nic.br

Núcleo de Informação e Coordenação do Ponto BR

cgi.br

Comitê Gestor da Internet no Brasil

registro.br cert.br cetic.br ceptro.br ceweb.br ix.br

nic.br cgi.br | cert.br

Curso de Capacitação
Uso consciente e responsável da Internet
São Paulo, SP | 19/03/19

membros e ex-membros do CGI.br
(somente os atuais membros têm direito a voto)

ASSEMBLEIA GERAL

7 membros eleitos pela Assembleia Geral

CONSELHO DE ADMINISTRAÇÃO

CONSELHO FISCAL

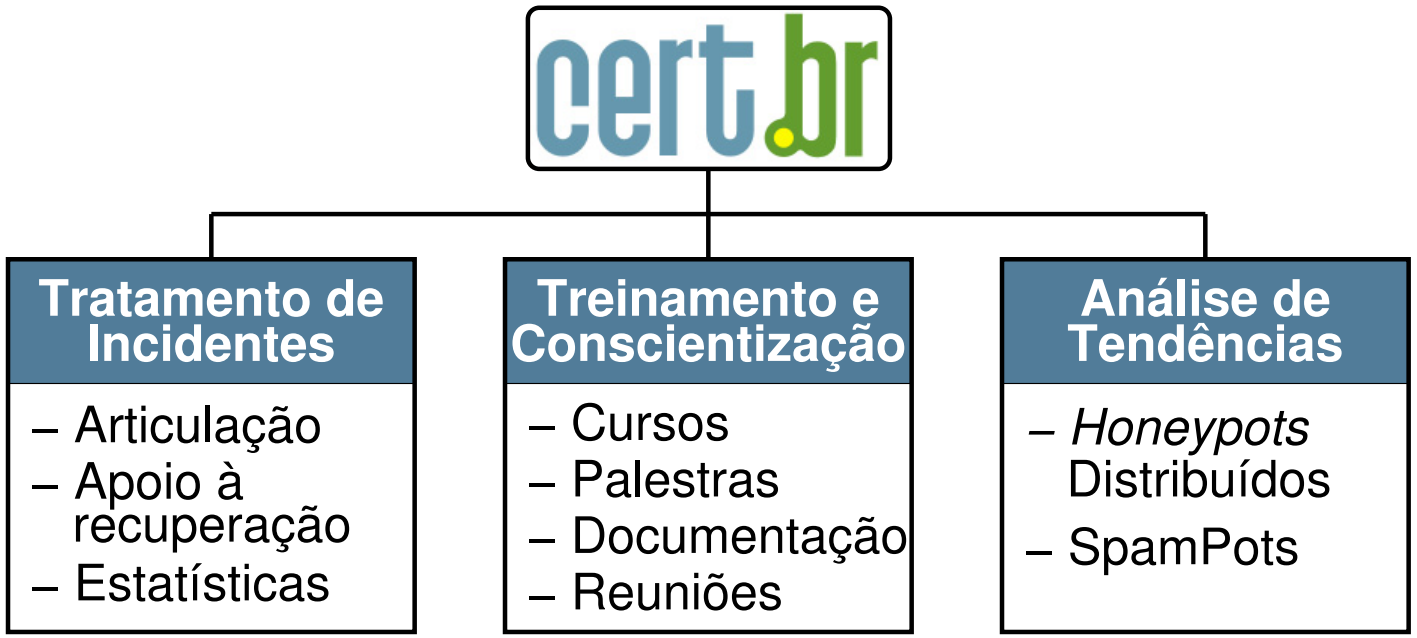
- ADMINISTRAÇÃO
- JURÍDICO
- COMUNICAÇÃO
- ASSESSORIAS: CGI.br e PRESIDÊNCIA

DIRETORIA EXECUTIVA

1 2 3 4 5

- registro.br — Domínios
- cert.br — Segurança
- cetic.br — Indicadores
- ceptro.br — Redes e Operações
- ceweb.br — Tecnologias Web
- ix.br — Troca de Tráfego
- W3C Brasil — Padrões Web

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



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

Criado em 1997 para:

- Ser um ponto de contato nacional para notificação de incidentes
- Prover a facilitação e o apoio necessários no processo de resposta a incidentes
- Estabelecer um trabalho colaborativo com outras entidades
- Aumentar a conscientização sobre a necessidade de segurança na Internet
- Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades

Internet Segura: proteção de contas e dispositivos

(atualizações, mecanismos de segurança, senha forte e *sites* seguros)

Miriam von Zuben
Analista de Segurança
miriam@cert.br

cert.br nic.br cgi.br

Internet
Riscos e oportunidades

cert.br nic.br cgi.br

Riscos

- **Ilusão: achar que não corre riscos**
  - “meus equipamentos não serão localizados”
  - “não tem nada de interessante nos meus equipamentos”
  - “dentro de casa está seguro”

- **Atacantes interessados em quantidade de equipamentos**
  - independente de quais são
  - informações cada vez mais valiosas

Riscos em Sistemas Conectados à Internet

- invasão de contas
- indisponibilidade de serviços
- exposição da 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

Riscos

- **Exploram:**
  - vulnerabilidades dos sistemas conectados a Internet
  - fragilidades de usuários (engenharia social)
    - códigos maliciosos (*malware*)
      - vírus, trojan, *ransomware*, RAT, etc
    - aplicativos maliciosos
    - páginas falsas (*phishing*)
    - golpes (antecipação de recursos)

Aplicativos maliciosos

TECHNOLOGY

New 'AdultSwine' Malware Displays Adult Images To Children

Here is what you need to know about pornography-displaying malware that has been found in multiple children's Android apps that were downloaded as many as 7 million times.

By Joseph Steinberg *CEO, SecureMySocial* @JosephSteinberg

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

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

Faking 'Pokémon GO' GPS Location Using iPhone Jailbreak App

Antony Leather, CONTRIBUTOR

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

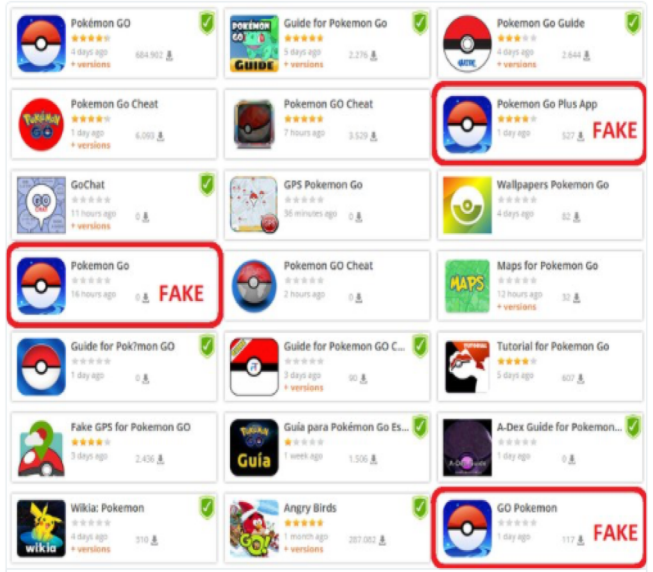
Opinions expressed by Forbes Contributors are their own.

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.

Rogue imitators

Meanwhile, security firms have warned that fake versions of Pokemon Go are downlo ransomware onto users' phones.



Rigo Technology
@rigotechnology
Follow

Watch out for fake Pokemon Go apps on 3rd party stores. It may contain malware. #PokemonGO #malware

1:06 AM - 19 Jul 2016

2 1

http://www.forbes.com/sites/antonyleather/2016/07/19/faking-pokemon-go-gps-location-using-iphone-jailbreak-app/#74f4c65c42bc
http://www.ifsecglobal.com/pokemon-go-security-risks-flagged-by-the-cia-middle-eastern-states-and-data-security-experts/
http://www.dailydot.com/debug/fake-apps-pokemon-olympics/
https://www.inc.com/joseph-steinberg/new-adultswine-malware-displays-pornography-to-children.html
https://www.cnbc.com/2018/01/12/google-deletes-malware-on-apps-for-kids.html

Phishing e outros golpes

'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.

http://www.hoax-slayer.net/your-account-will-be-deactivated-facebook-phishing-scam/
https://www.a10networks.com/blog/instagram-phishing-scam-targets-children
https://www.independent.co.uk/life-style/gadgets-and-tech/gaming/fortnite-battle-royale-download-safety-security-privacy-parent-advice-a8437226.html

Invasão de privacidade

Germany bans Q&A IoT doll 'Cayla' as illegal spy device

Liam Tung (CSO Online) on 21 February, 2017 06:39

0 Comments | 12 | 4

Germany's Federal Network Agency has banned a smart doll called My Friend Cayla after deeming it a hidden surveillance device.

BRIAN BARRETT SECURITY 12.20.17 02:08 PM

DON'T GET YOUR KID AN INTERNET-CONNECTED TOY

Call to ban sale of IoT toys with proven security flaws

Posted Nov 15, 2017 by Natasha Lomas (@riptari)

With toys like these and other connected toys expected to be popular around Black Friday and Christmas, we're calling for smart toys to be made secure, or taken off sale entirely.

https://www.wired.com/story/dont-gift-internet-connected-toys/
https://techcrunch.com/2017/11/15/call-to-ban-sale-of-iot-toys-with-proven-security-flaws
https://www.cso.com.au/article/614555/germany-bans-q-iot-doll-cayla-illegal-spy-device/

Vazamento de dados

The Switch

Toymakers are tracking more data about kids – leaving them exposed to hackers

By Andrea Peterson November 30, 2015

The Switch

VTech says 6.4 million children profiles were caught up in its data breach

By Hayley Tsukayama December 1, 2015

Leaked Personal Data of 200,000 Child Patients Being Sold for $4,900

C. J. | Apr 09, 2016 09:31 PM EDT

Thousands of patients' data stolen after Children's Mercy employees fall for scam

Criminals use kids personal identifiable information and healthcare data to create synthetic IDs, making data of minors more valuable in underground communities than adults.

This particular hack was caused by a phishing scam. Once hackers gained access to employee credentials, they were able to extract personal, sensitive health date of over 60,000 patients.

Organizations need to take an outside-in approach to protecting their domains and customer data. By receiving alerts when employee credentials are compromised and exposed in underground markets, organizations can take proactive security measures to prevent data breaches before damage is done. 4iQ can help.

> Personal data from more than 60,000 individuals may have been compromised as part of an email phishing scam that targeted Children's Mercy Hospital employees.

https://www.washingtonpost.com/news/the-switch/wp/2015/12/01/vtech-says-6-4-million-children-were-caught-up-in-its-data-breach/
https://www.washingtonpost.com/news/the-switch/wp/2015/11/30/toymakers-are-tracking-more-data-about-kids-leaving-them-exposed-to-hackers/?tid=a_inl
http://en.yibada.com/articles/115144/20160409/leaked-personal-data-personal-data-leak-china-hospital-data-theft.htm
https://news.4iq.com/post/102eyik/thousands-of-patients-data-stolen-after-childrens-mercy-employees-fall-for-scam

Senhas padrão e equipamentos desatualizados

73,000 webcams left vulnerable because people don't change default passwords

Shodan: The IoT search engine for watching sleeping kids and bedroom antics

[Opinion] Shodan is not the devil, but rather a messenger which should make us take responsibility for our own security in a world of webcams and mobile devices.

By Charlie Osborne for Zero Day | January 26, 2016 -- 11:43 GMT (03:43 PST) | Topic: Security

http://mashable.com/2014/11/10/naked-security-webcams/#WvbidQXQumqu
http://www.zdnet.com/article/shodan-the-iot-search-engine-which-shows-us-sleeping-kids-and-how-we-throw-away-our-privacy/

Como se prevenir

Primeiro passo

- **Qualquer conta, perfil ou equipamento conectado à Internet pode vir a ser alvo da ação de atacantes**

- **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

Como se prevenir

- **Aplicar soluções técnicas**
  - ajuda a proteger das ameaças já conhecidas
    - para as quais já existem formas de prevenção

- **Adotar postura preventiva**
  - ajuda a proteger das:
    - ameaças que envolvem engenharia social
    - ameaças ainda não conhecidas
    - ameaças que ainda não possuem solução

Proteja seus equipamentos

- **Mantenha os equipamentos seguros**
  - com a versão mais recente do sistema operacional e dos aplicativos
  - com todas atualizações aplicadas
- **Use as opções de configuração disponíveis**
- **Use e mantenha atualizados mecanismos de segurança**
  - antivírus
  - *antispam*
  - *antiransomware*
  - *firewall* pessoal
  - controle parental

Controle parental

- **Proteção adicional**
  - deve ser usado como um aliado
    - não substitui o diálogo e a mediação
    - apresenta falhas e pode ser burlado
- **Conjunto de recursos de segurança**
  - sistemas operacionais, *sites*, equipamentos e aplicativos
- **Permitem definir:**
  - filtros de pesquisa
  - *sites* que podem ou não ser acessados
  - aplicativos que podem ser executados
  - limites de tempo
  - com quem pode ou não conversar

Proteja suas contas de acesso

- **Elabore boas senhas**
  - evite usar:
    - 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 conhecidas
    - palavras associadas ao contexto em que estão sendo usadas
  - use:
    - números aleatórios
    - senhas longas e com diferentes tipos de caracteres

Dicas práticas para elaborar boas senhas

- **Escolha uma frase e selecione a primeira, a segunda ou a última letra de cada palavra**
  - Frase: “O Cravo brigou com a Rosa debaixo de uma sacada”
  - Senha: “?OCbcaRddus”
- **Escolha uma frase longa, fácil de ser memorizada e com diferentes tipos de caracteres**
  - Senha: “1 dia ainda verei os aneis de Saturno!!!”
- **Invente um padrão de substituição próprio**
  - Padrão: substituir “o” por “0” e duplicar as letras “s” e “r”
  - Frase: “Sol, astro-rei do Sistema Solar”
  - Senha: “SS0l, asstrr0-rrei d0 SSisstema SS0larr”

Uso seguro de senhas

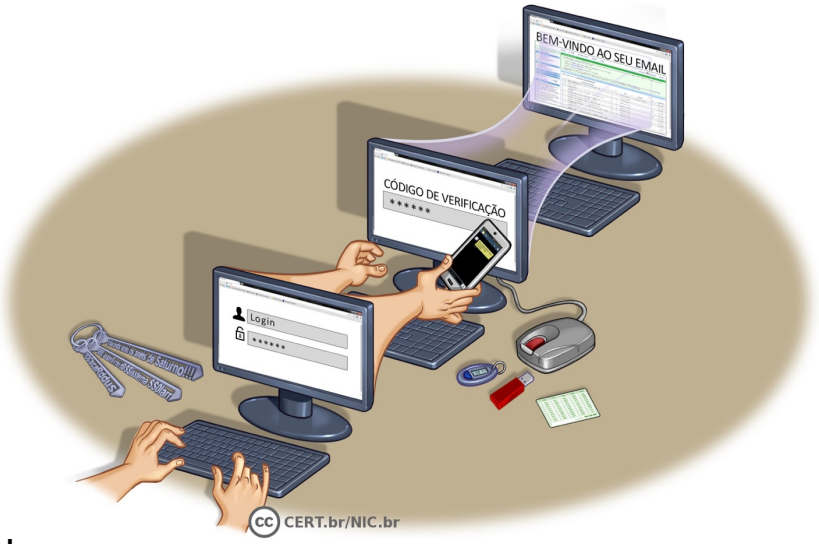
- **Não reutilize suas senhas**
  - basta ao atacante descobrir uma senha para invadir outras contas onde a mesma senha é usada
- **Não informe senhas por e-mails ou telefonemas**
- **Crie grupos de senhas, de acordo com o risco envolvido:**
  - crie senhas:
    - únicas, fortes, e use-as onde haja recursos valiosos envolvidos
    - únicas, um pouco mais simples, e use-as onde o valor dos recursos protegidos é inferior
    - simples e reutilize-as para acessos sem risco
- **Armazene suas senhas de forma segura:**
  - anote-as em um papel e guarde-o em local seguro
  - grave-as em um arquivo criptografado
  - use programas gerenciadores de contas/senhas

Alteração de senhas

- **Troque periodicamente suas senhas**
  - não existe um prazo recomendado
  - prazo depende da exposição da senha e do “valor” das informações
- **Sugestão:**
  - Imediatamente: se desconfiar que elas tenham sido descobertas ou usadas em equipamentos invadidos ou infectados
  - Rapidamente:
    - se perder um equipamento onde elas estejam gravadas
    - se usar:
      - um padrão de formação e desconfiar que alguma tenha sido descoberta
      - uma mesma senha em mais de um lugar e desconfiar que ela tenha sido descoberta em algum deles
  - Regularmente: nos demais casos

Habilite a verificação em duas etapas

- **Uso de informações adicionais para checar a identidade**
- **Para invadir uma conta o atacante terá que:**
  - descobrir a sua senha (primeira etapa)
  - realizar com sucesso a segunda etapa
    - o que você é
      - informações biométricas, como impressão digital, rosto, voz e olho
    - algo que apenas você sabe
      - outra senha, pergunta de segurança, número PIN, informação pessoal
    - algo que apenas você possui
      - código de verificação, cartão de senhas bancárias, token gerador de senhas, acesso a um determinado equipamento



Use conexões seguras

- **Alguns indícios apresentados pelo navegador Web são:**
  - o endereço começa com https://
  - o desenho de um “cadeado fechado” é mostrado na barra de endereço
    - ao clicar sobre ele são exibidos detalhes sobre a conexão e certificado digital em uso
  - um recorte colorido (branco ou azul) com o nome do domínio do site é mostrado ao lado da barra de endereço (à esquerda ou à direita)
    - ao passar o mouse ou clicar sobre o recorte são exibidos detalhes sobre a conexão e certificado digital em uso
  - a barra de endereço e/ou recorte são apresentados em verde e no recorte é colocado o nome da instituição dona do site

Outros cuidados

- **Faça *backups***
  - única garantia efetiva contra *ransomware*
  - devem ser mantidos desconectados

- **Seja cuidadoso ao:**
  - abrir anexos
  - clicar em links
  - baixar aplicativos
  - acessar páginas Web

- **Proteja a sua privacidade**
  - diminuir a quantidade de dados expostos

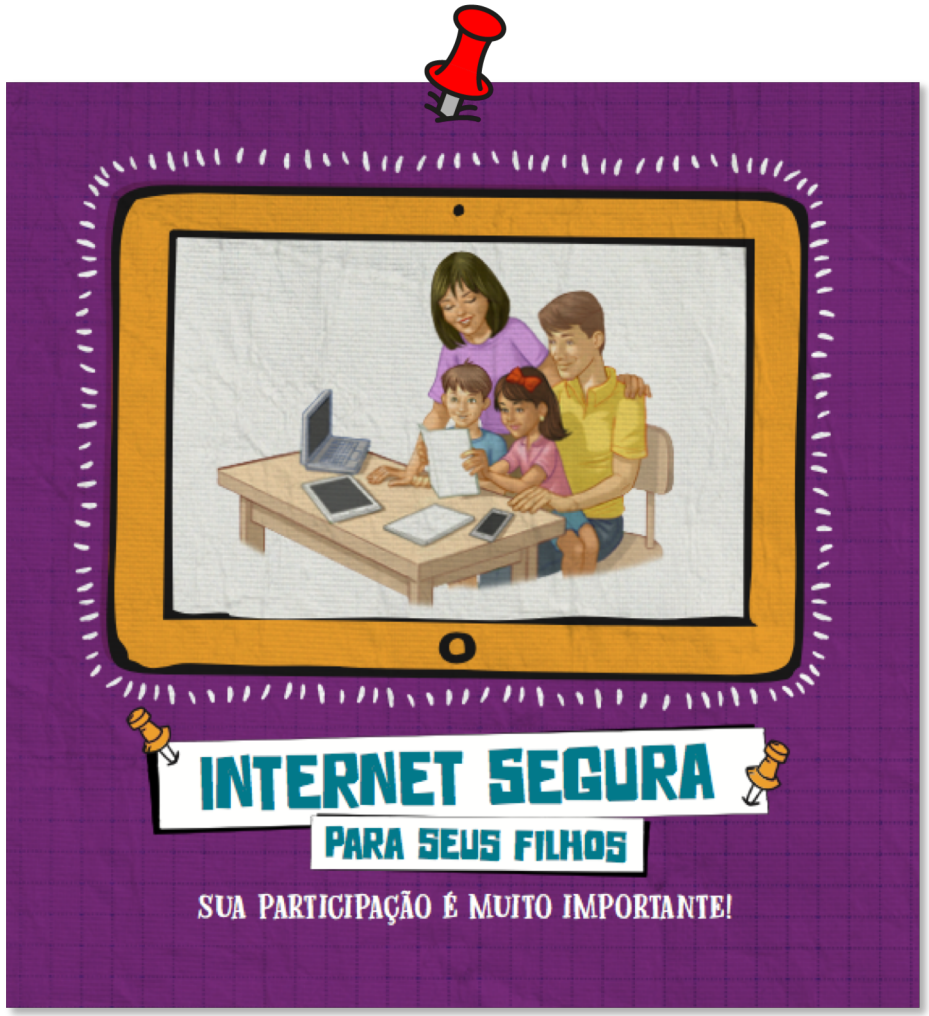
Postura Preventiva e a Mediação

cert.br nic.br cgi.br

Mediação

- **Restritiva**
  - proibições reduzem os riscos e também as oportunidades
  - surtem pouco ou nenhum efeito
    - Internet onipresente, uso privativo associado à facilidade de uso
- **Ativa**
  - essencial para desenvolver a postura preventiva
  - aproveitar o momento de aprendizagem
  - escola como um ambiente importante para criação de habilidades no uso da Internet e de novas tecnologias
    - crianças/adolescentes: multiplicadores de boas práticas de segurança
    - maior facilidade de reter os conhecimentos

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

PROTEJA A PRIVACIDADE DAS OUTRAS PESSOAS

ESCREVA E FALE CORRETAMENTE

RESPEITE OS LIMITES DE IDADE

NÃO ACREDITE EM TUDO QUE VOCÊ LÊ

PROTEJA A SUA PRIVACIDADE

RESPEITE O TRABALHO DOS OUTROS

CUIDADO PARA NÃO PERDER SEUS EQUIPAMENTOS

INTERNET NÃO É TUDO!

PROTEJA OS SEUS EQUIPAMENTOS

PROTEJA SUAS SENHAS

AQUI ESTÁ TODA A TURMA DO MAL:

PROCURADO — WORM
ESPALHA-SE PELAS REDES, ENVIANDO CÓPIAS DELE DE EQUIPAMENTO PARA EQUIPAMENTO.

PROCURADO — ADWARE
MOSTRA PROPAGANDAS PARA VOCÊ.

PROCURADO — SCREENLOGGER
ARMAZENA A TELA E A POSIÇÃO DO CURSOR, NOS MOMENTOS EM QUE VOCÊ CLICA O MOUSE, OU A REGIÃO QUE CIRCUNDA A POSIÇÃO ONDE VOCÊ CLICOU O MOUSE.

PROCURADO — BACKDOOR
ABRE UMA "PORTA DOS FUNDOS" NO SEU EQUIPAMENTO PARA QUE O INVASOR POSSA RETORNAR QUANDO QUISER.

PROCURADO — ROOTKIT
CONJUNTO DE FERRAMENTAS QUE PERMITE QUE O INVASOR OU OUTRO CÓDIGO MALICIOSO FIQUE ESCONDIDO NO SEU EQUIPAMENTO.

PROCURADO — CAVALO DE TROIA
TAMBÉM CHAMADO DE *TROJAN*, ALÉM DE FAZER O QUE VOCÊ ESPERA QUE ELE FAÇA, TAMBÉM FAZ OUTRAS COISAS, NORMALMENTE MALICIOSAS, SEM QUE VOCÊ SAIBA.

PROCURADO — RANSOMWARE
GÂNGSTER DA TURMA. NÃO DEIXA QUE VOCÊ ACESSE OS SEUS DADOS ATÉ QUE PAGUE RESGATE POR ELES.

PROCURADO — VÍRUS
ESPALHA-SE PELA REDE INSERINDO CÓPIAS DELE MESMO E SE TORNANDO PARTE DE OUTROS PROGRAMAS E ARQUIVOS.

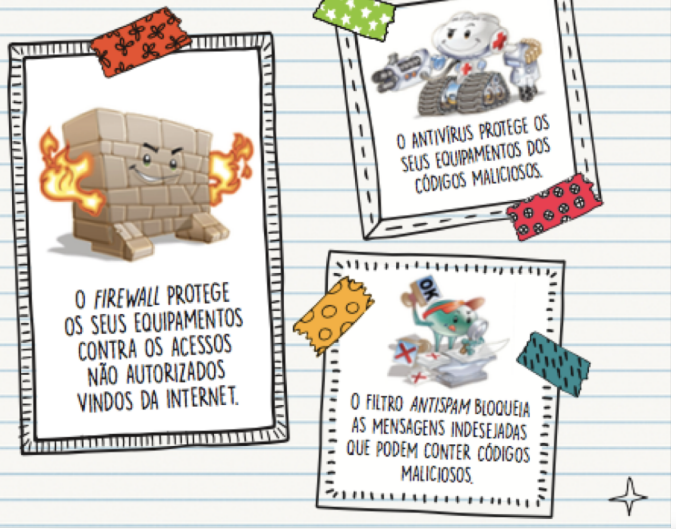
PROCURADO — KEYLOGGER
CAPTURA O QUE VOCÊ DIGITA NO TECLADO DO EQUIPAMENTO E ENVIA AO INVASOR.

PROCURADO — BOT
TRANSFORMA O SEU EQUIPAMENTO EM UM ZUMBI CONTROLADO REMOTAMENTE PELO INVASOR.

PROCURADO — SPYWARE
ESPIÃO DA TURMA. OBSERVA O QUE VOCÊ FAZ NO SEU EQUIPAMENTO E CONTA PARA O INVASOR.

TURMA DO BEM

Não se preocupe, você não está sozinho na batalha contra a Turma do Mal! A Turma do Bem está aqui para ajudar:



CONHEÇA OS RISCOS

- Acesso a conteúdos impróprios
- Contato com estranhos
- Uso excessivo
- Superexposição
- Exposição da privacidade
- Falta de maturidade emocional
- Dificuldade de exclusão
- *Cyberbullying*
- Brincadeiras perigosas
- Códigos maliciosos e *phishing*

AJUDE SEUS FILHOS A SE PROTEGEREM

- Dê o exemplo
- Estimule o diálogo
- Reforce os cuidados com estranhos
- Ensine–os sobre privacidade
- Fique atento aos limites de idade
- Observe o comportamento
- Cuidado com o *cyberbullying*
- Estabeleça regras
- Utilize o controle parental
- Ajude-os a protegerem as contas de acesso
- Proteja os equipamentos que eles usam

NÃO SEJA VOCÊ O VILÃO

- Você costuma postar fotos e vídeos dos seus filhos?
- Você já criou perfis em nome dos seus filhos?
- Você costuma postar mensagens nas redes sociais dos seus filhos?

internetsegura.br

nic.br | INTERNET SEGURABR

Sobre | Outras iniciativas | Como Pedir Ajuda

Internet Segura – Faça sua parte e todos teremos uma Internet mais segura!

para **Crianças**

para **Adolescentes**

para **Pais e Educadores**

CONFIRA A NOVIDADE!

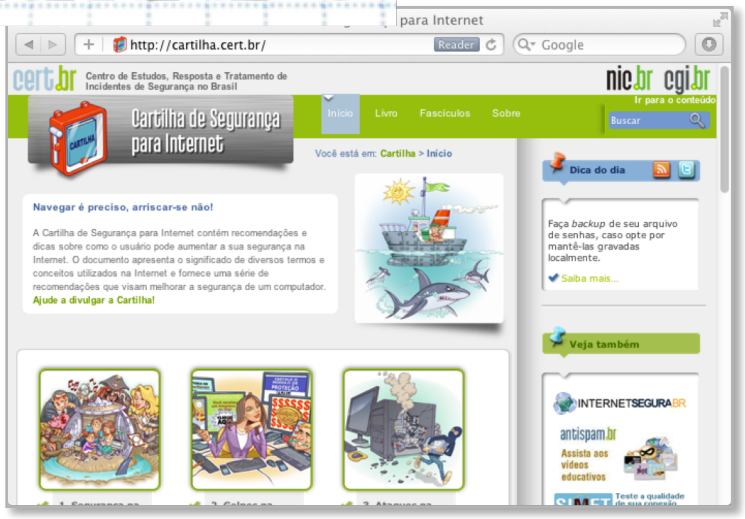
para **60+**

para **Técnicos**

para **Interesse Geral**

MANTENHA-SE INFORMADO

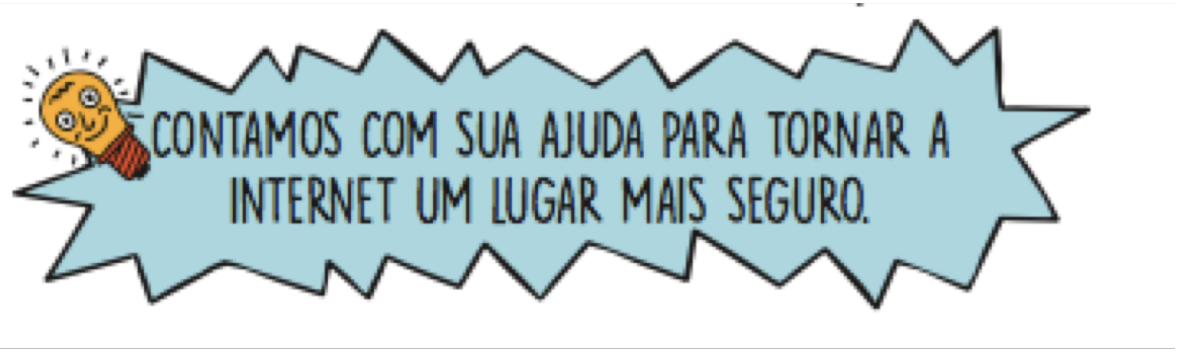
- **Cartilha de Segurança para Internet**
  - Livro (PDF e ePub)
  - Conteúdo no site
  - Fascículos e slides
  - Dica do dia no site, via Twitter e RSS



https://cartilha.cert.br/

"A Internet é como um espelho da sociedade.
Se você não gosta do que nele vê,
quebrá-lo não é a solução."

Vint Cerf, 2010, fórum em Vilna, Lituânia.



Solicitação de materiais: doc@cert.br
Instituições que desejarem imprimir os materiais podem inserir a marca como "Impresso por:"

INTERNET SEGURA.BR

Obrigada

www.cert.br

miriam@cert.br @certbr

19 de março de 2019

nic.br cgi.br

www.nic.br | www.cgi.br