Navegação Segura: Recomendações em Segurança da Informação

Colégio Loyola
Agosto/2020

COLÉGIO LOYOLA
Rede Jesuíta de Educação

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.

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;

COLÉGIO LOYOLA
Rede Jesuíta de Educação

Segurança em Camadas:
Layered Security & Defense in Depth

- Quando estamos em um ambiente coorporativo, **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?

COLÉGIO LOYOLA
Rede Jesuíta de Educação

Conceitos introdutórios: Segurança da informação

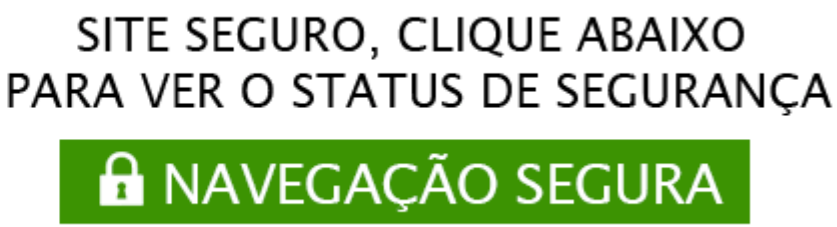
- A segurança da informação é **proporcionada** por três fatores (pilares):

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).

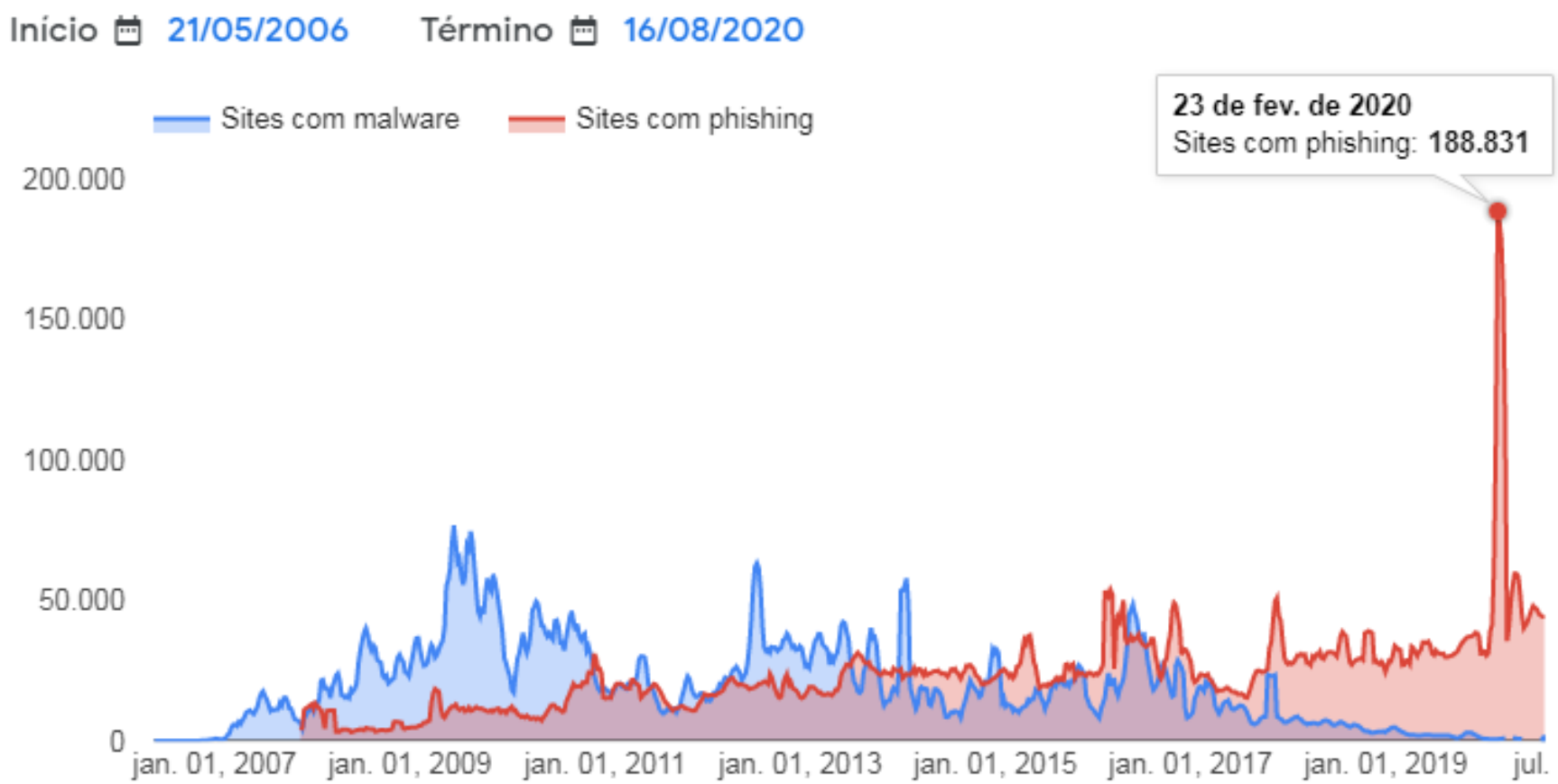
Dados sobre Navegação Segura

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



Dados sobre Navegação Segura

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



Relatório de sites inseguros identificados por semana.
Fonte: Google Transparency Report
Disponível em: https://transparencyreport.google.com/safe-browsing/overview?hl=pt_BR

Dados sobre Navegação Segura

- O que isso quer dizer?

Safe Browsing
Google

Relatório de sites inseguros identificados por semana.
Fonte: Google Transparency Report
Disponível em: https://transparencyreport.google.com/safe-browsing/overview?hl=pt_BR

COLÉGIO LOYOLA
Rede Jesuíta de Educação

Dados sobre Navegação Segura

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

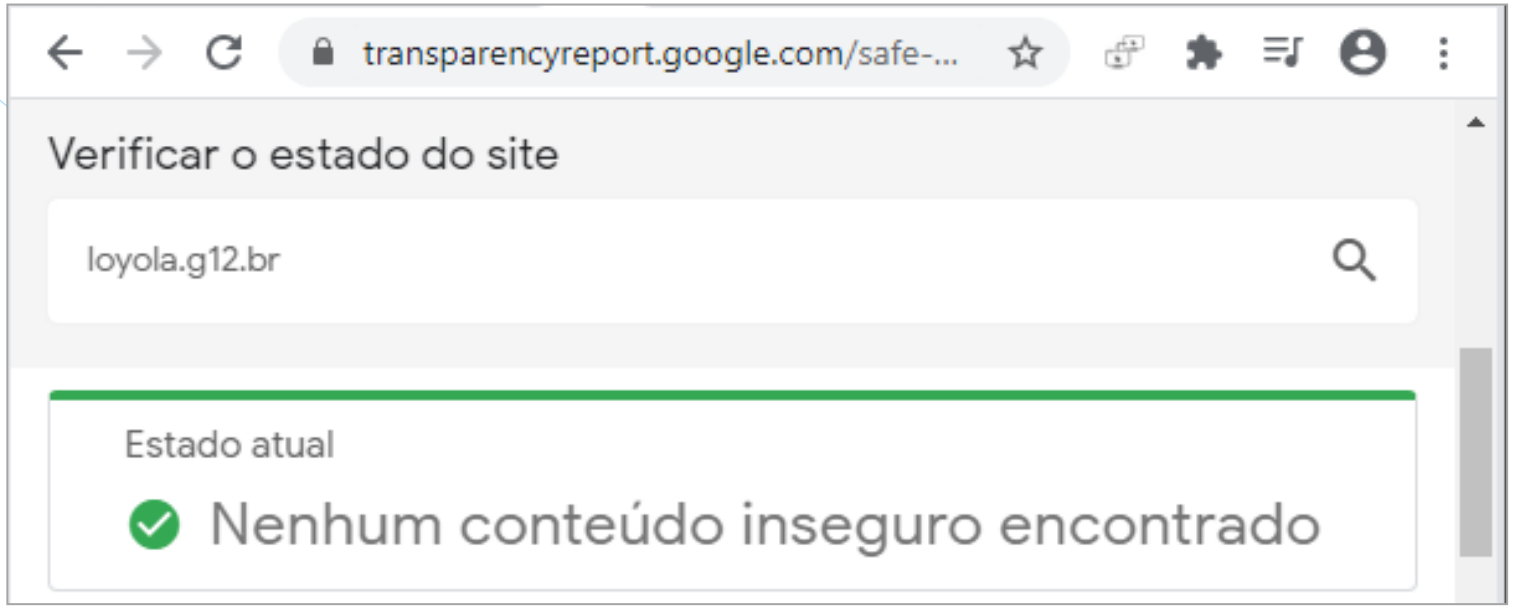
Relatório de sites inseguros identificados por semana. Fonte: Google Transparency Report
Disponível em: https://transparencyreport.google.com/safe-browsing/overview?hl=pt_BR

COLÉGIO LOYOLA
Rede Jesuíta de Educação

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).

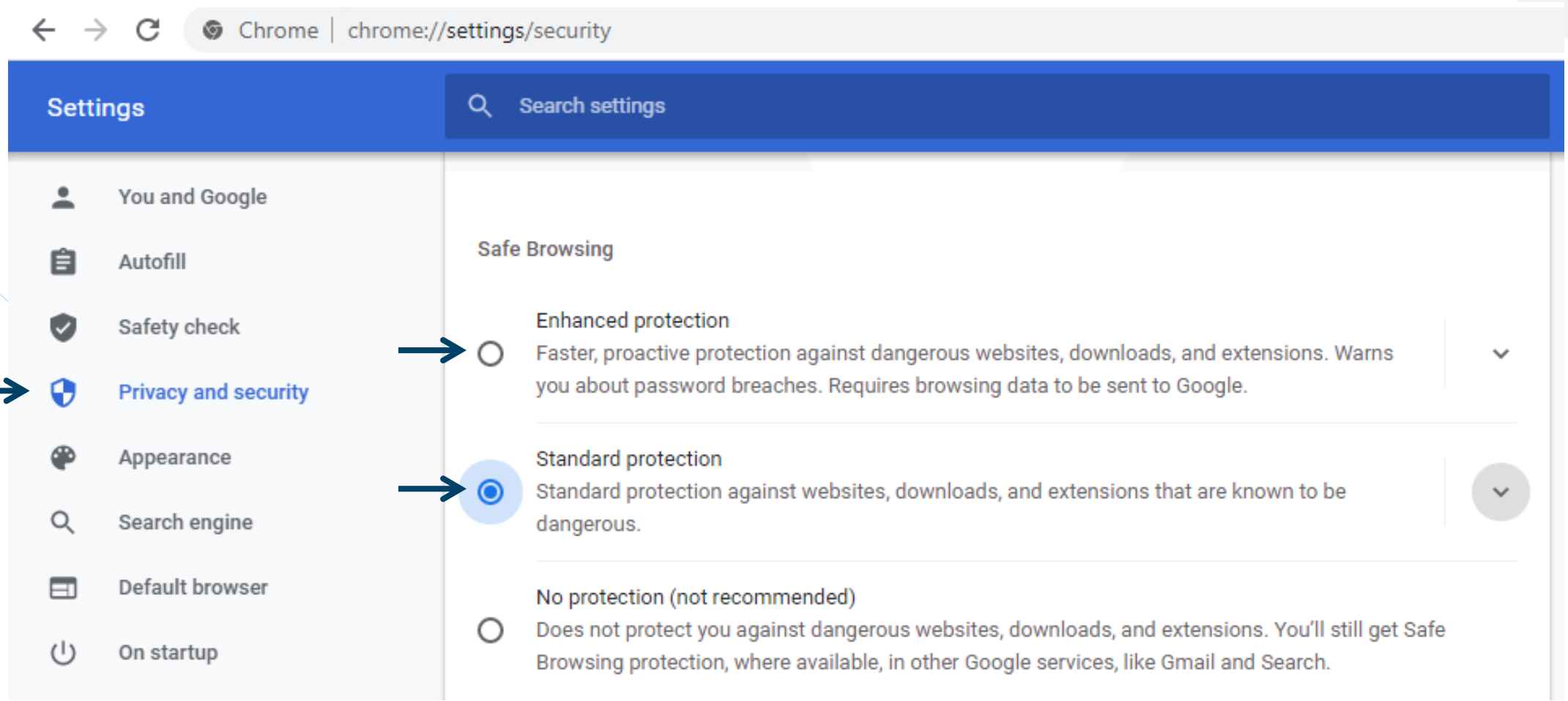
- Em caso de dúvidas, consulte a reputação do site antes de acessá-lo:



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

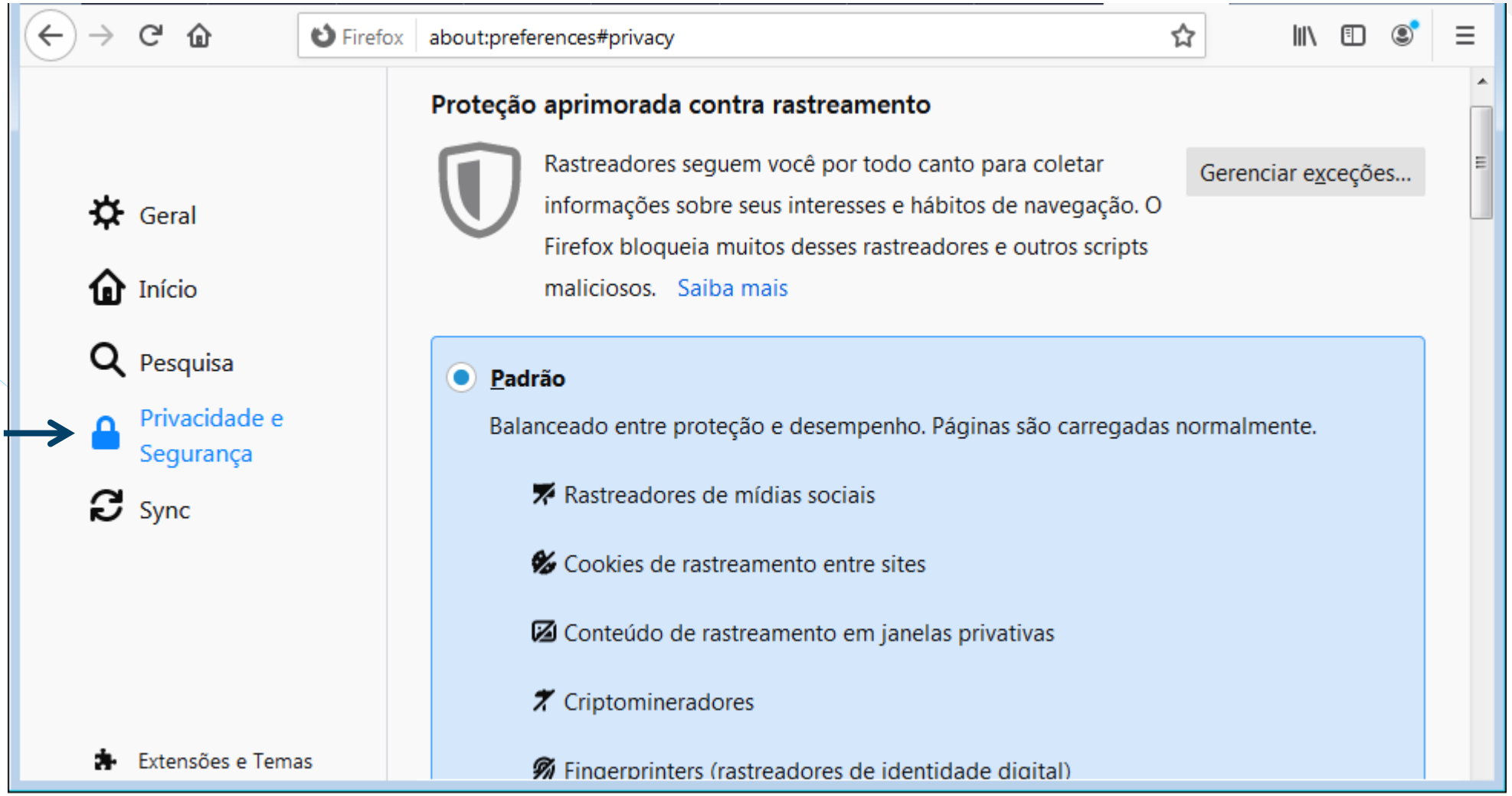
COLÉGIO LOYOLA
Rede Jesuíta de Educação

Configurações do Chrome



COLÉGIO LOYOLA
Rede Jesuíta de Educação

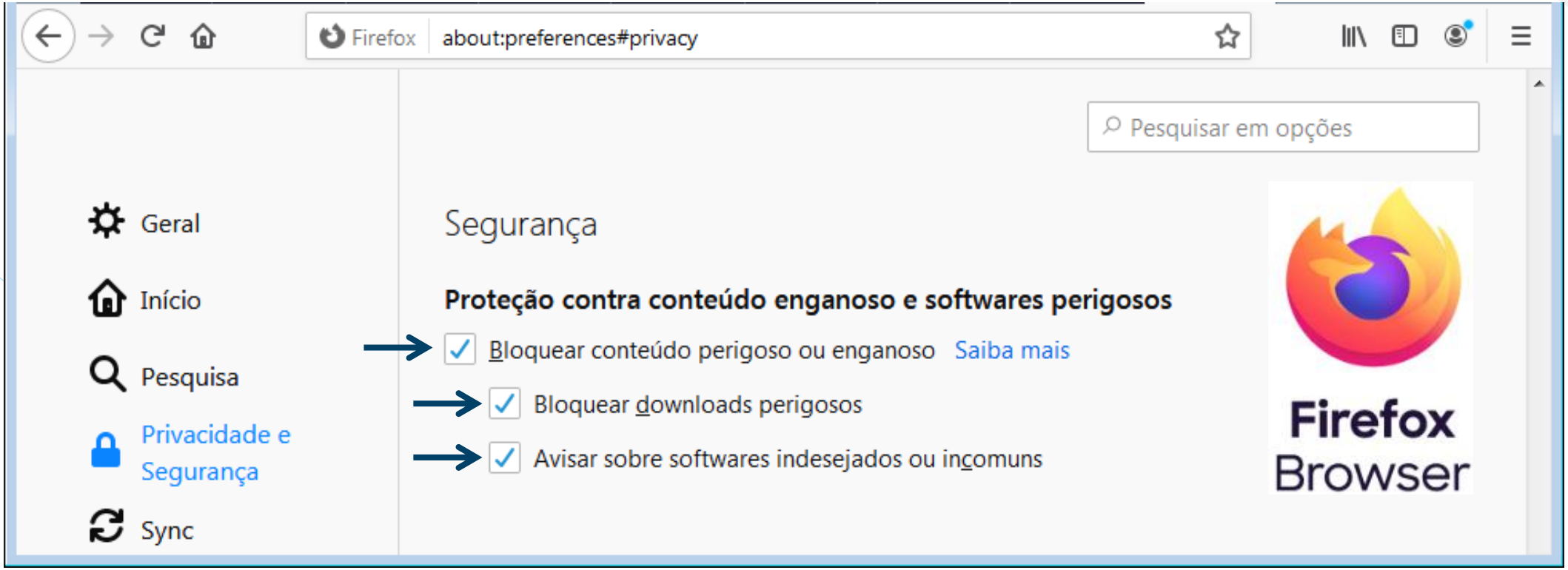
Configurações do Firefox



Firefox Browser

COLÉGIO LOYOLA
Rede Jesuíta de Educação

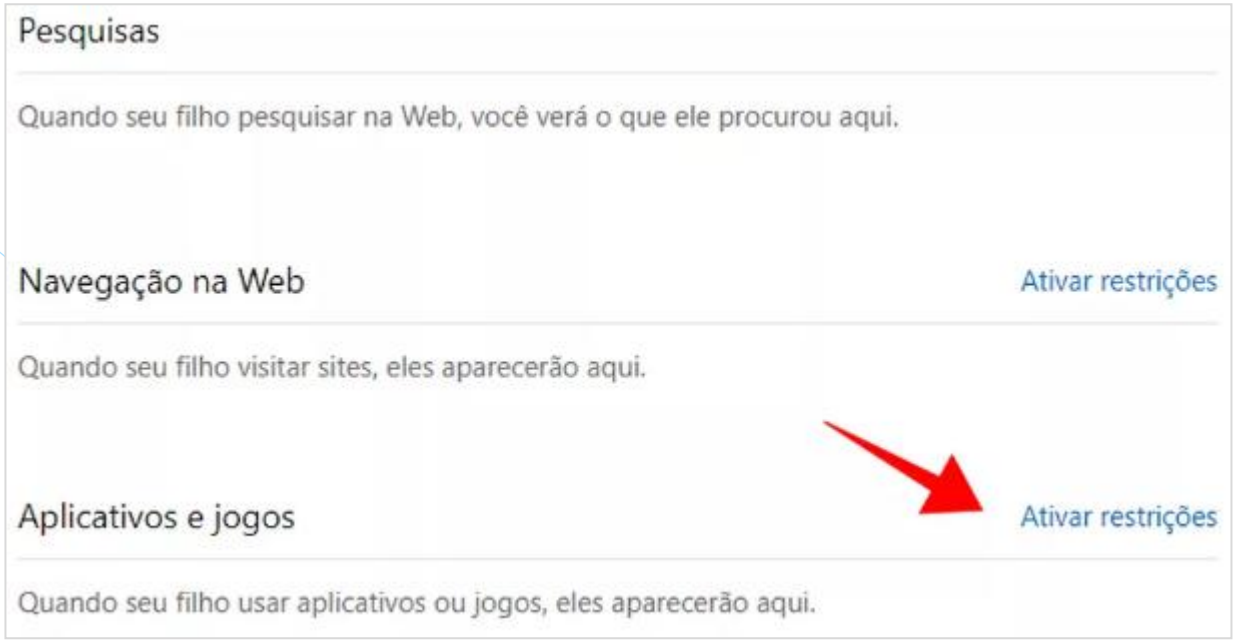
Configurações do Firefox

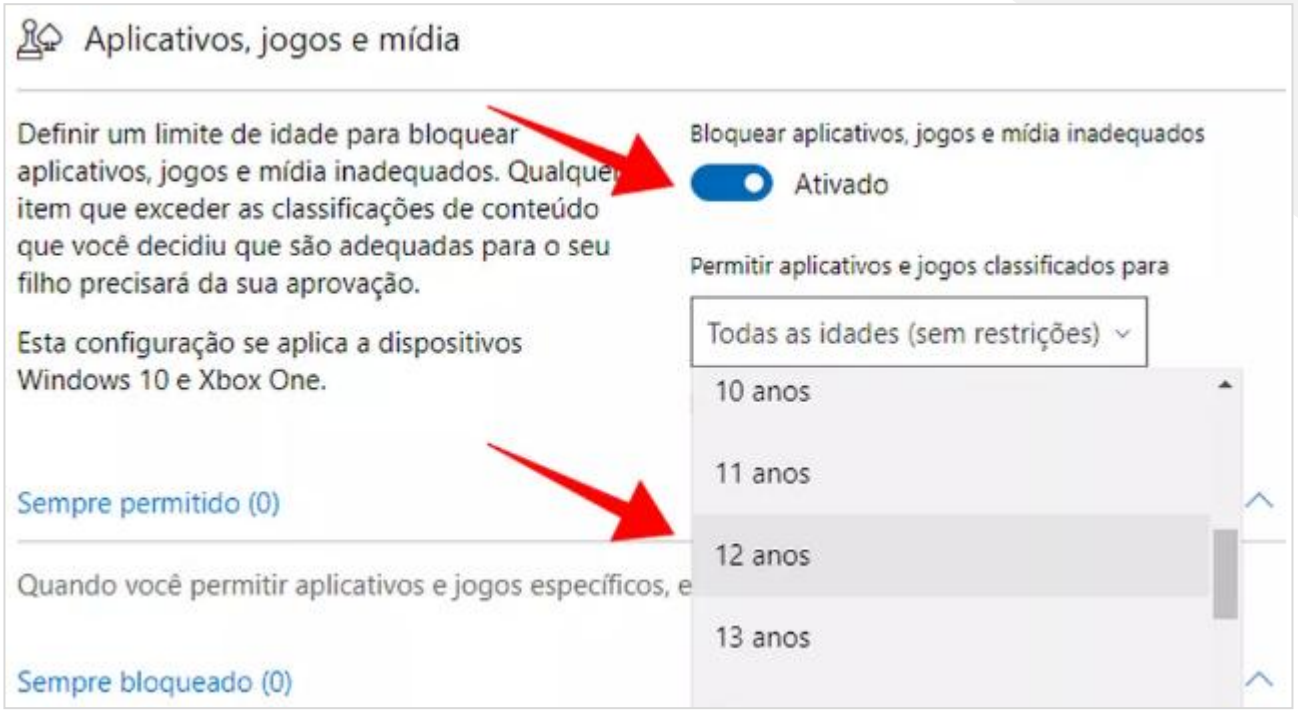


COLÉGIO LOYOLA
Rede Jesuíta de Educação

Outras medidas preventivas: Controle Parental

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



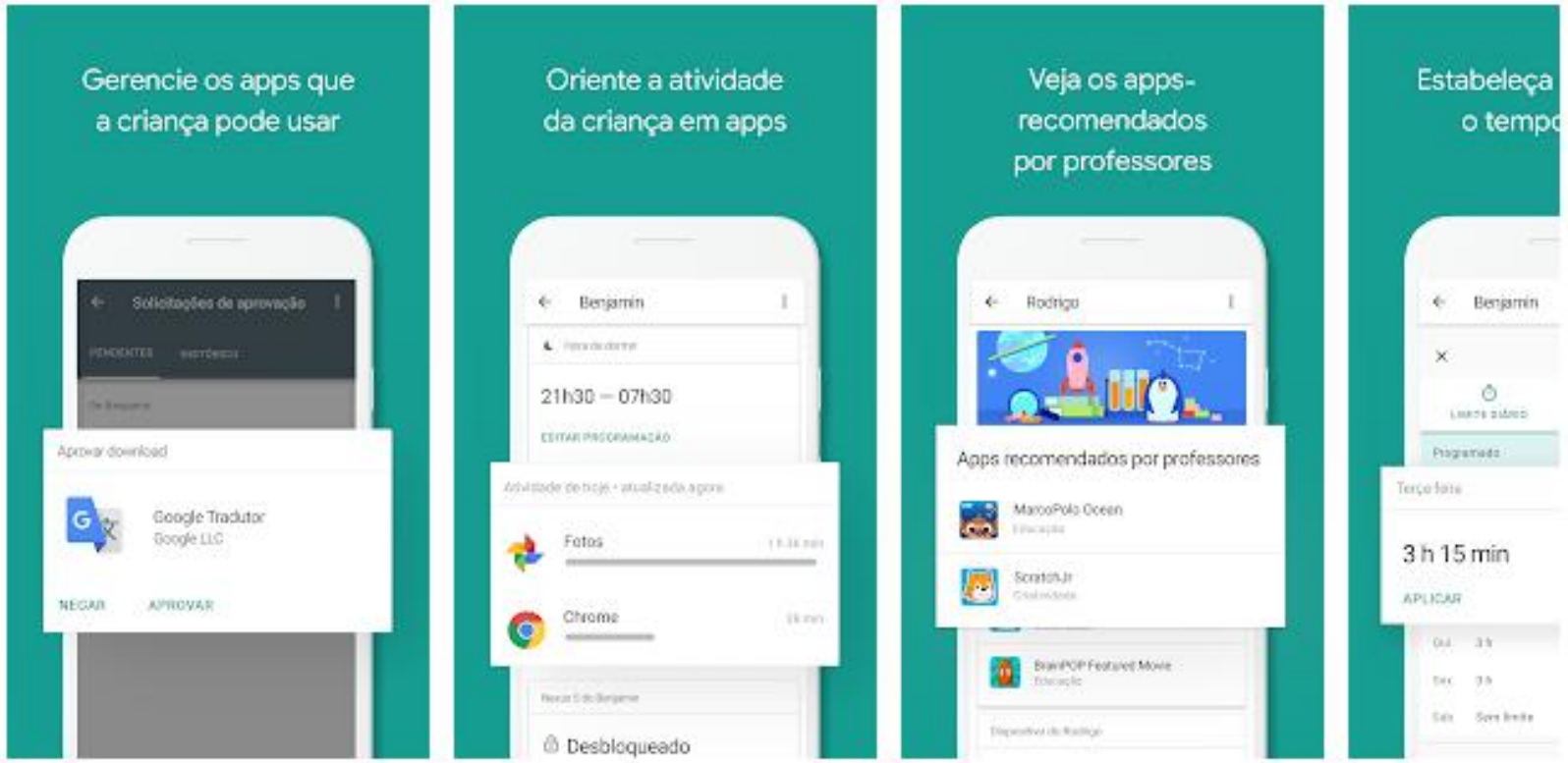


Fonte: TechTudo (Paulo Alves).
Disponível em: https://www.techtudo.com.br/dicas-e-tutoriais/2018/03/como-controlar-o-que-as-criancas-acessam-no-pc-com-windows-10.ghtml

COLÉGIO LOYOLA
Rede Jesuíta de Educação

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

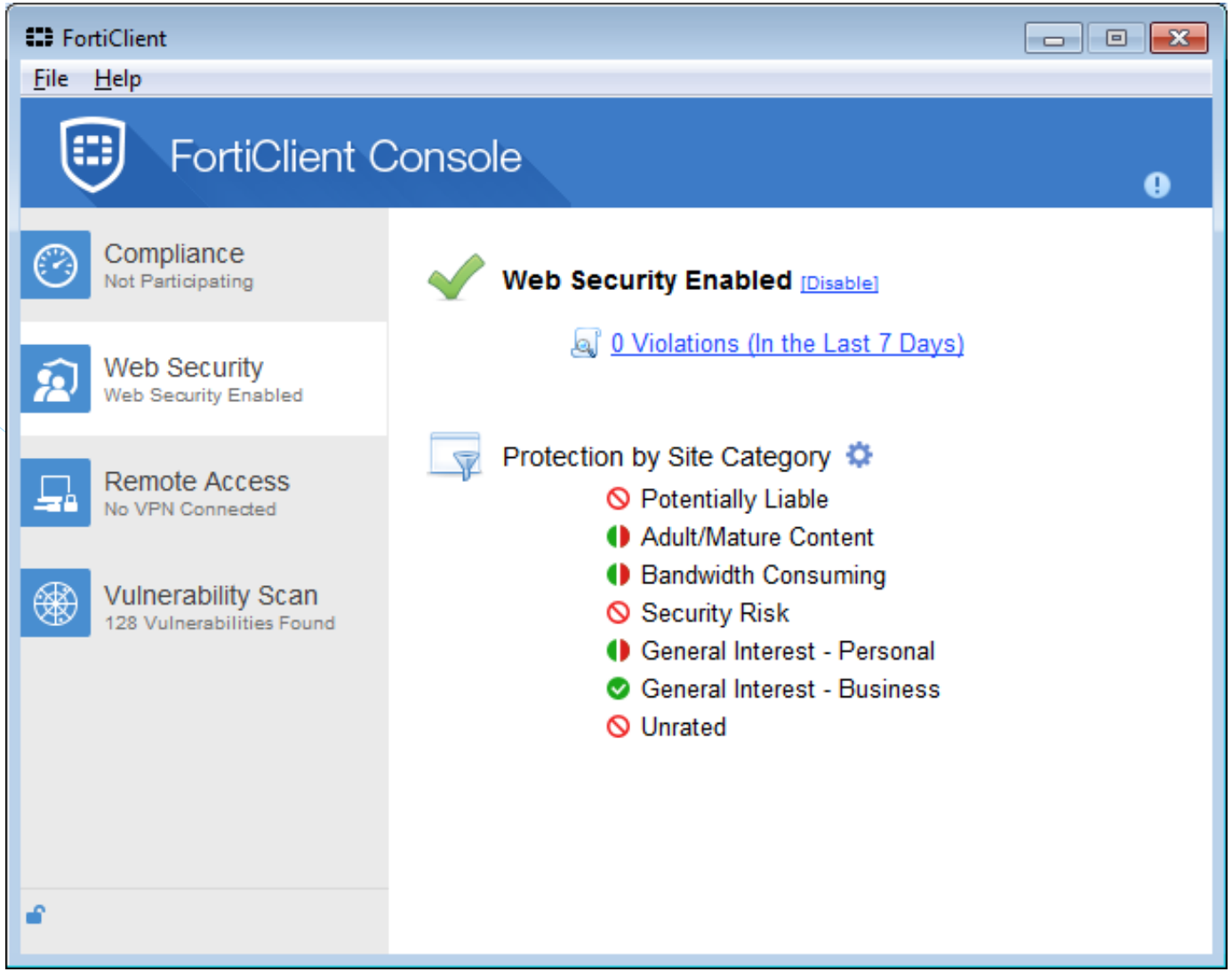
COLÉGIO LOYOLA
Rede Jesuíta de Educação

Outras medidas preventivas:
Web Filter no AntiVirus

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

COLÉGIO LOYOLA
Rede Jesuíta de Educação

Outras medidas preventivas: Web Filter no AntiVirus



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

COLÉGIO LOYOLA
Rede Jesuíta de Educação

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/

CLOUDFLARE

COLÉGIO LOYOLA
Rede Jesuíta de Educação

DGP

Tecnologia da Informação

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...”*

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

COLÉGIO LOYOLA
Rede Jesuíta de Educação

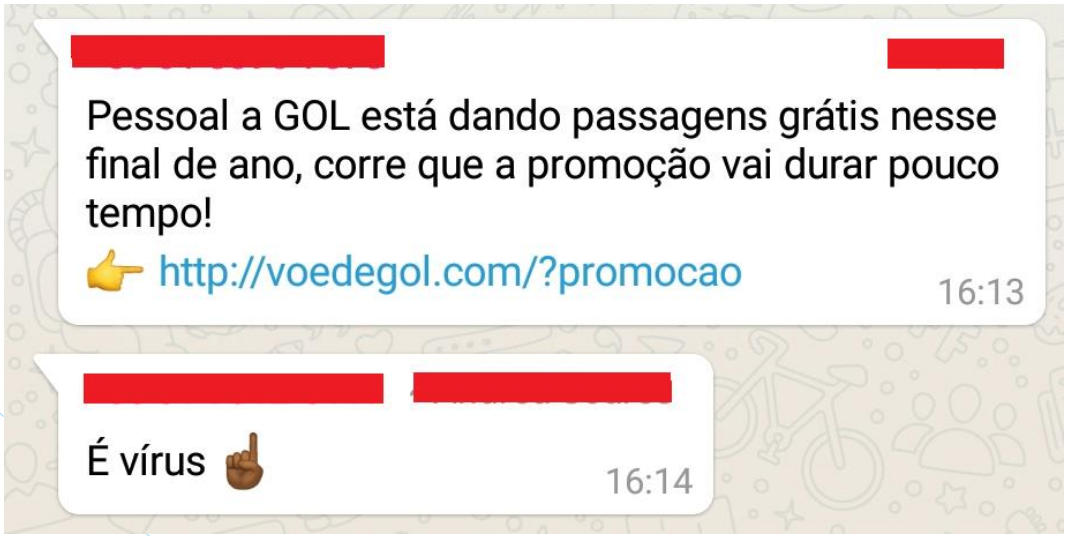
Tipos de Phishing

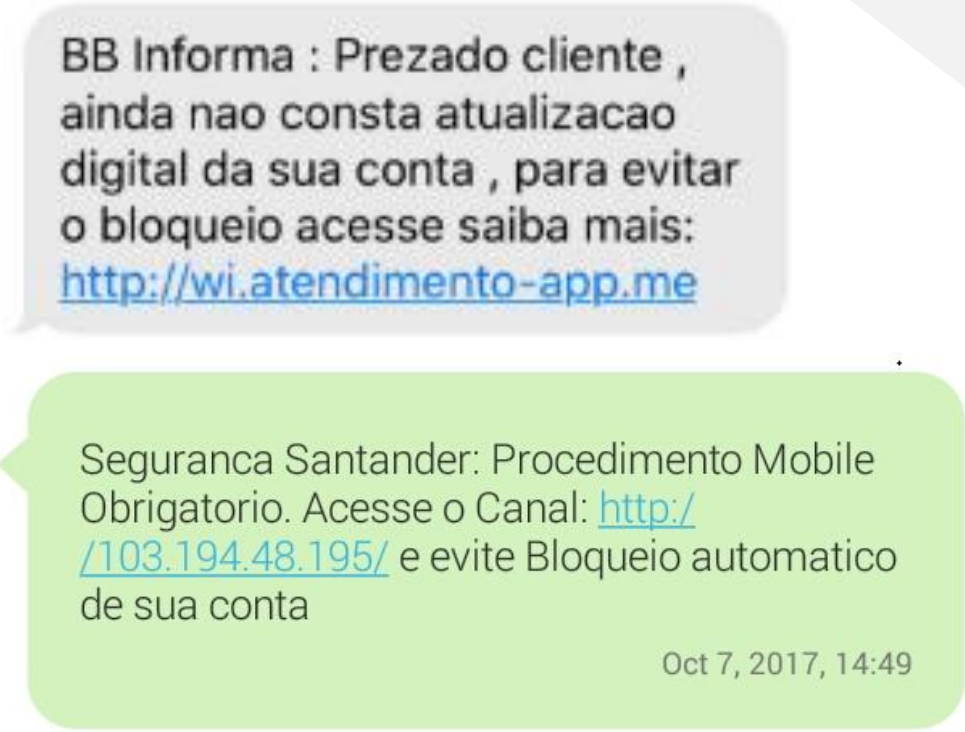
- Dentre os principais tipos de ataques de Phishing, temos:
  - **E-mail Phishing:** o atacante utiliza domínios falsos, ou usam o nome da empresa no campo do usuário, bem como outros “truques” como as letras “r” e “n” juntas (“rn” ao invés de “m”).
  - **Spear Phishing:** Mais sofisticado e direcionado 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.

Fonte: https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack

Alguns exemplos de Phishing

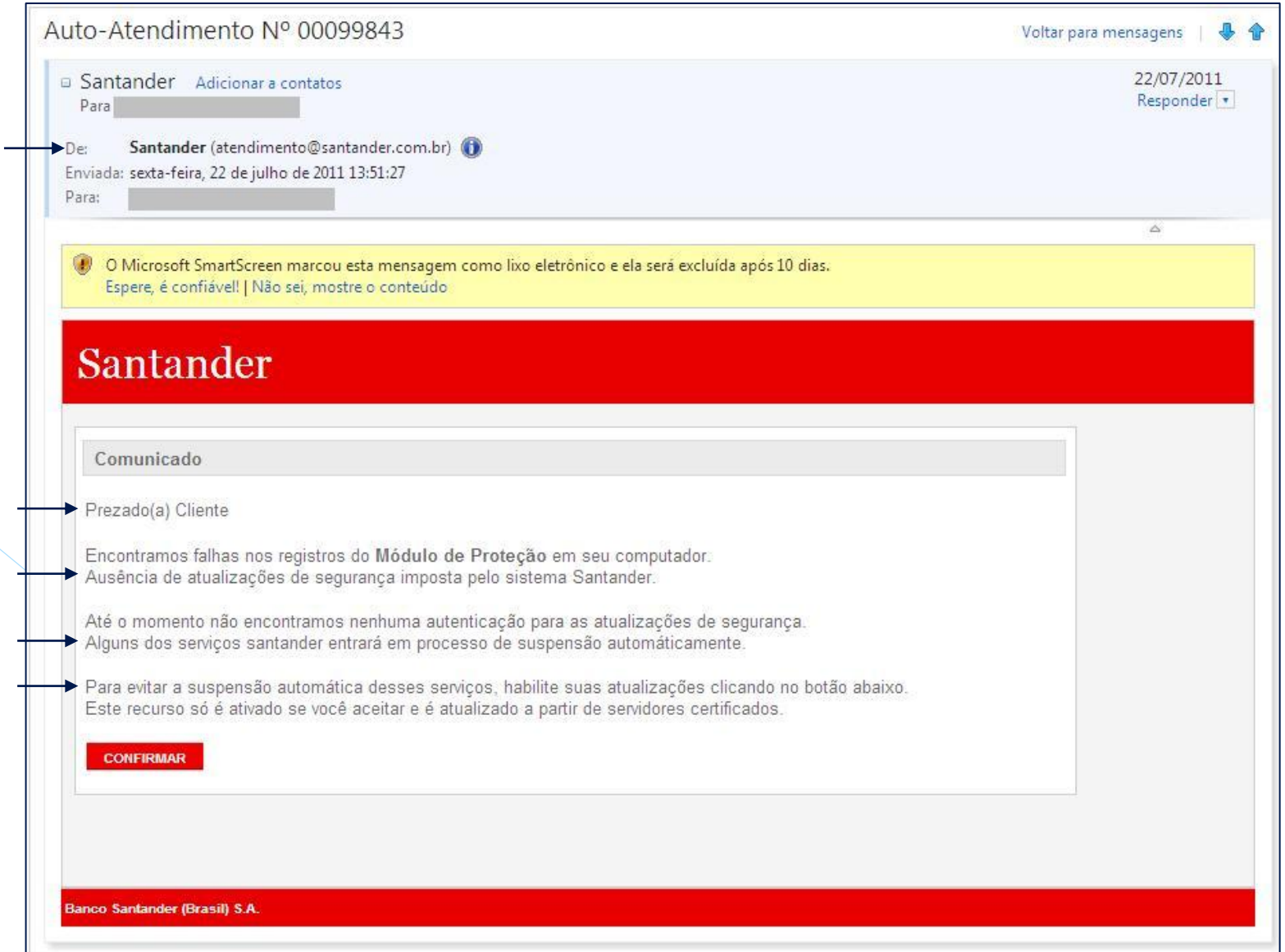
- Tipo: Smishing and Vishing.





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

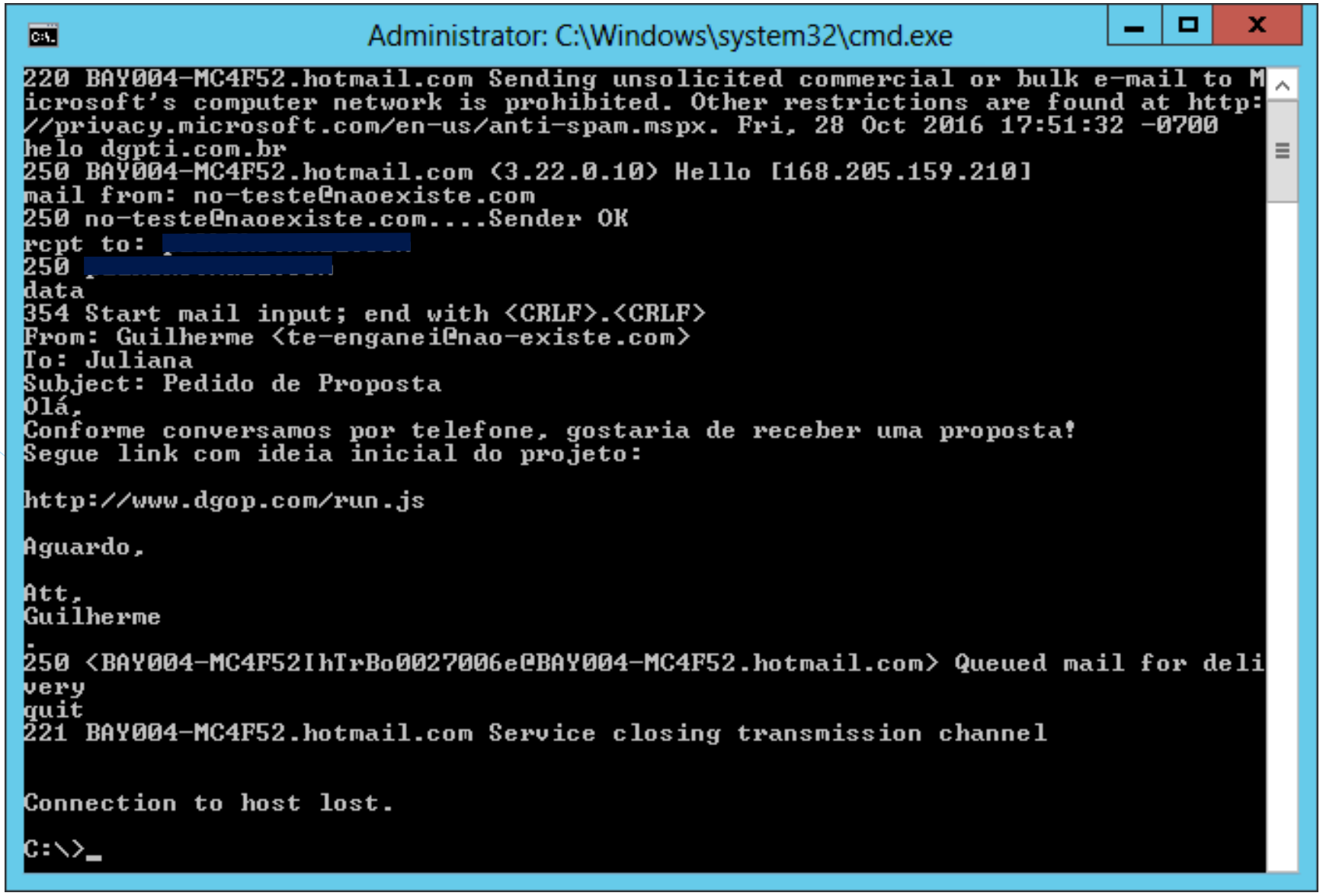
Alguns exemplos de Phishing



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

COLÉGIO LOYOLA
Rede Jesuíta de Educação

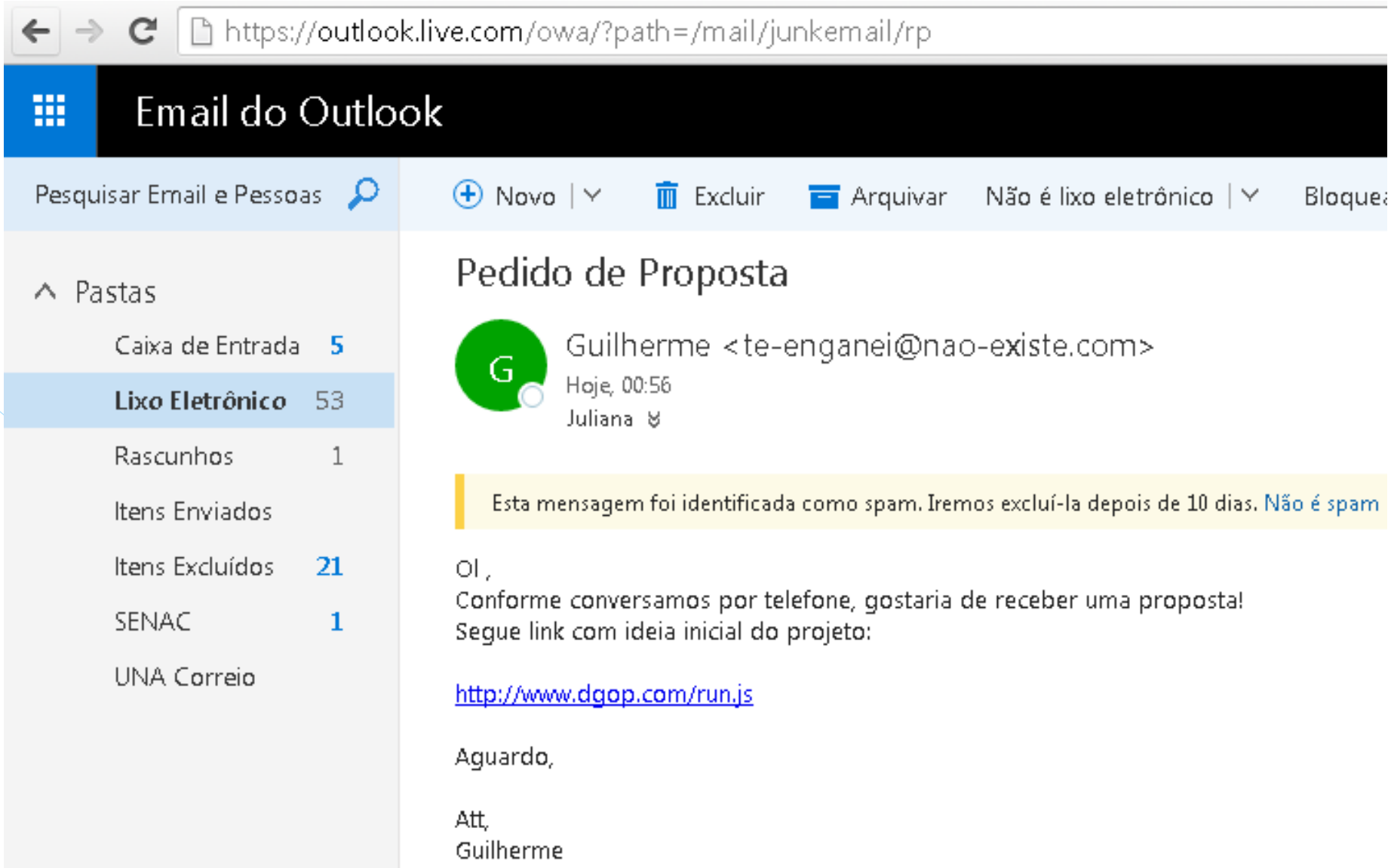
Phishing: Lançando a isca!



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

COLÉGIO LOYOLA
Rede Jesuíta de Educação

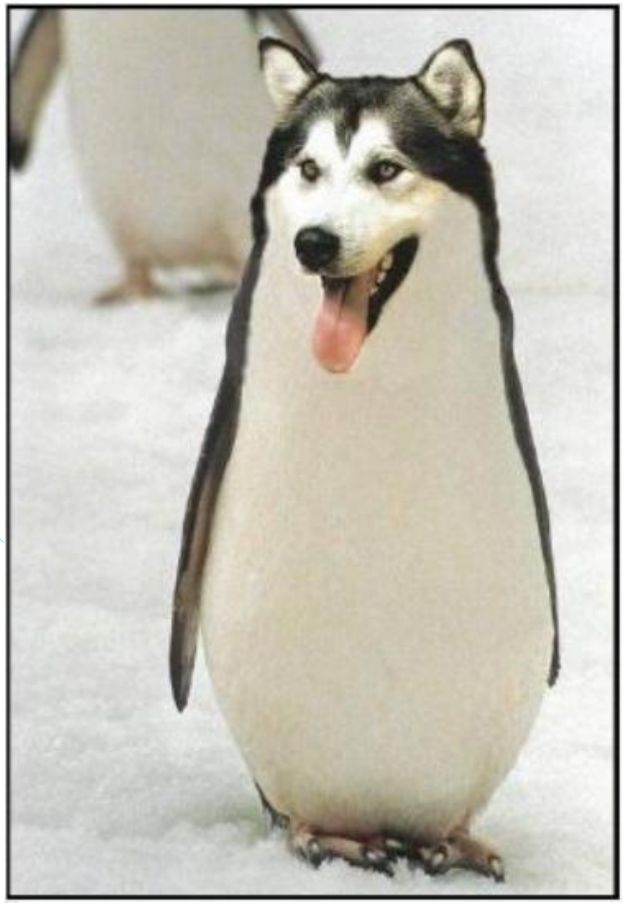
Phishing: Lançando a isca!

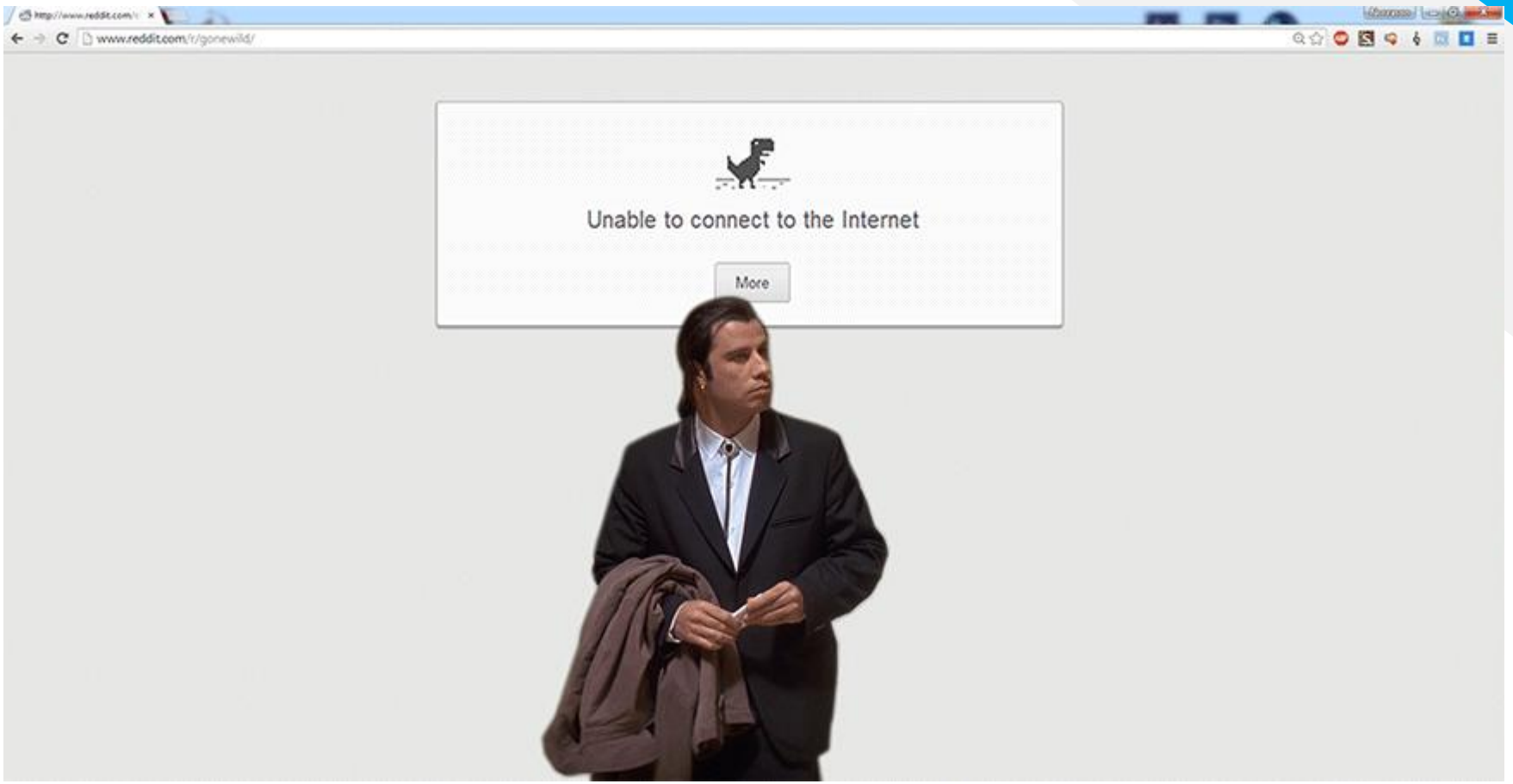


- E-mail recebido!
- Fraude entregue com “sucesso” em ambiente Microsoft.

COLÉGIO LOYOLA
Rede Jesuíta de Educação

Fraude?




www.reddit.com/r/gonewild/
Unable to connect to the Internet
More

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.

COLÉGIO LOYOLA
Rede Jesuíta de Educação

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.jT9lWwlY.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]om
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/0

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 -0700 (PDT)
```

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>
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>
To: [redacted]mail.com
Message-ID: <p4Dqq.p4Dqq@pdr8-services-05v.prod.jT9lWwlY.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
```

Remetentes diferentes em “Return-Path” e em “From”

Remetentes diferentes em “Return-Path” e em “From”

Exemplo de mensagem válida

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

```
Return-Path: <bruno.
Received: from NAM11-CO1-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


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@dgp
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
```

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

COLÉGIO LOYOLA

Rede Jesuíta de Educação

Phishing: Medidas de prevenção

- Segundo documentação da McAfee[1] e SonicWall[2], 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???

Fonte: https://www.sonicwall.com/phishing-iq-test/
Fonte: https://www.kaspersky.com.br/blog/cyber-savvy-quiz/

DGP

Tecnologia da Informação

Obrigado!

Guilherme Rodrigues

guilherme@dgpti.com.br

www.dgpti.com.br