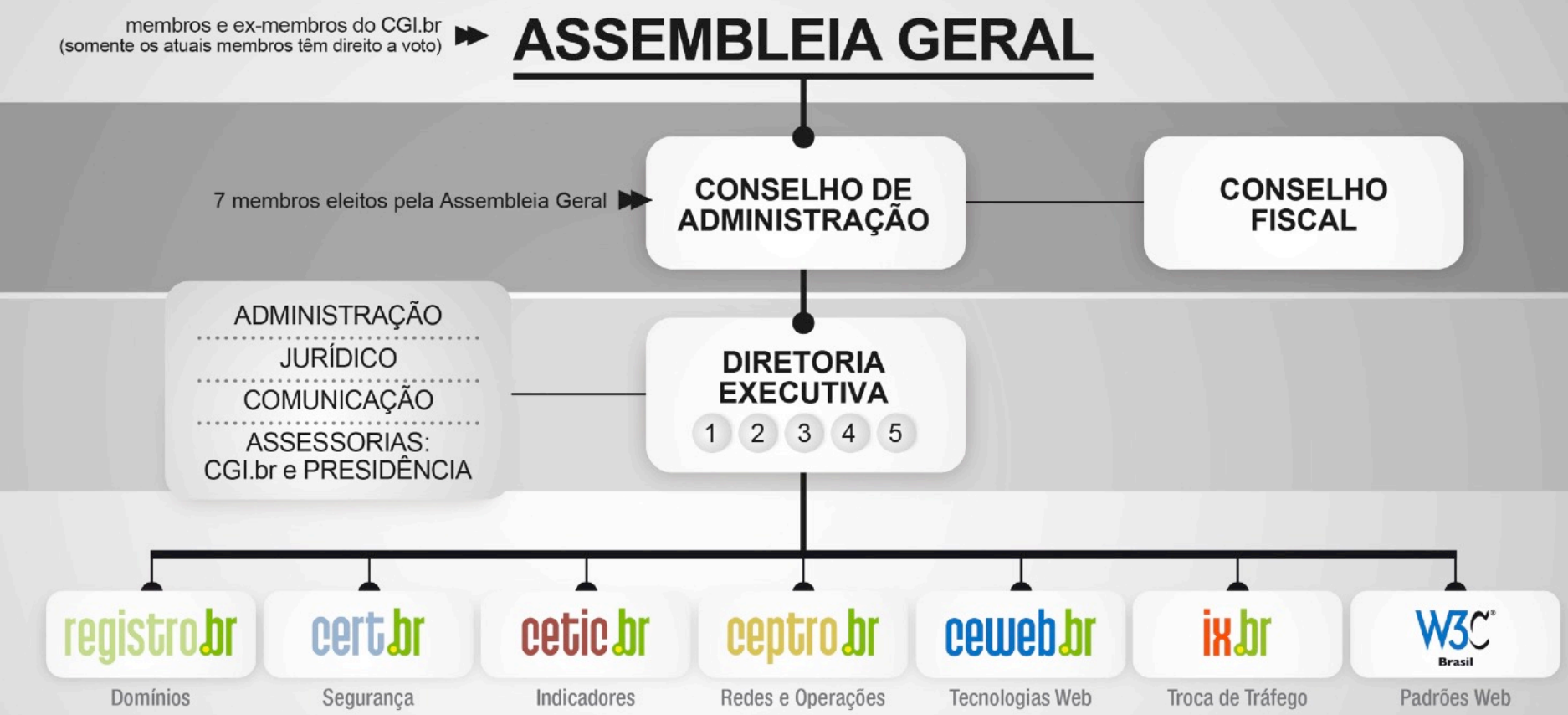
nic.br cgi.br | 20 anos cert.br

Curso de capacitação
Uso consciente e responsável da Internet
São Paulo / SP
24 de agosto de 2018

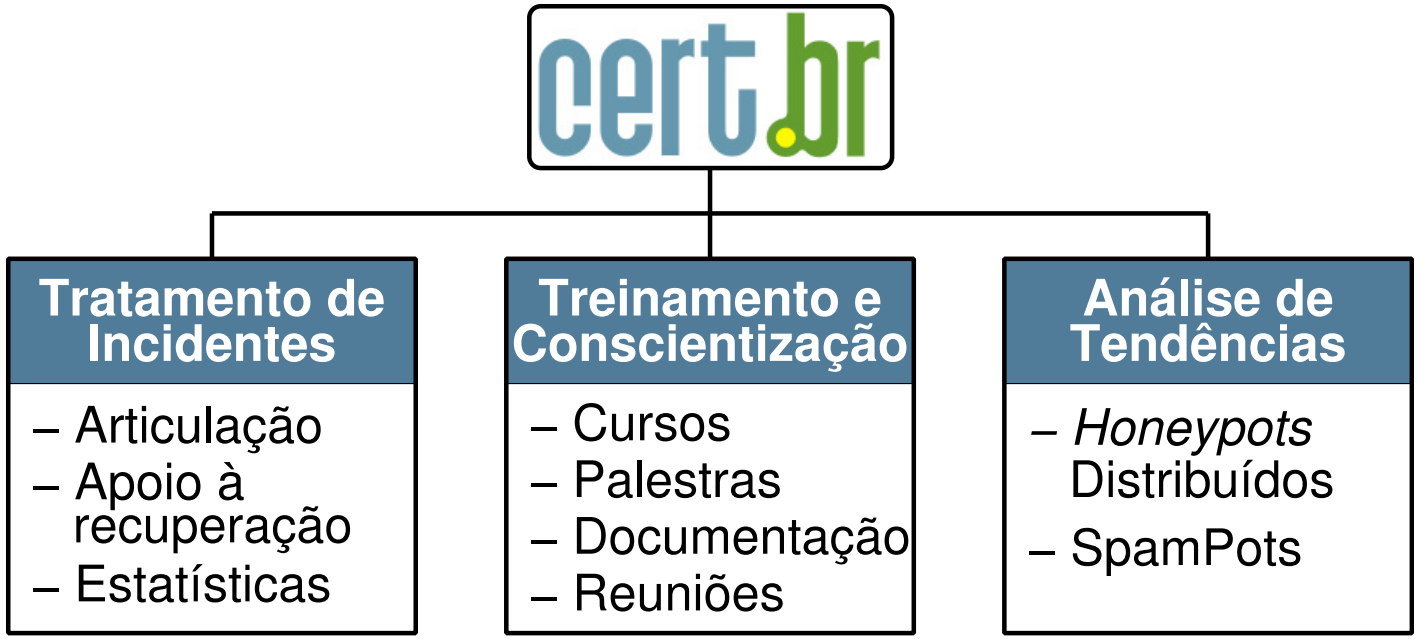
Internet Segura: proteção de contas e dispositivos
(atualizações, mecanismos de segurança, senha forte e *sites* seguros)

Miriam von Zuben
miriam@cert.br

cert.br nic.br cgi.br



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**

Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil
http://www.nic.br/grupo/historico-gts.htm | http://www.cert.br/sobre/

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

Riscos em Sistemas Conectados à Internet

- 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

Riscos

- **Uso de engenharia social**
  - exploram fragilidades de usuários
    - códigos maliciosos (*malware*)
      - vírus, *trojan*, *ransomware*, RAT, etc
    - aplicativos maliciosos
    - páginas falsas (*phishing*)
    - golpes (antecipação de recursos)

Novos desafios

- **Internet das Coisas**
  - babás eletrônicas, câmeras
- **Internet dos Brinquedos**


BRIAN BARRETT SECURITY 12.20.17 02:08 PM

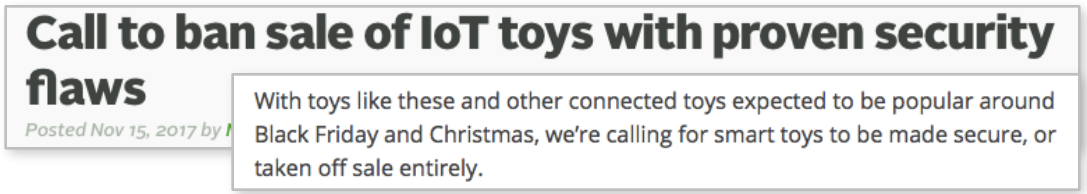
DON'T GET YOUR KID AN INTERNET-CONNECTED TOY


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

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

0 Comments

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


Call to ban sale of IoT toys with proven security flaws

Posted Nov 15, 2017 by

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/

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

July 17, 2017

Alert Number
I-071717(Revised)-PSA

uestions regarding this PSA
hould be directed to your local
BI Field Office.

ocal Field Office Locations:
ww.fbi.gov/contact-us/field

CONSUMER NOTICE: INTERNET-CONNECTED TOYS COUL PRESENT PRIVACY AND CONTACT CONCERNS FOR CHILDREN

The FBI encourages consumers to consider cyber security prior to introdu smart, interactive, internet-connected toys into their homes or trusted environments. Smart toys and entertainment devices for children are increasingly incorporating technologies that learn and tailor their behavio based on user interactions. These toys typically contain sensors, microphones, cameras, data storage components, and other multimedia capabilities – including speech recognition and GPS options. These featur could put the privacy and safety of children at risk due to the large amou of personal information that may be unwittingly disclosed.

WHY DOES THIS MATTER TO MY FAMILY?

The features and functions of different toys vary widely. In some cases, t with microphones could record and collect conversations within earshot o the device. Information such as the child's name, school, likes and dislike and activities may be disclosed through normal conversation with the toy in the surrounding environment. The collection of a child's personal information combined with a toy's ability to connect to the Internet or oth devices raises concerns for privacy and physical safety. Personal informat (e.g., name, date of birth, pictures, address) is typically provided when creating user accounts. In addition, companies collect large amounts of additional data, such as voice messages, conversation recordings, past a real-time physical locations, Internet use history, and Internet addresses, The exposure of such information could create opportunities for child ider fraud. Additionally, the potential misuse of sensitive data such as GPS location information, visual identifiers from pictures or videos, and known interests to garner trust from a child could present exploitation risks.

Any toy with Bluetooth, wi-fi connection or a mobile app that's not secured could pose a risk to your child's privacy or security. If you're shopping for a connected toy for your child, make sure you carry out these 10 vital checks:

Before buying

1 **Read the description of the connected toy carefully in the shop or online**. Find out what the toy actually does and how your child will interact with it.

2 **Check what technology it uses**. Does it require a wi-fi internet or Bluetooth connection and, more importantly, does it really need one? If you'd think twice before giving your child a internet-connected smartphone, a toy should be no different.

3 **Is there a mobile app?** If there is, what does it do and does the company talk about security features, such as usernames and passwords?

4 **Search online for the toy's name** to see if there have been any concerns raised online over its security, or how it safeguards the privacy of your child or personal data. Also, search for the manufacturer's name to see if it has had any controversies, such as a leak of customer data.

5 **Consider whether you really need a connected toy for your child**. You don't have to deny them fun, but consider whether its best to avoid having to think about internet threats until they get older.

When setting it up

1 **Submit only the minimal amount of personal data required** when setting up an account for your child. That means not too much data is exposed if things do go wrong.

2 **Read the company's T&Cs and privacy policies**, even though it's tedious. You should look for things like how your data will be stored and who has access to it. What happens if the company is hit by a cyber attack? And if a vulnerability is found with the toy, will they notify you?

3 **Download any available security updates** for the app or toy to make sure you're protected by the most recent security developments.

4 **Look for any security features available** (usually in the settings). You should be able to set passwords on any accounts, but make sure you use strong terms containing lower and upper case letters, numbers, and special characters.

5 **Keep an eye on your child when they're playing with the toy**, particularly if it can send or receive messages When they're not playing with it, make sure you turn it off.

Which? Read more at **which.co.uk/toysafety**

https://www.ic3.gov/media/2017/170717.aspx
https://www.which.co.uk/documents/pdf/connected-toy-safety-469632.pdf

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

Utilize o 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**
  - disponível em sistemas operacionais, *sites*, equipamentos ou instalado por meio de 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 conhecida
    - 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

Mediação 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
    - cursos de lógica e programação específicos
      - podem aprender certo desde o início
- **Necessidade de desmitificar as palavras "*Hack*" e "*Hacker*"**
  - outros termos: *cracker*, *whitehat*, *blackhat*, *greyhat*, *lammer*, ...
  - responsabilização por uso indevido:
    - modificações não autorizadas, *hack*, *jailbreak*, furto de identidade, linguagem inadequada
      - consequências: perda de "pontos"/progresso, suspensão, banimento, responsabilização jurídica

Materiais de apoio

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

PROTEJA A PRIVACIDADE DAS OUTRAS PESSOAS

INTERNET NÃO É TUDO!

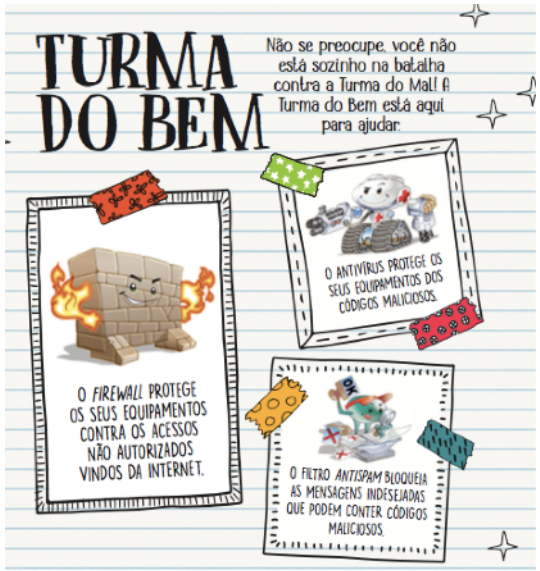
NÃO ACREDITE EM TUDO QUE VOCÊ LÊ

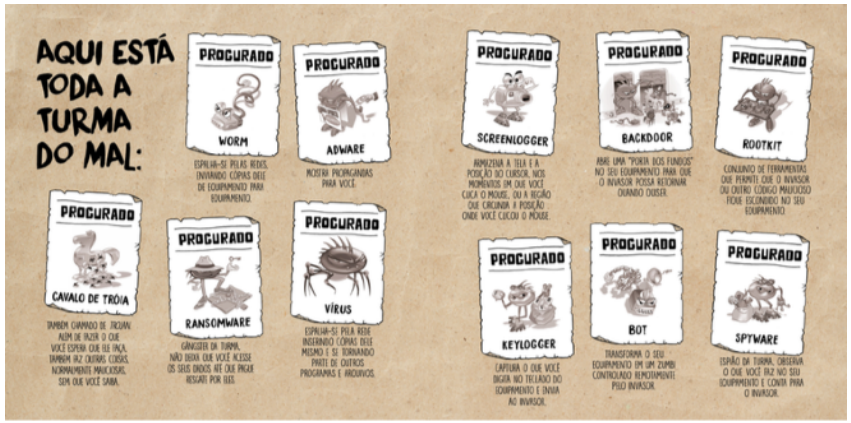
RESPEITE O TRABALHO DOS OUTROS

CUIDADO PARA NÃO PERDER SEUS EQUIPAMENTOS

PROTEJA OS SEUS EQUIPAMENTOS

PROTEJA SUAS SENHAS





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?

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

Quer se divertir e aprender a usar a Internet com segurança? Clique aqui para baixar o Guia.

Vai encarar? Conheça nossos desafios e divirta-se. Aqui você encontra caça-palavras, palavras cruzadas, dominox, desenhos para colorir e muito mais.

Pronto para conferir suas respostas? Mas não vale colar, só pode conferir depois de tentar resolver.

Está com dúvidas? Precisa de ajuda? Quer fazer alguma denúncia? Veja aqui como fazer.

MANTENHA-SE INFORMADO

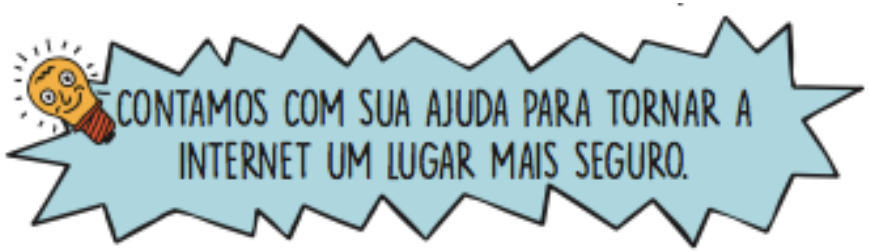
Cartilha de Segurança para Internet

- 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.



INTERNET SEGURA.BR

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

Obrigada

www.cert.br

miriam@cert.br

certbr

24 de agosto de 2018

nic.br cgi.br

www.nic.br | www.cgi.br