nic.br cgi.br | cert.br

Semana de Segurança na CAIXA 2020
23 a 27 de novembro de 2020
Evento *On-line*

cert.br

TLP:WHITE

Tratamento de Incidentes	Treinamento e Conscientização	Análise de Tendências
▶ Articulação	▶ Cursos	▶ *Honeypots* Distribuídos
▶ Análise Técnica	▶ Palestras	▶ SpamPots
▶ Apoio à recuperação	▶ Boas Práticas	▶ Processamento de *threat feeds*
	▶ Reuniões	

Filiações e Parcerias:

FIRST Improving Security Together MEMBER

ACCREDITED BY TI TRUSTED INTRODUCER

APWG RESEARCH PARTNER www.antiphishing.org

CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE

SEI Partner Network

HN/P

Criação:

Agosto/1996: o relatório "Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil" é publicado pelo CGI.br[1]

Junho/1997: o CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório[2]

[1]https://www.nic.br/grupo/historico-gts.htm | [2]https://www.nic.br/pagina/gts/157

Missão

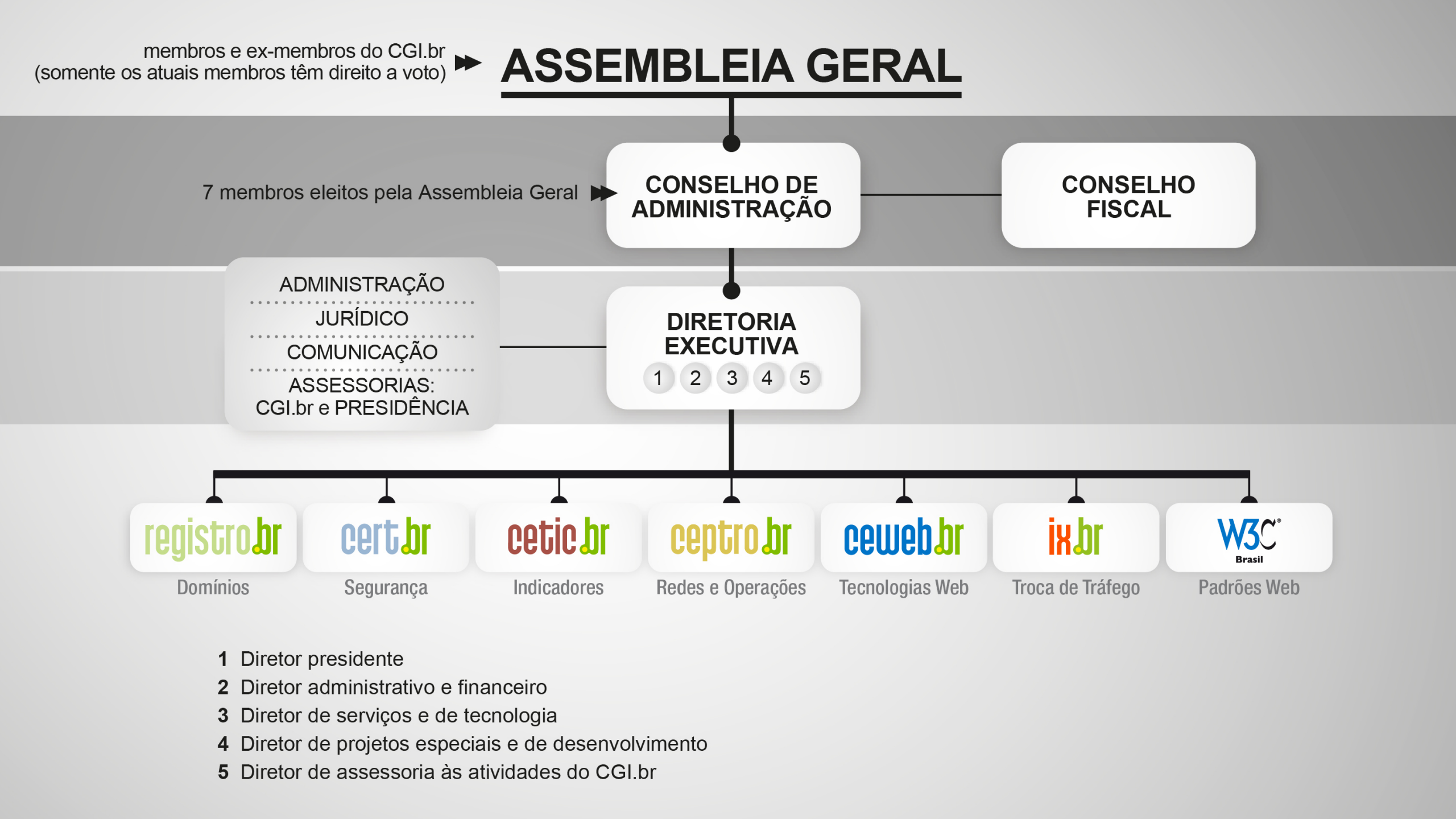
Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Público Alvo (*Constituency*)

Redes que utilizam recursos alocados pelo NIC.br (endereços IP ou ASNs alocados ao Brasil e domínios sob o ccTLD .br).

Foco das Atividades

- Ponto de contato nacional
- Trabalho colaborativo com outras entidades
- Auxiliar na análise técnica e compreensão de ataques e ameaças
- Aumentar a detecção, correlação de eventos e determinação de tendências
- Transferir o conhecimento através de cursos, boas práticas e conscientização



1 Diretor presidente
2 Diretor administrativo e financeiro
3 Diretor de serviços e de tecnologia
4 Diretor de projetos especiais e de desenvolvimento
5 Diretor de assessoria às atividades do CGI.br

Internet Segura : Dicas de uso seguro da Internet

Lucimara Desiderá, M.Sc
Analista de Segurança
lucimara@cert.br

cert.br nic.br cgi.br

Segurança na Internet

Internet é parte integrante do nosso cotidiano:

- Alguns usos:
  - comércio eletrônico
  - *Internet Banking*
  - redes sociais
  - estudo a distância
  - governo eletrônico
  - tele trabalho
- Aproveitar esses benefícios de forma segura requer que alguns cuidados
  - conhecer os riscos
  - adotar medidas preventivas

Não existe segurança 100%

- invasão de contas
- indisponibilidade de serviços
- perda de privacidade
- furto de dados
- perdas financeiras
- danos à imagem
- perda de confiança na tecnologia

Sistemas na Internet

Riscos

Atacantes

- criminosos
- espionagem industrial
- governos
- vândalos

Vulnerabilidades

- projeto sem levar em conta segurança
- defeitos de *software*
- falhas de configuração
- uso inadequado
- fraquezas advindas da complexidade dos sistemas

Conheça os riscos

cert.br nic.br cgi.br

Golpes na Internet

- Golpistas utilizam-se de engenharia social:
  - procuram enganar e persuadir as potenciais vítimas a:
    - fornecerem informações sensíveis
    - realizarem ações, como executar *malware* e acessar páginas falsas
- Alguns dos principais golpes aplicados na Internet:
  - Furto de identidade
  - Fraude de antecipação de recursos
  - *Phishing scam*
    - via mensagens eletrônicas
      - Páginas falsas
      - Mensagens contendo formulários
      - links para códigos maliciosos
- Vários dos golpes aplicados na Internet podem ser considerados crimes contra o patrimônio, tipificados como estelionato
  - golpista ➔ estelionatário

Ataques na Internet – tipos

- Exploração de vulnerabilidades
- Varredura em redes (*scan*)
- Falsificação de e-mail (*e-mail spoofing*)
- Interceptação de tráfego (*sniffing*)
- Força bruta (*brute force*)
- Negação de serviço (DoS e DDoS)
- Desfiguração de página (*defacement*)
  - *sites* de grandes instituições
  - hospedagem de *malware*

Qualquer serviço, computador ou rede acessível via Internet pode:

- ser alvo de um ataque
- participar de um ataque

Códigos maliciosos (*Malware*)

- Programas desenvolvidos para executar ações danosas e atividades maliciosas
  - infectam computadores, dispositivos móveis, *IoT*
- Uma vez instalados:
  - Acessam dados armazenados no dispositivo
    - ou bloqueiam o acesso a eles
  - podem executar ações em nome dos usuários
- São usados como intermediários, possibilitam:
  - prática de golpes, realização de ataques, disseminação de spam, furto de dados
- Vírus, *worm*, bot, *spyware*, *backdoor*, *trojan*, *rootkit*, *ransomware*

Outros riscos

- Conteúdos maliciosos e impróprios:
  - códigos maliciosos, páginas falsas, aplicativos falsos, *spam*, boatos, conteúdos inadequados, desafios perigosos e violentos

- Contato com pessoas mal-intencionadas:
  - *cyberbullying*, aliciamento, chantagem, pornografia infantil e sequestro

- Comportamentais (diretos e indiretos):
  - invasão de privacidade, uso excessivo
  - exposição excessiva

Desmistificando...

“Internet é um mundo virtual”

“Internet é uma terra sem lei”

“Internet é a grande vilã da atualidade”

“Sistema 100% seguro”

“Meus equipamentos jamais serão localizados na Internet”

“Não tem nada de interessante em meus equipamentos”

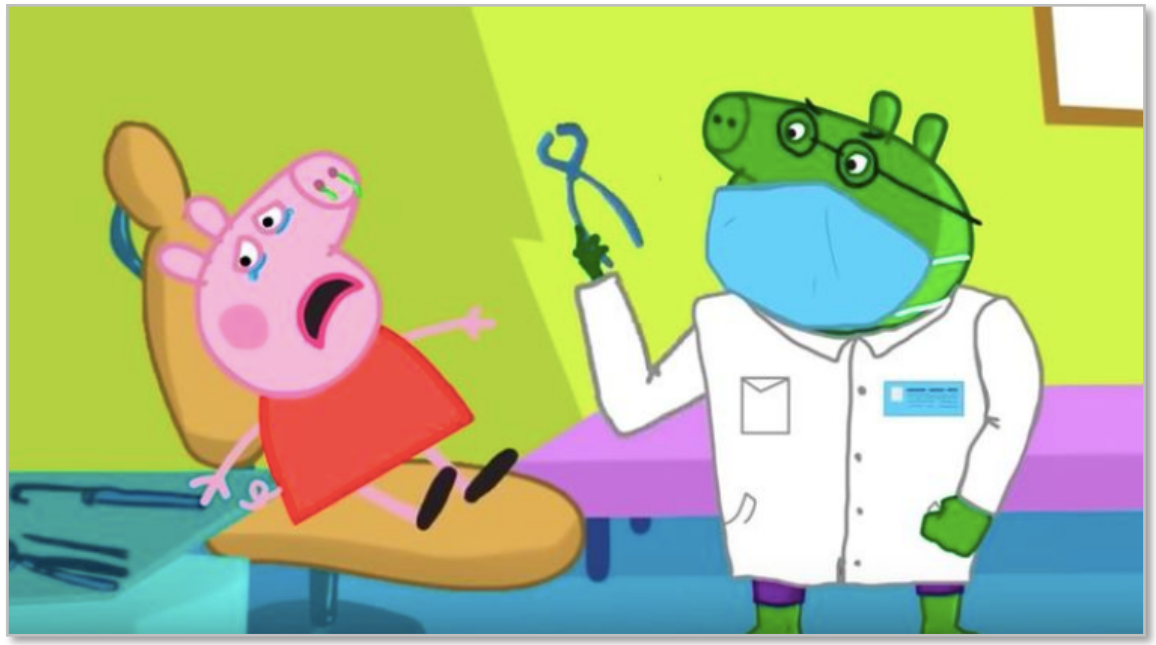
“Crianças são nativos digitais e seus pais são analfabetos digitais,

por isso pais não conseguem auxiliá-las”

“Crianças estão protegidas em casa”

Acesso a conteúdos impróprios

Parents warned to beware of FAKE Peppa Pig cartoons on Youtube with disturbing storylines



Facebook crime rises 19% as government introduces code of conduct

As the Daily Telegraph reports that social media sites will face a new government code of conduct, indepdent police figures show that Facebook crimes have rocketed by 19% in a single year, with harassment, sexual offences and malicious communications included in the 32,451 incidents

by Patrick Sullivan, Political Editor on 22 January 2020 10:29

There have been a total of 55,643 crimes linked to Facebook, according to official police figures. The news comes following the revelation that social media firms will be legally required to protect children from harmful content under the first-ever code to police the internet, according to front page news in The Daily Telegraph.

http://lifestyle.one/closer/entertainment/soaps/fake-peppa-pig-cartoons-youtube-disturbing-storylines/
http://www.thecommentator.com/article/7573/facebook_crime_rises_19_as_government_introduces_code_of_conduct/

Phishing e outros golpes

tecnoblog

Usuários do Facebook perdem US$ 4 milhões com malware de anúncios

Um malware batizado de SilentFade era usado para acessar contas do Facebook e pagar por anúncios na rede social em nome das vítimas

Por Victor Hugo Silva
02/10/2020 às 16:46

NEWS

O Facebook revelou que um malware usado em sua plataforma permitiu que os usuários perdessem US$ 4 milhões. Os autores do golpe usaram a quantia para criar anúncios de itens que vão de comprimidos para dieta e produtos para saúde sexual até objetos falsos, como bolsas, sapatos e óculos.

'Your Account Will Be Deactivated' Facebook Phishing Scam

By Brett M. Christensen On July 23, 2016 In Facebook Scams, Phishing Scams, Scams Tagged account deactivated scam, Facebook phishing scam

Outline:

Message purporting to be from the Facebook Ads team claims that your account will be deactivated because someone has reported it.

Brief Analysis:

The message is not an official Facebook warning and the claim that your account is set to be deactivated is untrue. Instead, the message is a phishing scam designed to steal your Facebook login details and other personal information. This is just one version in a long line of very similar phishing attacks.

https://tecnoblog.net/372088/usuarios-do-facebook-perdem-us-4-milhoes-com-malware-de-anuncios/
http://www.hoax-slayer.net/your-account-will-be-deactivated-facebook-phishing-scam/
https://www.a10networks.com/blog/instagram-phishing-scam-targets-children

Aplicativos maliciosos

Google had to delete 60 apps, many aimed at kids, after they showed users pornographic content

- The security firm Check Point discovered a type of malware dubbed "AdultSwine" that could display pornographic content and other malicious pop-ups on a user's smartphone screen.
- Google had to delete roughy 60 apps, mostly games or drawing tutorials aimed at children, from its Play store.

Jillian D'Onfro | @jillianiles

Published 9:00 AM ET Fri, 12 Jan 2018 | Updated 4:50 PM ET Fri, 12 Jan 2018

CNBC

11 apps maliciosos da Google Play assinavam serviços caros pelo usuário

Aplicativos tinham um malware conhecido como 'Joker' e já foram removidos da loja do Android

Daniel Junqueira 11/07/2020 11h00

Veja como identificar aplicativos não oficiais que prometem auxílio emergencial de R$ 600

É importante que os usuários fiquem atentos ao aplicativo que vão fazer o download

Mayra Cavalcanti, com agências

Publicado em 08/04/2020 às 8:39

COMPARTILHE:

NOTÍCIA

É possível ver diversos aplicativos, além do oficial, quando se busca por "auxílio emergencial" no Play Store - **FOTO: REPRODUÇÃO/GOOGLE PLAY STORE**

Faking 'Pokémon GO' GPS Location Using iPhone Jailbreak App

Antony Leather, CONTRIBUTOR

I'm passionate about gadgets, PC hardware and computer modding. FULL BIO

Opinions expressed by Forbes Contributors are their own.

Pokémon GO has undoubtedly encouraged millions of us get outside this summer to join the hunt and I've seen plenty of families involved together too (some parents even seemed to take things very seriously). So long as you stay safe and don't get stuck in a cave as some unfortunate UK players managed to do recently, the game is likely a healthier option that sitting at home on a console or PC.

However, if your local area is devoid of PokéStops and Pokémon or you need to stay at home to charge your smartphone (see several ways to boost battery life while playing *Pokémon GO* **here**), then there is another way to get around and play the game. In fact, you could be anywhere in seconds, scooping up the local Pokémon.

The newest trend in fake apps: Pokémon Go and the Olympics

Selena Larson —July 29 at 10:04AM GMT-3 | Last updated July 29 at 10:04AM GMT-3

https://www.cnbc.com/2018/01/12/google-deletes-malware-on-apps-for-kids.html
https://www.forbes.com/sites/antonyleather/2016/07/19/faking-pokemon-go-gps-location-using-iphone-jailbreak-app/#74f4c65c42bc
https://www.dailydot.com/debug/fake-apps-pokemon-olympics/
https://olhardigital.com.br/fique_seguro/noticia/11-apps-maliciosos-da-google-play-assinavam-servicos-caros-pelo-usuario/103347
https://jc.ne10.uol.com.br/brasil/2020/04/5605341-veja-como-identificar-aplicativos-nao-oficiais-que-prometem-auxilio-emergencial-de-r--600.html

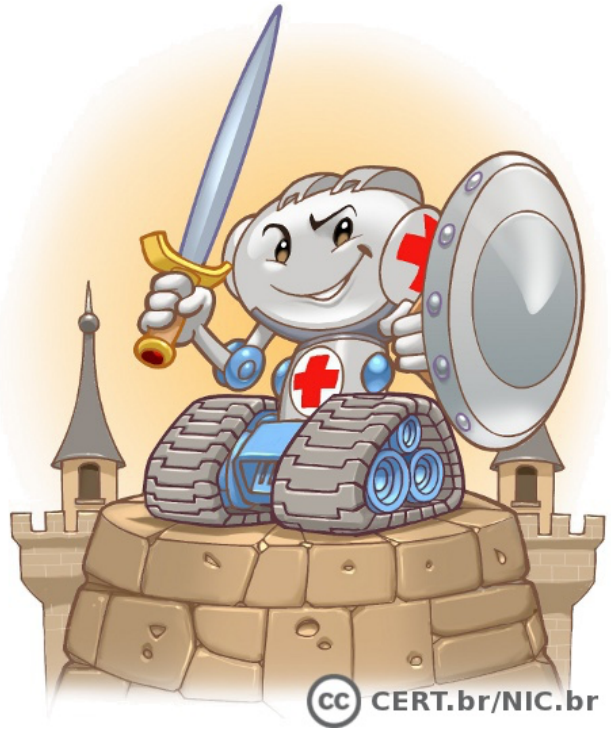
Prevenção

Internet não tem nada de virtual

- Mesmos riscos do cotidiano
  - mesmas pessoas, mesmas empresas, mesmos golpes
  - consequências reais
- Agravantes:
  - falsa sensação de anonimato
  - velocidade de propagação das informações
  - dificuldade de detectar sentimentos
  - dificuldade de exclusão das informações
- Necessário levar para a Internet os mesmos cuidados e preocupações do dia a dia
  - atenção com a segurança deve ser um hábito incorporado à rotina
  - independente de local, tecnologia ou meio utilizado
- Necessário aliar:
  - postura preventiva
  - mecanismos técnicos de segurança

Protegendo-se de golpes na Internet

- Mantenha sua privacidade
  - quanto mais informação você disponibiliza maiores são as chances de alguém se passar por você e de atacantes serem bem sucedidos em ataques
- Fique atento a indícios
  - problemas com órgãos de proteção ao crédito, retorno de e-mails, notificações de acessos indevidos, lançamentos estranhos no extrato bancário/cartão de crédito
- Saiba como identificar mensagens
  - quantias astronômicas, pedido de sigilo, urgência
  - erros de linguagem
  - por que você foi escolhido?
  - use a sabedoria popular
    - quando a esmola é demais o Santo desconfia
    - tudo que vem fácil vai fácil
  - NUNCA RESPONDER



Protegendo os equipamentos (1/2)

- Manter os equipamentos atualizados
  - com a versão mais recente do sistema operacional e dos aplicativos
  - com todas atualizações aplicadas
- Alterar as senhas padrão de fábrica
- Usar as opções de configuração disponíveis
  - Ex: proteção de tela com autenticação, PIN chip celular, etc
- Usar e manter atualizados mecanismos de segurança
  - antivírus, *antispam*, *firewall* pessoal, controle parental
- Seja cuidadoso na instalação de aplicativos
- Controle parental: proteção adicional
  - deve ser usado como um aliado, não substitui o diálogo e a mediação
  - apresenta falhas e pode ser burlado
- Fazer *backups*
  - devem ser mantidos desconectados

Protegendo os equipamentos (2/2)
Dispositivos móveis

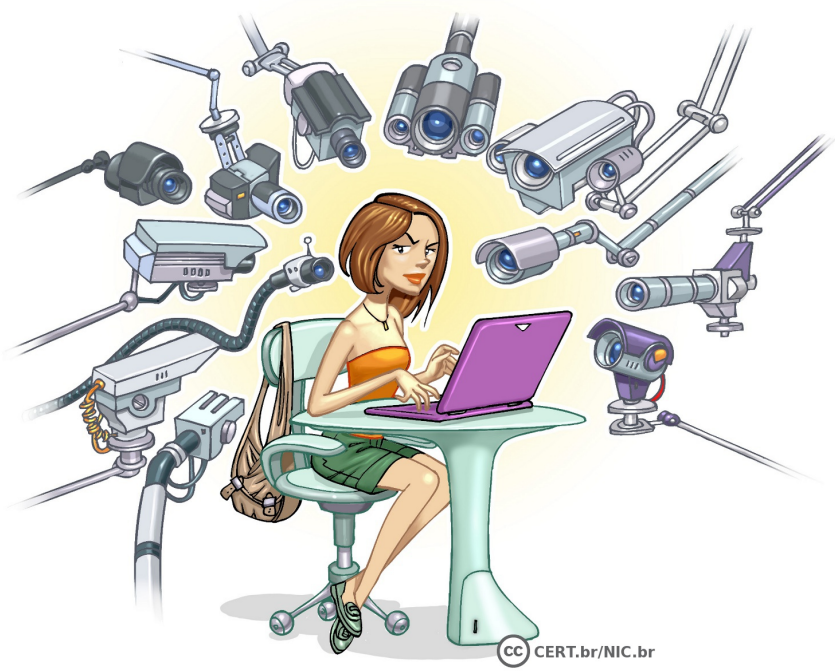
- Em caso de perda ou furto:
  - Informe:
    - a sua operadora
      - solicite o bloqueio do seu número (chip)
    - a empresa onde você trabalha
      - caso haja dados e senhas profissionais nele armazenadas
  - Altere as senhas que possam estar nele armazenadas
    - e-mail, redes sociais, e-gov, lojas de aplicativos, etc.
  - Bloqueie cartões de crédito cujo número esteja nele armazenado
  - Ative a localização remota, caso você a tenha configurado
    - se necessário, apague remotamente os dados nele gravados
- Ao se desfazer do seu dispositivo
  - Apague todas as informações nele contidas
  - Restaure as configurações de fábrica

Protegendo as contas de acesso

- Elaborar boas senhas
  - evitar o uso de:
    - dados que possam ser obtidos em redes sociais e páginas Web
    - dados pessoais, como nomes, sobrenomes e contas de usuário
    - sequências de teclado, como “1qaz2wsx” e “QwerTAsdfG”
    - palavras que fazem parte de listas publicamente conhecida
    - palavras associadas ao contexto em que estão sendo usadas
  - usar:
    - números aleatórios
    - senhas longas e com diferentes tipos de caracteres
- Não reutilizar as senhas
  - basta ao atacante descobrir uma senha para invadir outras contas onde a mesma senha é usada
- Não informar senhas por *e-mails* ou telefonemas
- Armazenar suas senhas de forma segura:
  - Usar programas gerenciadores de senhas
- Habilitar a verificação em duas etapas (2FA)

Preserve a sua privacidade nas redes sociais

- Considere que você está em um local público
- Pense bem antes de divulgar (não há como voltar atrás)
- Use as opções de privacidade oferecidas pelos *sites*
  - procure ser o mais restritivo possível
- Seja seletivo ao aceitar seus contatos
- Mantenha seu perfil e seus dados privados
- Restrinja o acesso ao seu endereço de *e-mail*
- Seja cauteloso ao dar acesso à aplicativos
- Seja cuidadoso ao se associar a grupos e comunidades
- **Não acredite em tudo que você lê**
  - Verifique sempre a fonte das informações
  - Não repasse boatos nem, mensagens que possam gerar pânico ou ódio



Respeite a privacidade alheia

- Evite falar sobre as ações, hábitos e rotina de outras pessoas
- Não divulgue sem autorização:
  - imagens em que outras pessoas apareçam
  - mensagens ou imagens copiadas do perfil de usuários que restrinjam o acesso
- Tente imaginar como a outra pessoa se sentiria ao saber que aquilo está se tornando público

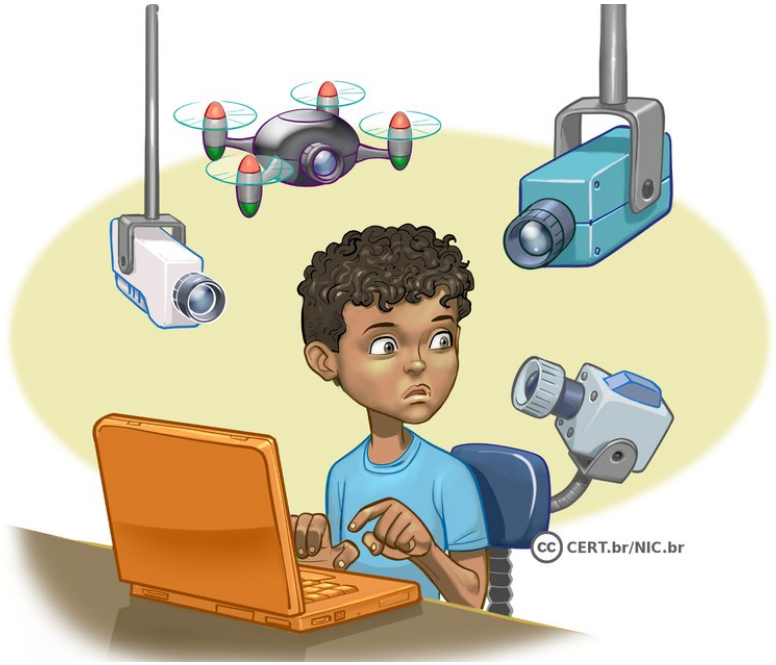
Proteja os seus filhos (1/2)

- Informe-os sobre os riscos
  - Ajude-os a desenvolver pensamento crítico
- Dê o exemplo
- Estimule o diálogo
- Reforce os cuidados com estranhos
  - nunca fornecerem informações pessoais, enviarem fotos ou vídeos, usar webcam
  - para não marcarem / irem a encontros desacompanhados
- Ensine-os sobre privacidade
- Observe o comportamento
- Estabeleça regras e cumpra o combinado
- Ajude a protegerem os equipamentos

Proteja os seus filhos (2/2)

- Respeite os limites de idade estipulados pelos *sites*

- Não exponha excessivamente seus filhos:
  - muitos pais criam perfis em nome dos filhos e postam sobre eles ou como se fossem eles
    - isso pode confundir e desagradar as crianças
  - evite constranger seus filhos divulgando fotos ou comentários que possam embaraçá-los
  - seja cuidadoso ao divulgar imagens de seus filhos
    - o que para você pode ser algo inocente, para outras pessoas pode ter uma conotação diferente



Proteja a sua vida profissional

- Cuide da sua imagem profissional
- Antes de divulgar uma informação:
  - avalie se ela pode atrapalhar:
    - o seu emprego atual
    - um processo seletivo futuro
  - lembre-se que ela poderá ser acessada por seus chefes e colegas de trabalho
  - observe se ela não fere o código de conduta da sua empresa
- Cuidado ao permitir que seus filhos usem o mesmo computador ou dispositivo móvel que você usa para tratar de assuntos profissionais:
  - alguns aplicativos, como jogos, divulgam automaticamente nas redes sociais, dependendo das configurações
- Oriente seus familiares para não divulgarem informações sobre a sua empresa e vida profissional

CARREIRA / TWITTER - 30/03/2010

Mensagem no Twitter causa demissão de executivo da Locaweb

Curtir 22 Tweetar

Diretor comercial foi demitido depois de ter publicado mensagens contra o São Paulo Futebol Clube, durante o clássico contra o Corinthians. A Locaweb era um dos patrocinadores do time do Morumbi

http://epocanegocios.globo.com/Revista/Common/0,,EMI130181-16349,00-MENSAGEM+NO+TWITTER+CAUSA+DEMISSAO+DE+EXECUTIVO+DA+LOCAWEB.html

Protegendo a empresa

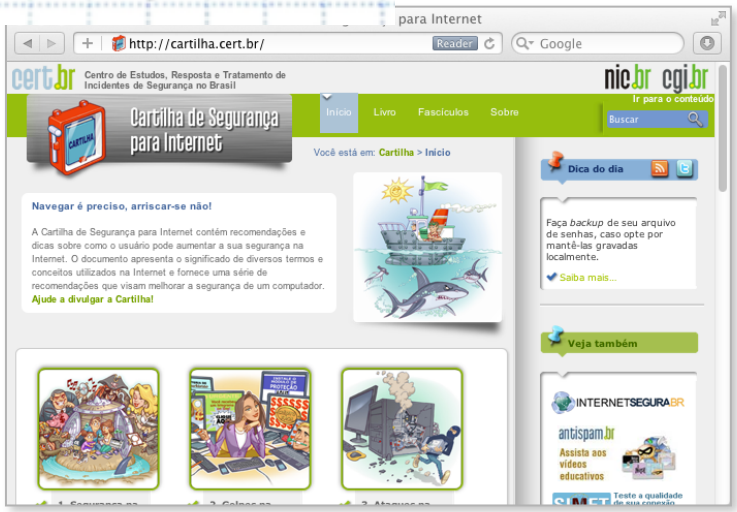
- Crie um código de conduta e uma política de uso aceitável
- Informe os funcionários sobre:
  - os riscos de uso das redes sociais
  - as regras de acesso durante o expediente
  - o comportamento esperado, referente a:
    - divulgação de informações profissionais (sigilosas ou não)
    - emissão de opiniões que possam comprometer a empresa
- Invista em treinamento e campanhas de conscientização
- Cuide da imagem
  - observe a opinião de clientes e consumidores
  - observe ações que envolvam o nome da empresa

Mantenha-se Informado: Materiais de Apoio

cert.br nic.br cgi.br

MANTENHA-SE INFORMADO

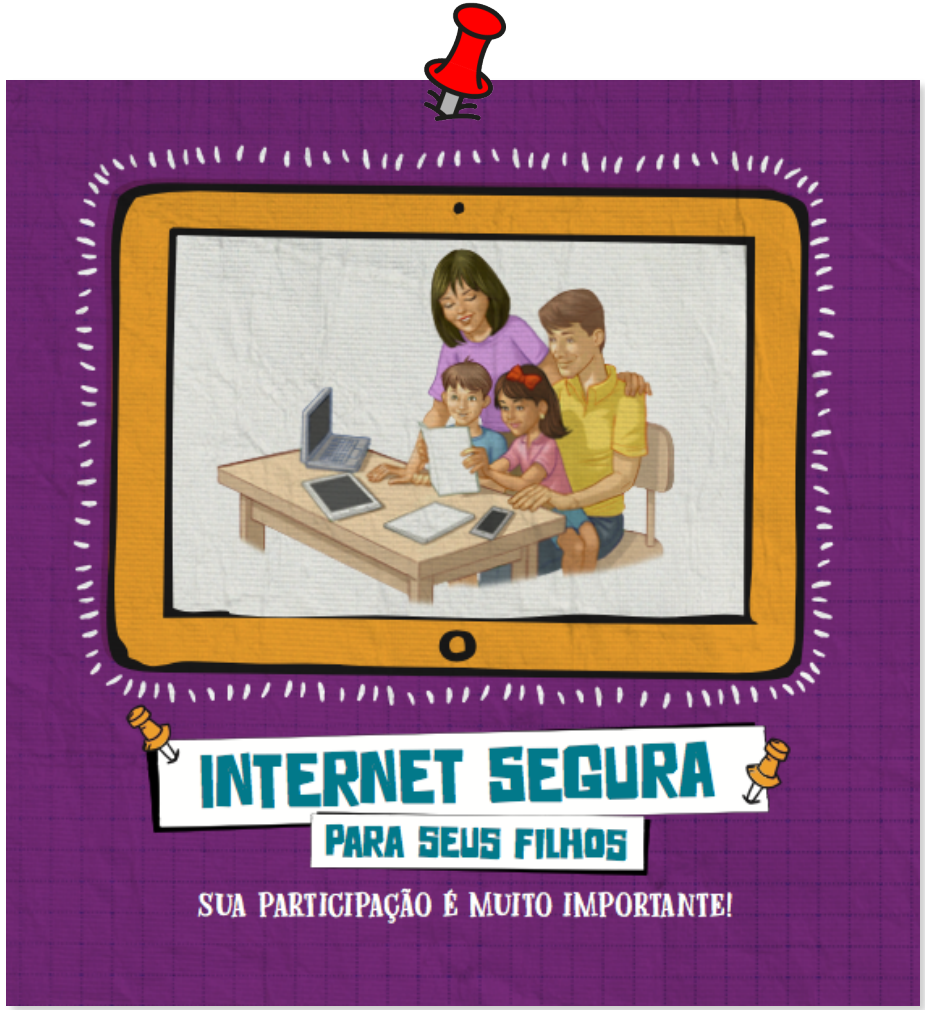
- **Cartilha de Segurança para Internet**
  - Livro (PDF e ePub)
  - Conteúdo no site
  - Fascículos e slides
  - Dica do dia no site, via Twitter e RSS



https://cartilha.cert.br/

https://internetsegura.br/

Guias Internet Segura



NÃO FAÇA COM OS OUTROS O QUE NÃO GOSTARIA QUE FIZESSEM COM VOCÊ

CUIDADO COM PESSOAS ESTRANHAS OU QUE VOCÊ CONHECE APENAS PELA INTERNET

ESCREVA E FALE CORRETAMENTE

RESPEITE OS LIMITES DE IDADE

PROTEJA A SUA PRIVACIDADE

INTERNET NÃO É TUDO!

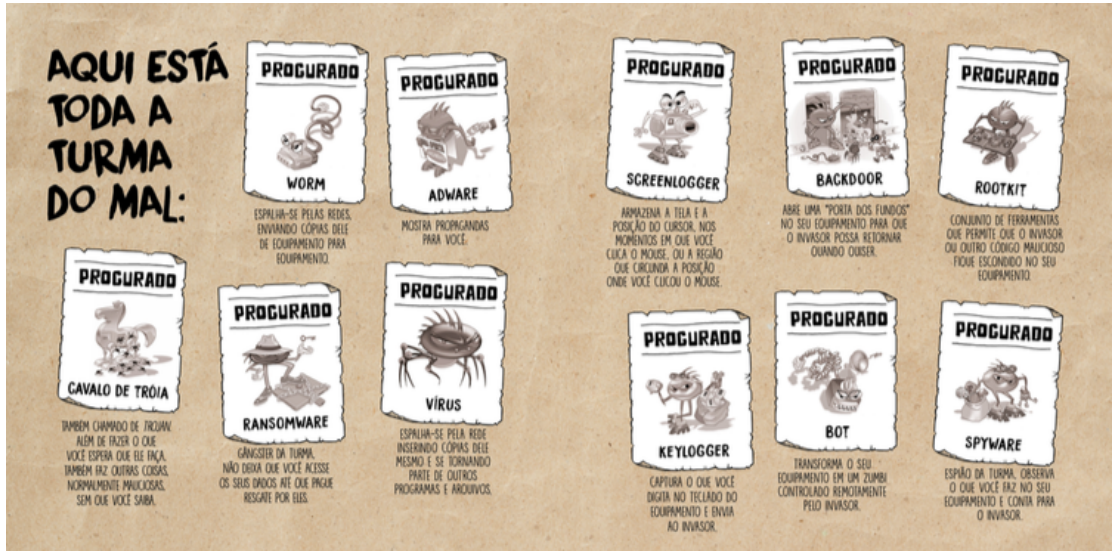
PROTEJA A PRIVACIDADE DAS OUTRAS PESSOAS

NÃO ACREDITE EM TUDO QUE VOCÊ LÊ

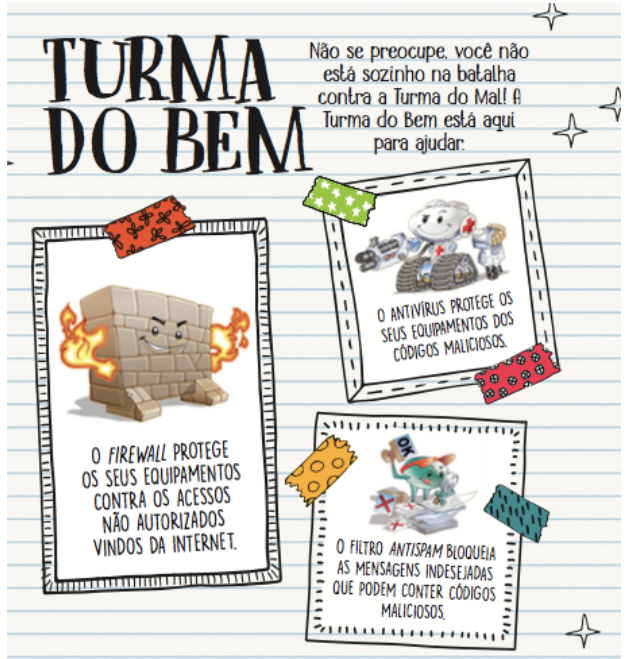
RESPEITE O TRABALHO DOS OUTROS

CUIDADO PARA NÃO PERDER SEUS EQUIPAMENTOS

PROTEJA OS SEUS EQUIPAMENTOS



PROTEJA SUAS SENHAS



Desafios

internetsegura.br

nic.br | INTERNET SEGURA BR

Sobre | Outras iniciativas | Como Pedir Ajuda

Personagens para montar

Monte os bonecos de papel tridimensionais da turma do bem e da turma do mal e crie suas próprias histórias! É só baixar os arquivos, imprimir e começar a brincar!

Antivírus: ajuda a turma do bem a detectar, anular e eliminar vírus e outros tipos de códigos maliciosos do computador.

Autenticação: o segurança da turma. Confirma se quem está ali é mesmo o dono do dispositivo. Pede senhas e outros códigos de verificação, checa tudo antes de liberar a entrada.

Backup: salva todas as informações do seu computador em outro dispositivo e não perde nada.

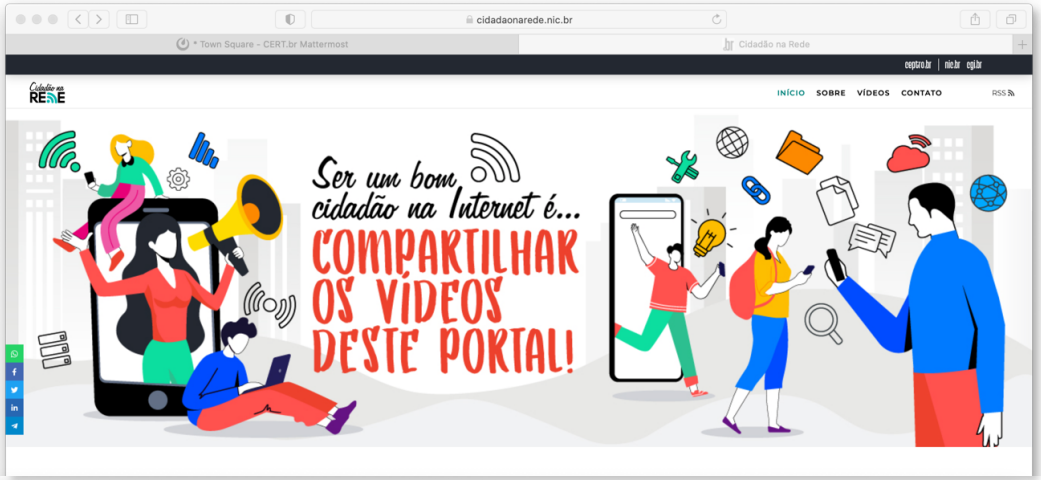
Firewall: é o dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores.

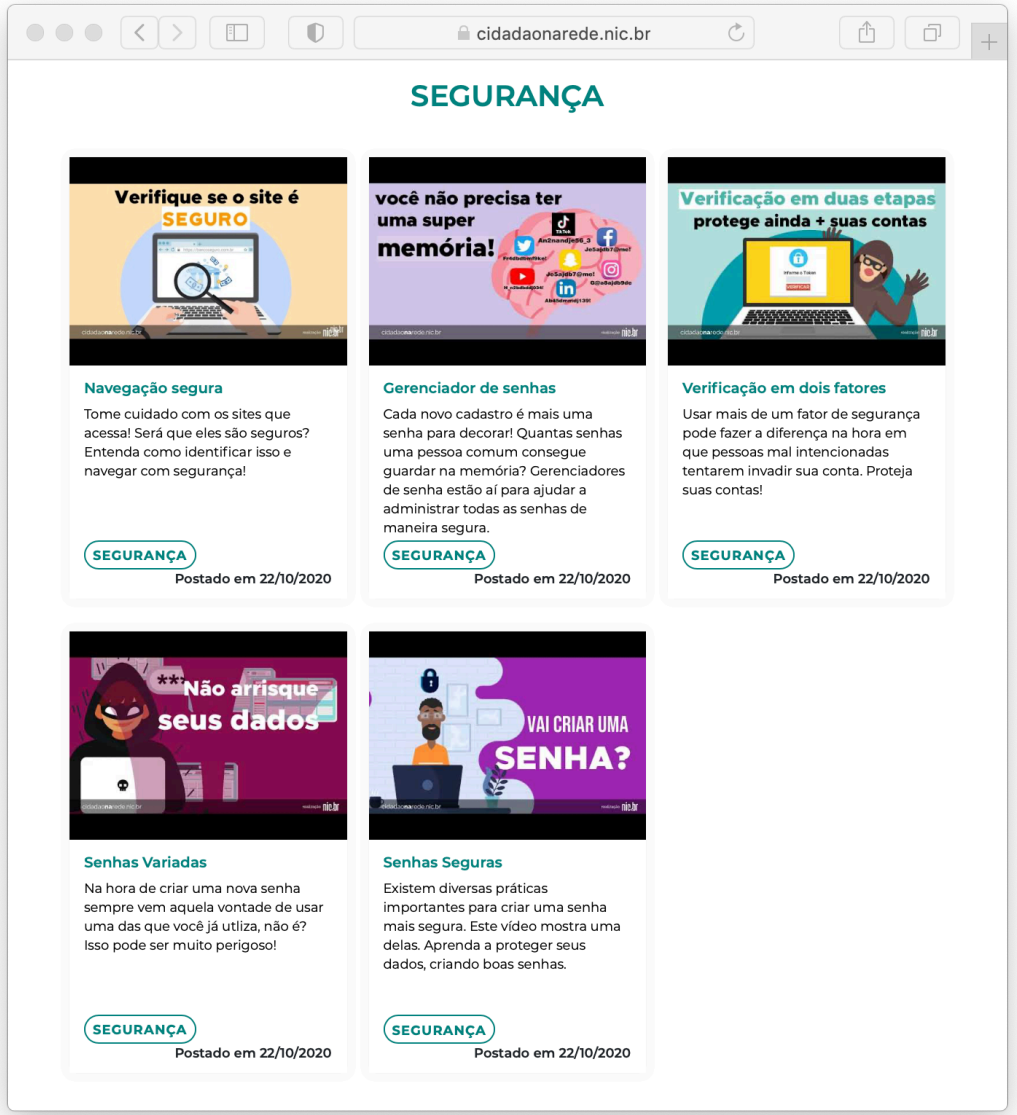
Spyware: espião da turma. Observa o que você faz no seu dispositivo e conta para o invasor.

Trojan: também chamado de Cavalo de Tróia. Além de fazer o que você espera que ele faça, também faz outras coisas, normalmente maliciosas, sem que você saiba.

Vírus: espalha-se pela rede inserindo cópias dele mesmo e se tornando parte de outros programas e arquivos.

Zumbi: esse é o nome do computador que foi infectado por um bot. Nesse caso, a máquina pode ser controlada remotamente, sem que você saiba.





https://cidadaonarede.nic.br/

https://fe.seg.br/

Obrigada!

lucimara@cert.br

Notificações para: cert@cert.br

@certbr

www.cert.br

23 de novembro de 2020

nic.br cgi.br

www.nic.br | www.cgi.br