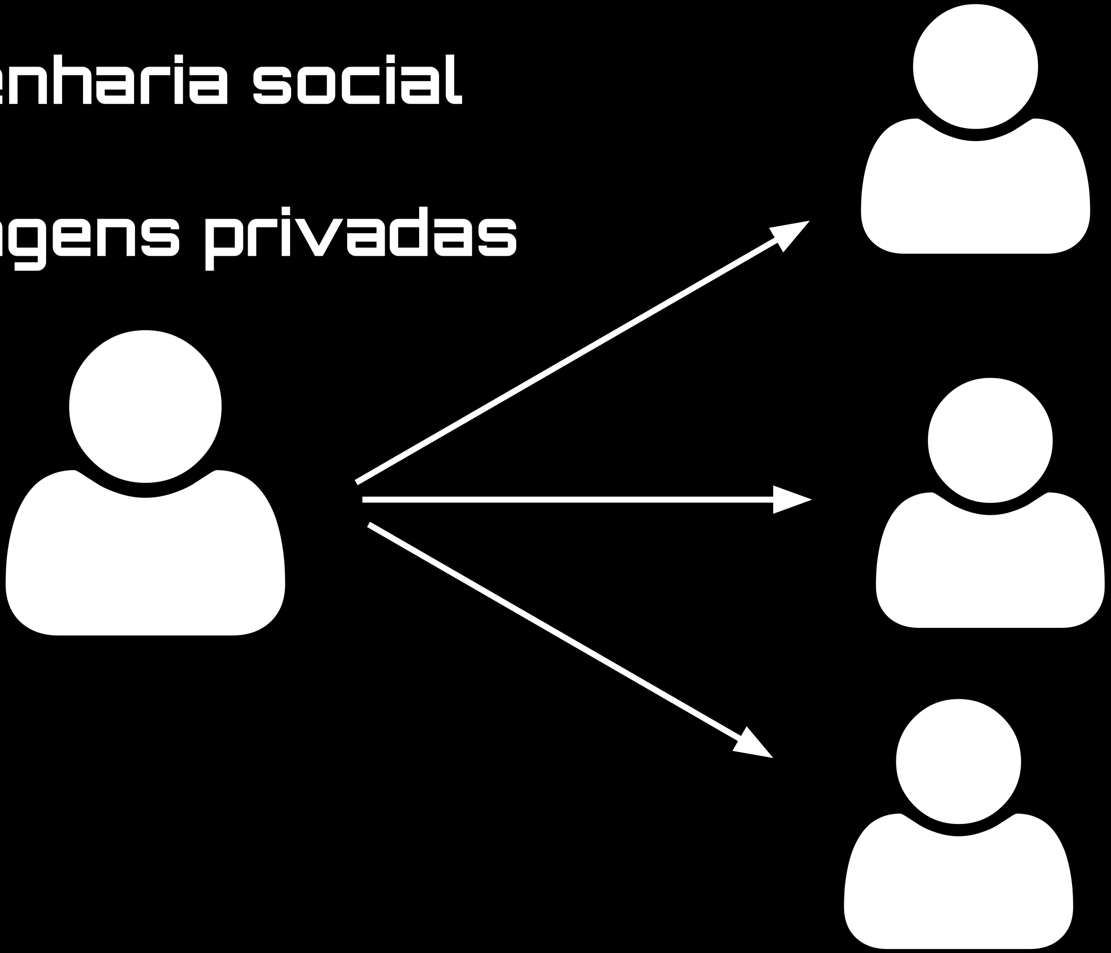
On your interest, let me hear from you URGENTLY.

Best Regards,
Dr William Monroe Financial Analysis and Remittance Manager
[Phone Number Removed]

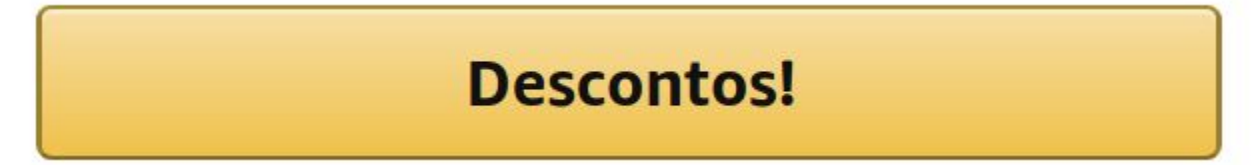
Tática 3 - “Amigo”

Engenharia social

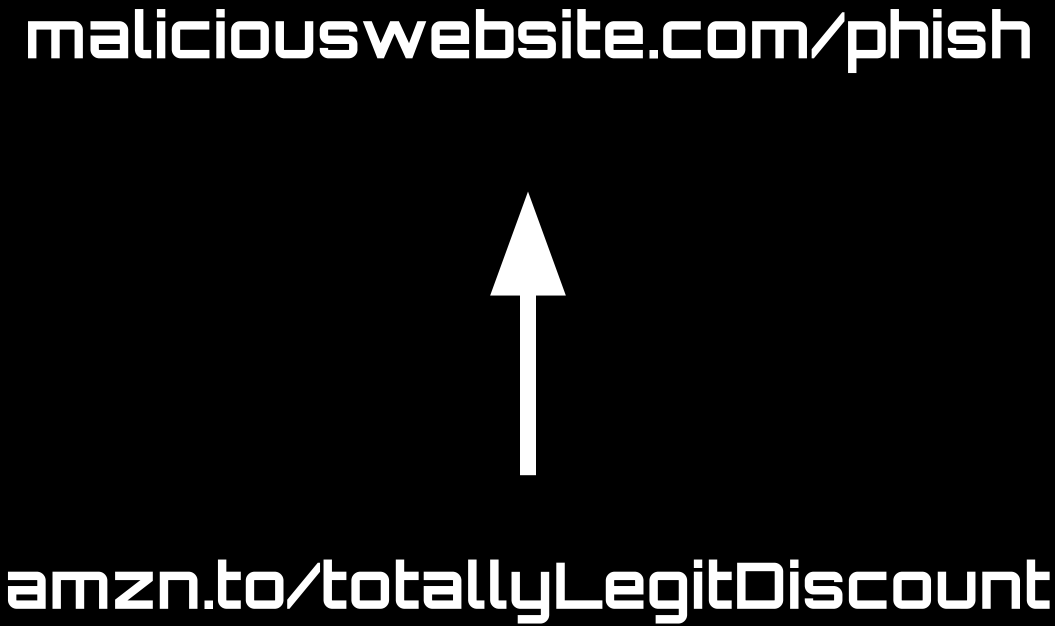
Mensagens privadas



Tática 4 - Link Shortener



amzn.to/totallyLegitDiscount



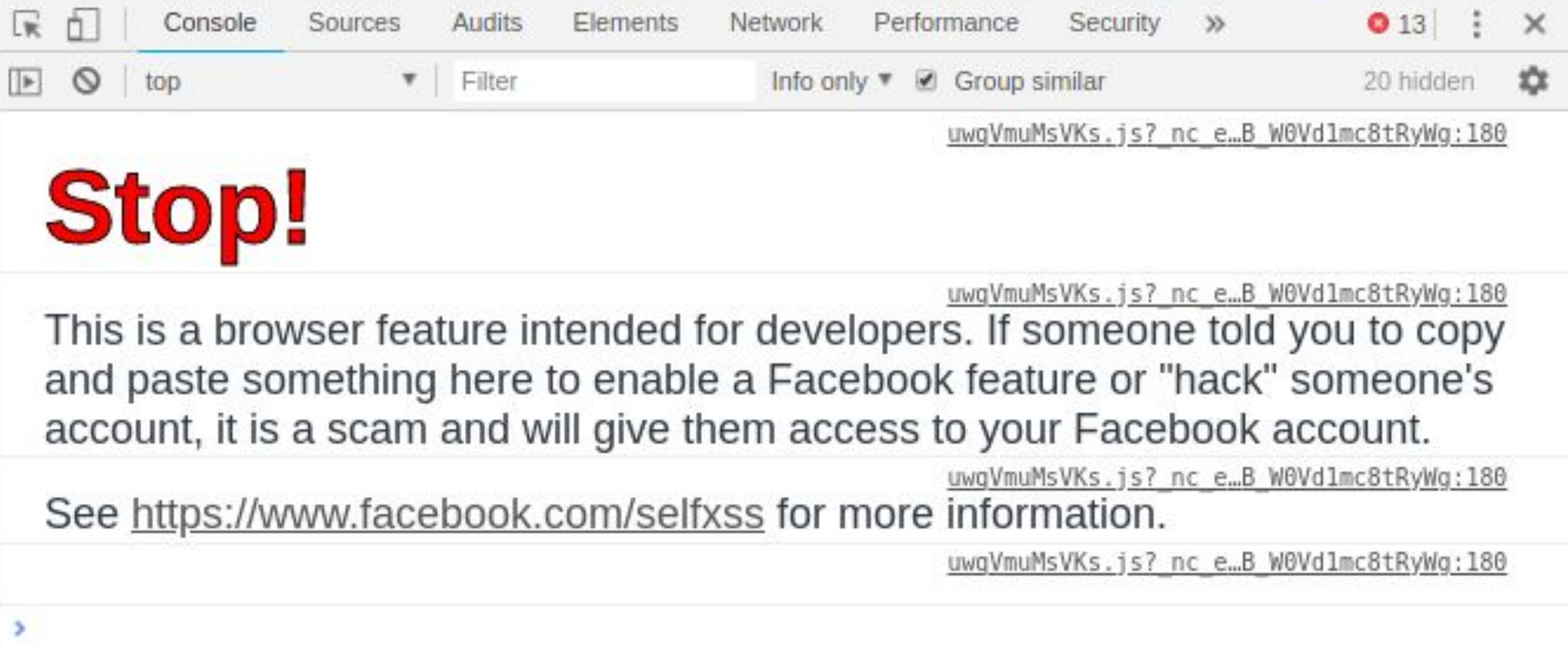
maliciouswebsite.com/phish

amzn.to/totallyLegitDiscount

Tática 5 - XSS (e outros)

Site anfitrião tem vulnerabilidade =>

informação fake no site genuíno



uwgVmuMsVKs.js?_nc_e…B_W0Vd1mc8tRyWg:180

Stop!

uwgVmuMsVKs.js?_nc_e…B_W0Vd1mc8tRyWg:180

This is a browser feature intended for developers. If someone told you to copy and paste something here to enable a Facebook feature or "hack" someone's account, it is a scam and will give them access to your Facebook account.

uwgVmuMsVKs.js?_nc_e…B_W0Vd1mc8tRyWg:180

See https://www.facebook.com/selfxss for more information.

uwgVmuMsVKs.js?_nc_e…B_W0Vd1mc8tRyWg:180

Mais?

http://www.phishing.org/phishing-examples

https://phishing-cujwhblmvp.now.sh/ (expirado após apresentação)

Finalidades

Roubo de credenciais

Roubo de credenciais

Roubar usuário e senha da pessoa

Roubo de credenciais

Roubar usuário e senha da pessoa

Problemas: 2-factor authentication, alarmes

Session Hijacking

Session Hijacking

Roubar o cookie do usuário

Session Hijacking

Roubar o cookie do usuário

Problema: Logout => invalidação do cookie

Roubo de informações

Roubo de informações

Às vezes não é necessário o login e senha de alguém - só a informação que essa pessoa detém

Obrigado!