

nic.br cgi.br

cert.br

ITU 2020 Global CyberDrill – Regional Dialog for the America Region
September 15, 2020
Online Event

Incidents and Trends in Brazil

Dr. Cristine Hoepers
General Manager
cristine@cert.br

cert.br **nic.br** **egi.br**

Incident Management

- ▶ Coordination
- ▶ Technical Analysis
- ▶ Support for recovery

Training and Awareness

- ▶ Courses
- ▶ Presentations
- ▶ Best Practices
- ▶ Meetings

Trend Analysis

- ▶ Distributed Honeypots
- ▶ SpamPots
- ▶ Processing of threat feeds

Filiations and Partnerships:



SEI
Partner
Network



Creation:

August/1996: a report proposing a model for incident management for the country is published by the Brazilian Internet Steering Committee – CGI.br¹

June/1997: CGI.br creates CERT.br (at that time called NBSO – *NIC BR Security Office*) based on the report’s recommendations²

¹<https://www.nic.br/grupo/historico-gts.htm>

²<https://www.nic.br/pagina/gts/157>

Mission

To increase the level of security and incident handling capacity of the networks connected to the Internet in Brazil.

Constituency

Networks that use Internet Resources allocated by NIC.br (IPs or ASNs allocated to Brazil, and domains under the ccTLD .br)

Focus of the Activities

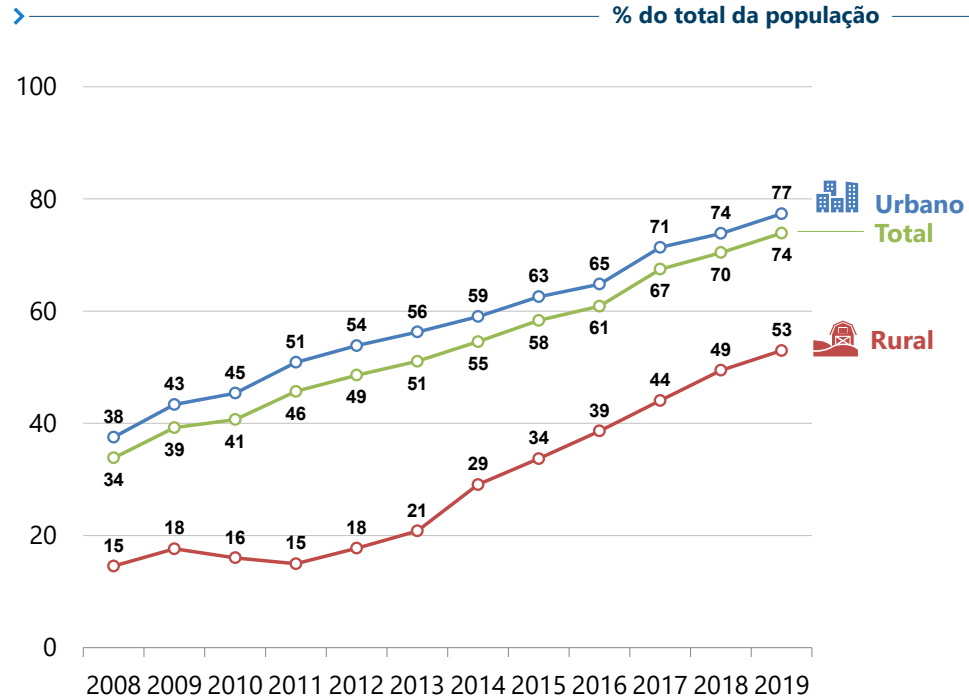
- National focal point for incident reports
- Support technical analysis and the understanding of attacks and threats
- Develop collaborative relationships with other entities
- Increase incident detection, event correlation and trend analysis in the country
- Transfer knowledge through courses, best practices and awareness materials

Brazilian Internet in Numbers

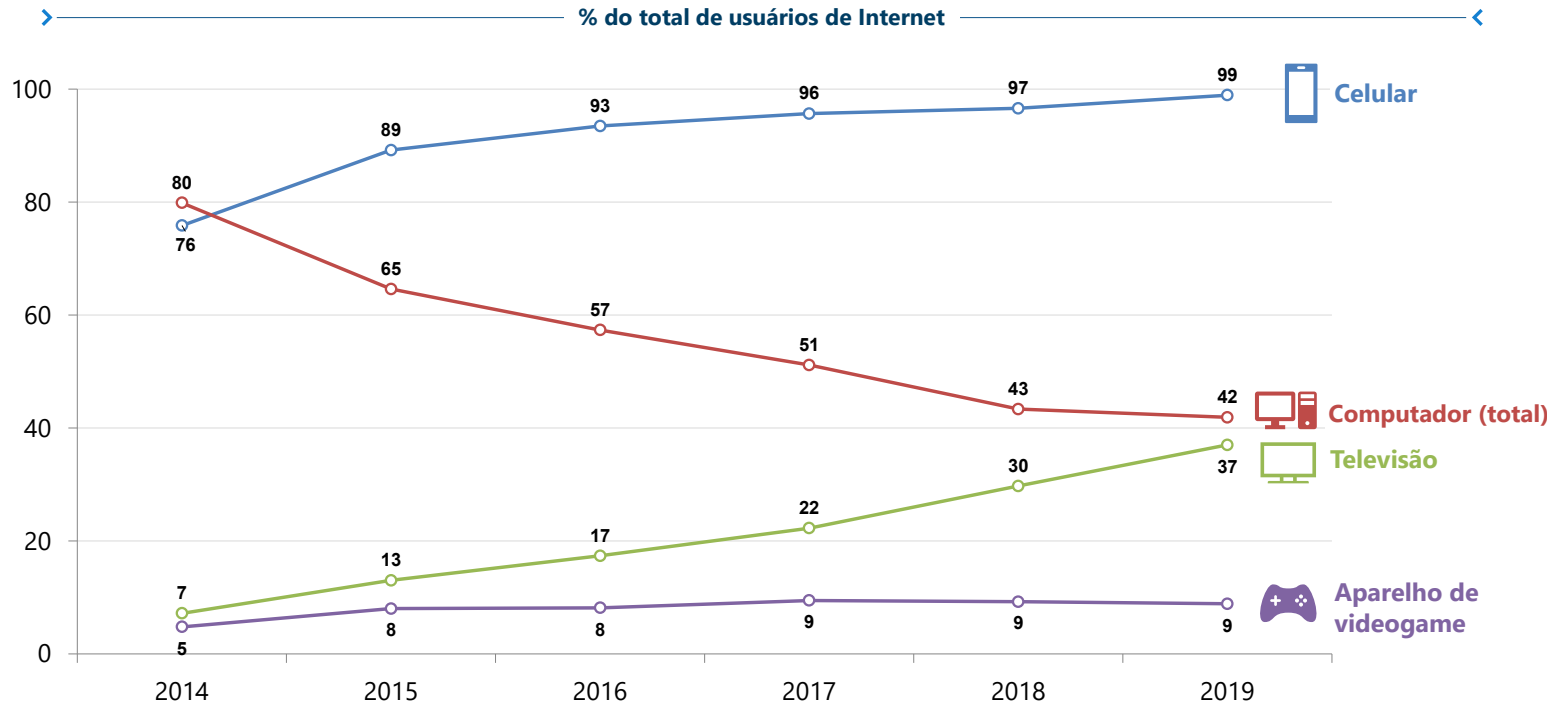
cert.br nic.br egi.br

Brazilian Internet in Numbers: Users and Devices

Internet Users (% of population)



Device Used for Individual Access (% of internet users)



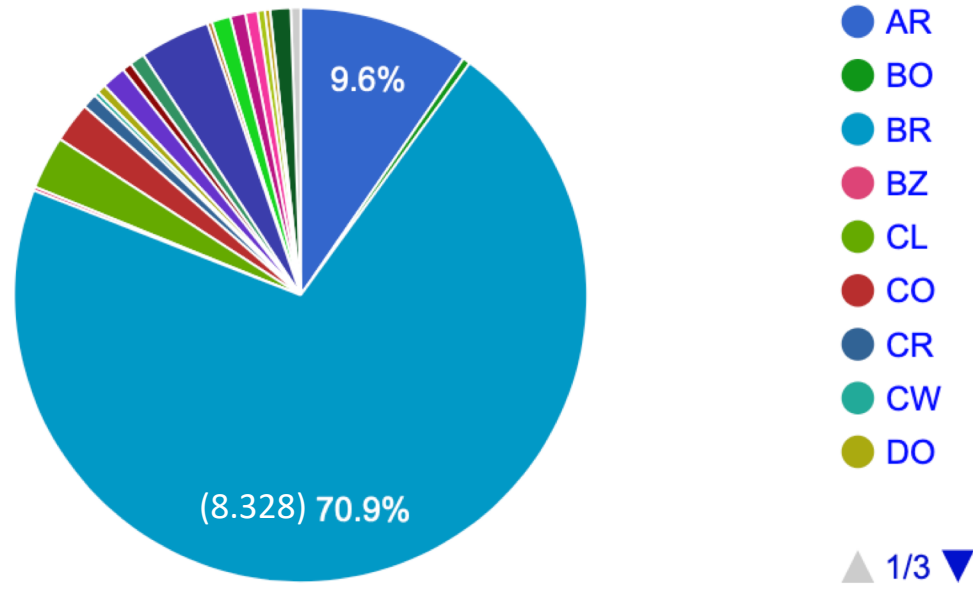
133,8 Million Internet Users

Source: CGI.br/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Domicílios Brasileiros – TIC Domicílios 2019. <https://www.cetic.br/pesquisa/domicilios/indicadores>

Brazilian Internet in Numbers: ASNs, ISPs and Traffic eXchange

Autonomous Systems Allocated in the Latin American and Caribbean Region

Distribution of ASN per country



Source: <https://www.lacnic.net/en/web/lacnic/estadisticas-asignacion>

Data updated on September 07, 2020

ISPs in Brazil

- Total (estimated): 6.618
- 75% have 1.000 clients or less

Source: <https://www.cetic.br/pesquisa/provedores/>

Internet Traffic eXchange

IX.br São Paulo – one of the biggest in the world

- nº 1 in participants (2.000)
- nº 2 in peak traffic (10.5Tbps)
- nº 3 in average traffic (4.78Tbps)

Source: <https://www.pch.net/ixp/dir>

CERT.br Data

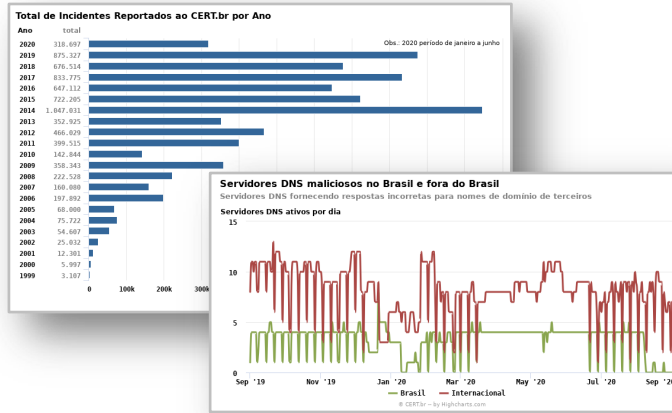
cert.br nic.br egi.br

CERT.br Data

Voluntary notification of incidentes to:

cert@cert.br

- 2019: 4.086.406 e-mails handled, related to 875.327 incidents notified to CERT.br



Sharing via MISP

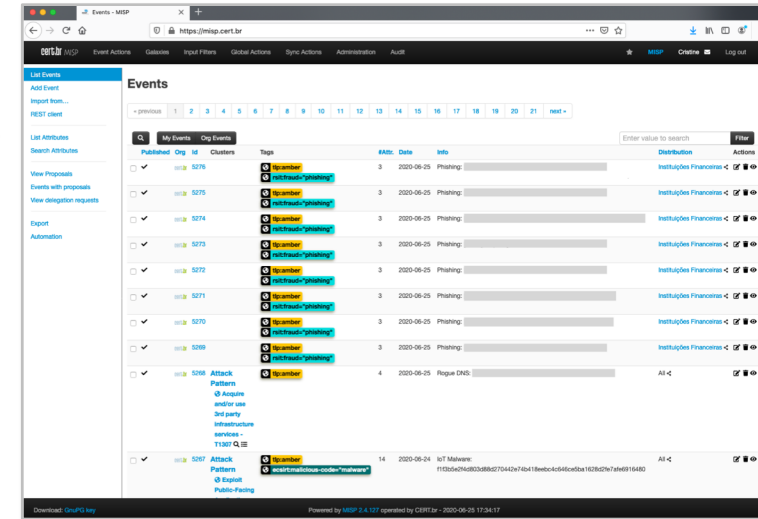
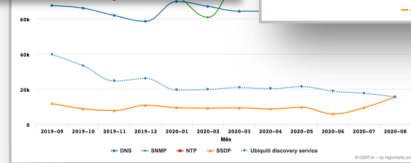
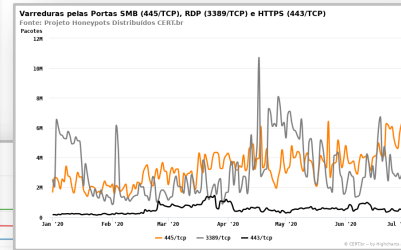
- Selected IoCs are shared with trusted partners
- Rogue DNS servers
- Phishing URLs
- IoT botnet binaries and Command and Control IPs
- Amplifiers that might be abused for DDoS attacks

Threat feeds

- CERT.br Distributed Honeypots Team Cymru
- SpamHaus
- ShadowServer
- Shodan
- Anti-Botnet operations (Microsoft/FBI)



Notifications sent to all ASNs and public statistics made available

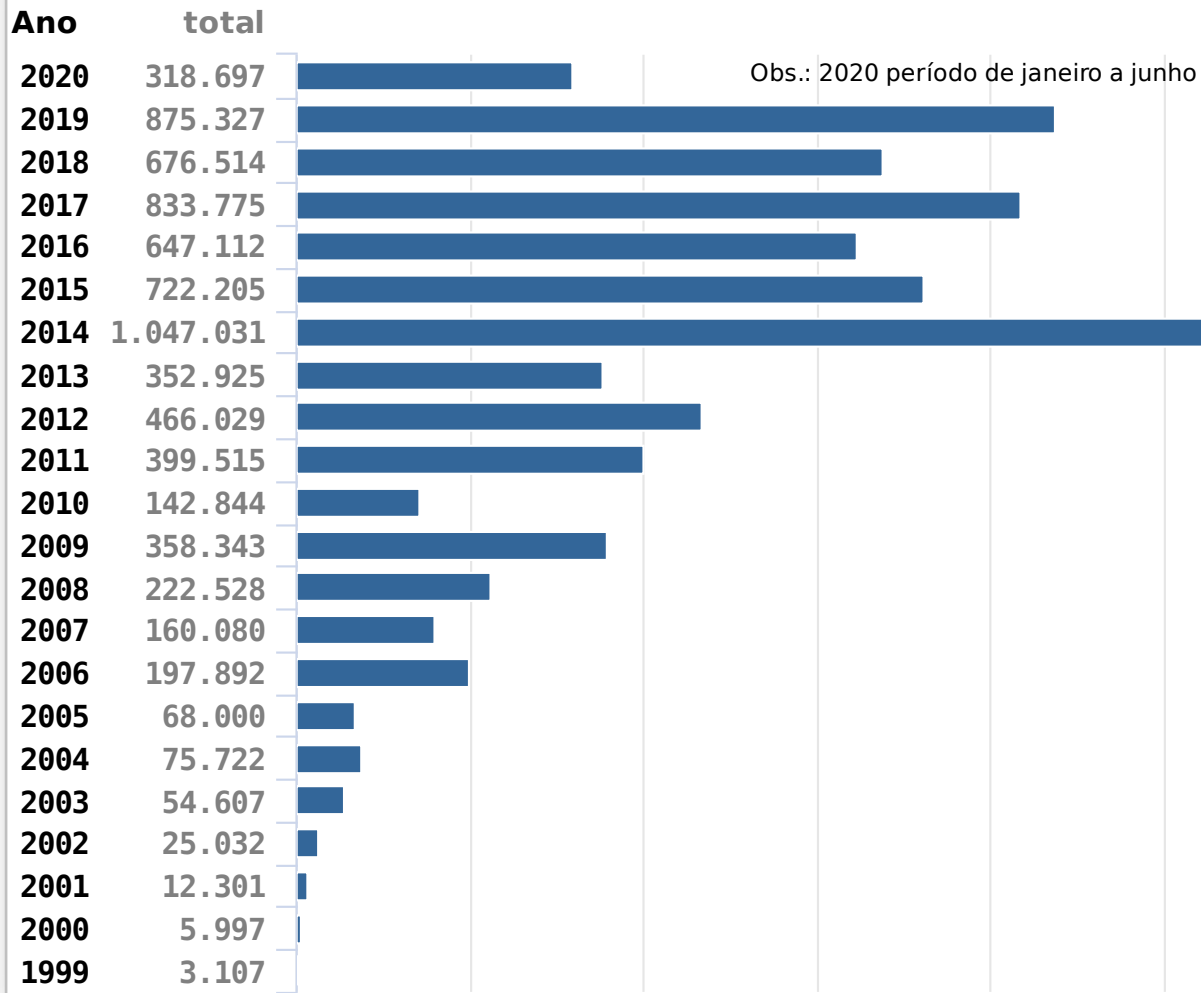


<https://cert.br/stats/>

<https://cert.br/misp/>

Incidents Reported to CERT.br: 1999 to 1st Half 2020

Total de Incidentes Reportados ao CERT.br por Ano

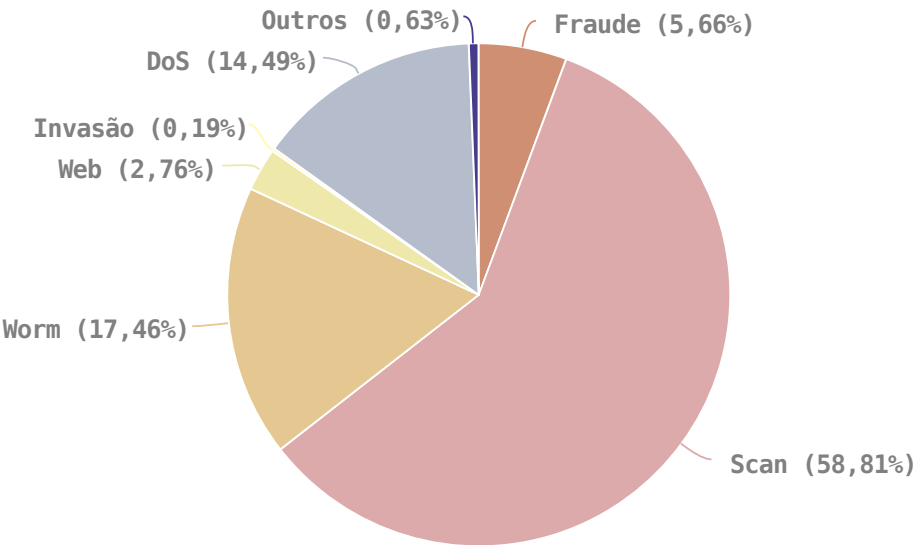


Source: <https://cert.br/stats/incidentes/>

Most common attacks – 1st half 2020

- Credential brute force attacks
 - *e-mails* (IMAP, SMTP e SMTPS)
 - SSH and TELNET
 - servers and network devices
 - IoT and broadband routers
- IoT abuse
 - Cameras, Smartphones, Smart TVs, Broadband and Wi-Fi routers
 - DDoS (UDP *flood*)
 - change the DNS resolution (to commit fraud)
 - crypto mining

Incidents Reported to CERT.br: Fraud attempts and DDoS in more detail

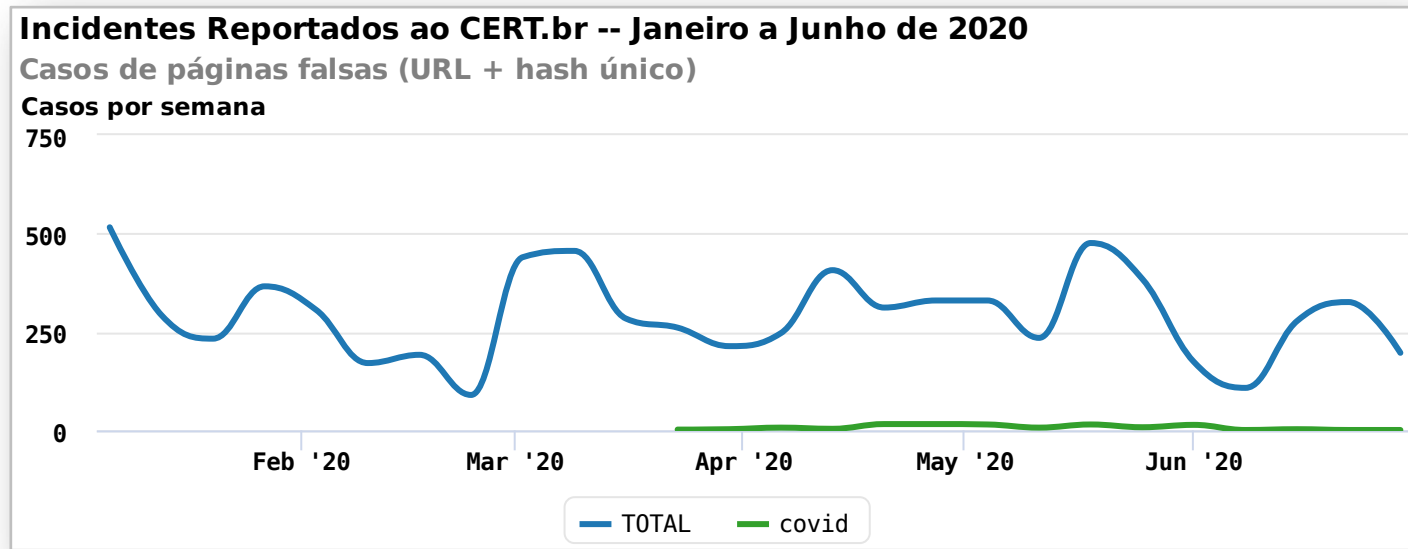


Fraud attempts **+54% 2019-S1** **-35% 2019-S2**

- 96% phishing attacks
 - less than 1% is COVID-19 related (see graph below)
 - increase in reports of phishing for credential of cloud document services, video streaming, webmail and social networks

DDoS **-81% 2019-S1** **-17% 2019-S2**

- 2019 was the record of reports
- most frequent reports
 - . IoT botnets
 - . traffic amplification



Lessons Learned

Continue normal operations

- The types of incidents are not likely to change
 - current/extreme events will be used as a lure
 - this has happened before
 - earthquakes, Olympics, tsunamis, etc
- Exposure is likely to change due to unplanned remote working (but nothing really new)
 - internal services exposed
 - less control over desktops/laptops security
 - use of new tools with no training
- Don't panic
 - even if others are panicking
 - don't be too quick to block everything and blacklist everyone

Always be prepared

- to work remotely **securely**
 - equipment and tools
 - multi-factor authentication
- to share information
 - participate in task forces
 - use information sharing platforms
- to provide high level information
 - statistics, briefings, reports, etc
- to educate your constituency!
 - have well known channels
 - enlist the help of others

National Initiatives for a Healthier Internet Ecosystem

cert.br nic.br egi.br

We need a healthier ecosystem: National Initiative – A More Secure Internet Program



Current Goal:

- Reduce the number of systems that can be abused for DDoS attacks

Incentive to adopt best practices:

- Hardening
- Routing Security
- Anti-spoofing (BCP 38)
- Close open services

Joint initiative involving several organizations

- ISOC and ISPs, Hosting and Telco Associations

<https://bcp.nic.br/i+seg>



Minimum Security Requirements for Customer Premises Equipment (CPE) Acquisition

Work developed by the LAC-AAWG – Latin American and Caribbean Anti-Abuse Working Group

Joint Publication of

- M³AAWG - Messaging, Malware and Mobile Anti-Abuse Working Group
- LACNOG - Latin American and Caribbean Network Operators Group
- Editor: Lucimara, LAC-AAWG Chair / CERT.br

Currently available in:

- English, Portuguese, Korean and Japanese

New translations to be released soon:

- Spanish, French and German

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



Awareness Materials: InternetSegura.br Portal



Algumas senhas podem ser facilmente descobertas, e é importante tomar alguns cuidados no momento de elaborá-las. Além disso, uma 2ª camada de segurança deve ser adicionada p/ reforçar a segurança de seus acessos e dispositivos. Veja mais dicas importantes: internetsegura.br/coronavirus/



internetsegura.br

nic.br INTERNET SEGURA BR

Sobre | Outras iniciativas | Como Pedir Ajuda

Edição Especial COVID-19

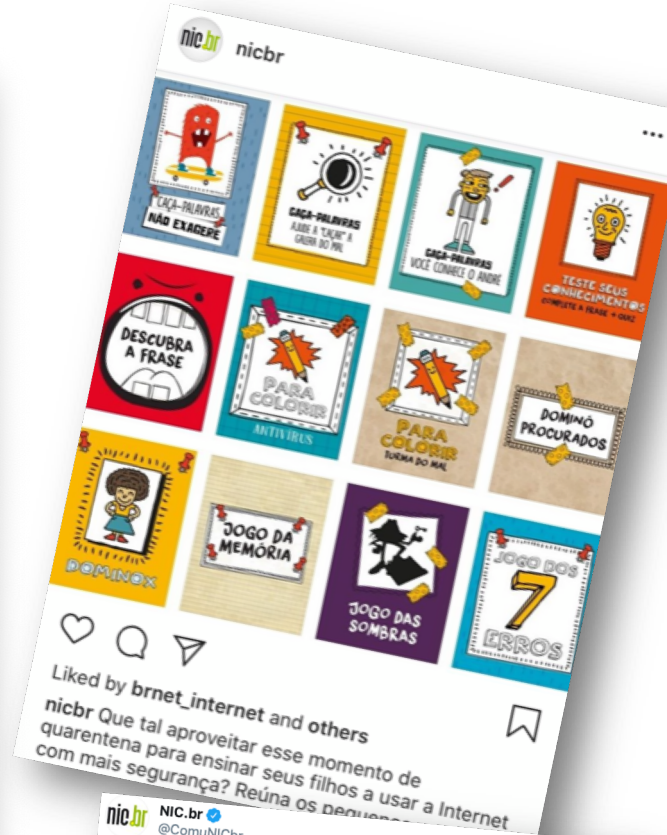
#InternetSeguraCoronavirus

Ilustração de quatro pessoas (três mulheres e um homem) em uma reunião, olhando para um laptop. Há três pontos de exclamação vermelhos acima delas.

Infelizmente, em momentos de incerteza e de busca por informações como os que estamos vivendo com a pandemia do Coronavírus, algumas pessoas se aproveitam para aplicar golpes e espalhar notícias falsas.

Por isso é importante que você adote na Internet a mesma postura preventiva que vem adotando para se proteger do Coronavírus. Para ajudá-lo nisso preparamos algumas dicas:

- Boatos ajudam a espalhar **desinformação** pela Internet e podem conter **códigos maliciosos** e **tentativas de golpes**. Ao receber notícias sobre o tema Coronavírus seja cuidadoso ao compartilhar, **verifique a fonte da informação** e em caso de dúvidas, **não compartilhe** e ajude a tornar a Internet um ambiente mais saudável, seguro e confiável.
- Caso tenha dúvidas sobre a **veracidade de uma informação**, como por exemplo um remédio milagroso, procure **consultar outras fontes** antes de repassá-la.
- Cuidado com mensagens solicitando **doações para as vítimas da doença**. Apesar de existirem várias ações reais a respeito, **muitos golpistas exploram a propensão à caridade** que as pessoas demonstram em momentos difíceis como estes para **criar campanhas falsas**. Antes de doar procure obter mais informações **consultando os sites oficiais de Campanhas**.
- Caso perceba **pessoas em seus grupos** compartilhando mensagens com suspeitas de golpes, **alerte-os sobre o conteúdo malicioso**.
- Cuidado com mensagens que tentem induzi-lo a fornecer **informações pessoais e dados bancários**, como páginas que prometem fazer testes on-line para verificar se você está infectado, mas que solicitam os **números do seu cartão de crédito**.
- Tenha cuidado ao instalar aplicativos que prometam informações sobre a pandemia, **procure baixá-los de desenvolvedores e lojas oficiais**, como as do sistema operacional do seu aparelho. Ao instalar aplicativos, **evite fornecer dados e permissões** quando não forem realmente necessários.



Portfolio under Creative Commons License Including Training Teachers to Use it in Class

Some materials in Spanish,
in partnership with ISOC:
<https://cartilla.cert.br/>

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

para Crianças

Guia Internet Segura
Apresenta conceitos de segurança na Internet de forma lúdica, com atividades para colorir, palavras cruzadas, desafios citados, 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.

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

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), Libre-Office (.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". ctic.br/pesquisa/kids-online
- TIC Educação**
A pesquisa entrevistou 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. ctic.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-bcp
- Curso "Fundamentals of Incident Handling":** cert.br/cursos/ih/
- 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 CGL.br "Combate ao spam na Internet no Brasil"
Histórico e reflexões sobre o combate ao spam e a gerência 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.

Thank You

© cristine@cert.br

© Incident reports to: cert@cert.br

© @certbr

<https://cert.br/>

nic.br cgi.br

www.nic.br | www.cgi.br