nic.br cgi.br | cert.br

LAC-CSIRTs
May 08, 2020
Online Event

Incident Handling Amid a Pandemic: Now What?

Dr. Cristine Hoepers
General Manager
cristine@cert.br

cert.br nic.br cgi.br

cert.br

TLP:WHITE

Incident Management	Training and Awareness	Trend Analysis
Coordination	Courses	Distributed Honeypots
Technical Analysis	Presentations	SpamPots
Support for recovery	Best Practices	Processing of threat feeds
	Meetings	

Filiations and Partnerships:

FIRST Improving Security Together MEMBER

ACCREDITED BY TI TRUSTED INTRODUCER

APWG RESEARCH PARTNER www.antiphishing.org

CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE — SEI Partner Network

HN/P

Creation:

August/1996: a report proposing a model for incident management for the country is published by the Brazilian Internet Steering Committee – CGI.br[1]

June/1997: CGI.br creates CERT.br (at that time called NBSO – *NIC BR Security Office*) based on the report's recommendations[2]

[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

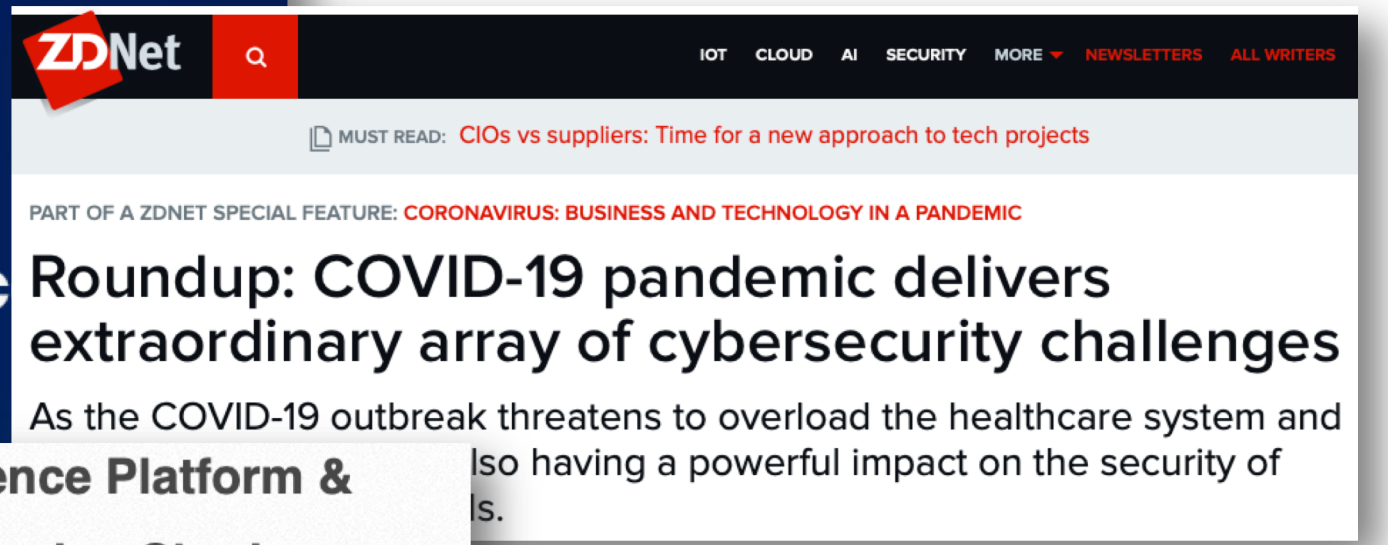
Networks that use Internet Resources allocated by NIC.br (IPs or ASNs allocated to Brazil, and domains under the ccTLD .br)

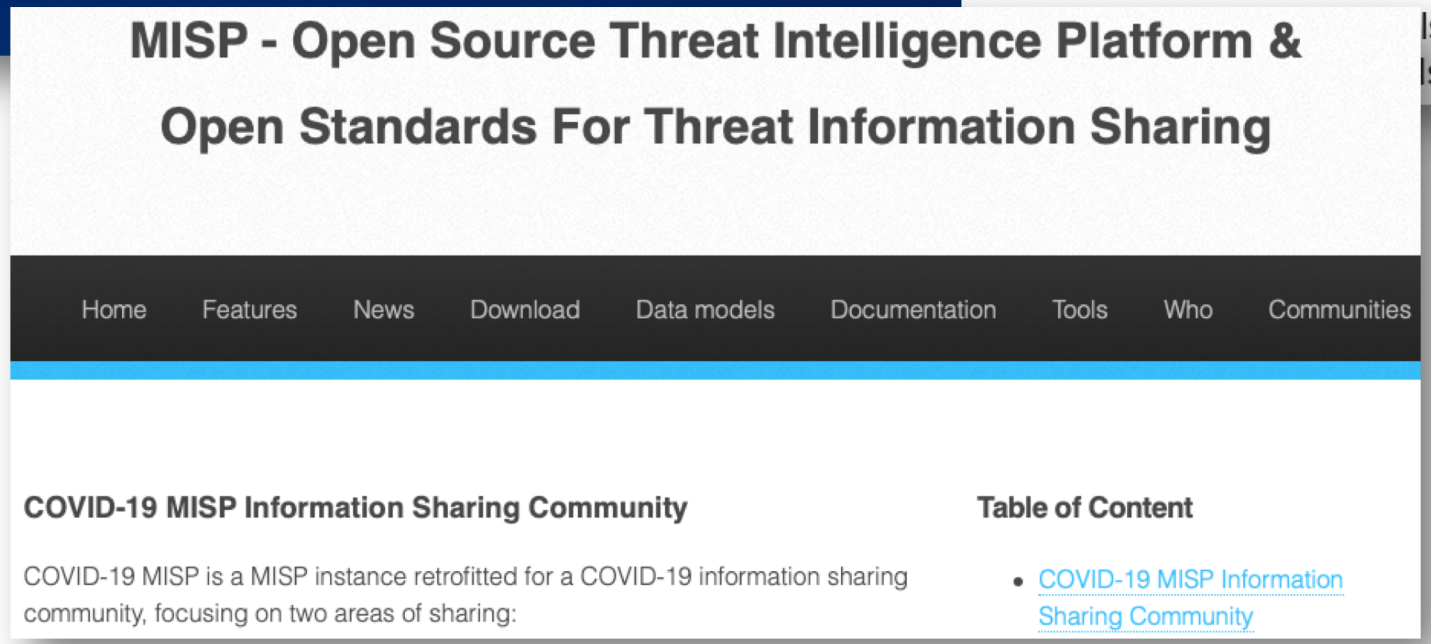
Focus of the Activities

- 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

TLP:WHITE


COVID-19
CYBER THREAT COALITION
Home Blocklist Join Us Events Advisories About Us
Join us in sharing pandemic related cyber threat intelligenc during this time of crisis


ZDNet
IOT CLOUD AI SECURITY MORE NEWSLETTERS ALL WRITERS
MUST READ: CIOs vs suppliers: Time for a new approach to tech projects
PART OF A ZDNET SPECIAL FEATURE: CORONAVIRUS: BUSINESS AND TECHNOLOGY IN A PANDEMIC
Roundup: COVID-19 pandemic delivers extraordinary array of cybersecurity challenges
As the COVID-19 outbreak threatens to overload the healthcare system and
lso having a powerful impact on the security of
ls.

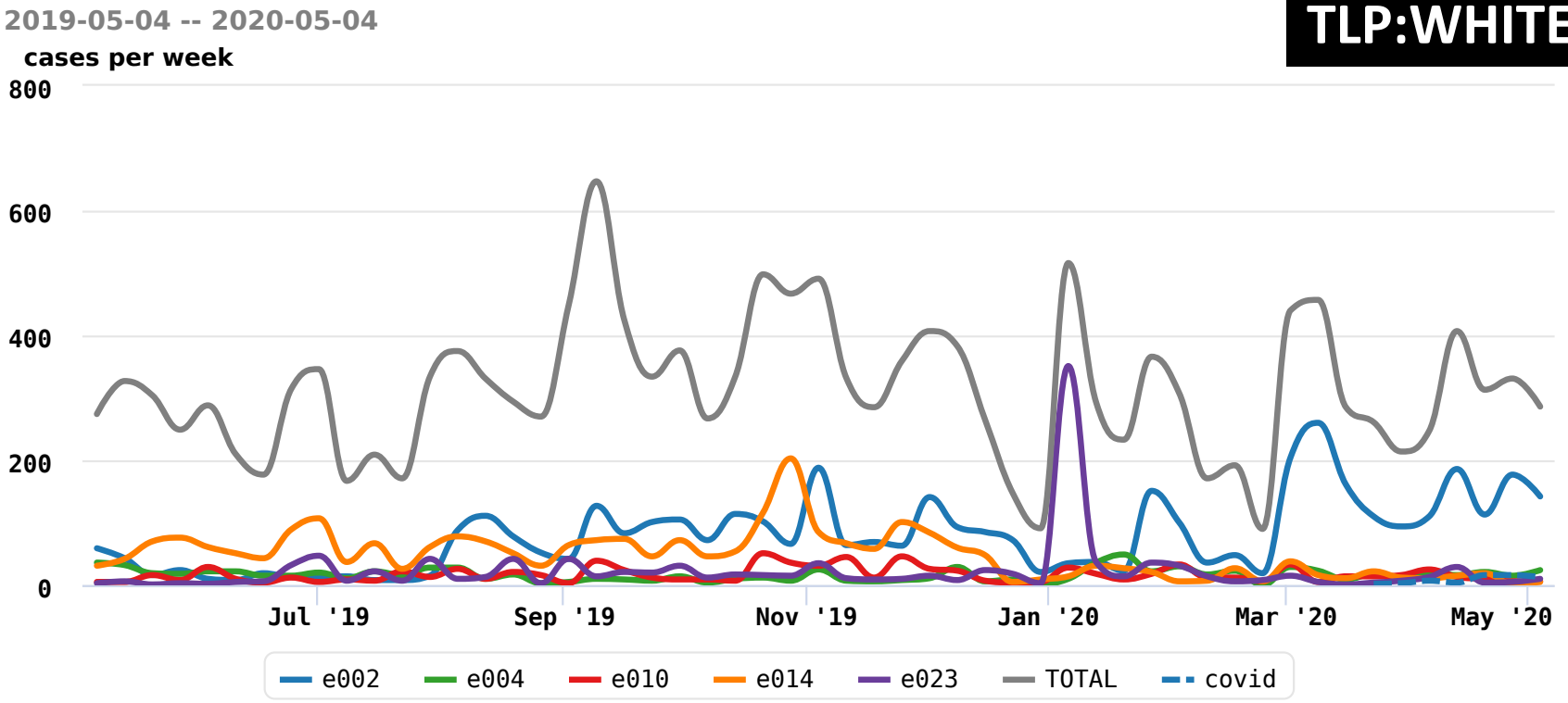

MISP - Open Source Threat Intelligence Platform &
Open Standards For Threat Information Sharing
Home Features News Download Data models Documentation Tools Who Communities
COVID-19 MISP Information Sharing Community
COVID-19 MISP is a MISP instance retrofitted for a COVID-19 information sharing community, focusing on two areas of sharing:
Table of Content
COVID-19 MISP Information Sharing Community

Phishing Statistics

TLP:WHITE

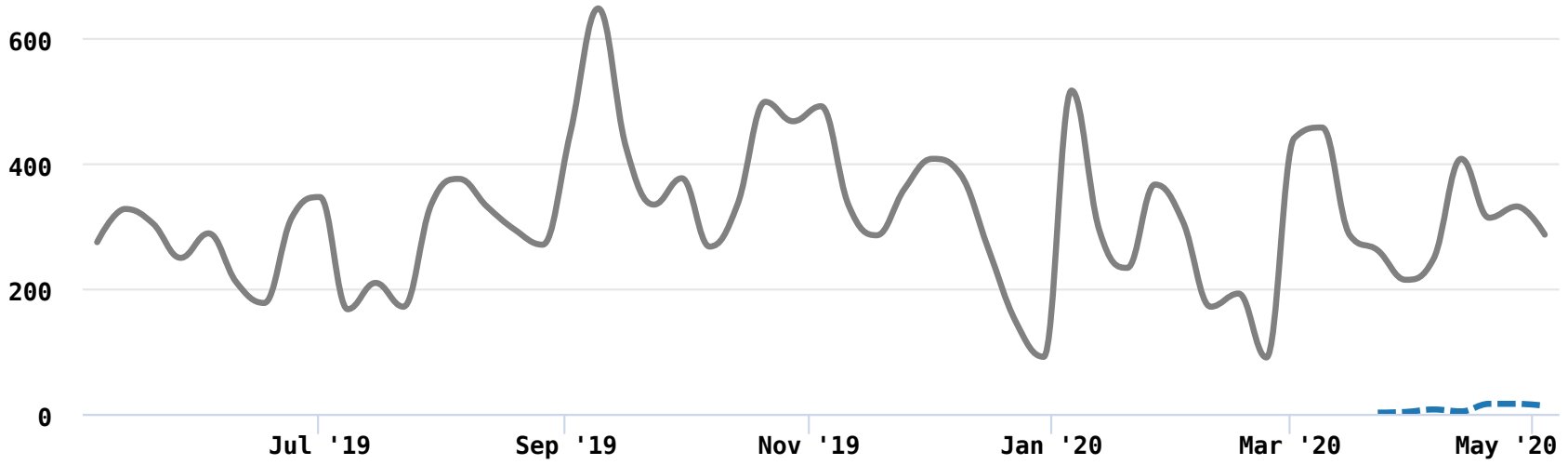
Top graphic includes:

- Total reports
- COVID-19 themed phishing reports
- Top 5 brands
  (e002, e004, e010, e014 and e023)



Bottom graphic includes:

- Total reports
- COVID-19 themed phishing reports



Another type of problem:
Fake News and Scams

TLP:WHITE

Usually spread trough social networks and messaging apps

- Facebook, Instagram, Twitter, WhatsApp, Telegram, etc

Underreported

- hard to detect
  - unless you are the owner of the platform
- hard to report
  - specially to CSIRTs

TLP:WHITE

The road to hell is paved with good intentions…

MISP covid instance blacklist

(covid_misp_filtered_ioc_list.csv)

- entries: 168.778
- `.br` domains: 624
- **legit `.gov.br` domains**: 60
- additionally, at least:
  - 8 legit telemedicine sites
  - 20 university covid-19 info pages
- other `.br` domains blacklisted include covid-19 information hot sites of hospitals and news outlets

This should make us think

How many people where prevented from getting help and access important information?

- The lists are basically a `grep` for anything that matches *covid* or *corona* in
  - passive DNS collectors
  - lists of newly generated domains
- Plus lots of other domains not related to COVID, like "regular" phishing (banks, ecommerce, etc)
  - how this affects the numbers being shouted in the media?
- No human validation
- No easy way to provide feedback

Source: https://www.misp-project.org/covid-19-misp/

Lessons Learned

Continue normal operations

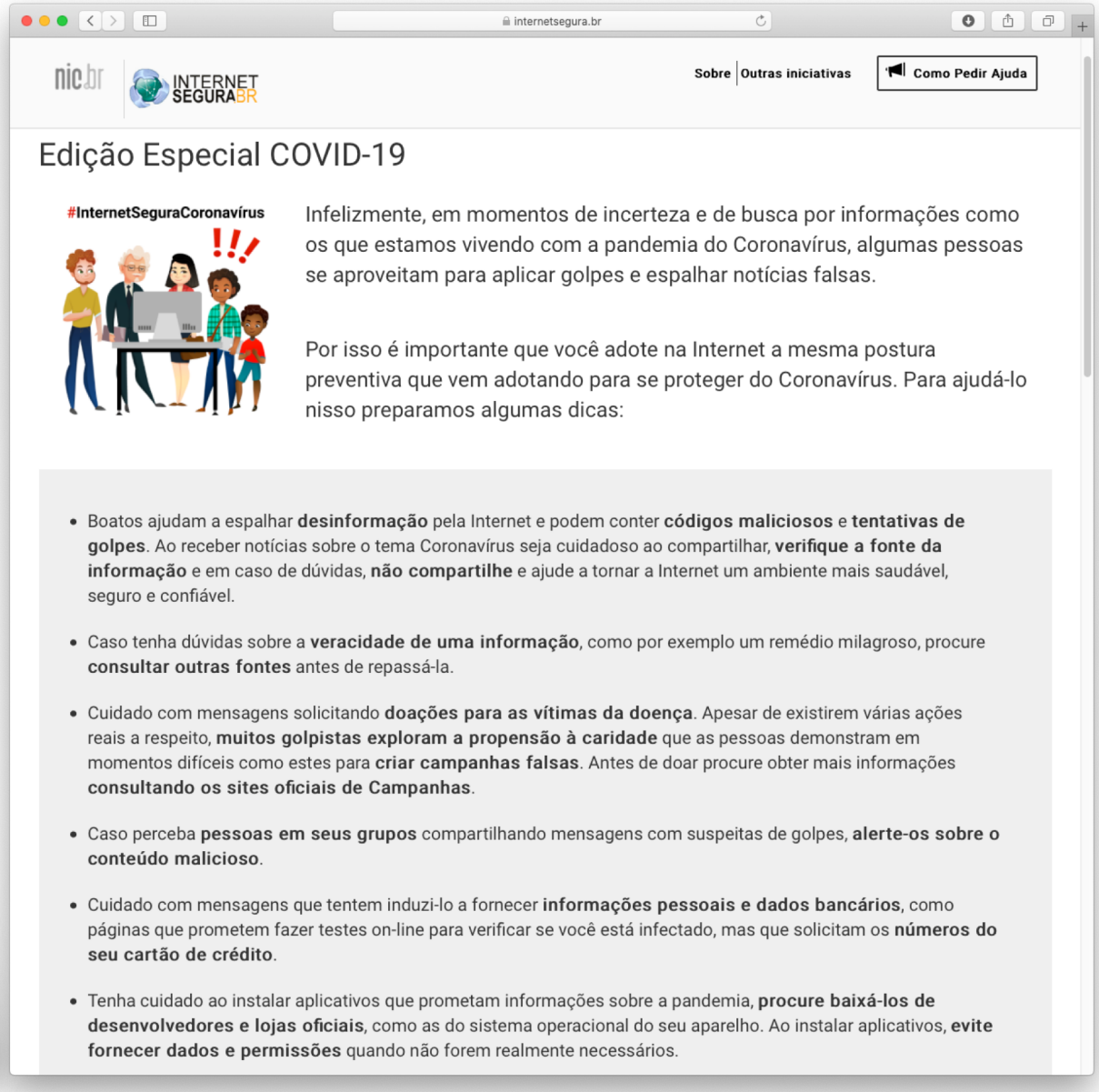
- The types of incidents are not likely to change
  - current/extreme events will be used as a lure
  - this has happened before
    - earthquakes, Olympics, tsunamis, etc
- Exposure is likely to change due to unplanned remote working (but nothing really new)
  - internal services exposed
  - less control 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

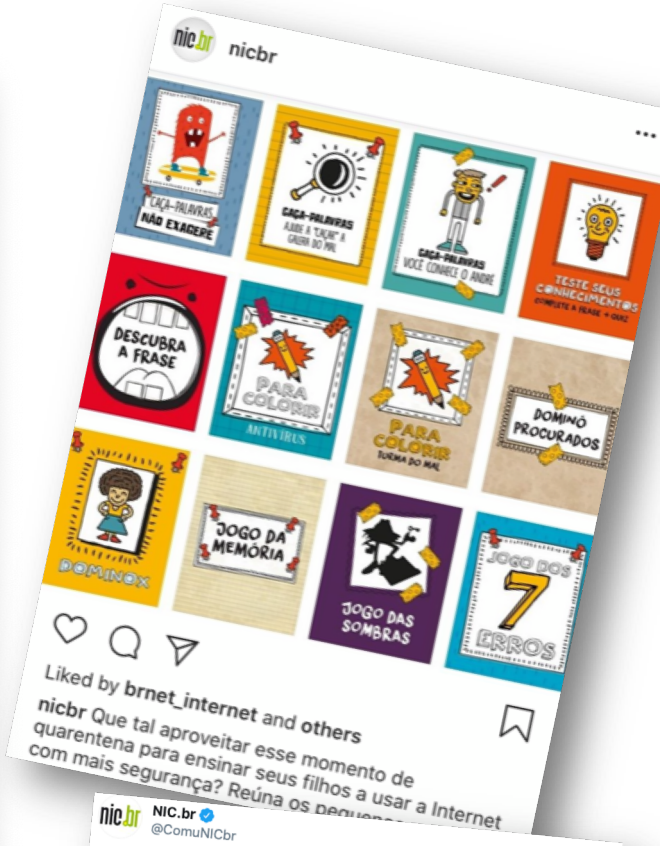
Always be prepared

- 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


NIC.br
@ComuNICbr
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/
Fascículo Verificação em duas etapas
#InternetSeguraCoronavírus
creative commons


nicbr
Fascículo
Códigos maliciosos
#InternetSeguraCoronavírus
creative commons
Liked by pessoapp and others
nicbr Pessoas mal intencionadas podem aproveitar a pandemia dao #Covid19 para aplicar golpes pela Internet e apps de mensagem. Saiba como se... more


internetsegura.br
nic.br
INTERNET SEGURA BR
Sobre
Outras iniciativas
Como Pedir Ajuda
Edição Especial COVID-19
#InternetSeguraCoronavírus
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.


nicbr
CAÇA-PALAVRAS NÃO EXAGERE
CAÇA-PALAVRAS
CAÇA-PALAVRAS
TESTE SEUS CONHECIMENTOS
DESCUBRA A FRASE
PARA COLORIR
PARA COLORIR
DOMINÓ PROCURADOS
DOMINOX
JOGO DA MEMÓRIA
JOGO DAS SOMBRAS
JOGO DOS 7 ERROS
Liked by brnet_internet and others
nicbr Que tal aproveitar esse momento de quarentena para ensinar seus filhos a usar a Internet com mais segurança? Reúna os pequ


NIC.br
@ComuNICbr
Além de ficar em casa e se proteger, lembre-se de proteger também seus equipamentos, mantendo-os atualizados e instalando mecanismos de segurança. Confira mais dicas para usar a Internet de forma segura:
internetsegura.br/coronavirus/ #FiqueEmCasaSeguro
Fascículo Dispositivos móveis
#InternetSeguraCoronavírus
creative commons

Thank You

cristine@cert.br

Incident reports to: cert@cert.br

@certbr

https://cert.br/

May 08, 2020

nic.br cgi.br

www.nic.br | www.cgi.br