Gerenciamento de Senhas

Porque de ter uma senha para cada aplicação, como criar senhas e como gerenciar

Tipos de ataques a senha

- Keylogger – hardware ou software que fica registrando a entrada do teclado.
- Observador – Espionagem ou oportunista de lugar publico, observa o que esta sendo digitado.
- Ataque Força Bruta – Poder computacional tentando adivinhar a senha por tentativa e erro.
- Phishing – Sites falsos para roubar senhas
- Vazamentos de Senhas – Vazamentos ou roubos de informação de login de usuários – Principal problema nesse momento.

Segundo o site Who is behind Have I Been Pwned (HIBP)

do pesquisador Troy Hunt, Developer Security, Microsoft Regional Director

- São conhecidos:

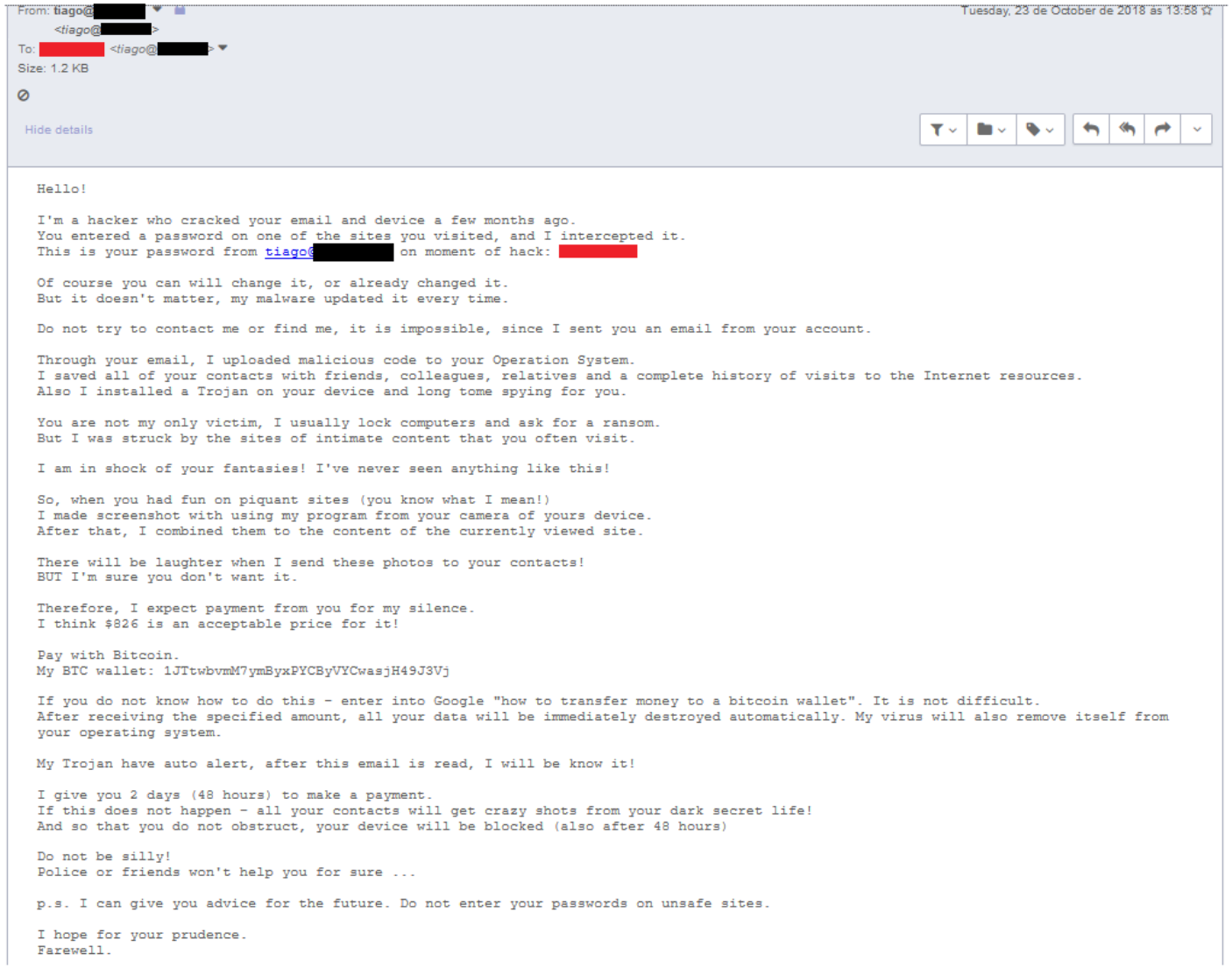
359 pwned websites

7,840,611,051 pwned accounts

Isso não atinge sites sérios...

- 2009 MySpace - 360 Milhões
- 2011 Sony/Playstation - 50mil
- 2012 Yahoo - 500 mil
- 2012 last.fm - 37 Milhões
- 2012 Dropbox - 68 Milhões
- 2013 Adobe - 152,5 milhões
- 2013 tumblr - 65,5 milhões de contas
- 2013 Badoo - 112 Milhões
- 2014 Avast - 420 mil contas
- 2014 Snapschat - 4,5 Milhões
- 2016 LinkedIn - 164 Milhões
- 2016 uTorrent 400 mil
- 2016 Dailymotion - 85 Milhões
- 2017 Netshoes - 500 mil
- 2018 Atlas Quantum - 260 mil
- 2019 Facebook - 25 mil

Isso não vai me atingir...



From: tiago@[redacted]
<tiago@[redacted]>
To: [redacted] <tiago@[redacted]>
Size: 1.2 KB

Tuesday, 23 de October de 2018 as 13:58

Hide details

Hello!

I'm a hacker who cracked your email and device a few months ago.
You entered a password on one of the sites you visited, and I intercepted it.
This is your password from tiago@[redacted] on moment of hack: [redacted]

Of course you can will change it, or already changed it.
But it doesn't matter, my malware updated it every time.

Do not try to contact me or find me, it is impossible, since I sent you an email from your account.

Through your email, I uploaded malicious code to your Operation System.
I saved all of your contacts with friends, colleagues, relatives and a complete history of visits to the Internet resources.
Also I installed a Trojan on your device and long tome spying for you.

You are not my only victim, I usually lock computers and ask for a ransom.
But I was struck by the sites of intimate content that you often visit.

I am in shock of your fantasies! I've never seen anything like this!

So, when you had fun on piquant sites (you know what I mean!)
I made screenshot with using my program from your camera of yours device.
After that, I combined them to the content of the currently viewed site.

There will be laughter when I send these photos to your contacts!
BUT I'm sure you don't want it.

Therefore, I expect payment from you for my silence.
I think $826 is an acceptable price for it!

Pay with Bitcoin.
My BTC wallet: 1JTtwbvmM7ymByxPYCByVYCwasjH49J3Vj

If you do not know how to do this - enter into Google "how to transfer money to a bitcoin wallet". It is not difficult.
After receiving the specified amount, all your data will be immediately destroyed automatically. My virus will also remove itself from your operating system.

My Trojan have auto alert, after this email is read, I will be know it!

I give you 2 days (48 hours) to make a payment.
If this does not happen - all your contacts will get crazy shots from your dark secret life!
And so that you do not obstruct, your device will be blocked (also after 48 hours)

Do not be silly!
Police or friends won't help you for sure ...

p.s. I can give you advice for the future. Do not enter your passwords on unsafe sites.

I hope for your prudence.
Farewell.

From: tiago@[redacted]
<tiago@[redacted]>
To: [redacted] <tiago@[redacted]>
Size: 1.4 KB

Saturday, 27 de October de 2018 às 22:00

Hide details

Hello!

I'm a programmer who cracked your email account and device about half year ago.
You entered a password on one of the insecure site you visited, and I catched it.
Your password from tiago@[redacted] on moment of crack: [redacted]

Of course you can will change your password, or already made it.
But it doesn't matter, my rat software update it every time.

Please don't try to contact me or find me, it is impo

Through your e-mail, I uploaded malicious code to you
I saved all of your contacts with friends, colleagues
Also I installed a rat software on your device and lo

You are not my only victim, I usually lock devices an
But I was struck by the sites of intimate content tha

I am in shock of your reach fantasies! Wow! I've neve
I did not even know that SUCH content could be so exc

So, when you had fun on intime sites (you know what I
I made screenshot with using my program from your cam
After that, I jointed them to the content of the curr

Will be funny when I send these photos to your contac
BUT I'm sure you don't want it. I definitely would no

I will not do this if you pay me a little amount.
I think $880 is a nice price for it!

I accept only Bitcoins.
My BTC wallet: 1HQ7wGdA5G9qUtM8jyDt5obDv1x3vEvjCy

If you have difficulty with this - Ask Google "how to
After receiving the above amount, all your data will
My virus will also will be destroy itself from your o

My Trojan have auto alert, after this email is looked

You have 2 days (48 hours) for make a payment.
If this does not happen - all your contacts will get
And so that you do not obstruct me, your device will

Do not take this frivolously! This is the last warnin
Various security services or antiviruses won't help y

Here are the recommendations of a professional:
Antiviruses do not help against modern malicious code

From: tiago@[redacted]
<tiago@[redacted]>
To: [redacted] <tiago@[redacted]>

Wednesday, 10 de April de 2019 às 19:52

list. Learn more

UNSUBSCRIBE

quizás Se está preguntando por qué recibe este correo electrónico,

orreo electrónico y aparatos hace pocos meses.
ontrarme, es imposible, desde que para ti envié un correo electrónico

From: tiago@[redacted]
<tiago@[redacted]>
To: [redacted] <tiago@[redacted]>
Size: 2.0 KB

Monday, 24 de December de 2018 às 11:30

Hide details

我问候你！

我有个坏消息。
28/09/2018 - 在这一天，我攻击了您的操作系统并完全访问了您的帐户 tiago@[redacted]。
那天您的帐户密码是：[redacted]

就是这样。
在您当天连接的路由器的软件中，存在一个漏洞。
我盲先攻击了这个路由器并将恶意代码放在上面。
当您通过Internet输入时，我的木马安装在您设备的操作系统上。

之后，我完成了你的磁盘转储（我有你所有的地址簿，查看网站的历史记录，所有文件，电话号码和所有联系人的地址）。

一个月前，我想锁定你的设备并要求少量资金解锁。
但我查看了您经常访问的网站。 你最喜欢的资源令我震惊。
我说的是成人网站。

我想说 - 你是个大变态者。你有一个令人眼花缭乱的幻想！

在那之后，我想到了一个想法。
我制作了你喜欢的成人网站的截图（你知道我的意思，是吗？）。
之后，我在浏览本网站时拍摄了你和你的娱乐照片（我使用了你设备的相机）。
结果很棒！ 不要犹豫！

我深信您不想向您的亲戚，朋友或同事展示这些照片。
我认为361美元对于我的沉默是少量的。
此外，我花了很多时间在你身上！

我在比特币接受钱。
我的BTC钱包： 1Brr1nKR278Tot5hRwEeX4sG1UZbcd5BpR

您不知道如何补充比特币钱包？
在任何搜索引擎中写"如何补充btc钱包"。
这很简单。

对于付款，你有两天多一点（恰好50小时）。
别担心，计时器将在您打开此信件时开始。是的，是的..它已经开始了！

Ninguém cai nisso...

BLOCKCHAIR

En

Search BTC, ETH, BCH, LTC, BSV, DASH, DOGE blockchains for any

/ Bitcoin / Address / 1JTtwbvmM7ymByxPYCByVYCwasjH49J3Vj

Permalink https://blockchair.com/bit

Monetary info

Balance	**0**.00000546 **BTC**	**0**.03 **USD** today
Total received	5.10376384 BTC	33,042.94 USD today
Total spent	5.10375838 BTC	32,966.25 USD today
First seen	Receiving: 2018-10-22 21:53	Spending: 2018-10-29 15:31
Last seen	Receiving: 2018-11-25 08:35	Spending: 2018-11-29 08:08

QR code

General info

Address type	pubkeyhash
Script	OP_DUP OP_HASH160 bf904fd4e39a2d1369db6ca8e852e3e5fe8be883 OP_EQUALVERIFY OP_CHECKSIG
Script [bin]	v���O��-i@l��R����旋@
Script [hex]	76a914bf904fd4e39a2d1369db6ca8e852e3e5fe8be88388ac
Transaction count	58
Output count	54
Unspent output count	1

Other blockchain explorers

BTC https://btc.com/1JTtwbvmM7ymByxPYCByVY...

https://www.blockchain.com/btc/address/1JTt...

https://explorer.bitcoin.com/btc/address/1JTt...

A Senha e um dos principais elos de segurança

- Se ela cai, pode cair tudo junto
- Uma senha para cada coisa evita que caia tudo ao mesmo tempo
- Evita o medo, o pânico e te dar a possibilidade de fazer contenção de danos.

Critérios para uma boa senha

- Memorizável
- Dificil de descobrir
- Privada

Métodos Criação Senha

- Aleatório

rIZ84#9´5M%L%jt6L

- Positivo: Difícil de quebrar
- Negativo: Difícil de Lembrar, Fácil de Errar

Métodos Criação Senha

- Inventar Palavras

  Monisare Cadeveta

- Parece randômico, mas quando fazemos neologismos eles acabam por ter uma certa “logica gramatical” ou “logica da língua”
- Positivo: Fácil de decorar, não é alvo de ataque dicionário
- Negativo: Fácil de quebrar por ter poucos tipos de caracteres ou poucos caracteres

Métodos Criação Senha

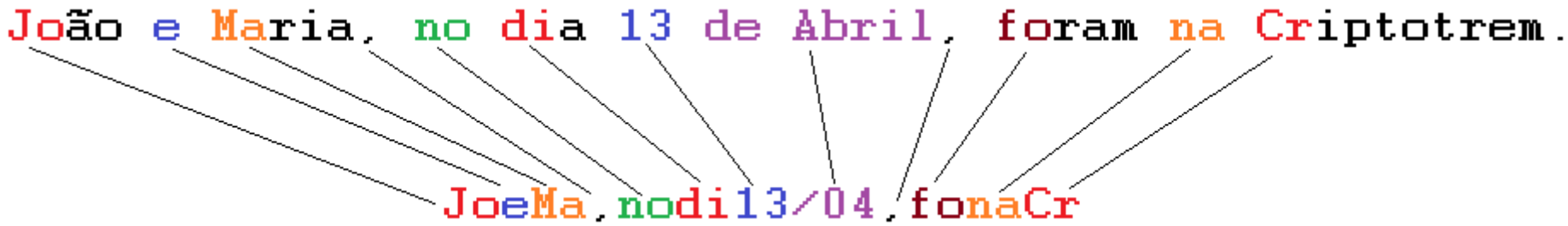
- Misturar Palavras com Símbolos e Números

  Cr|pt0tr3m

- Positivo: parece fácil de lembrar
- Negativo: Não é fácil de lembrar, sempre confunde um símbolo no meio, pode ser alvo de ataque “dicionários leet”

Métodos Criação Senha

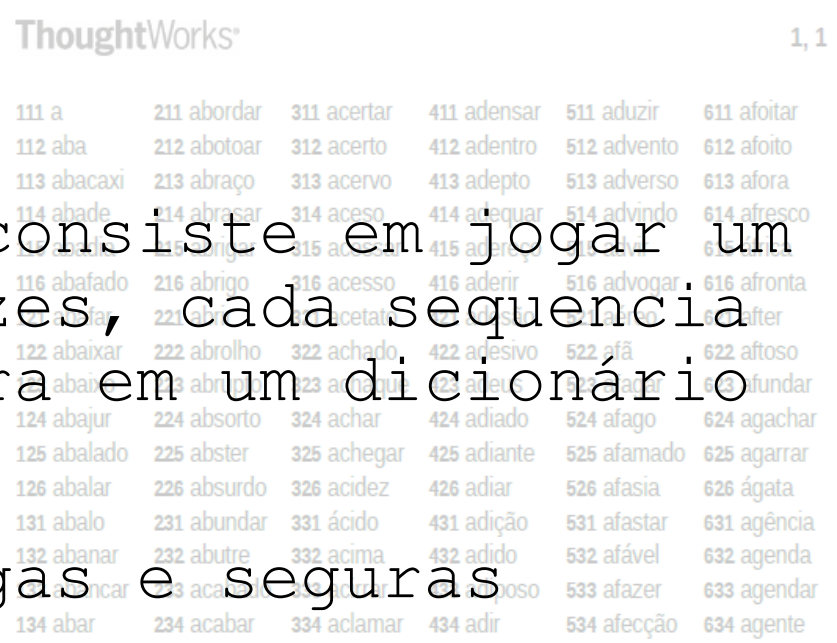
- Misturar Palavras com Símbolos e Números
  - Contar Historia



  - Requer lembrar não só a frase como a regra utilizada, nesse caso duas letras
  - Cuidado para não usar algo pessoal, como “Eu nasci...” tem que ser uma frase solta que facilite a memoria

Métodos Criação Senha

- Método do Dado

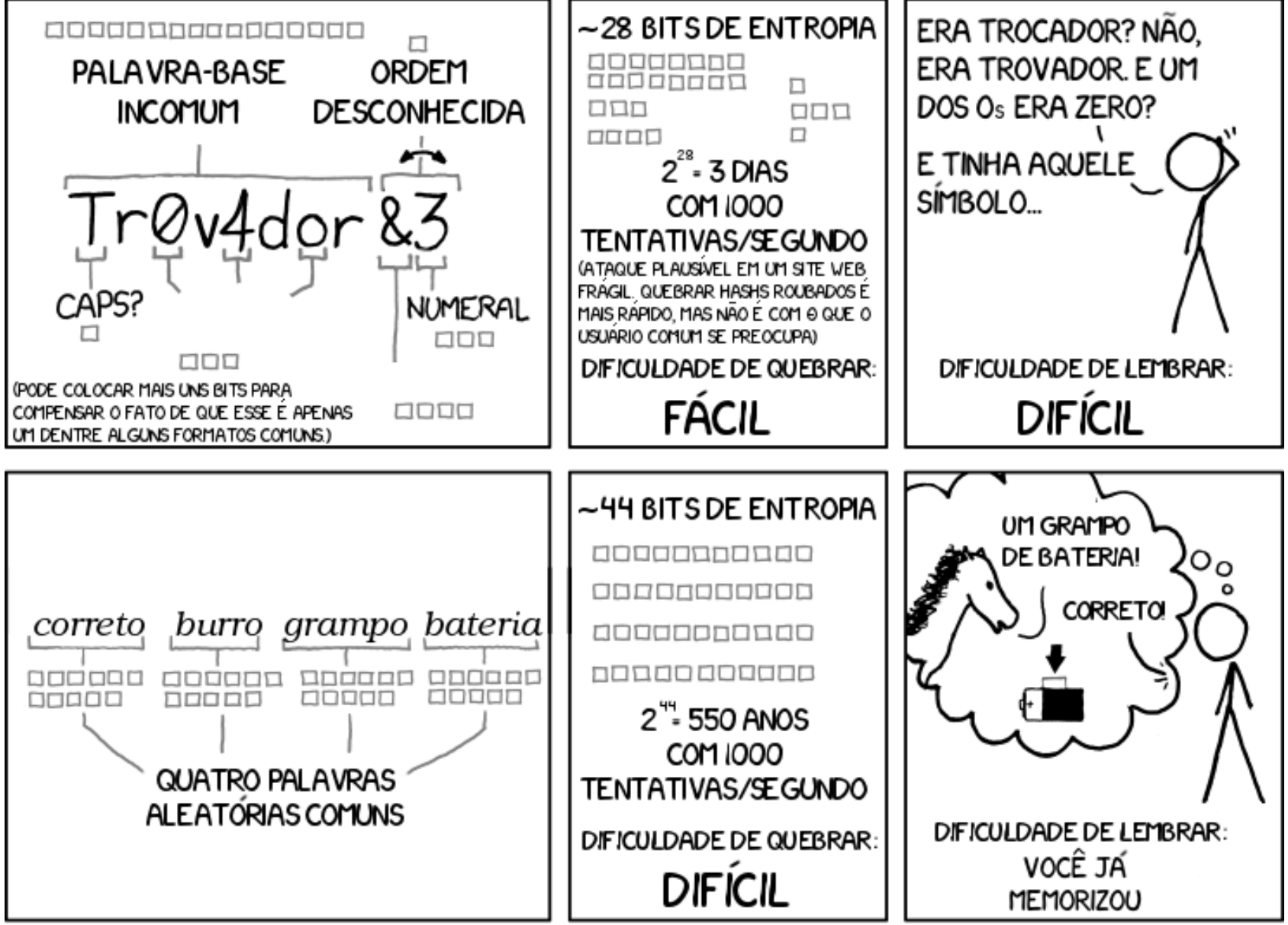


Um dos métodos mais utilizados, consiste em jogar um dado um determinado numero de vezes, cada sequencia de vezes corresponde a uma palavra em um dicionário

Positivo: consiste em senhas longas e seguras

Negativo: Pode ser alvo de ataques dicionários

Macete: Acrescente números ou símbolos em algum ponto



DEPOIS DE 20 ANOS DE ESFORÇO NÓS CONSEGUIMOS EFETIVAMENTE TREINAR TODO MUNDO A USAR SENHAS QUE SÃO DIFÍCEIS PARA OS HUMANOS MEMORIZAREM, MAS FÁCEIS PARA OS COMPUTADORES ADIVINHAREM..

https://xkcd.com/936/

Mas, se e uma senha para cada coisa, como lembrar de tudo?

- Em quantos sites, apps, serviços, etc... Você se cadastrou ao longo da vida? Quantos deles teve que colocar senha? Você consegue lembrar de todos?
- Se a senha que você colocou igual em todos, por que aquele site não tinha “nada sensível”, mas todos esses pequenos sites somados?
- Ai que entra a Gestão de Senhas
- Reduzir a suas senhas as essenciais, de forma que elas sempre sejam boas

Métodos de Armazenamento de Senhas

- Offline
  - Caderninho de anotações
  - Tabela Impressa
  - “Agendinha Codificada”
  - Planilha no Excel
  - Programas de Gestão de Senhas – KeePassXC
- Online
  - Criptografia Userside
  - Bitwarden

Ferramentas

- KeePass
- Bitwarden

Autenticação de Dois Fatores

- PIN
- Contra-Senha
- Biometria
- SMS
- OTP

Links:

Electronic Frontier Foundation

- https://ssd.eff.org/pt-br
- https://sec.eff.org/topics

Auto Defesa

- https://autodefesa.org/
- https://guia.autodefesa.org/

Security in-a-Box

- https://securityinabox.org/pt/

Senhas fáceis para você memorizar e que nem a NSA conseguirá desvendar

- https://theintercept.com/2016/12/29/senhas-faceis-para-voce-memorizar-e-que-nem-a-nsa-nao-consegue-desvendar/

Criação e gerenciamento de senhas

- https://pt.wikiversity.org/wiki/Cria%C3%A7%C3%A3o_e_gerenciamento_de_senhas

trr@tuta.io