



Navegação Segura: Recomendações em Segurança da Informação

Colégio Loyola
Agosto/2020

Sobre o instrutor



GUILHERME RODRIGUES

<http://br.linkedin.com/pub/guilherme-rodrigues-pereira/1b/5b4/891>

- Graduado em Redes de Computadores, Pós-graduado em Segurança da Informação, Gestão de Projetos e Mestre em Administração.
- Professor do Centro Universitário UNA (Graduação e Pós-graduação).
- Fundador da DGP TI (projetos, serviços e treinamentos em TI).
- Certificações: LPIC 1, CCNA, VCA-DCV, Microsoft 070-410 e ITIL.

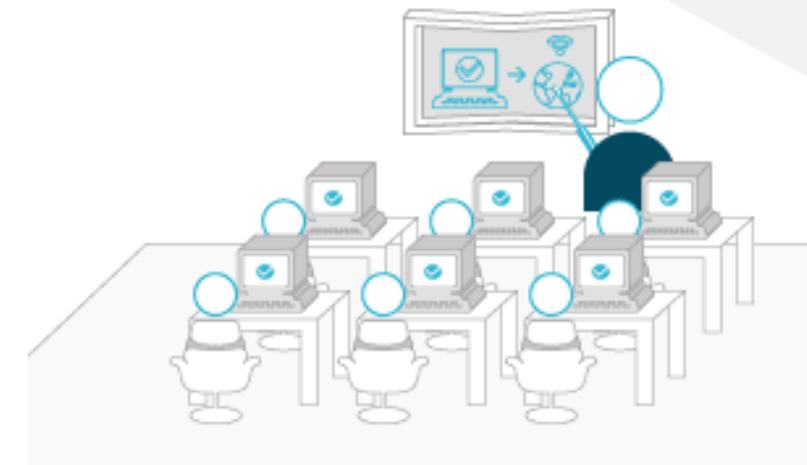


dgpti.com.br

Conteúdo da Apresentação

Navegação Segura e Recomendações

- Navegação segura, riscos e medidas de prevenção
- Phishing: Principais táticas e medidas de prevenção





Navegação Segura

- Existem algumas recomendações mais conhecidas sobre navegação segura.
- Entretanto, o que podemos fazer em relação ao que “não vemos”?
 - Códigos Maliciosos (Malware) na página;
 - Download/Instalação automática de componentes para coleta de dados no seu dispositivo;
 - Phishing: Redirecionamentos e PopUps para sites falsos;



Segurança em Camadas: *Layered Security & Defense in Depth*



- Quando estamos em um ambiente corporativo, **geralmente** temos diversas camadas de proteção (conforme **recomendam** os **frameworks** da área de TI):

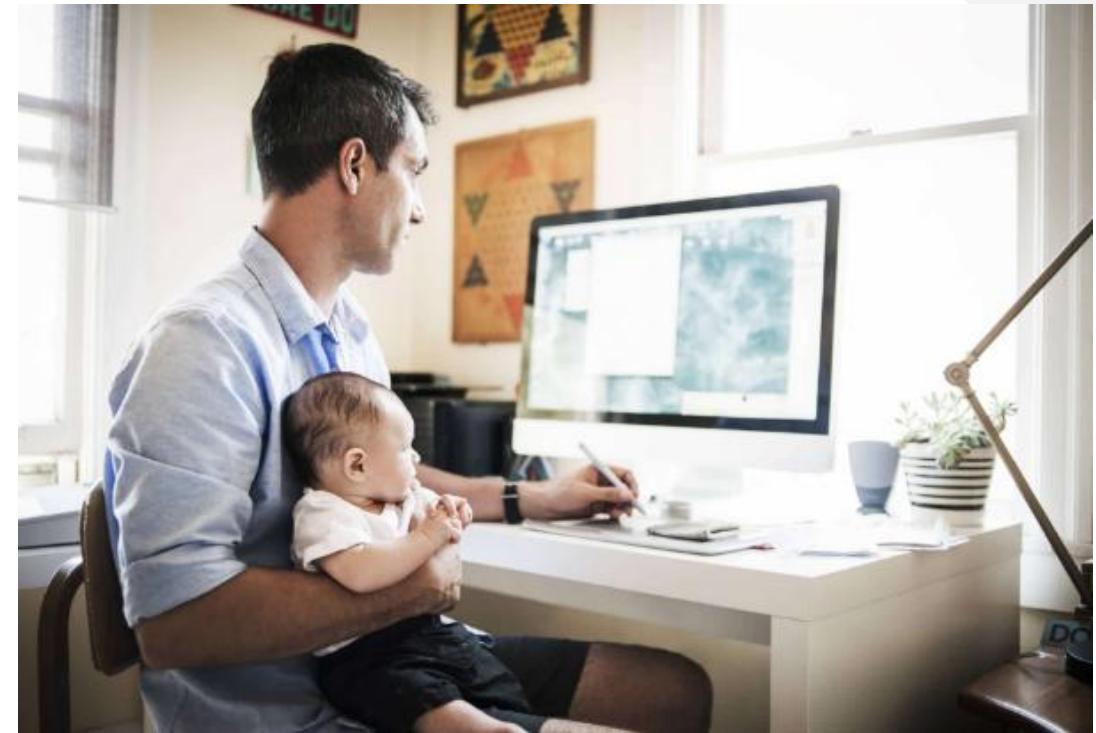


Fonte: Intel IT Center – Segurança da consumerização para um ambiente corporativo em transformação (Junho de 2013)



Tempos de Home Office...

- Mas quando **não estamos em ambiente corporativo**, como evitar estes riscos?

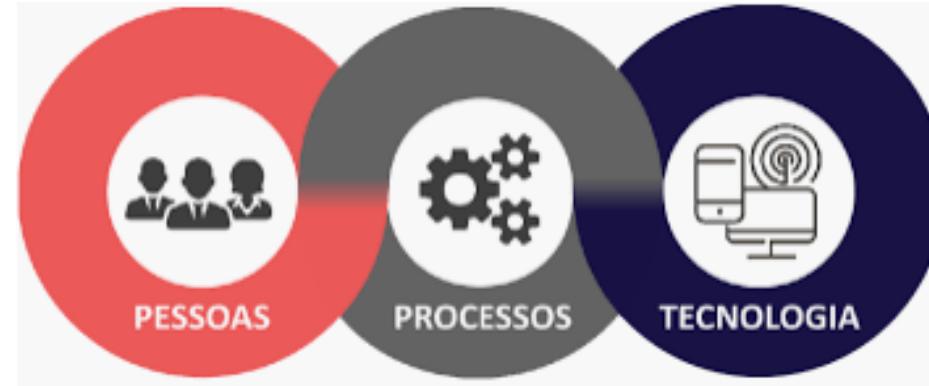


Conceitos introdutórios:

Segurança da informação



- A segurança da informação é **proporcionada** por três fatores (pilares):



OBS.: Atenção com o verbo (**proporcionar** ao invés de **garantir**).

- Então, como podemos definir o termo “Segurança da Informação”?
 - Preservação da **confidencialidade, integridade e disponibilidade** da informação (ISO 27001).



Dados sobre Navegação Segura

- O Google criou um serviço (Navegação Segura) para identificar sites não seguros, notificando usuários (no momento do acesso) e desenvolvedores para realizar as correções.



NAVEGAÇÃO SEGURA
Google

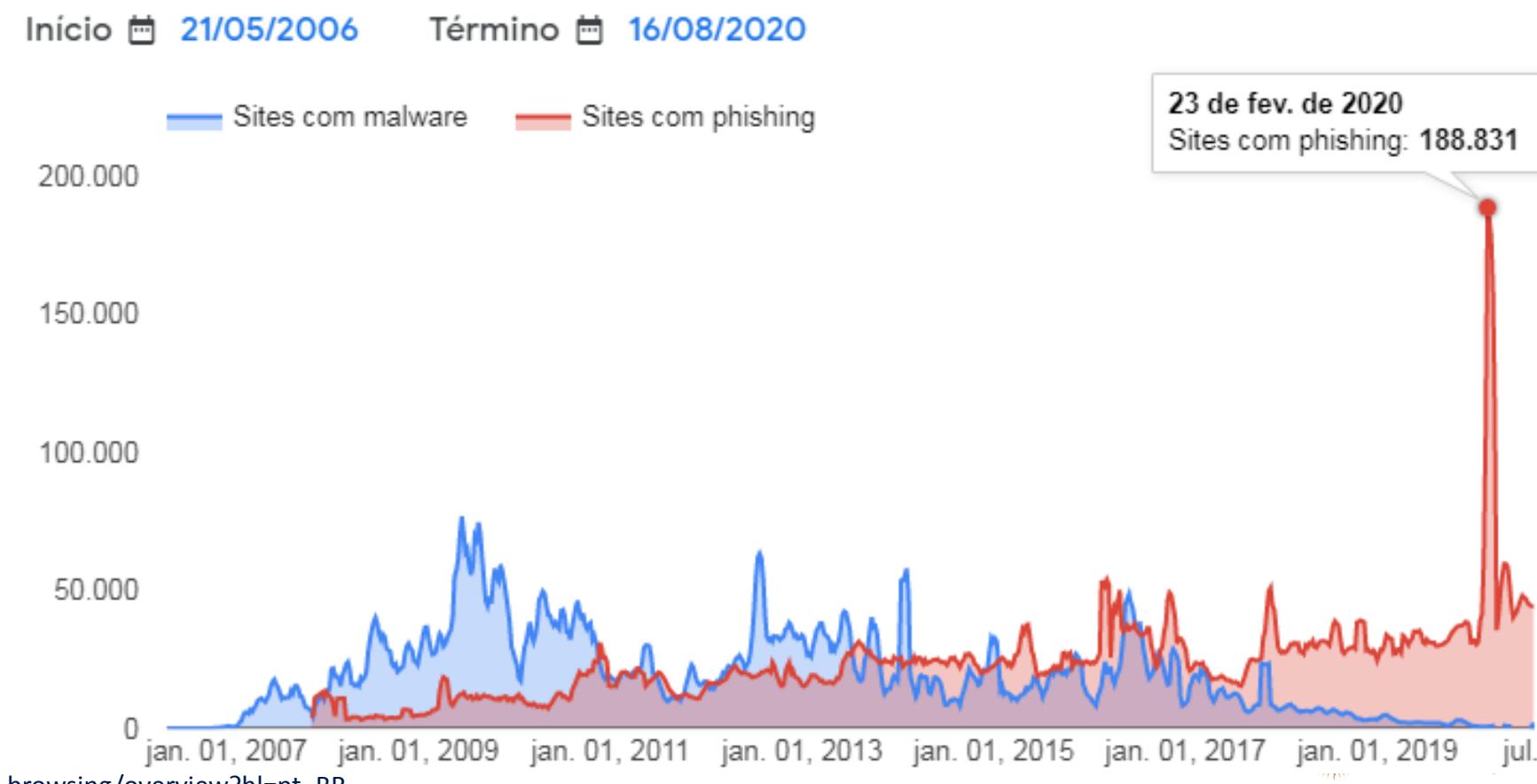
SITE SEGURO, CLIQUE ABAIXO
PARA VER O STATUS DE SEGURANÇA

 NAVEGAÇÃO SEGURA



Dados sobre Navegação Segura

- O gráfico ilustra o número de sites identificados com as ameaças mais recorrentes:
 - Sites com Malware.
 - Sites com Phishing.





Dados sobre Navegação Segura

- O que isso quer dizer?

 transparencyreport.google.com/safe-browsing/overview?hl=pt_BR

Sites não seguros detectados por semana

Todos os dias, o Navegação segura descobre milhares de novos sites não seguros. Muitos deles são websites legítimos que foram invadidos por hackers. Os sites não seguros são divididos em duas categorias que ameaçam a privacidade e a segurança do usuário: phishing e malware.





Dados sobre Navegação Segura

- Em relação aos sites legítimos comprometidos... Qual a quantidade?





Malware: Medidas de prevenção

- Recomendações (âmbito pessoal e profissional):
 - Utilizar software antivírus com boas avaliações (Kaspersky, McAfee, F-Secure, BitDefender, etc).
 - Não utilizar softwares piratas (Full Crack Keygen...). Baixar sempre no site do fabricante.
 - Manter o sistema operacional atualizado (Windows, MacOS, iOS, Android, Linux).
- Em caso de dúvidas, consulte a reputação do site antes de acessá-lo:

A screenshot of a web browser window. The address bar shows the URL: transparencyreport.google.com/safe... The main content area is titled 'Verificar o estado do site' and contains the URL 'loyola.g12.br'. Below the URL is a search icon. A green progress bar is labeled 'Estado atual'. At the bottom, a green checkmark icon is followed by the text 'Nenhum conteúdo inseguro encontrado'.

https://transparencyreport.google.com/safe-browsing/search?hl=pt_BR



Configurações do Chrome



← → C Chrome | chrome://settings/security

Settings

Search settings

- You and Google
- Autofill
- Safety check
- Privacy and security** →
- Appearance
- Search engine
- Default browser
- On startup

Safe Browsing

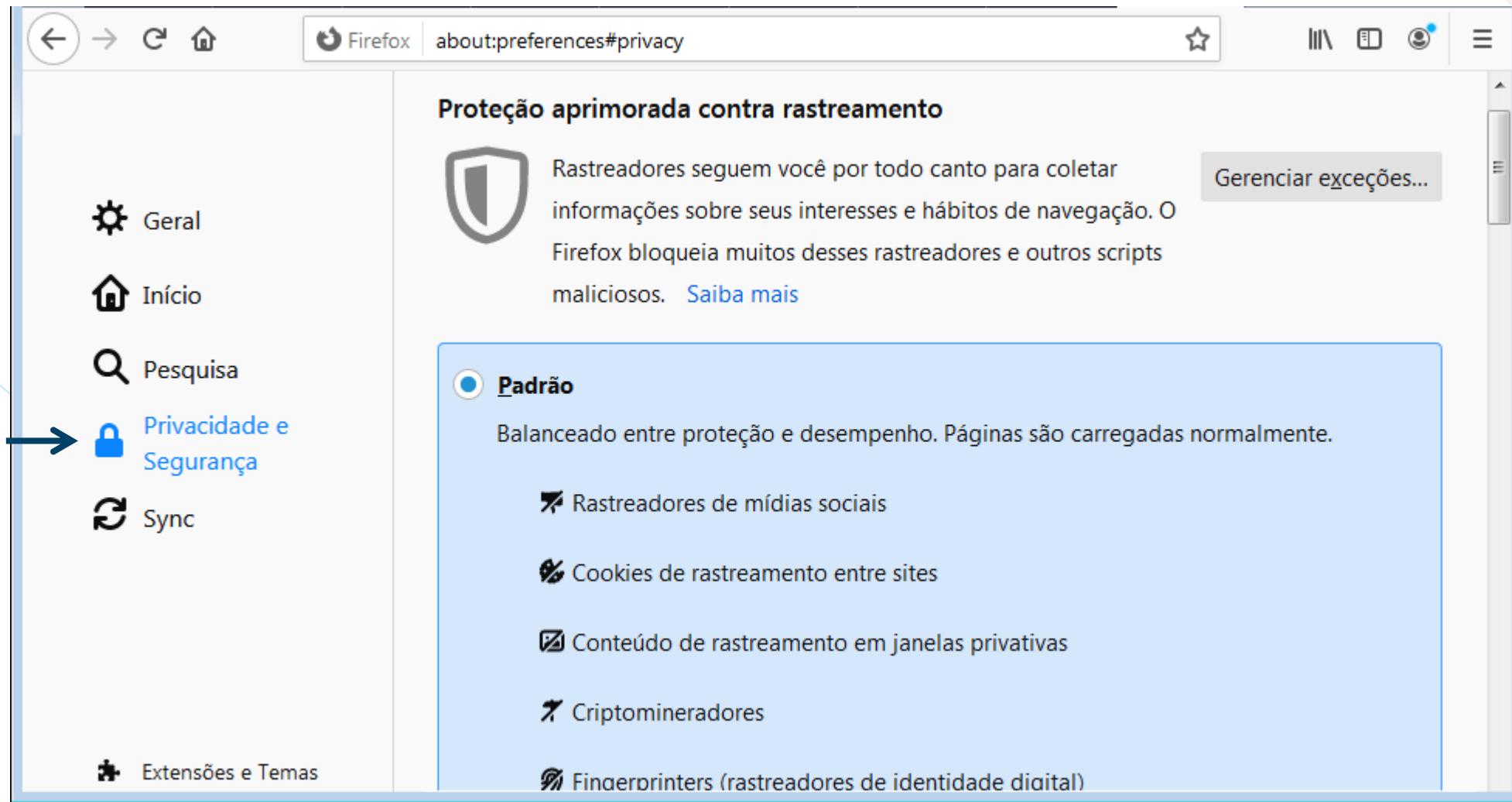
Enhanced protection
Faster, proactive protection against dangerous websites, downloads, and extensions. Warns you about password breaches. Requires browsing data to be sent to Google.

Standard protection
Standard protection against websites, downloads, and extensions that are known to be dangerous.

No protection (not recommended)
Does not protect you against dangerous websites, downloads, and extensions. You'll still get Safe Browsing protection, where available, in other Google services, like Gmail and Search.



Configurações do Firefox



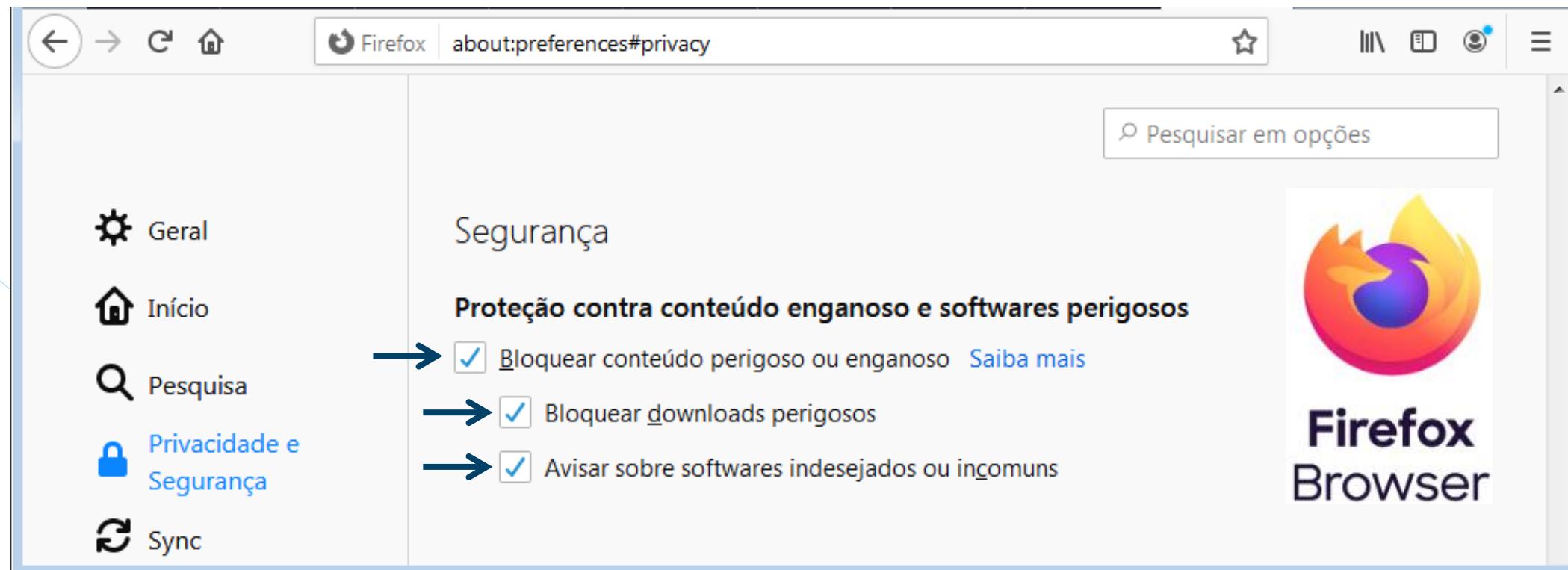
A screenshot of the Firefox browser window. The address bar shows 'Firefox about:preferences#privacy'. The left sidebar has icons for Geral, Início, Pesquisa, **Privacidade e Segurança** (which is selected and highlighted with a blue arrow), Sync, and Extensões e Temas. The main content area is titled 'Proteção aprimorada contra rastreamento' and describes how trackers follow users to collect information about their interests and browsing habits. It mentions that Firefox blocks many trackers and malicious scripts. A 'Gerenciar exceções...' button is present. Below this, a 'Padrão' (Default) section is selected, described as a balance between protection and performance. It lists several tracking-related settings with checkboxes: 'Rastreadores de mídias sociais' (checked), 'Cookies de rastreamento entre sites' (checked), 'Conteúdo de rastreamento em janelas privativas' (unchecked), 'Criptomineradores' (unchecked), and 'Fingerprinters (rastreadores de identidade digital)' (unchecked).



Firefox
Browser



Configurações do Firefox



The screenshot shows the Firefox privacy settings page (`about:preferences#privacy`). The left sidebar has links for Geral, Início, Pesquisa, Privacidade e Segurança (which is highlighted in blue), and Sync. The main content area is titled "Segurança" and "Proteção contra conteúdo enganoso e softwares perigosos". Three checkboxes are shown, all of which are checked (indicated by a blue arrow pointing to the first one): "Bloquear conteúdo perigoso ou enganoso" (Block dangerous or misleading content), "Bloquear downloads perigosos" (Block dangerous downloads), and "Avisar sobre softwares indesejados ou incomuns" (Warn about unwanted or uncommon software). A search bar at the top right says "Pesquisar em opções". On the right side, there is a large Firefox logo and the text "Firefox Browser".

Outras medidas preventivas: Controle Parental



- É possível configurar em alguns sistemas e softwares, restrições por faixa etária.
 - Windows 10:

Pesquisas
Quando seu filho pesquisar na Web, você verá o que ele procurou aqui.

Navegação na Web Ativar restrições
Quando seu filho visitar sites, eles aparecerão aqui.

Aplicativos e jogos Ativar restrições
Quando seu filho usar aplicativos ou jogos, eles aparecerão aqui.

Aplicativos, jogos e mídia

Definir um limite de idade para bloquear aplicativos, jogos e mídia inadequados. Qualquer item que exceder as classificações de conteúdo que você decidiu que são adequadas para o seu filho precisará da sua aprovação.

Esta configuração se aplica a dispositivos Windows 10 e Xbox One.

Bloquear aplicativos, jogos e mídia inadequados Ativado

Permitir aplicativos e jogos classificados para
Todas as idades (sem restrições) ▾

- 10 anos
- 11 anos
- 12 anos
- 13 anos

Sempre permitido (0)

Quando você permitir aplicativos e jogos específicos, e

Sempre bloqueado (0)

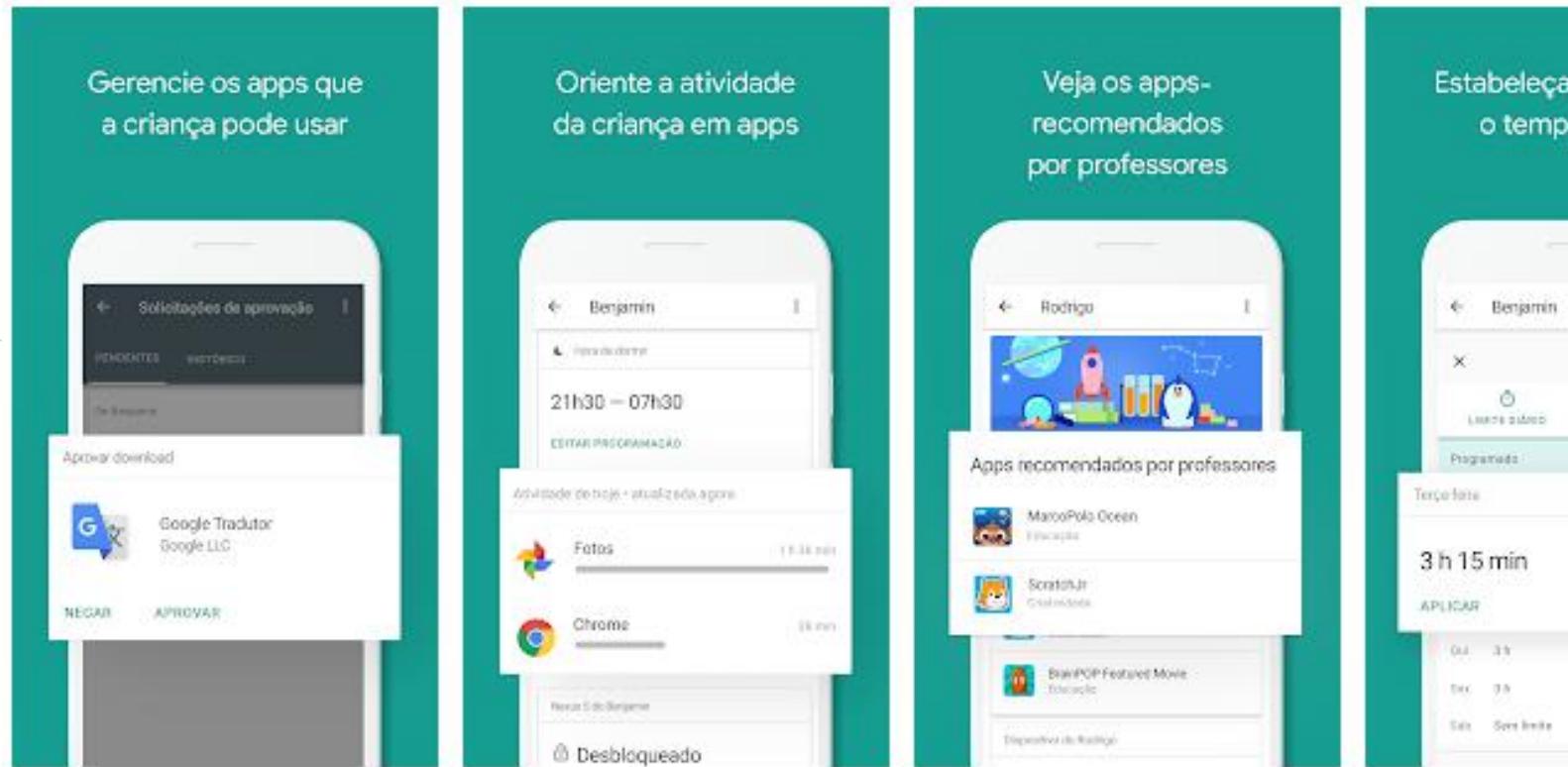
Fonte: TechTudo (Paulo Alves).

Disponível em: <https://www.techtudo.com.br/dicas-e-tutoriais/2018/03/como-controlar-o-que-as-criancas-acessam-no-pc-com-windows-10.ghtml>

Outras medidas preventivas: Controle Parental



- É possível configurar em alguns sistemas e softwares, restrições por faixa etária.
 - Smartphones e Tablets (Android e iOS):



Google Family
Link para pais

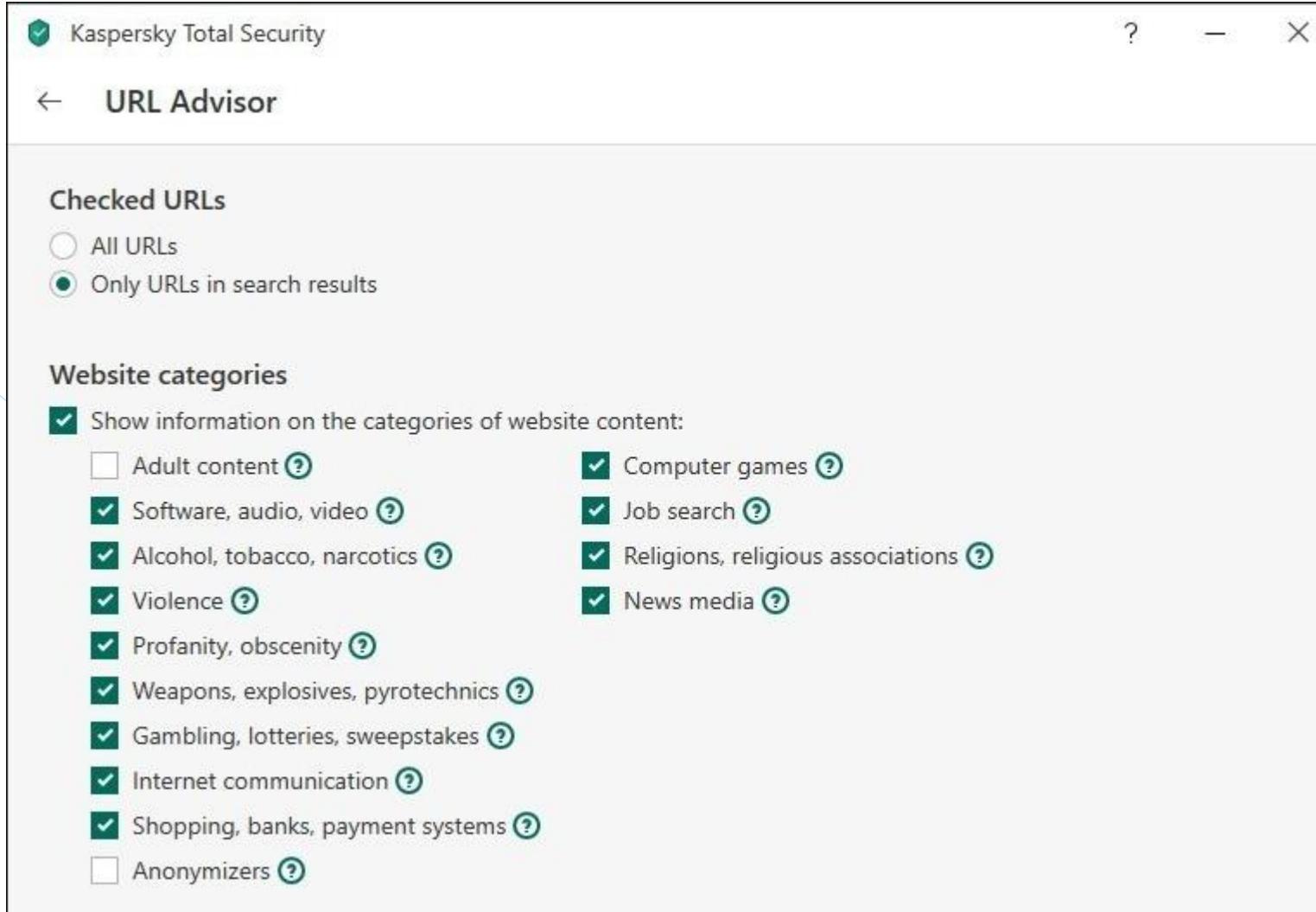
Google LLC Ferramentas



Fonte: TechTudo (Adriano Ferreira).

Disponível em: <https://www.techtudo.com.br/noticias/2019/05/aplicativo-para-monitorar-filhos-veja-5-opcoes-gratis-para-o-seu-celular.ghtml>

Outras medidas preventivas: Web Filter no AntiVirus



Kaspersky Total Security

URL Advisor

Checked URLs

All URLs (radio button)

Only URLs in search results (radio button, selected)

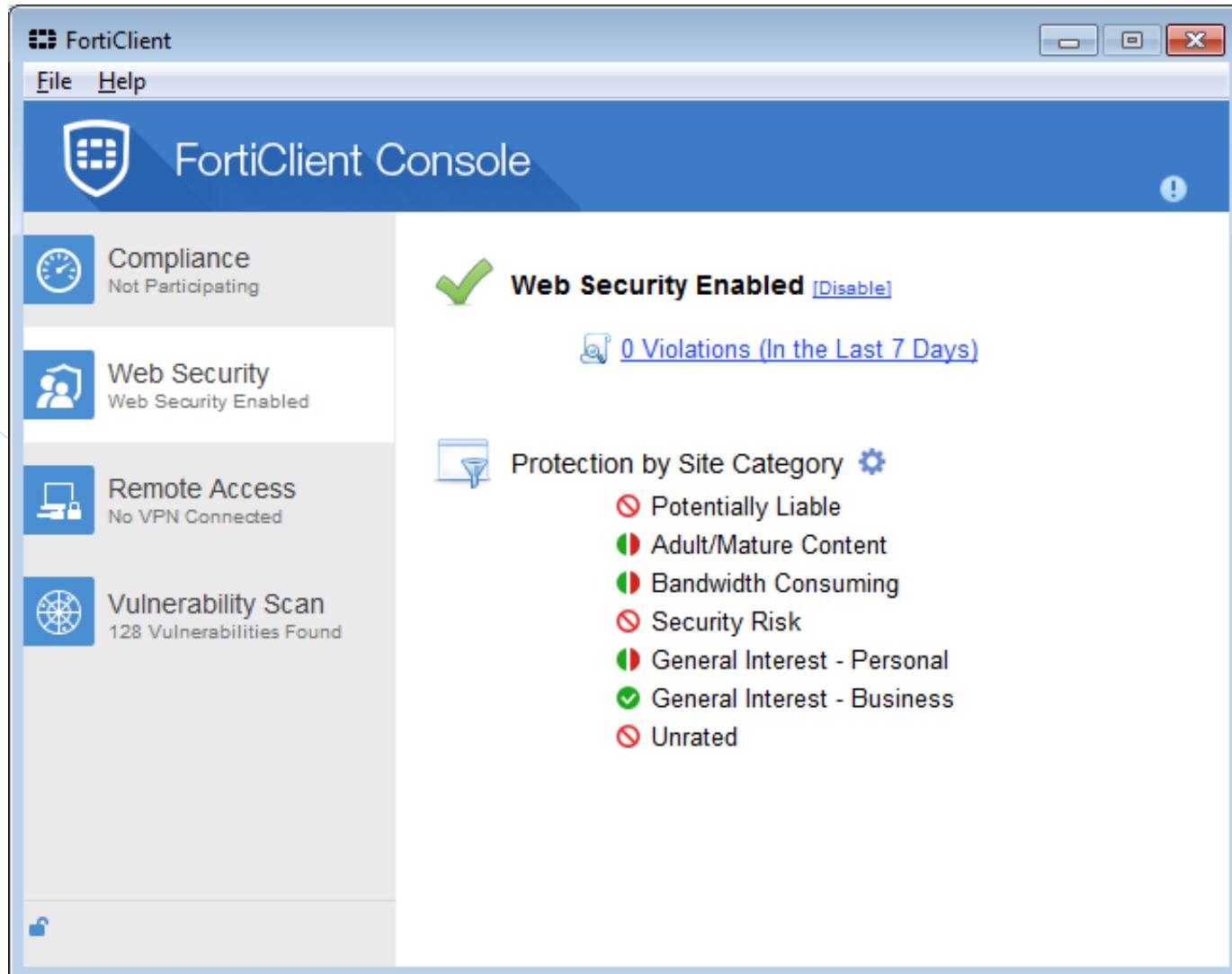
Website categories

Show information on the categories of website content:

- Adult content
- Computer games
- Software, audio, video
- Job search
- Alcohol, tobacco, narcotics
- Religions, religious associations
- Violence
- News media
- Profanity, obscenity
- Weapons, explosives, pyrotechnics
- Gambling, lotteries, sweepstakes
- Internet communication
- Shopping, banks, payment systems
- Anonymizers

- Alguns softwares de Antivírus possuem a funcionalidade de *Web Filter* com base em categorias.

Outras medidas preventivas: Web Filter no AntiVirus



- Alguns softwares de Antivírus possuem a funcionalidade de *Web Filter* com base em categorias.

Outras medidas preventivas: DNS Filter Cloudflare



- Serviço de DNS público da Cloudflare: Filtro de sites de risco e conteúdo adulto.

Malware Blocking Only

Change your router DNS to:

- 1.1.1.2
- 1.0.0.2

Ready to set it up? You'll find an easy guide for every device in the [setup instructions](#) page.

Malware and Adult Content Blocking Together

Change your router DNS to:

- 1.1.1.3
- 1.0.0.3

Ready to set it up? You'll find an easy guide for every device in the [setup instructions](#) page.

- Pode ser configurado no Modem de Internet.

Fonte: Cloudflare

Disponível em: <https://1.1.1.1/family/>





Phishing

Principais táticas e medidas de prevenção



Conceito: Phishing

- **Phishing:** tentativa fraudulenta de **obter informações confidenciais** (usuário, senha, dados de cartões de crédito) **ao se passar por uma entidade confiável** em uma **comunicação eletrônica**.



- *“O Google afirma que detecta cerca de 100 milhões de mensagens de phishing por dia.”*
 - Publicado em: 26/11/2019

Fonte: https://olhardigital.com.br/fique_seguro/noticia/eua-sao-o-maior-alvo-de-phishing-no-mundo-diz-google/93542



Conceito: Phishing

- “Ah... Duvido. Brasileiro não acredita em tudo o que lê na Internet...”

https://olhardigital.com.br/fique_seguro/noticia/brasil-e-o-pais-com-mais-ataques-de-phishing-no-mundo/72546

GERAL PRO NOTÍCIAS VÍDEOS INTERNACIONAL OFERTAS LOGIN

Brasil é o país com mais ataques de phishing no mundo

JULIANA AMÉRICO 23/11/2017 17H13

CIBERATAQUE :: CIBERCRIME :: PHISHING

Os brasileiros são os mais afetados por ataques de phishing no mundo. De acordo com um levantamento realizado pela empresa de segurança Kaspersky, o Brasil aparece em primeiro lugar na lista com maior número de vítimas até novembro desse ano.

Ao todo, 28,3% dos internautas brasileiros caíram em algum golpe de phishing, ficando à frente da Austrália, que registrou 21,79% dos usuários de internet atacados, e da China, com 19,58%.

Fonte: https://olhardigital.com.br/fique_seguro/noticia/brasil-e-o-pais-com-mais-ataques-de-phishing-no-mundo/72546



Tipos de Phishing

- Dentre os principais tipos de ataques de Phishing, temos:
 - **E-mail Phishing:** o atacante utiliza domínios falsos, ou usam o nome da empresa no campo do usuário, bem como outros “truques” como as letras “r” e “n” juntas (“rn” ao invés de “m”).
 - **Spear Phishing:** Mais sofisticado e direcionado a uma pessoa específica. Ou seja, para realizá-lo, o atacante já possuirá dados como:
 - Nome, Cargo, Telefone, E-mail, entre outros dados profissionais.
 - **Whaling:** Ainda mais sofisticado, visa executivos de uma determinada organização, utilizando temas que possam induzir a pessoa ao erro. Neste caso, o atacante já possui informações sobre preferências pessoais e comportamento de navegação.
 - **Smishing and Vishing:** Similar ao E-mail Phishing, porém, utiliza o telefone como meio de ataque (SMS e aplicativos de mensagem), geralmente relacionados a instituições financeiras e prêmios.



Alguns exemplos de Phishing

- Tipo: Smishing and Vishing.



BB Informa : Prezado cliente ,
ainda nao consta atualizacao
digital da sua conta , para evitar
o bloqueio acesse saiba mais:
<http://wi.atendimento-app.me>

Segurancia Santander: Procedimento Mobile
Obrigatorio. Acesse o Canal: <http://103.194.48.195/> e evite Bloqueio automatico
de sua conta

Oct 7, 2017, 14:49

IP ADDRESS	CONTINENT	FLAG	COUNTRY	REGION	CITY	TIME ZONE
103.194.48.195	Asia		Bangladesh		Dhaka	GMT+6



Alguns exemplos de Phishing

Auto-Atendimento Nº 00099843

Voltar para mensagens |

Santander [Adicionar a contatos](#)

Para:

22/07/2011

De: **Santander** (atendimento@santander.com.br)

Responder

Enviada: sexta-feira, 22 de julho de 2011 13:51:27

Para:

O Microsoft SmartScreen marcou esta mensagem como lixo eletrônico e ela será excluída após 10 dias.
[Espere, é confiável](#) | [Não sei, mostre o conteúdo](#)

Santander

Comunicado

Prezado(a) Cliente

Encontramos falhas nos registros do **Módulo de Proteção** em seu computador:
Ausência de atualizações de segurança imposta pelo sistema Santander.

Até o momento não encontramos nenhuma autenticação para as atualizações de segurança.

Alguns dos serviços santander entrará em processo de suspensão automaticamente.

Para evitar a suspensão automática desses serviços, habilite suas atualizações clicando no botão abaixo.
Este recurso só é ativado se você aceitar e é atualizado a partir de servidores certificados.

CONFIRMAR

Banco Santander (Brasil) S.A.

Atenção aos erros de português
e saudações genéricas
(Ex.: Prezado Cliente)

Phishing: Lançando a isca!



```
Administrator: C:\Windows\system32\cmd.exe
220 BAY004-MC4F52.hotmail.com Sending unsolicited commercial or bulk e-mail to Microsoft's computer network is prohibited. Other restrictions are found at http://privacy.microsoft.com/en-us/anti-spam.mspx. Fri, 28 Oct 2016 17:51:32 -0700
he.lo dgpti.com.br
250 BAY004-MC4F52.hotmail.com <3.22.0.10> Hello [168.205.159.210]
mail from: no-teste@naoexiste.com
250 no-teste@naoexiste.com...Sender OK
rcpt to: [REDACTED]
250 [REDACTED]
data
354 Start mail input; end with <CRLF>.<CRLF>
From: Guilherme <te-enganei@nao-existe.com>
To: Juliana
Subject: Pedido de Proposta
Olá,
Conforme conversamos por telefone, gostaria de receber uma proposta!
Segue link com ideia inicial do projeto:

http://www.dgop.com/run.js

Aguardo,
Att,
Guilherme
.
250 <BAY004-MC4F521hTrBo0027006e@BAY004-MC4F52.hotmail.com> Queued mail for delivery
quit
221 BAY004-MC4F52.hotmail.com Service closing transmission channel

Connection to host lost.

C:\>_
```

- Não se trata de um processo complexo, basta entender o protocolo SMTP.
- OBS.: Existem diversos softwares prontos, com interface gráfica, para realizar ataques personalizados.

Phishing: Lançando a isca!



https://outlook.live.com/owa/?path=/mail/junkemail/rp

Email do Outlook

Pesquisar Email e Pessoas

Novo | Excluir Arquivar Não é lixo eletrônico | Bloquear

^ Pastas

- Caixa de Entrada 5
- Lixo Eletrônico 53**
- Rascunhos 1
- Itens Enviados
- Itens Excluídos 21
- SENAC 1
- UNA Correio

Pedido de Proposta

Guilherme <te-enganei@nao-existe.com>
Hoje, 00:56
Juliana

Esta mensagem foi identificada como spam. Iremos excluí-la depois de 10 dias. [Não é spam](#)

Olá,
Conforme conversamos por telefone, gostaria de receber uma proposta!
Segue link com ideia inicial do projeto:

<http://www.dgop.com/run.js>

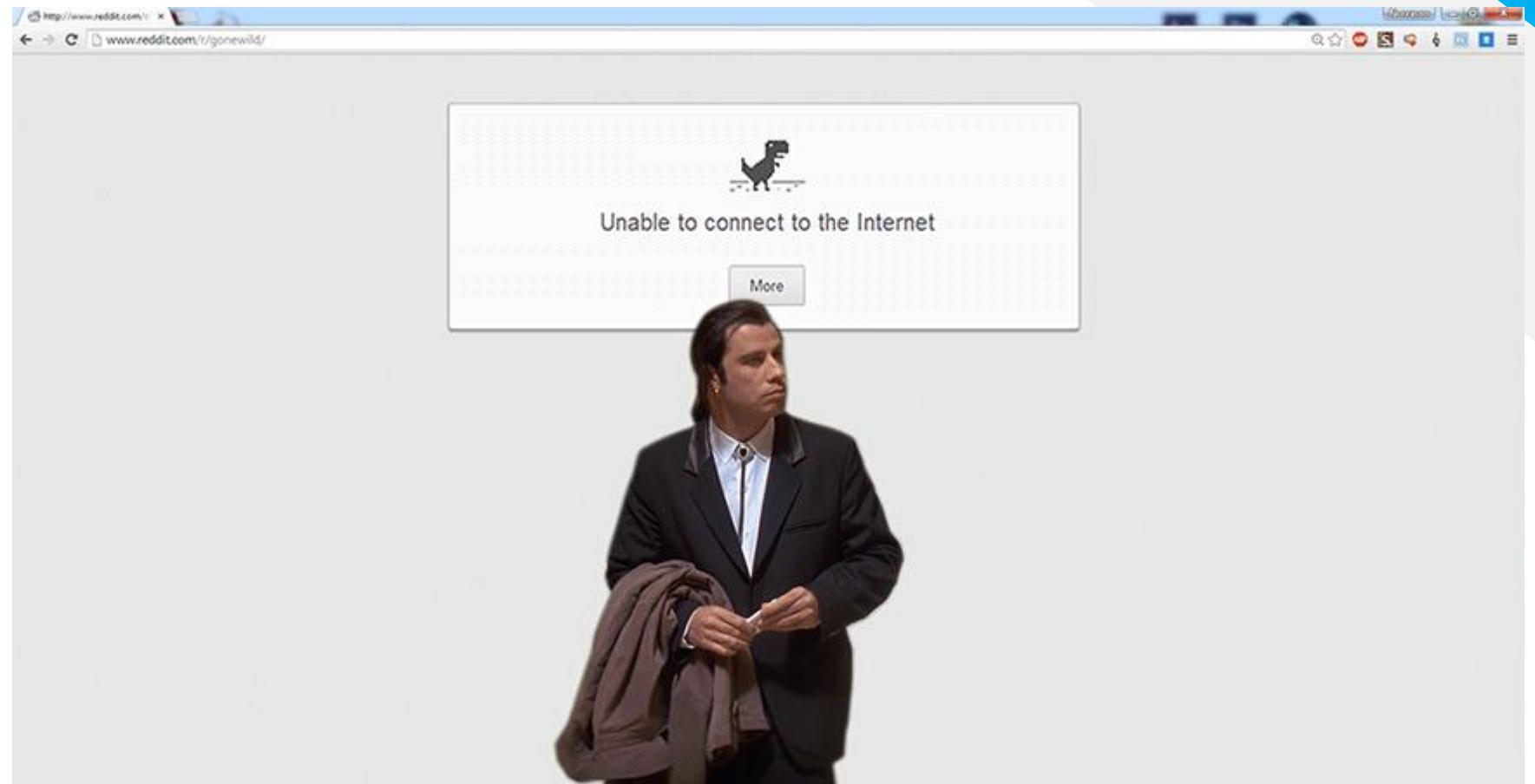
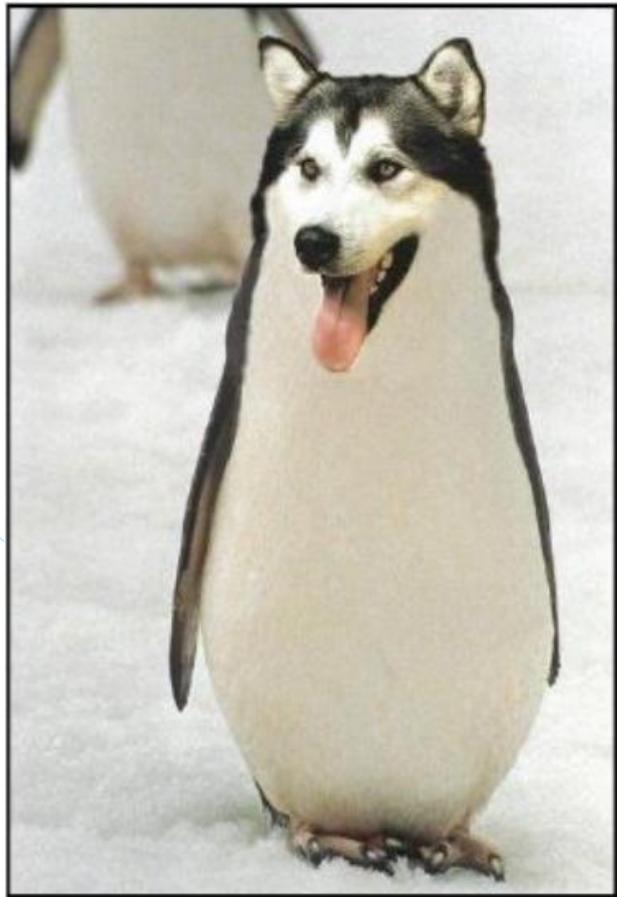
Aguardo,

Att,
Guilherme

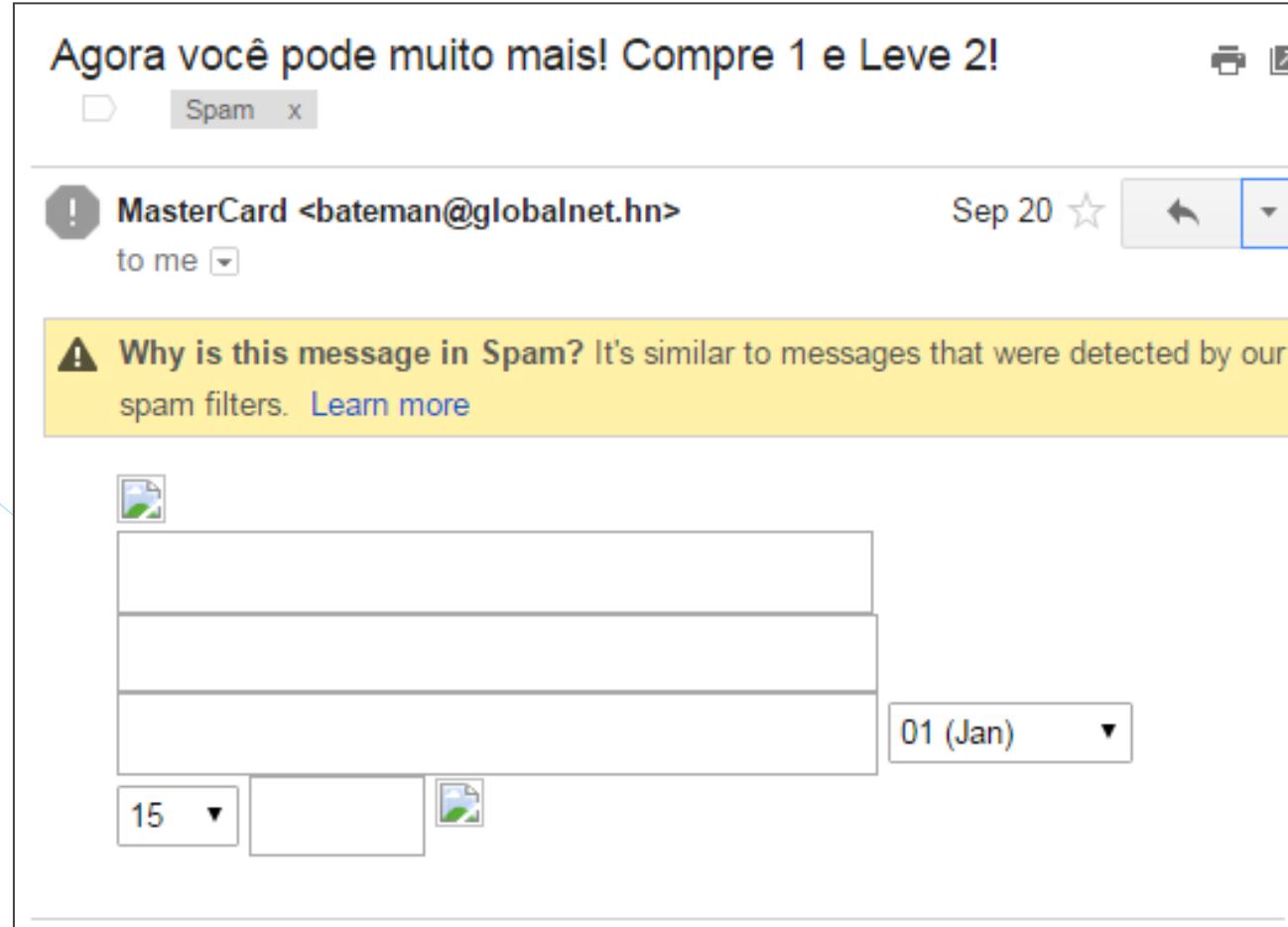
- E-mail recebido!
- Fraude entregue com “sucesso” em ambiente Microsoft.



Fraude?



Em caso de dúvidas, como acionar a TI?



- Clique em “Mais Opções” e “Exibir fonte da mensagem” ou “Mostrar original”.
- Observe no slide a seguir as informações que podem ser obtidas através do cabeçalho da mensagem.



🛡️ | 🔒 <https://mail.google.com/mail/u/0/?ik=00c0d5a6e9&view=om&permmsgid=msg-f%3A1669642478508669808>

Mensagem original

ID da mensagem <p4Dqq.p4Dqq@pdr8-services-05v.prod.jT9IWwlY.org>

Criado em: → 31 de dezembro de 1969 21:00 (entregue após 1592295149 segundos)

De: "Bluoxyn ." <Free.Trial@p4dqq.us>

Para: [REDACTED].com

Assunto: 14 Day Trial of Bluoxyn - Where do we send your Trial Bottle?

SPF: PASS com o IP 52.29.74.240 [Saiba mais](#)

[Fazer download da mensagem original](#)

Delivered-To: [REDACTED].com
Received: by 2002:a50:769d:0:0:0:0:0 with SMTP id f29csp3446387ecf;
Tue, 16 Jun 2020 01:12:29 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJzy0Fan1MBFmNt0J64AAr6SXTTlQ2q84KiM77Yn4E+giTTsYRqxPJwG1Vs8E6Z/8oQGko7j
X-Received: by 2002:adf:97cb:: with SMTP id t11mr1734391wrb.314.1592295149171;
Tue, 16 Jun 2020 01:12:29 -0700 (PDT)



🛡️ | 🔒 <https://mail.google.com/mail/u/03>

Mensagem original

ID da mensagem

Criado em:

De:

Para:

Assunto:

SPF:

[Fazer download da mensagem original](#)



Delivered-To: [REDACTED]

Received: by 2002:a50:769d:0:0:0:0

Tue, 16 Jun 2020 01:12:29

X-Google-Smtp-Source: ABdhPJzy0Fan

X-Received: by 2002:adf:97cb:: wit

Tue, 16 Jun 2020 01:12:29

0/00 (FDI)



Exemplo de possível fraude (Phishing)

ARC-Authentication-Results: i=1; mx.google.com;
spf=pass (google.com: best guess record for domain of return@compute-1.amazonaws.com
designates 52.29.74.240 as permitted sender) smtp.mailfrom=return@compute-1.amazonaws.com

→ Return-Path: <return@compute-1.amazonaws.com> **Remetentes diferentes em “Return-Path” e em “From”**
Received: from o23.m.reply1.ebay.com (ec2-52-29-74-240.eu-central-1.compute.amazonaws.com.
[52.29.74.240])
by mx.google.com with ESMTP id 8si2079845wmk.7.2020.06.16.01.12.28
for <guilhermedgp@gmail.com>;
Tue, 16 Jun 2020 01:12:29 -0700 (PDT)

→ Received-SPF: pass (google.com: best guess record for domain of return@compute-1.amazonaws.com
designates 52.29.74.240 as permitted sender) client-ip=52.29.74.240;
Authentication-Results: mx.google.com;
spf=pass (google.com: best guess record for domain of return@compute-1.amazonaws.com
designates 52.29.74.240 as permitted sender) smtp.mailfrom=return@compute-1.amazonaws.com
Date: p4Dqq

→ From: "Bluoxyn ." <Free.Trial@p4dqq.us> **Remetentes diferentes em “Return-Path” e em “From”**
To: [REDACTED] mail.com
Message-ID: <p4Dqq.p4Dqq@pdr8-services-05v.prod.jT9lWw1Y.org>
Subject: 14 Day Trial of Bluoxyn - Where do we send your Trial Bottle?
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="00000000p4Dqq.1NndRSZ@gmail.comp4Dqq.1NndRSZ4v4qJ7svv";
report-type=delivery-status



Exemplo de mensagem válida



Return-Path: <bruno. O mesmo remetente em “Return-Path” e em “From”

```
Received: from NAM11-C01-obe.outbound.protection.outlook.com (mail-co1nam11on2051.outbound.protection.outlook.com. [40.107.220.51])
  by mx.google.com with ESMTPS id q11si8921535pgg.575.2020.05.04.09.39.12
  for <guilherme@dgpti.com.br>
  (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
  Mon, 04 May 2020 09:39:13 -0700 (PDT)
Received-SPF: pass (google.com: domain of bruno.paim@loyola.g12.br designates 40.107.220.51 as permitted sender) client-ip=40.107.220.51;
Authentication-Results: mx.google.com;
  dkim=pass header.i=@loyolaacojeorg.onmicrosoft.com header.s=selector2-loyolaacojeorg-onmicrosoft-com header.b=jwUDUzYn;
  arc=pass (i=1 spf=pass spfdomain=loyola.g12.br dkim=pass dkdomain=loyola.g12.br dmarc=pass fromdomain=loyola.g12.br);
  spf=pass (google.com: domain of bruno.paim@loyola.g12.br designates 40.107.220.51 as permitted sender)
  smtp.mailfrom=bruno.paim@loyola.g12.br
```



O mesmo remetente em “Return-Path” e em “From”

```
Received: from DM6PR02MB4843.namprd02.prod.outlook.com ([fe80::58f0:ff52:d9c5:96cd]) by DM6PR02MB4843.namprd02.prod.outlook.com
  ([fe80::58f0:ff52:d9c5:96cd%4]) with mapi id 15.20.2958.030; Mon, 4 May 2020 16:39:12 +0000
From: "Bruno de Alcântara e Silva Paim" <bruno
To: Guilherme Rodrigues Pereira <guilherme@dgpti.com.br>
CC: Silvia de Almeida Del Penho Silva <silvia.penho@loyola.g12.br>, Marcos Amaral <marcos.amaral@loyola.g12.br>
Subject: RE: Documentação para criação de contas no Microsoft Teams via Power Shell
```



Phishing: Medidas de prevenção

- Segundo documentação da McAfee¹ e SonicWall², observe os seguintes itens ao receber uma mensagem suspeita:
 - Geralmente, uma mensagem de PHISHING é enviada a várias pessoas simultaneamente. Portanto, o destinatário será referenciado de forma genérica (na maioria dos casos).
 - Passe o mouse sobre os links da mensagem e verifique o endereço final.
 - Verifique se o endereço de e-mail do remetente realmente pertence ao suposto domínio de origem.
 - Devido o grande número de fraudes, grandes organizações não solicitam a confirmação de dados ou pagamentos por e-mail.
 - Observe e analise antes de clicar em links recebidos (mesmo que sejam de remetentes confiáveis).
 - Evite clicar em conteúdos (imagens) recebidos por e-mail.
 - Evite o download automático de conteúdos em aplicativos.
 - Arquivos do Office podem conter macros maliciosas.

Fonte 1: https://service.mcafee.com/webcenter/portal/cp/home/articleview?locale=pt-BR&articleId=TS101810&_afrLoop=1274006494439258
Fonte 2: <https://www.sonicwall.com/en-us/phishing-iq-test>



Phishing: Medidas de prevenção

- Vamos praticar???

The screenshot shows a web browser with the URL <https://www.sonicwall.com/en-us/phishing-iq-test>. The page features the SonicWall logo at the top. Below it, a large blue section contains the text: "Over 90% of cyberattacks start with a phishing email. Can you tell the difference between a legitimate and phishing email? Take the test to find out your phishing IQ." At the bottom of this section is a large orange button with the text "TAKE THE PHISHING IQ TEST".

Fonte: <https://www.sonicwall.com/phishing-iq-test/>

Fonte: <https://www.kaspersky.com.br/blog/cyber-savvy-quiz/>

The screenshot shows a web browser with the URL <https://kaspersky.com.br/blog/cyber-savvy-quiz/>. The page has a navigation bar with links: Produtos, Renovar, Downloads, Suporte, Centro de recursos, Blog (which is underlined), and Secure Futures. The main content area features the heading "Você é ciberesperto?". Below this, there is a section with the Kaspersky Lab logo and the text: "A Internet, assim como o mundo, pode ser segura ou perigosa, dependendo dos seus hábitos. Você está seguro nas ruas se usa a faixa de pedestres e obedece à sinalização, mas não é recomendável andar sozinho à noite com o bolso cheio da grana. A vida na Internet tem algumas regras igualmente óbvias, mas nem todo mundo está por dentro delas. Neste teste, você vai saber qual seu grau de exposição na sua vida online e qual a chance de perder dados valiosos e até dinheiro usando a Internet do jeito que normalmente usa." At the bottom of this section is the text "Passo 1 de 5".



Obrigado!

-  Guilherme Rodrigues
-  guilherme@dgpti.com.br
-  www.dgpti.com.br