nic.br cgi.br | cert.br

5º Congresso Brasileiro e Latino-Americano de IoT

20 a 23 de outubro de 2020

Evento *Online*

PAINEL:
Segurança do Consumidor de Soluções IoT

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

cert.br nic.br cgi.br

Singapore home cams hacked and stolen footage sold on pornographic sites

Group behind hacking claims it has shared 3TB worth of clips with subscribers who paid $200 for its service

David Sun

Oct 12, 2020 06:00 am

2033 Engagements

Security cameras in Singapore homes have been hacked, with the footage stolen and shared online.

Clips from the hacked footage have been uploaded on pornographic sites recently, with several explicitly tagged as being from Singapore.

A screen shot of a video taken by a security camera in what looks like a Housing Board flat in Singapore. Other videos were more explicit. PHOTO: INTERNET

https://www.tnp.sg/news/singapore/hackers-hawk-explicit-videos-taken-spore-home-cams

Alerta à População - Câmeras de Segurança

por imprensa — publicado 01/04/2020 15h30, última modificação 02/04/2020 11h21

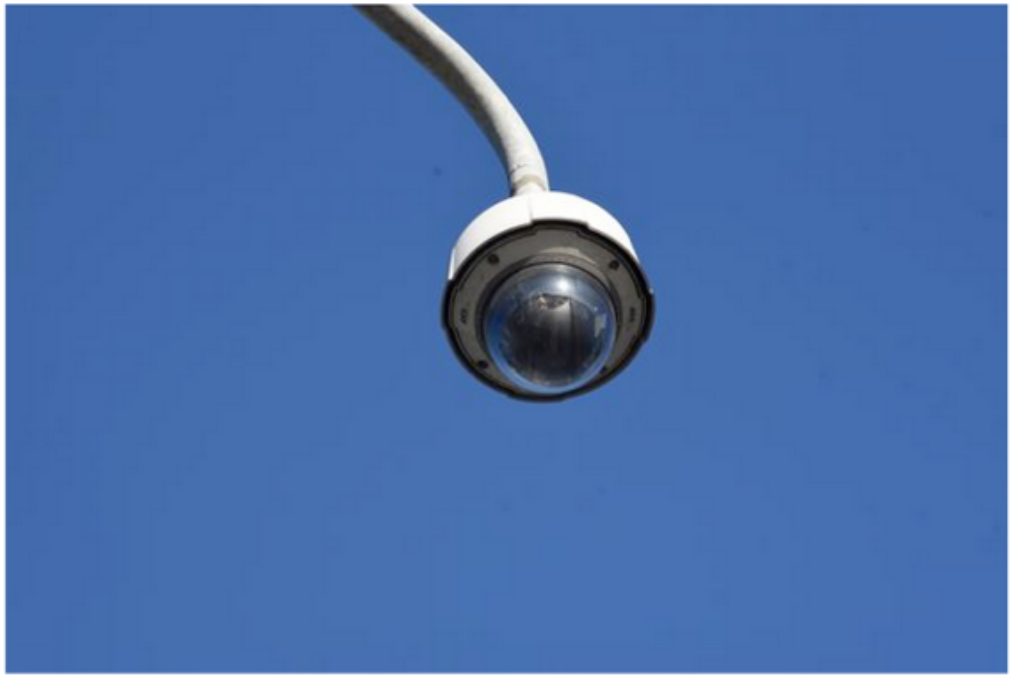
http://www.pf.gov.br/imprensa/materias_banner/aviso-cameras-de-seguranca

PF descobre invasão de babás eletrônicas e câmeras residenciais

Os investigadores da Unidade de Repressão a Crimes de Ódio e Pornografia Infantil da Polícia Federal já identificaram a invasão de 141 equipamentos na residência de famílias que vivem em 35 municípios do País

Agência Estado
atende.ae@estadao.com

Publicado em 07/04/2020 às 15h15



Uma investigação da Polícia Federal identificou que criminosos estão invadindo dispositivos eletrônicos residenciais em diversas regiões do Brasil. Crédito: Ricardo Medeiros

https://www.agazeta.com.br/brasil/pf-descobre-invasao-de-babas-eletronicas-e-cameras-residenciais-0420

Hackers stole a casino's high-roller database through a thermometer in the lobby fish tank

Oscar Williams-Grut Apr 15, 2018, 12:32 PM

https://www.insider.com/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4

ars TECHNICA SUBSCRIBE SIGN IN

*INTERNET OF SH*T —*

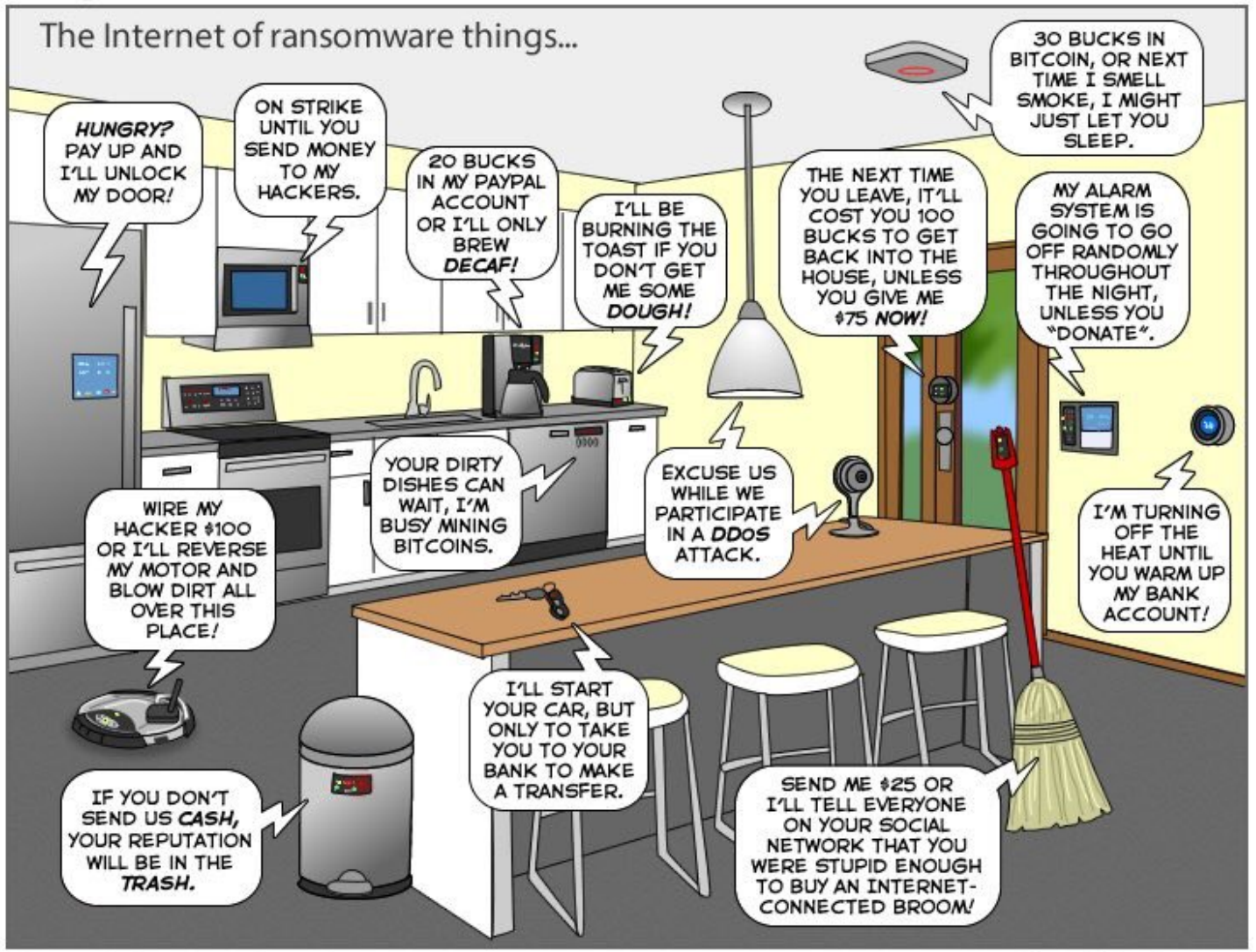
When coffee makers are demanding a ransom, you know IoT is screwed

Watch along as hacked machine grinds, beeps, and spews water.

DAN GOODIN - 9/26/2020, 11:58 AM

https://arstechnica.com/information-technology/2020/09/how-a-hacker-turned-a-250-coffee-maker-into-ransom-machine/
https://decoded.avast.io/martinhron/the-fresh-smell-of-ransomed-coffee/

The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com

St. Jude Medical drops after Muddy Water findings of 'negligent product design'

PUBLISHED THU, AUG 25 2016·4:43 PM EDT | UPDATED THU, AUG 25 2016·4:43 PM EDT

Richard Washington
@HTTPS://WWW.LINKEDIN.COM/IN/RICHARD-WASHINGTON-58A506100/
@IAMRICHWASH

SHARE

In a report published Thursday, the short selling firm suggested the recall and remediation of St. Jude Medical's cardiac devices. Such an event would result in roughly a 50 percent decrease in St. Jude Medical's revenue for the next two years — the estimated period for remediation.

(In)Segurança em IoT

Segurança é negligenciada

- até mesmo em dispositivos de segurança!
- “é problema da equipe de segurança”

Maioria dos fabricantes ainda repete velhos erros:

- autenticação falha ou inexistente
  - com senhas padrão comum, senhas *hardcoded*, contas ocultas (*backdoors*)
- protocolos obsoletos, sem criptografia (ex: Telnet)
- serviços desnecessários ativos por padrão

Poucos fabricantes possuem ciclo de vida de suporte/*updates*

- mecanismo de *bug report*
- distribuição de *updates*
- políticas claras

Como melhorar o cenário?

cert.br nic.br cgi.br

Solução depende de diversos atores

- Fabricantes
- Desenvolvedores
- Área acadêmica
- Administradores
- Usuários

O que devemos demandar do mercado? Desenvolvedores/Fabricantes/Indústria

Segurança *by design* e *by default*

- não opcional
- considerar requisitos de segurança desde o início projeto
- implementar padrões (versões correntes)
- usar boas práticas de desenvolvimento seguro
- configurações padrão de fábrica seguras
  - restritiva ao invés de permissiva

***Updates* e gerenciamento remoto**

- Deve ser possível e deve ser seguro (*supply chain attacks*)

Planejar para fazer *updates* em larga escala

Idealmente ter grupo de resposta a incidentes de segurança em produto preparado para lidar com os problemas (PSIRT)➔ Maturity

Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition

Requisitos mínimos de segurança:

- Um *checklist* de referência para aquisição de equipamentos

Trabalho desenvolvido no LAC-AAWG – *Latin American and Caribbean Anti-Abuse Working Group*

- Editora: Lucimara, *Chair* LAC-AAWG / CERT.br

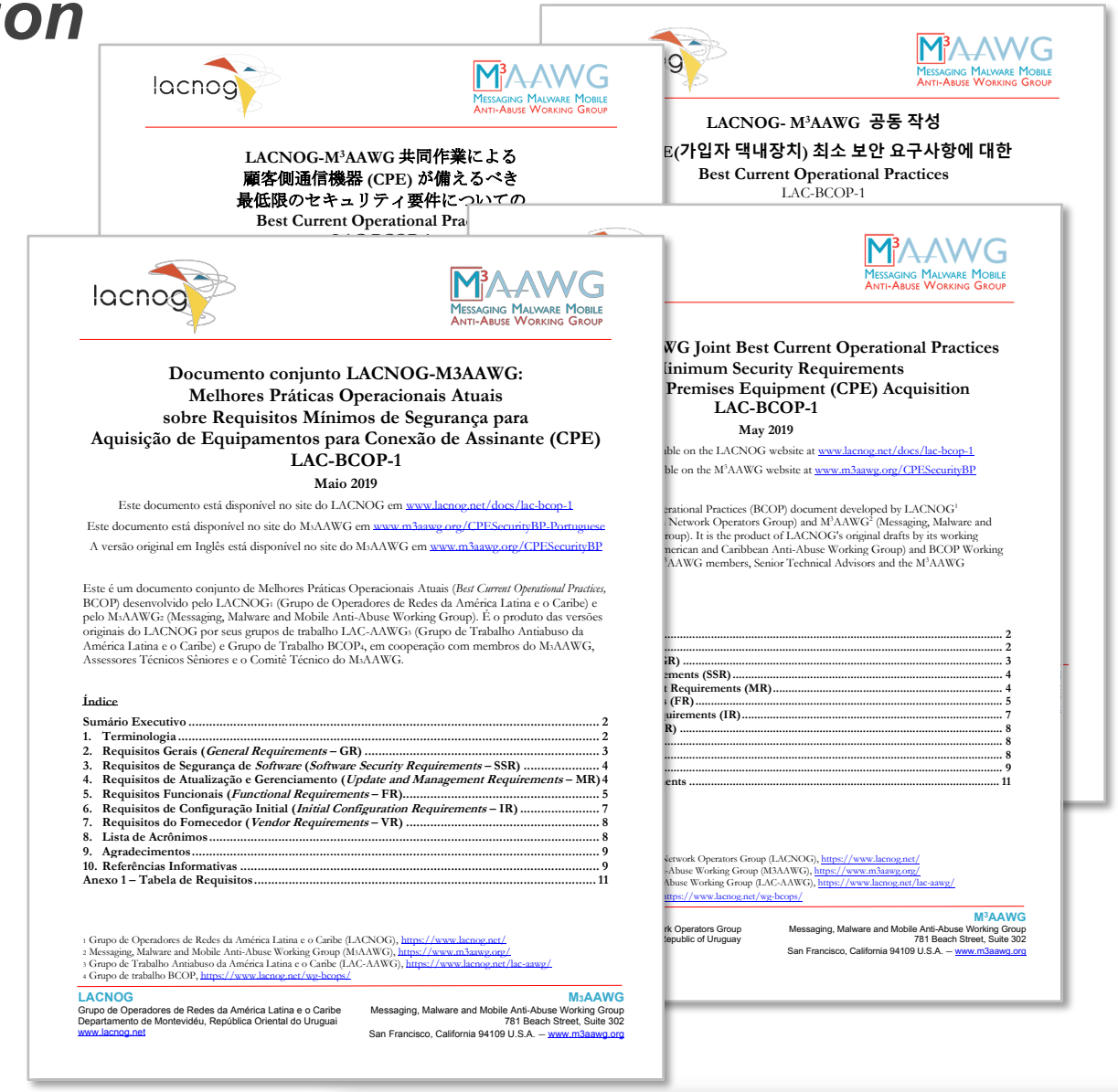
Publicação conjunta:

- **M³AAWG** - *Messaging, Malware and Mobile Anti-Abuse Working Group*
- **LACNOG** - *Latin American and Caribbean Network Operators Group*

Disponível em:

Português, Inglês, Japonês e Koreano

www.m3aawg.org/CPESecurityBP
www.lacnog.net/docs/lac-bcop-1
www.m3aawg.org/CPESecurityBP-Portuguese



Solução depende de diversos atores (cont.)

Área acadêmica

- ensinar segurança / programação segura já nos primeiros anos
- ensinar gerenciamento de riscos (negócio)

Administradores

- Manter softwares e firmwares atualizados
- Desabilitar serviços desnecessários
- Ser cuidadoso ao usar e elaborar senhas
  - se disponível, usar verificação em duas etapas
- Planejar a implantação antecipadamente
  - segregar redes
  - como gerenciar remotamente
  - como fazer *updates*

Usuários

Antes de comprar

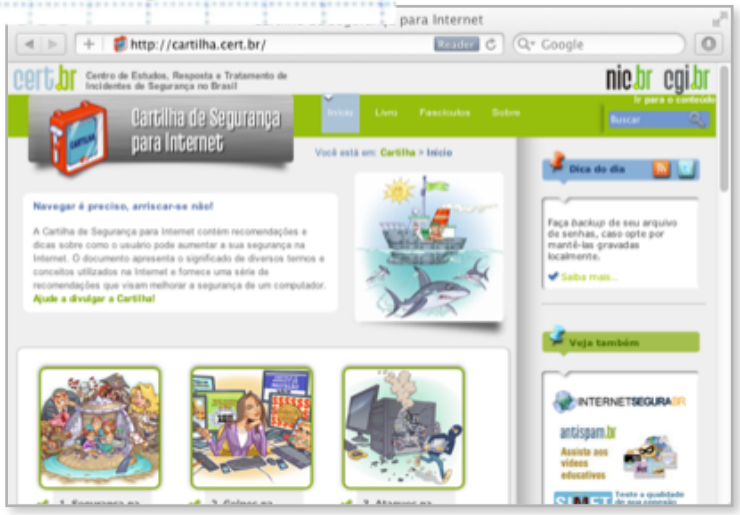
- ser criterioso ao escolher o fabricante
  - verificar se possui política de atualização de *firmware*
  - verificar histórico de tratamento de vulnerabilidades

Assumir que os dispositivos virão com problemas

- mantê-los atualizados
- desabilitar o acesso remoto se não for necessário
- **alterar as senhas padrão**
- desabilitar serviços desnecessários (*hardening*)

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/

Conscientização:
Portal InternetSegura.br

Conscientização:
Materiais sob Licença Creative Commons

Segurança na INTERNET

Faça sua parte e todos teremos uma Internet mais segura!

Já há muito tempo que segurança na Internet não é um assunto somente de interesse de um público especializado. Com a iniciativa InternetSegura.br, o NIC.br produz e disponibiliza gratuitamente uma série de materiais, em diversos formatos, que orientam diferentes públicos sobre o uso seguro da Internet.
www.internetsegura.br

Catálogo de materiais e iniciativas do NIC.br

Formato impresso, colorido e permite inclusão de logo de parceiros de impressão

para Crianças

Guia Internet Segura
Apresenta conceitos de segurança na Internet de forma lúdica, com atividades para colorir, palavras cruzadas, desafios cifrados, dicas, complete a frase, caça-palavras, entre outros.

Desafios
Contém tanto os desafios do guia Internet Segura como materiais adicionais, atualizados periodicamente.
internetsegura.br/desafios

para Adolescentes

Encarte #FikDik
Encarte do guia #Internet com Responsa - Cuidados e Responsabilidades no Uso da Internet, que apresenta os principais cuidados, riscos e consequências do uso inadequado da Internet de forma resumida.

para Pais e Educadores

Guia Internet Segura para seus filhos
Informações para pais e responsáveis sobre como proteger os filhos, seja zelando pela privacidade das crianças, ou utilizando tecnologias de controle parental.

Guia #Internet com Responsa - Cuidados e responsabilidades no uso da Internet
Orienta pais, responsáveis e educadores de adolescentes em temas sensíveis, como exposição excessiva na Internet, liberdade de expressão e danos à imagem e reputação, *cyberbullying*, danos e riscos da prática de nude, *selfie*, entre outros. Acompanha o encarte #FikDik

Guia #Internet com Responsa na sua Sala de Aula
Explica os desafios do uso da Internet a partir da exposição excessiva, dos direitos e possíveis danos à imagem dos professores e alunos, e dos limites da liberdade de expressão.

Slides: Fascículos da Cartilha de Segurança para Internet
Slides para a divulgação de boas práticas sobre o uso seguro da Internet. Há versões de apoio para professores, com notas explicativas.
Disponíveis em formatos PowerPoint (.ppt), LibreOffice (.odp), PDF sem notas explicativas e PDF com notas explicativas.
cartilha.cert.br/downloads

VEJA TAMBÉM

Curso de Formação de Professores Multiplicadores para o Uso Consciente e Responsável da Internet:
cursointernetcomresponsa.nic.br

Materiais de referência:

TIC Kids Online Brasil
Indicadores com mapeamento de possíveis riscos e oportunidades *on-line* a partir dos usos que crianças e adolescentes de 9 a 17 anos fazem da Internet. Contém dados distintos para "crianças e adolescentes" e "pais e responsáveis".
cetic.br/pesquisa/kids-online

TIC Educação
A pesquisa entrevista alunos, professores, coordenadores pedagógicos e diretores para mapear o acesso, o uso e a apropriação das tecnologias de informação e comunicação (TIC) em escolas públicas e privadas de educação básica.
cetic.br/pesquisa/educacao

Para quem tem 60 anos ou mais

#Internet com Responsa 60+: Cuidados e responsabilidades no uso da Internet
Apresenta cuidados específicos para essa faixa etária, pois esse ambiente repleto de informações e oportunidades também oferece alguns riscos para quem ingressou no uso das novas tecnologias recentemente.

para Técnicos

Portal BCP e Programa Por uma Internet Mais Segura
Reúne um conjunto de boas práticas operacionais para Sistemas Autônomos (ASs) conectados à Internet. São destacadas algumas práticas que, embora extremamente importantes, ainda não são adotadas amplamente pelos ASs brasileiros.
O portal também disponibiliza conteúdos e iniciativas direcionadas à comunidade de operadores de redes e serviços que formam a Internet por meio do **Programa por uma Internet Mais Segura.**
bcp.nic.br

VEJA TAMBÉM

Curso de Boas Práticas Operacionais para Sistemas Autônomos – Presencial:
bcp.nic.br/curso-bcop

Curso "*Fundamentals of Incident Handling*"
cert.br/cursos/fih/

Curso "*Advanced Topics in Incident Handling*"
cert.br/cursos/atih/

Interesse geral

Cartilha de Segurança para Internet
Documento com recomendações e dicas sobre como o usuário de Internet deve se comportar para aumentar a sua segurança e se proteger de possíveis ameaças. Apresenta o significado de diversos termos e conceitos utilizados na Internet, aborda os riscos de uso desta tecnologia e fornece uma série de dicas e cuidados a serem tomados pelos usuários.
Também disponível em **cartilha.cert.br** e em espanhol em cartilla.cert.br

Fascículos da Cartilha de Segurança para Internet
Aborda tópicos específicos contidos na Cartilha de Segurança para Internet e complementa conteúdos que não estavam disponíveis à época da última edição da Cartilha, como Boatos, cuidados atualizados para Redes Sociais e Códigos Maliciosos. Também disponíveis em **cartilha.cert.br/fasciculos** e em espanhol em cartilla.cert.br/fasciculos.

Guia #Internet com Responsa Vai às Compras
Detalha os cuidados necessários para realizar compras na Internet de forma responsável, além de enfatizar a importância de exercer direitos previstos no Código de Defesa do Consumidor.

Portal Antispam.br
Fonte de referência imparcial e embasada tecnicamente sobre o *spam*. Contém desde informações para administradores de redes e usuários finais, incluindo vídeos que abordam de forma simples e divertida os perigos aos quais os usuários estão expostos, explicam o que é *spam* e dão dicas de como navegar com mais segurança na rede.
antispam.br

VEJA TAMBÉM

Materiais de referência:

Caderno CGI.br "Combate ao spam na Internet no Brasil"
Histórico e reflexões sobre o combate ao spam e a gerencia da porta 25 coordenados pelo Comitê Gestor da Internet no Brasil.
cgi.br/publicacao/combate-ao-spam-na-internet-no-brasil

DISTRIBUIÇÃO DOS MATERIAIS
O NIC.br tem o compromisso de atender todos os interessados em seus materiais, da forma mais racional possível. Para que o máximo de interessados sejam atendidos, sem desperdício, limitamos o envio de materiais a lotes de 100 unidades. Caso sua instituição tenha interesse em distribuir uma quantidade maior, teremos o prazer em disponibilizar o conteúdo para que a impressão, com seu logotipo, seja realizada de acordo com sua capacidade.

SEJA UM PARCEIRO PARA A IMPRESSÃO DOS MATERIAIS!
Escreva para **info@nic.br** solicitando a inclusão do seu logotipo e especifique quais materiais você gostaria de imprimir.

LICENCIAMENTO
O objetivo primordial da produção dos nossos materiais é o compartilhamento de conteúdo, portanto a maioria deles está disponível gratuitamente para *download* e uso sob licenças *Creative Commons*. Sua instituição pode utilizá-los livremente, sem necessidade de autorização prévia, desde que a fonte seja mencionada, o uso do material não seja comercial (venda do material) e que o conteúdo não seja alterado. Para usos específicos fora do escopo da licença, escreva para **info@nic.br**.

Confira todas as nossas publicações e atividades em nic.br.

nic.br cgi.br

Obrigada!

lucimara@cert.br

Notificações para: cert@cert.br

@certbr

www.cert.br

23 de outubro de 2020

nic.br cgi.br

www.nic.br | www.cgi.br