

nic.br egi.br

cert.br

Eletronuclear – Pausa para o café
28 de outubro de 2020
Evento *On-line*

Tratamento de Incidentes

- ▶ Articulação
- ▶ Análise Técnica
- ▶ Apoio à recuperação

Treinamento e Conscientização

- ▶ Cursos
- ▶ Palestras
- ▶ Boas Práticas
- ▶ Reuniões

Análise de Tendências

- ▶ *Honeypots* Distribuídos
- ▶ SpamPots
- ▶ Processamento de *threat feeds*

Filiações e Parcerias:



SEI
Partner
Network



Criação:

Agosto/1996: o relatório “Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil” é publicado pelo CGI.br¹

Junho/1997: o CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório²

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

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

Internet Segura para seus filhos

Miriam von Zuben
Analista de Segurança
miriam@cert.br

cert.br nic.br egi.br

Desmistificando...

“Internet é um mundo virtual”

“Internet é uma terra sem lei”

“Internet é a grande vilã da atualidade”

“Sistema 100% seguro”

“Risco zero”

“Meus equipamentos jamais serão localizados na Internet”

“Não tem nada de interessante em meus equipamentos”

Desmistificando...

“Novas gerações são mais inteligentes”

“Crianças são nativos digitais e seus pais são analfabetos digitais, por isso pais não conseguem auxiliá-las”

“Crianças estão protegidas em casa”

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

Riscos em sistemas conectados a 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

TIC Kids Online Brasil 2019

- 9 a 17 anos
 - 89% são usuários de Internet
 - 24.3 milhões de crianças e adolescentes conectados
- Celular como principal dispositivo usado (95%)
- Limitações:
 - 58% acessam exclusivamente pelo celular
 - 3 milhões não são usuários de Internet no Brasil
 - 1.4 milhão nunca usou a Internet
 - 4.8 milhões de crianças e adolescentes vivem em domicílios que não possuem acesso a rede
 - principal motivo de não acessar: não ter Internet em casa

Fonte: https://cetic.br/media/analises/tic_kids_online_brasil_2019_coletiva_imprensa.pdf

Conheça os riscos

cert.br nic.br egi.br

Tipos de 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

Exposição excessiva

- Virais, webcelebridades, publicidade
 - falta de maturidade emocional (quantidade de curtidas, comentários negativos)
- Feita também pelos próprios pais e responsáveis (*sharenting*)
 - postar fotos e vídeos que podem constrangê-los, criar perfis em nome dos filhos, postar nas redes sociais dos filhos, comentar sobre os filhos em grupos de mensagens
 - assunto difícil de ser tratado, não há um limite claro entre:
 - o direito dos pais e responsáveis de postar sobre seus filhos
 - o direito das crianças de terem a privacidade preservada
- Dica: pensar em como eles se sentirão no futuro ao ver aquilo
- Tudo que é postado pode fazer parte da reputação on-line/digital futura

Uso excessivo

- Pode acarretar em problemas físicos e psicológicos
- Equilíbrio entre qualidade e quantidade
- O que é excessivo?



<https://www.tecmundo.com.br/cultura-geek/136671-vicio-fortnite-pais-mandarem-filhos-clinicas-reabilitacao.htm>



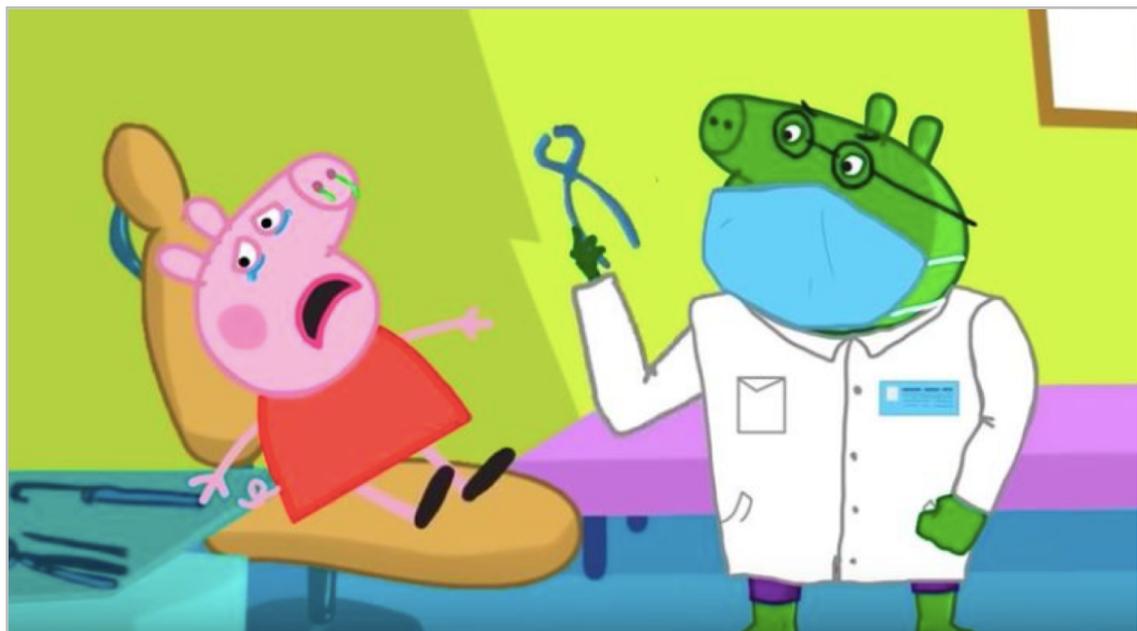
https://www.sbp.com.br/index.php?eID=cw_filedownload&file=596

Bullying e cyberbullying

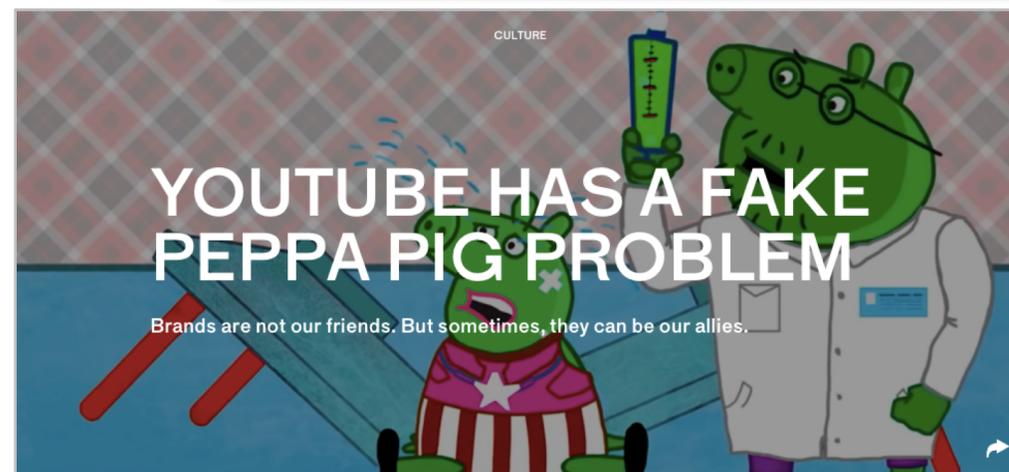
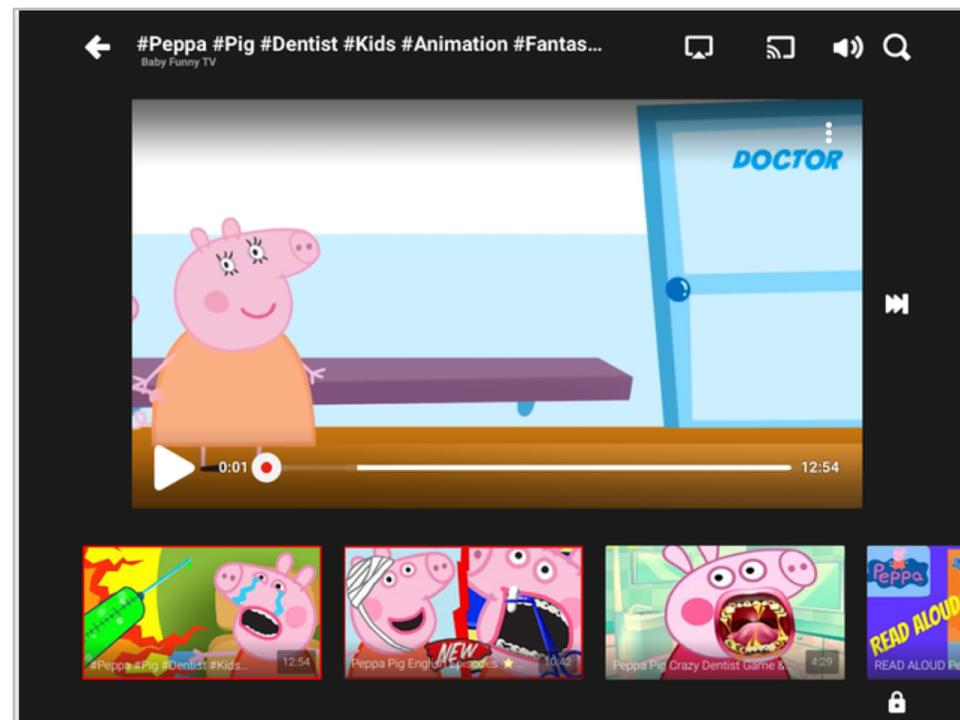
- Agressões físicas ou verbais que ocorrem várias vezes e que causam e tenham o intuito de causar dor, sofrimento e angústia a alguém
- Envolve:
 - agressor/agressores
 - vítimas
 - testemunhas
- Ficar atento a mudanças de comportamentos
- Manter o diálogo em aberto
- Explicar sobre o respeito e a empatia

Acesso a conteúdos impróprios

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



<https://theoutline.com/post/1239/youtube-has-a-fake-peppa-pig-problem>
<http://lifestyle.one/closer/entertainment/soaps/fake-peppa-pig-cartoons-youtube-disturbing-storylines/>



Phishing e outros golpes



A gamer plays "Fortnite" against Twitch streamer and professional gamer Tyler "Ninja" Blevins during Ninja Vegas '18 at Esports Arena Las Vegas at Luxor Hotel and Casino on April 21, 2018 in Las Vegas, Nevada (Getty)

FORTNITE BATTLE ROYALE EXPOSES CHILDREN TO SCAMS THAT COULD ALSO ENDANGER PARENTS, WARN EXPERTS

Malicious actors on the internet are taking advantage of children's fascination with the game

Andrew Griffin | @_andrew_griffin
Monday 9 July 2018 00:59 | 2 comments

Click to follow The Independent Tech

<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>

'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.



CYBER SECURITY PHISHING SOCIAL MEDIA

Instagram's Ugly List

Andrew Hickey | September 23, 2016

CBS: 'Ugly List' Instagram Phishing Scam Targets Children, Young Users

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.

in f t



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 roughly 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



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



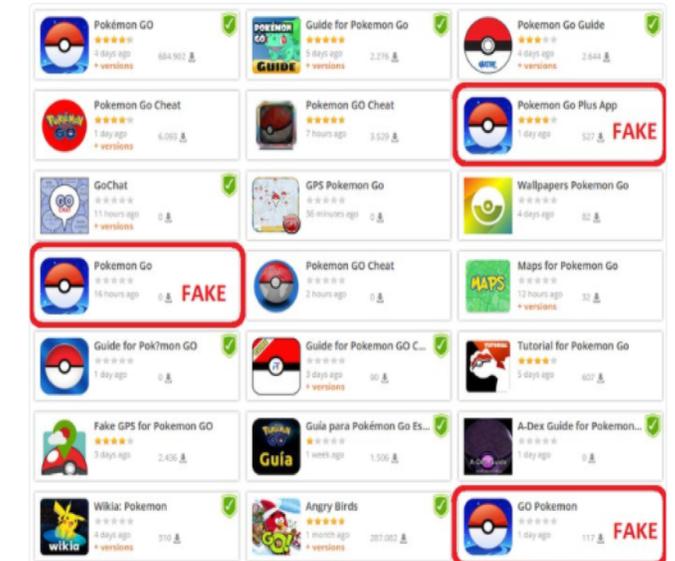
Antony Leather, CONTRIBUTOR
I'm passionate about gadgets, PC hardware and computer modding. [FULL BIO](#) ✓
Opinions expressed by Forbes Contributors are their own.

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 than 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 *Pokémon Go* are downloading ransomware onto users' phones.



Rigo Technology
@rigotechnology



Watch out for fake *Pokémon Go* apps on 3rd party stores. It may contain malware. #PokémonGO #malware

1:06 AM - 19 Jul 2016



<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>

Invasão de privacidade

News > Technology News

'My Friend Cayla' Doll Records Children's Speech, Is Vulnerable to Hackers

Consumer groups say the doll, which has a microphone and uses Bluetooth to transmit audio recordings via the Internet, poses both a security and a privacy threat.

By David Emery

Feb 24th, 2017



Boneca que pode espionar famílias teve a venda proibida na Alemanha

Cayla tem microfone e conexão bluetooth embutidos; o que é considerado ferramentas de espionagem

The Switch

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

by [Ayley Tsukayama](#) December 1, 2015



The Switch

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

By [Andrea Peterson](#) November 30, 2015

<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/>

<http://www.snopes.com/2017/02/24/my-friend-cayla-doll-privacy-concerns/>

http://www.em.com.br/app/noticia/internacional/2017/02/17/interna_internacional,848314/boneca-que-pode-espionar-familias-teve-a-venda-proibida-na-alemanha.shtml

**Ajude seus filhos a
se protegerem**

cert.br nic.br egi.br

Necessidade de mediação

- Mediação restritiva:
 - proibições reduzem os riscos mas 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 e estimular o pensamento crítico
 - conhecer, entender e reconhecer os riscos ajuda a preveni-los
 - papel das escolas e dos pais
 - 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

Como os pais podem ajudar

- Sendo um exemplo (“influenciador digital”)
- Estimulando o diálogo
- Reforçando os cuidados com estranhos
- Ensinando sobre privacidade
- Observando o comportamento
- Estabelecendo regras e fazendo combinados
- Ajudando a protegerem seus equipamentos

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
- Desenvolver o pensamento crítico

Proteger os equipamentos

- Manter os equipamentos seguros
 - com a versão mais recente do sistema operacional e dos aplicativos
 - com todas atualizações aplicadas
- Usar as opções de configuração disponíveis
- Usar e manter 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



Proteger 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
- Usar programas gerenciadores de contas/senhas
- Habilitar a verificação em duas etapas



Outros cuidados

- Fazer *backups*
 - devem ser mantidos desconectados
- Postura preventiva
 - ser cuidadoso ao abrir anexos, clicar em *links*, baixar aplicativos e acessar páginas Web
- Proteger a privacidade
 - diminuir a quantidade de dados expostos



Materiais de apoio

cert.br nic.br egi.br

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



para Crianças



para Adolescentes



para Pais e Educadores



para 60+



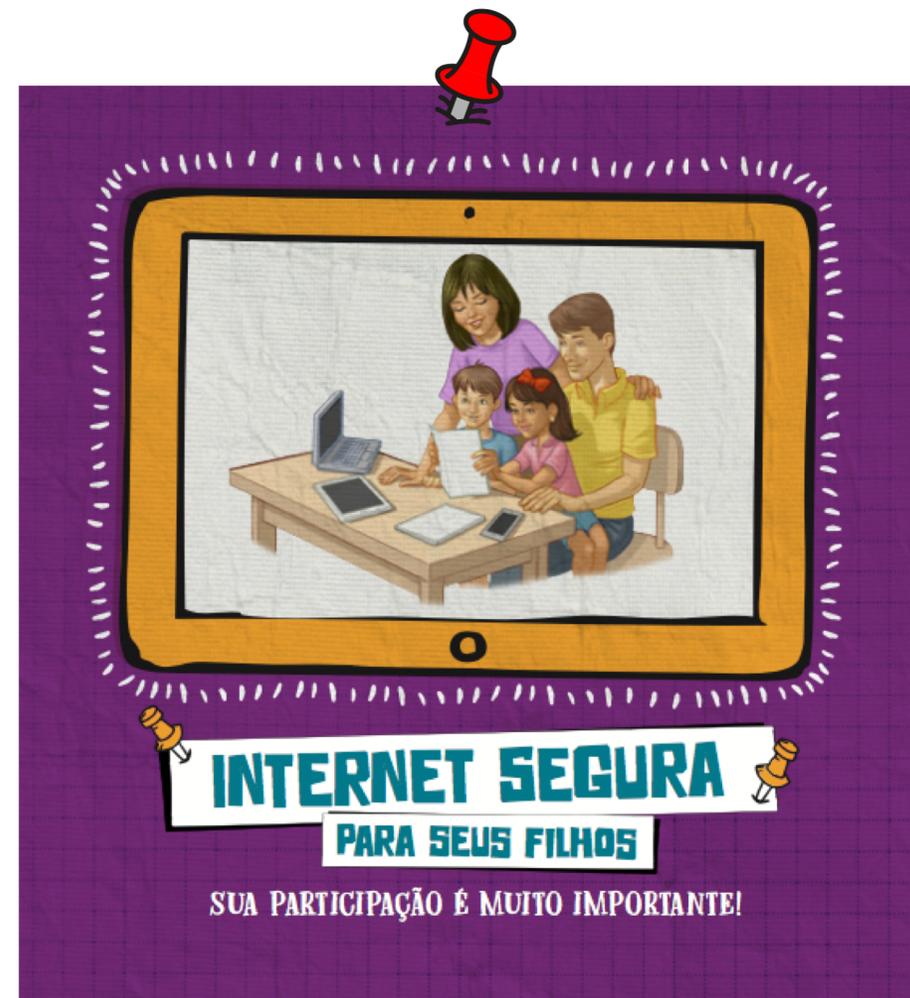
para Técnicos



para Interesse Geral

<https://internetsegura.br/>

Guias Internet Segura



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

PROTEJA A SUA PRIVACIDADE

RESPEITE O TRABALHO DOS OUTROS

CUIDADO COM PESSOAS ESTRANHAS OU QUE VOCÊ CONHECE APENAS PELA INTERNET

ESCREVA E FALE CORRETAMENTE

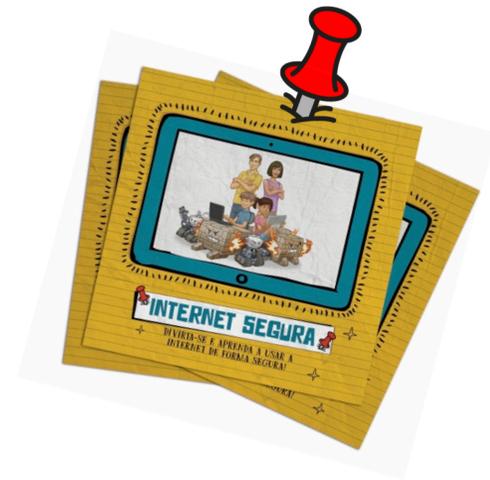
RESPEITE OS LIMITES DE IDADE

PROTEJA A PRIVACIDADE DAS OUTRAS PESSOAS

INTERNET NÃO É TUDO!

NÃO ACREDITE EM TUDO QUE VOCÊ LÊ

CUIDADO PARA NÃO PERDER SEUS EQUIPAMENTOS



PROTEJA OS SEUS EQUIPAMENTOS

PROTEJA SUAS SENHAS

AQUI ESTÁ TODA A TURMA DO MAL:

PROCURADO WORM ESPALHA-SE PELAS REDES, ENVIANDO CÓPIAS DE SEU EQUIPAMENTO PARA EQUIPAMENTOS.	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 ESCONDIRADO 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 GANGSTER DA TURMA, NÃO DIXA QUE VOCÊ ACESSE OS SEUS DADOS ATÉ QUE PAGUE RESGATE POR ELES.	PROCURADO VIRUS ESPALHA-SE PELA REDE INSERINDO CÓPIAS DE SEU MESMO E SE TORNANDO PARTE DE OUTROS PROGRAMAS E ARQUIVOS.	PROCURADO KEYLOGGER CAPTURA O QUE VOCÊ DIGITA NO TECLADO DO EQUIPAMENTO E ENVAIA AO INVASOR.	PROCURADO BOT TRANSFORMA O SEU EQUIPAMENTO EM UM ZUMBI CONTROLADO REMOTAMENTE PELO INVASOR.	PROCURADO SPYWARE ESPION DA TURMA, OBSERVA O QUE VOCÊ FAZ NO SEU EQUIPAMENTO E ENVIA 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.

 O FIREWALL PROTEGE OS SEUS EQUIPAMENTOS CONTRA OS ACESSOS NÃO AUTORIZADOS vindos da INTERNET.	 O ANTIVÍRUS PROTEGE OS SEUS EQUIPAMENTOS DOS CÓDIGOS MALICIOSOS.
 O FILTRO ANTISPAM BLOQUEIA AS MENSAGENS INDESEJADAS QUE PODEM CONTER CÓDIGOS MALICIOSOS.	

Desafios



nic.br

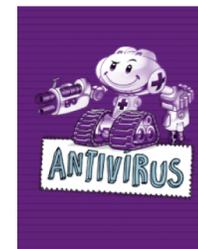


Sobre | Outras iniciativas

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 Cavalos 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.



•Acesso a conteúdos impróprios

•Contato com estranhos

•Uso excessivo

•Superexposição

•Exposição da privacidade

•Dificuldade de exclusão

•Cyberbullying

•Brincadeiras perigosas

•Códigos maliciosos e *phishing*



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



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?

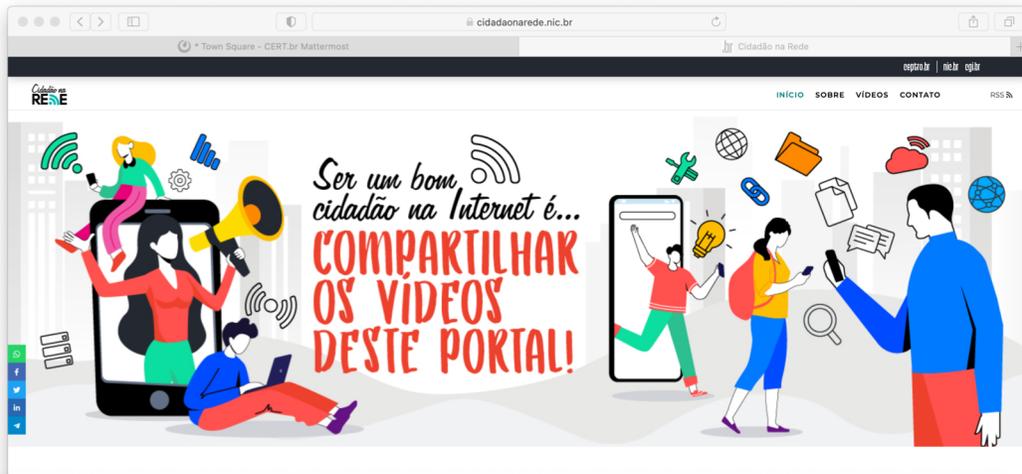
MANTENHA-SE INFORMADO

- **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/>



Início / Vídeos / Uso responsável e deveres na Internet

USO RESPONSÁVEL E DEVERES NA INTERNET

Nem tudo é brincadeira

Cyberbullying: e se fosse com você?

Não se deixe enganar, nem toda piada feita às custas de outra pessoa pode soar como uma simples brincadeira. O que pode parecer inocente ou muito engraçado para alguém, pode ter um impacto extremamente negativo no outro. Bullying ou Cyberbullying pode trazer consequências sérias.

USO RESPONSÁVEL E DEVERES NA INTERNET
Postado em 22/10/2020

A lei protege seus direitos também na Internet

Comprei on-line e me arrependi! O que fazer?

Fez uma compra on-line e se arrependeu, o que fazer? O Código de Defesa do Consumidor garante alguns direitos especiais para compras feitas fora do estabelecimento comercial, por exemplo, via Internet.

USO RESPONSÁVEL E DEVERES NA INTERNET
Postado em 22/10/2020

PODE SER UM ... BOATO

Boatos

A Internet está repleta de notícias, mas será que todas são verdadeiras? Cuidado ao compartilhar! E na dúvida, não compartilhe!

USO RESPONSÁVEL E DEVERES NA INTERNET
Postado em 22/10/2020

SEGURANÇA

Verifique se o site é SEGURO

Navegação segura

Tome cuidado com os sites que acessa! Será que eles são seguros? Entenda como identificar isso e navegar com segurança!

SEGURANÇA
Postado em 22/10/2020

Você não precisa ter uma super memória!

Gerenciador de senhas

Cada novo cadastro é mais uma senha para decorar! Quantas senhas uma pessoa comum consegue guardar na memória? Gerenciadores de senha estão aí para ajudar a administrar todas as senhas de maneira segura.

SEGURANÇA
Postado em 22/10/2020

Verificação em duas etapas protege ainda + suas contas

Verificação em dois fatores

Usar mais de um fator de segurança pode fazer a diferença na hora em que pessoas mal intencionadas tentarem invadir sua conta. Proteja suas contas!

SEGURANÇA
Postado em 22/10/2020

Não arrisque seus dados

Senhas Variadas

Na hora de criar uma nova senha sempre vem aquela vontade de usar uma das que você já utiliza, não é? Isso pode ser muito perigoso!

SEGURANÇA
Postado em 22/10/2020

VAI CRIAR UMA SENHA?

Senhas Seguras

Existem diversas práticas importantes para criar uma senha mais segura. Este vídeo mostra uma delas. Aprenda a proteger seus dados, criando boas senhas.

SEGURANÇA
Postado em 22/10/2020

<https://cidadaonarede.nic.br/>

Curso Online Filhos Conectados

- Dividido em 12 capítulos:
 - Duração média de 5 minutos cada capítulo – total 3 horas de duração
- Alguns capítulos:
 - Os 8 segredos para os (as) filhos (as) terem boas ações no uso da Internet
 - Exposição na Internet
 - Nudes
 - Bullying e Cyberbullying
 - Postar e compartilhar
 - Dá para apagar o que se publica na Internet
 - Meu (minha) filho (a) quer ser youtuber, e agora?
 - Desafios perigosos na Internet
 - Softwares de controle parental e configurações de privacidade

<https://cursoseventos.nic.br/curso/curso-online-filhos-conectados/>

fe.seg.br

#FIQUE ESPERTO

Dicas | Sobre a campanha

Dicas de segurança contra diversos tipos de fraudes.



PROTEJA SUAS CONTAS COM SENHAS FORTES E DUPLO FATOR DE AUTENTICAÇÃO



NUNCA USE A MESMA SENHA EM DIFERENTES SERVIÇOS



SEMPRE HABILITE OS MECANISMOS DE DUPLA AUTENTICAÇÃO FORNECIDOS, POR MEIO DE OUTRAS FERRAMENTAS DE AUTENTICAÇÃO OU MESMO VIA SMS, ESPECIALMENTE NOS APLICATIVOS DE MENSAGENS E REDES SOCIAIS. DESSA FORMA, SE ALGUÉM DESCOBRIR SUA SENHA, NÃO CONSEGUIRÁ ACESSAR A CONTA

<https://fe.seg.br/>



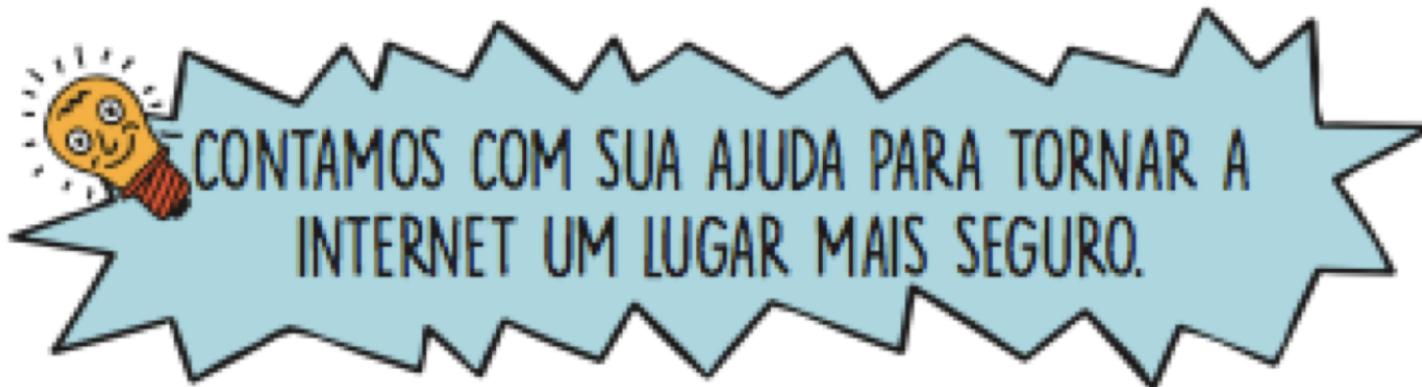
<https://workshopexposicaoainternet.nic.br/>

Desmistificando...

“É tudo culpa da Internet...”

*“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.



Obrigada

www.cert.br

© miriam@cert.br

© @certbr

28 de outubro de 2020

nic.br cgi.br

www.nic.br | www.cgi.br