nic.br cgi.br | cert.br

Semana da Segurança da Informação

Tribunal Regional Federal da Primeira Região

28 de setembro de 2022 – *Online*

Internet Segura: Para Todas as Idades

Lucimara Desiderá, M.Sc, CISSP
Analista de Segurança, CERT.br/NIC.br
lucimara@cert.br

cert.br nic.br cgi.br

nic.br

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

1 Diretor presidente
2 Diretor administrativo e financeiro
3 Diretor de serviços e tecnologia
4 Diretor de projetos especiais e de desenvolvimento
5 Diretor de assessoria às atividades do CGI.br

- 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

https://nic.br/sobre/

Antes de falar do CERT.br algumas definições: **Incidentes de Segurança e CSIRTs/CERTs**

Incidente de Segurança em Computadores – qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores

Exemplos:

- Tentativas de ataques: varreduras, tentativa de adivinhar senhas, tentativas de infecção por *malware*, etc
- Ataques com sucesso: invasões, infecção por *malware*, negação de serviço (DDoS), desfiguração de página (*defacement*), etc

As consequências dos incidentes podem ou não:

- ter ramificações jurídicas ou ser crime
- levar à exposição de dados pessoais

nesses casos o tratamento precisa seguir os trâmites definidos em leis ou regulamentos

Tratamento de Incidentes – processo de identificar e mitigar os incidentes de segurança; também envolve a prevenção

CSIRT – acrônimo internacional para designar um Grupo de Resposta a Incidentes de Segurança, responsável por tratar incidentes de segurança para um público alvo específico

Outros acrônimos: IRT, CERT, CIRC, CIRT, SERT, SIRT, ETIR, CTIR

OBS.: "CERT.br" é uma marca registrada com permissão da *Carnegie Mellon University*, e precisa ser grafado sempre com:

- "CERT" em maiúsculas
- acompanhado do ".br"

cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CERT Nacional de Último Recurso

Serviços Prestados à Comunidade

Gestão de Incidentes

- Coordenação
- Análise Técnica
- Suporte à Mitigação e Recuperação

Consciência Situacional

- Aquisição de Dados
  - *Honeypots* Distribuídos
  - SpamPots
  - *Threat feeds*
- Compartilhamento das Informações

Transferência de Conhecimento

- Conscientização
  - Desenvolvimento de Boas Práticas
  - Cooperação, Eventos e Reuniões (*Outreach*)
- Treinamento
- Aconselhamento Técnico e de Políticas

Filiações e Parcerias:

FIRST: Membro pleno desde 2002 **TF-CSIRT Trusted Introducer:** *Accredited* desde 2020

APWG: Research partner desde 2004 **SEI/CMU:** Cursos autorizados desde 2003

***Honeynet Project*:** Mantém o capítulo do Brasil desde 2003

https://cert.br/sobre/ | https://cert.br/sobre/filiacoes/ | https://cert.br/about/rfc2350/

25 anos cert.br

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 administrados pelo NIC.br

- endereços IP ou ASNs alocados ao Brasil
- domínios sob o ccTLD .br

Principais Atividades

- Facilitar a coordenação do tratamento de incidentes entre as partes
  - Ponto de contato nacional de último recurso
  - Trabalho colaborativo com outras entidades
  - Auxílio 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

Foco do CERT.br nestes 25 anos:
Aumentar a Capacidade Nacional de Tratamento de Incidentes

Nenhum time ou estrutura única conseguirá fazer sozinho a segurança ou a resposta a incidentes

Comunidade Nacional

- Ações junto a setores chave, para **criação e treinamento de Times** de Tratamento de Incidentes de Segurança (CSIRTs)
- **Auxiliar na análise** técnica e **facilitar** o tratamento de incidentes por outros CSIRTs
- Gerar massa crítica para possibilitar a **cooperação** e melhora na segurança das redes
- Ter uma visão sobre as principais **tendências** de ataques no Brasil

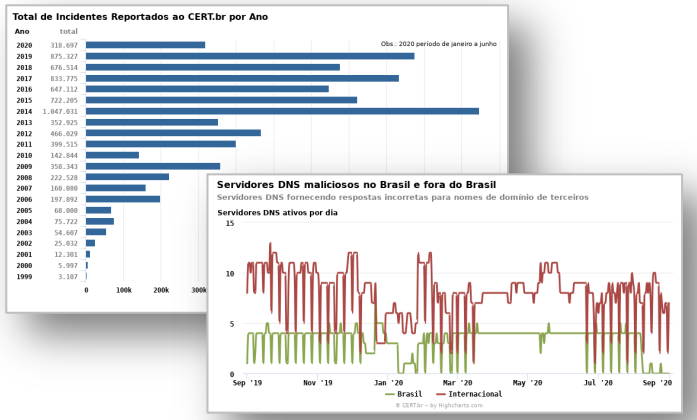
Comunidade Internacional

- Estabelecer **relações de confiança**
  - facilitar a comunicação em casos de incidentes
  - dar acesso a informações que ajudem a comunidade local
- **Influenciar** os padrões e certificações sendo construídos para CSIRTs
- Levar a **visão nacional** aos fóruns pertinentes

Tratamento de Incidentes e Consciência Situacional: **Fontes dos Dados, Métricas e Compartilhamento**

Notificações voluntárias de incidentes enviadas para: **cert@cert.br**

- Volume em 2021: 1.318.960 *e-mails* tratados, relativos a 457.270 incidentes notificados ao CERT.br



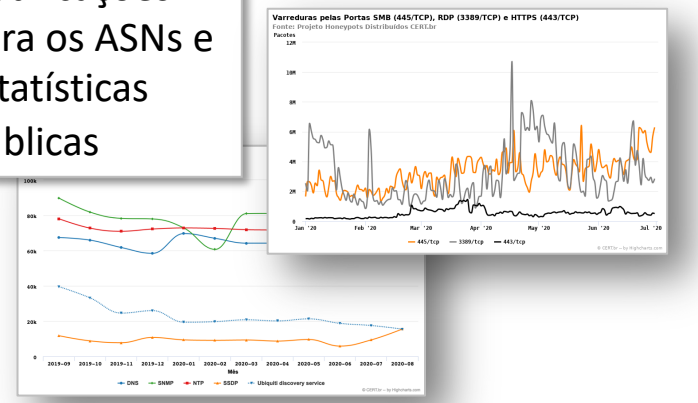
Compartilhamento via MISP

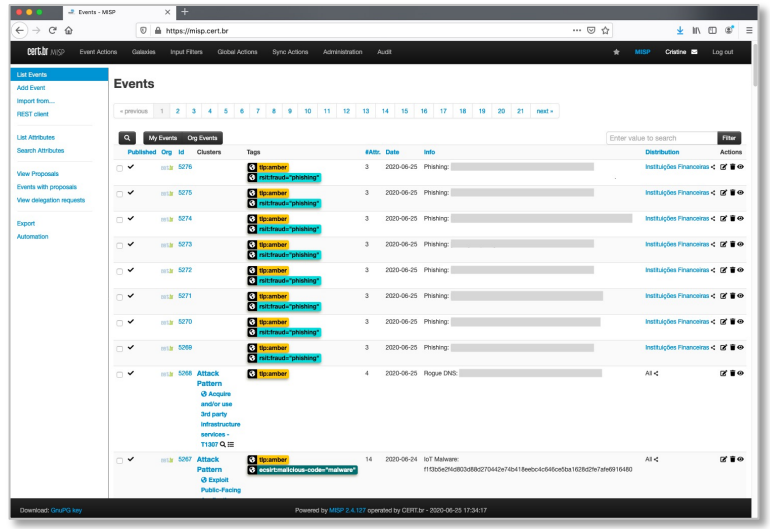
- Indicadores selecionados são compartilhados com parceiros
  - Servidores DNS maliciosos
  - *Phishing*
  - Binários e Comando e Controle de *botnets* IoT
  - Amplificadores usados em ataques DDoS

Threat feeds

- *Honeypots* Distribuídos do CERT.br
- Team Cymru
- SpamHaus
- ShadowServer
- Shodan
- Operações Anti-Botnet (Microsoft/FBI)

Notificações para os ASNs e estatísticas públicas





https://cert.br/stats/

https://cert.br/misp/

Público Técnico:
Capacitação em Tratamento de Incidentes

SEI Partner
Carnegie Mellon

Objetivo

- Criar/aproximar CSIRTs (Grupos de Tratamento de Incidentes de Segurança) no Brasil
- Possuir profissionais preparados para resolver os problemas de segurança no país

Fórum Brasileiro de CSIRTs

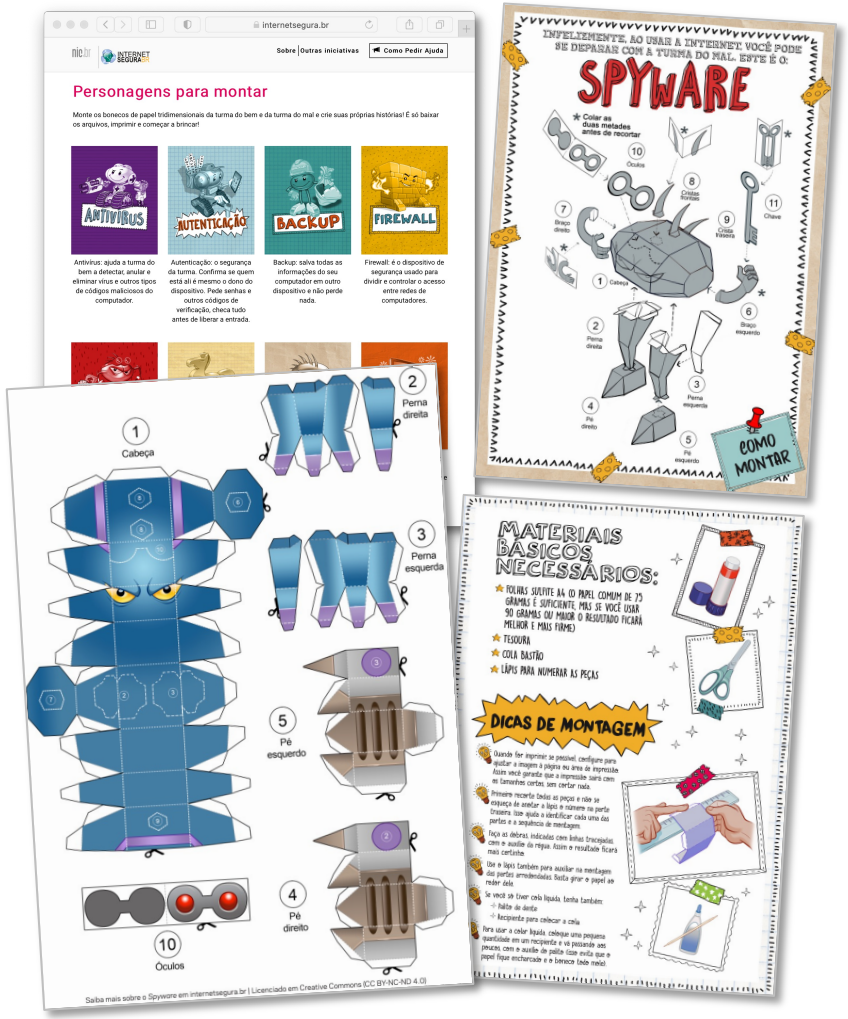
- Evento anual para profissionais da área de Tratamento de Incidentes
- Workshops sobre assuntos específicos

Cursos de Gestão de Incidentes

Ministra os cursos do *CERT® Division, do SEI/Carnegie Mellon,* desde 2004:

- https://cert.br/cursos/
  - *Overview of Creating and Managing CSIRTs*
  - *Fundamentals of Incident Handling*
  - *Advanced Incident Handling for Technical Staff*
- 93 turmas, atingindo 2165 profissionais de diversos setores

Conscientização:
Materiais para Crianças, Pais e Público em Geral



https://internetsegura.br/criancas/ | https://internetsegura.br/pais/ | https://cartilha.cert.br/

Alguns Mitos Sobre a Internet

cert.br nic.br cgi.br

Desmistificando...

“Internet é um mundo virtual”

“Internet é uma terra sem lei”

“Internet é a grande vilã da atualidade”

“Sistema 100% seguro”

“Meus equipamentos jamais serão localizados na Internet”

“Não tem nada de interessante em meus equipamentos”

“Crianças são nativos digitais”

“Idosos não são capazes de usar a Internet”

“Crianças estão protegidas em casa”

Agravantes

- Agravantes trazidos pela Internet
  - falsa sensação de anonimato
  - velocidade de propagação das informações
  - dificuldade de detectar sentimentos
  - dificuldade de exclusão das informações

Conheça os Riscos

cert.br nic.br cgi.br

Riscos
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

Riscos
Engenharia Social

- Técnica usada por atacantes para tentar enganar e persuadir potenciais vítimas à:
  - fornecerem informações sigilosas
    - ex: senhas e códigos
  - realizarem ações
    - executar *malware*, acessar páginas falsas
- Explora sentimentos humanos para persuasão:
  - automatismo, urgência
  - medo, obediência à autoridade
  - mentalidade de manada, distração, desejo
  - desonestidade, orgulho
  - ganância, curiosidade, preguiça, caridade, gentileza
- Prática de má-fé
  - a fim de aplicar golpes

Riscos

- Conteúdos:
  - maliciosos e impróprios:
    - códigos maliciosos, páginas falsas (*phishing*), 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):
  - exposição excessiva
  - uso excessivo

Riscos
Phishing

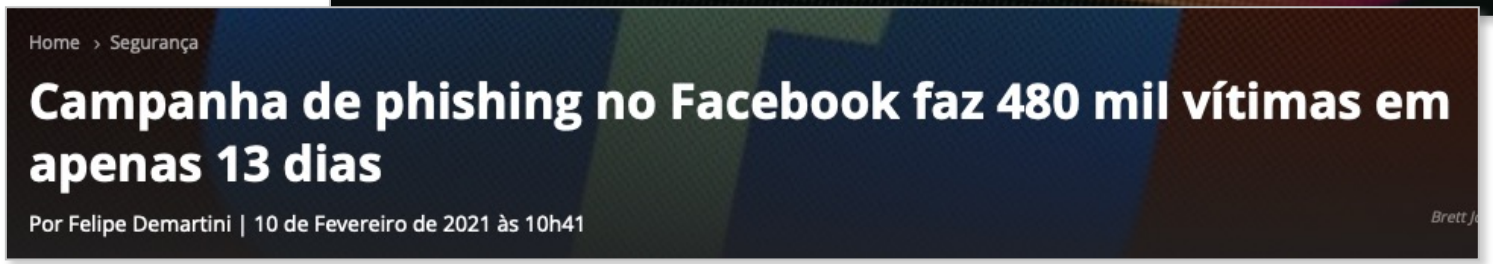
Phishing Scam Aims to Hijack TikTok 'Influencer' Accounts

Author: Elizabeth Montalbano

November 17, 2021 / 8:44 am

Threat actors used malicious emails to target more than 125 people with high-profile TikTok accounts in an attempt to steal info and lock them out.

A recently discovered phishing scam tried to takeover more than 125 high-profile user accounts on TikTok. Researchers said the campaign marks one of the first major attacks on "influencers" found on the TikTok social-media platform.



Campanhas de phishing por e-mail crescem 80% usando as datas de Black Friday e Cyber Monday

Pesquisadores ressaltam que os e-mails de phishing aumentaram em mais de 13 vezes nas últimas seis semanas, sendo que um em cada 826 e-mails enviados em todo o mundo é um golpe de phishing

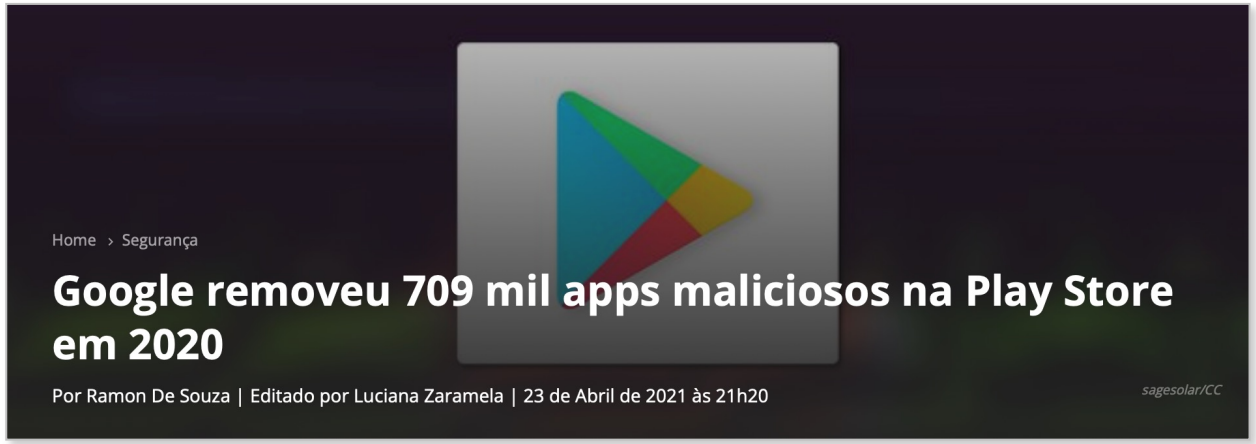
Por: Redação, 20/11/2020 às 17h32 - Atualizado em 20/11/2020 às 17h32

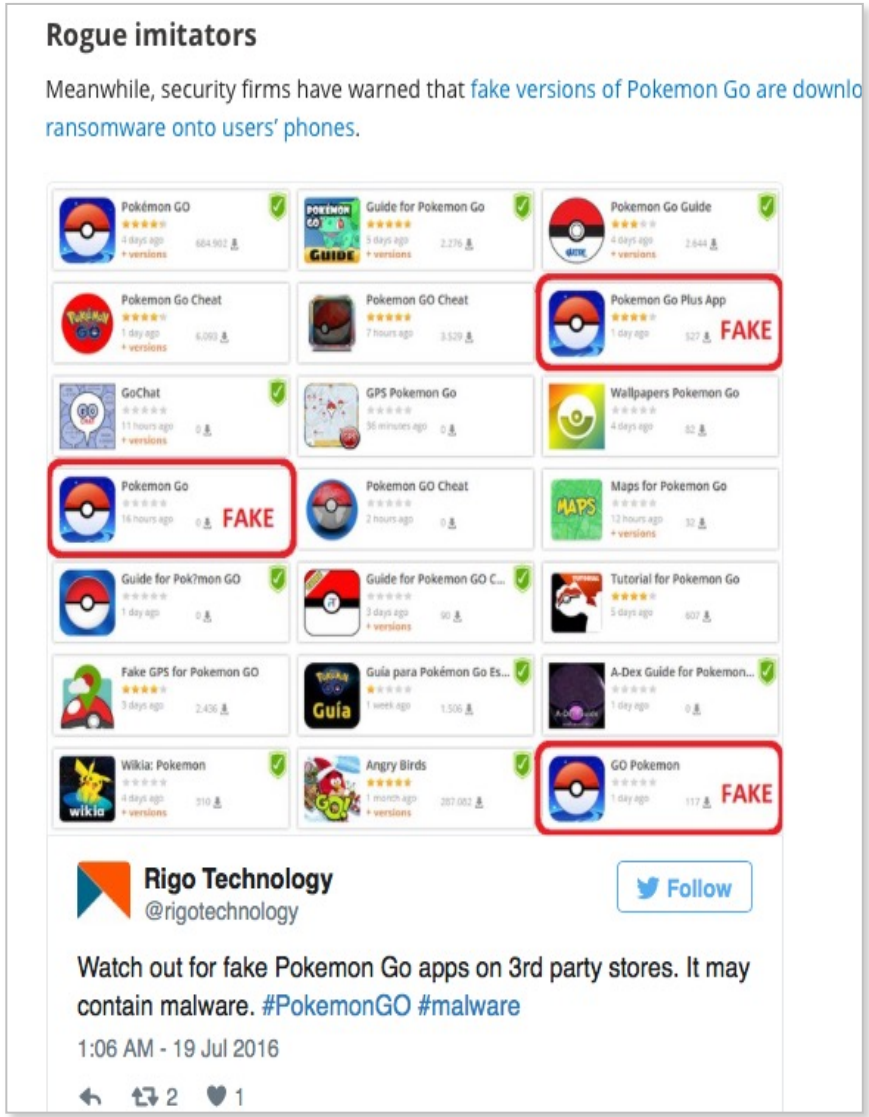
https://threatpost.com/phishing-scam-tiktok-influencer/176391/
https://olhardigital.com.br/2019/08/27/seguranca/usuarios-do-instagram-sao-alvos-de-novo-ataque-de-phishing-proteja-se/
https://canaltech.com.br/seguranca/campanha-de-phishing-no-facebook-faz-480-mil-vitimas-em-apenas-13-dias-178763/
https://www.securityreport.com.br/overview/campanhas-de-phishing-por-e-mail-crescem-80-usando-as-datas-de-black-friday-e-cyber-monday/#.YaUwCC-cbUI

Riscos
Aplicativos Maliciosos

PF alerta para fraude de aplicativo malicioso sobre o novo coronavírus

Por: **Diario de Pernambuco** Publicado em: **20/03/2020 13:30** | Atualizado em: **20/03/2020 13:47**





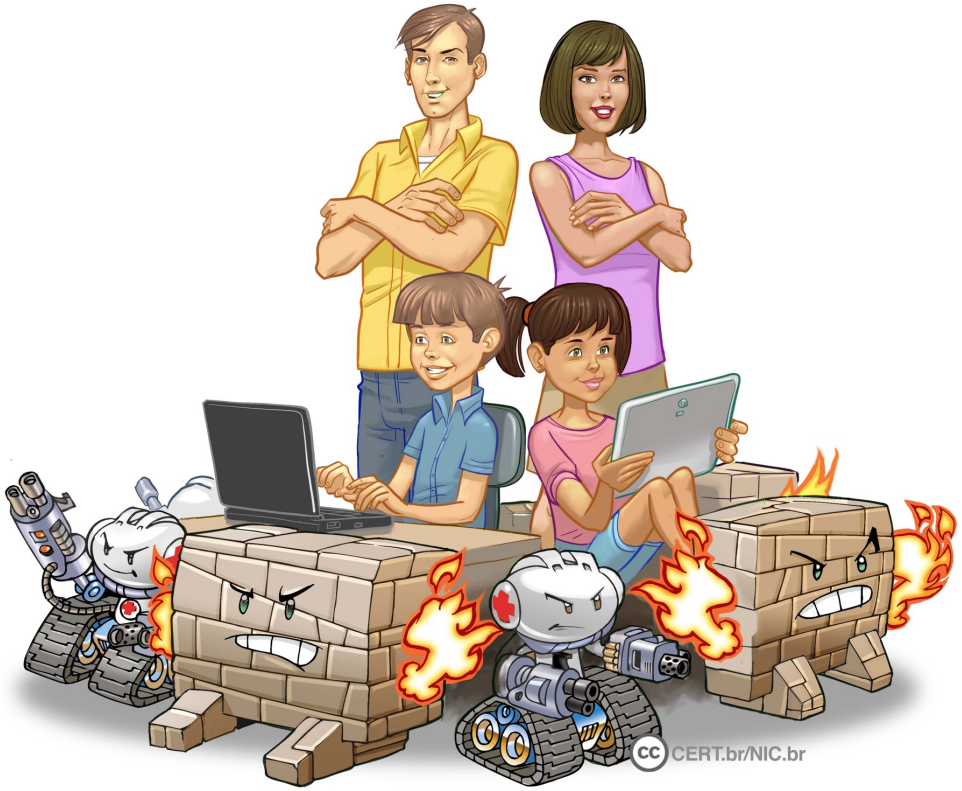
https://canaltech.com.br/seguranca/google-removeu-709-mil-apps-maliciosos-na-play-store-em-2020-183443/
https://www.diariodepernambuco.com.br/noticia/vidaurbana/2020/03/pf-alerta-para-fraude-de-aplicativo-malicioso-sobre-o-novo-coronavirus.html
https://www.ifsecglobal.com/pokemon-go-security-risks-flagged-by-the-cia-middle-eastern-states-and-data-security-experts/

Como se Prevenir

Como se Prevenir

- Internet não tem nada de virtual
  - pessoas, empresas, golpes
  - consequências reais

- 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

- Desenvolver o pensamento crítico

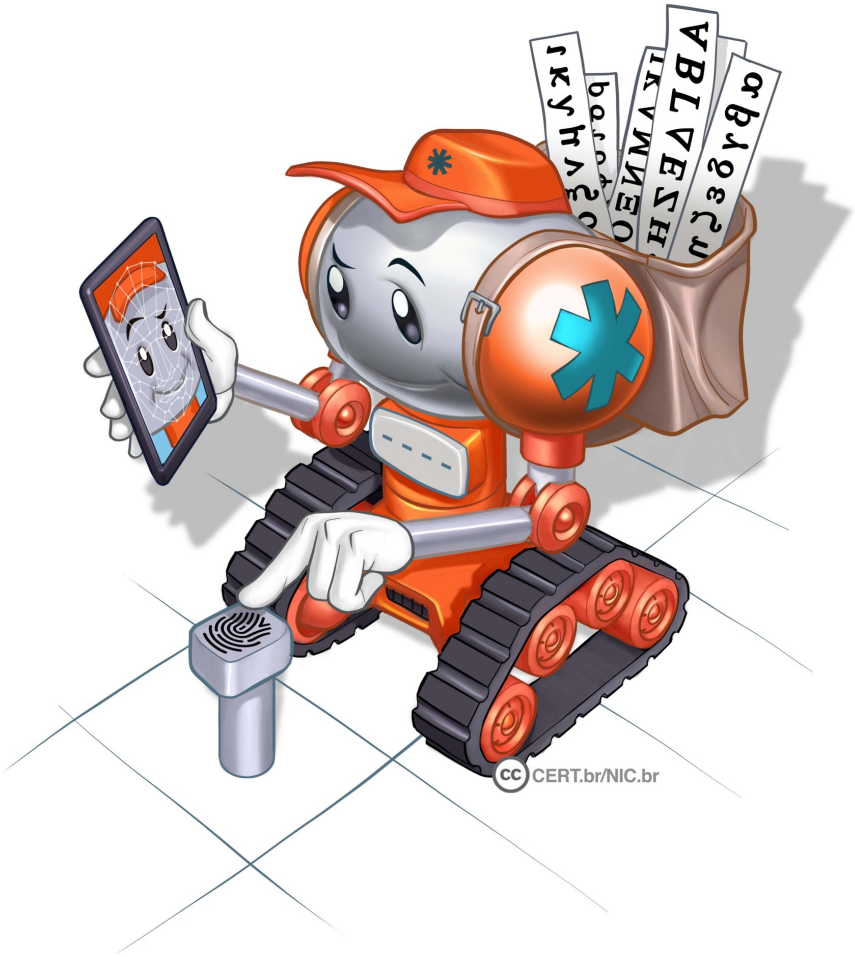
Como se Prevenir
Proteger os Equipamentos

- 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
- Seja seletivo na instalação de aplicativos

- Para crianças
  - controle parental: proteção adicional
    - deve ser usado como um aliado, não substitui o diálogo e a mediação
    - apresenta falhas e pode ser burlado

Como se Prevenir
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 conhecidas
    - palavras associadas ao contexto em que estão sendo usadas
  - usar:
    - senhas longas e com diferentes tipos de caracteres
- Não reutilizar as senhas
- Armazenar suas senhas de forma segura
  - usar programas gerenciadores de senhas
- Não informar senhas por *e-mails* ou telefonemas
- Habilitar a verificação em duas etapas



Como se Prevenir
Outros Cuidados

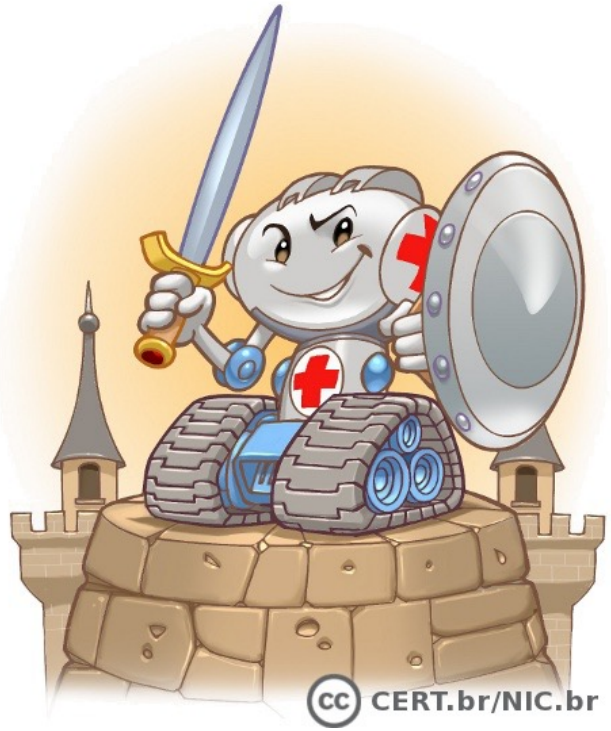
- Fazer *backups*
  - devem ser mantidos desconectados

- 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

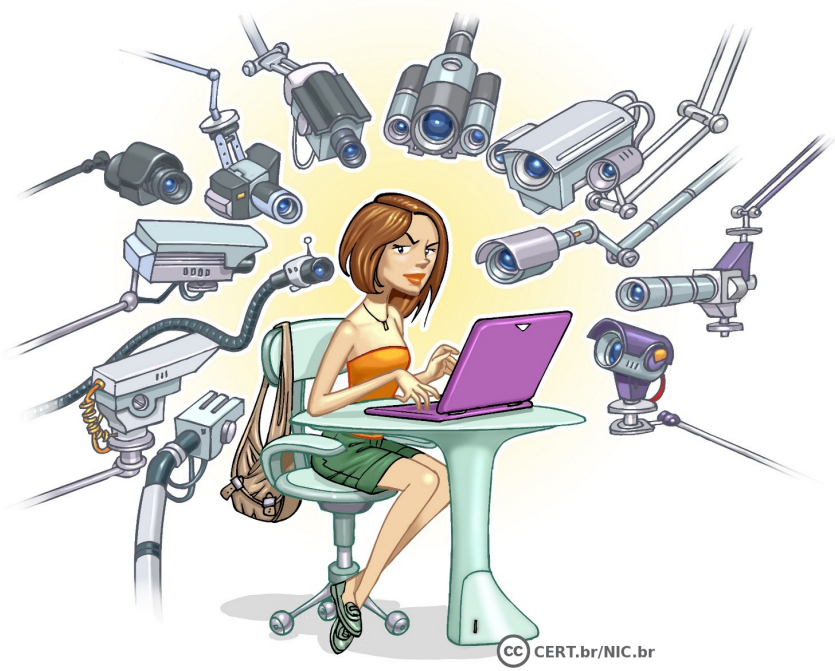
Protegendo-se de golpes na Internet

- Mantenha sua privacidade
  - quanto mais informação você disponibiliza maiores são as chances de alguém se passar por você e de atacantes serem bem sucedidos em ataques
- Fique atento a indícios
  - problemas com órgãos de proteção ao crédito, retorno de e-mails, notificações de acessos indevidos, lançamentos estranhos no extrato bancário/cartão de crédito
- Desconfie de mensagens:
  - quantias astronômicas, pedido de sigilo, urgência, atualização de dados
  - erros de linguagem
  - por que você foi escolhido?
  - use a sabedoria popular
    - quando a esmola é demais, o santo desconfia
    - se é bom demais para ser verdade, pode ser golpe
  - NUNCA RESPONDER



Preserve a sua privacidade nas redes sociais

- Considere que você está em um local público
- Pense bem antes de divulgar (não há como voltar atrás)
- Use as opções de privacidade oferecidas pelos *sites*
  - procure ser o mais restritivo possível
- Seja seletivo ao aceitar seus contatos
- Mantenha seu perfil e seus dados privados
- Restrinja o acesso ao seu endereço de *e-mail* e telefone
- Seja cauteloso ao dar acesso à aplicativos
- Seja cuidadoso ao se associar a grupos e comunidades
- **Não acredite em tudo que você lê**
  - Verifique sempre a fonte das informações
  - Não repasse boatos nem, mensagens que possam gerar pânico ou ódio



Proteja os seus filhos

- Informe-os sobre os riscos
  - Ajude-os a desenvolver pensamento crítico
- Dê o exemplo
- Estimule o diálogo
- Reforce os cuidados com estranhos
  - nunca fornecerem informações pessoais, enviarem fotos ou vídeos, usar *webcam*
  - para não marcarem / irem a encontros desacompanhados
- Ensine-os sobre privacidade
- Observe o comportamento
- Estabeleça regras e cumpra o combinado
- Respeite os limites de idade estipulados pelos sites
- Não exponha excessivamente seus filhos

Proteja a sua vida profissional

- Cuide da sua imagem profissional
- Antes de divulgar uma informação:
  - avalie se ela pode atrapalhar:
    - o seu emprego atual
    - um processo seletivo futuro
  - lembre-se que ela poderá ser acessada por seus chefes e colegas de trabalho
  - observe se ela não fere o código de conduta da sua empresa
- Cuidado ao permitir que seus filhos usem o mesmo computador ou dispositivo móvel que você usa para tratar de assuntos profissionais:
  - alguns aplicativos, como jogos, divulgam automaticamente nas redes sociais, dependendo das configurações
- Oriente seus familiares para não divulgarem informações sobre a sua empresa e vida profissional

CARREIRA / TWITTER - 30/03/2010

Mensagem no Twitter causa demissão de executivo da Locaweb

Curtir 22 Tweetar

Diretor comercial foi demitido depois de ter publicado mensagens contra o São Paulo Futebol Clube, durante o clássico contra o Corinthians. A Locaweb era um dos patrocinadores do time do Morumbi

http://epocanegocios.globo.com/Revista/Common/0,,EMI130181-16349,00-MENSAGEM+NO+TWITTER+CAUSA+DEMISSAO+DE+EXECUTIVO+DA+LOCAWEB.html

Protegendo a empresa

- Crie um código de conduta e uma política de uso aceitável
- Informe os funcionários sobre:
  - os riscos de uso das redes sociais
  - as regras de acesso durante o expediente
  - o comportamento esperado, referente a:
    - divulgação de informações profissionais (sigilosas ou não)
    - emissão de opiniões que possam comprometer a empresa
- Invista em treinamento e campanhas de conscientização
- Cuide da imagem
  - observe a opinião de clientes e consumidores
  - observe ações que envolvam o nome da empresa

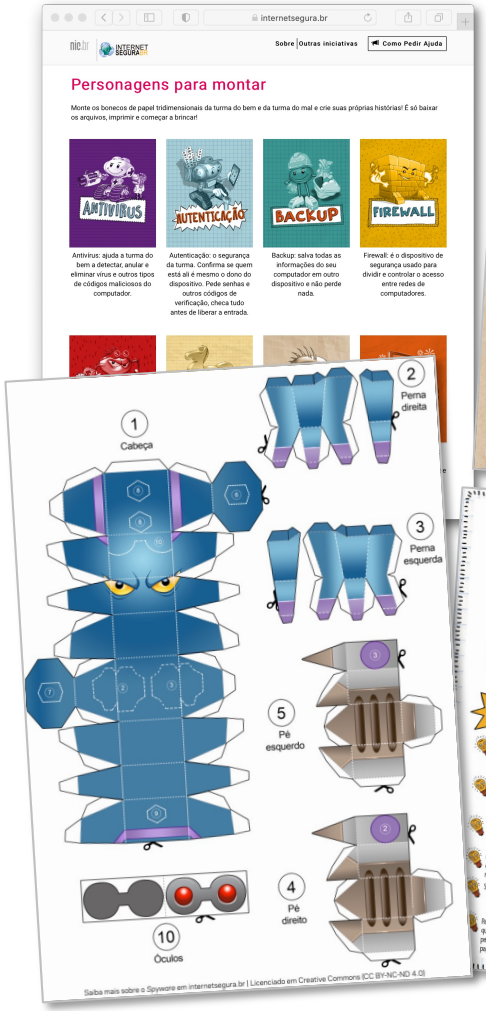
Materiais de apoio

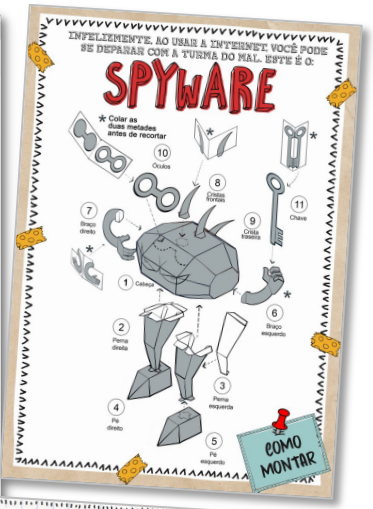
cert.br nic.br cgi.br

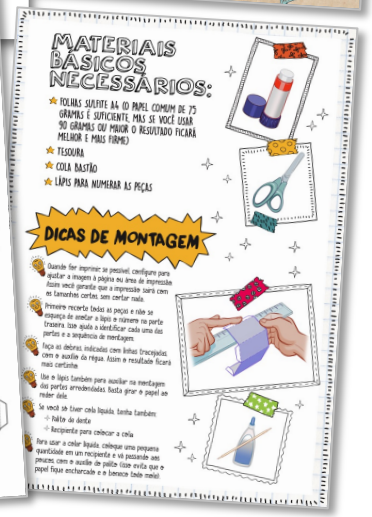
Conscientização de Todos é Essencial:
Portal InternetSegura.br – materiais gratuitos

https://internetsegura.br/ – Todo o conteúdo disponível *online* gratuitamente sob Licença *Creative Commons*

Portal InternetSegura.br:
Crianças – Dicas, Passatempos + Personagens de Montar

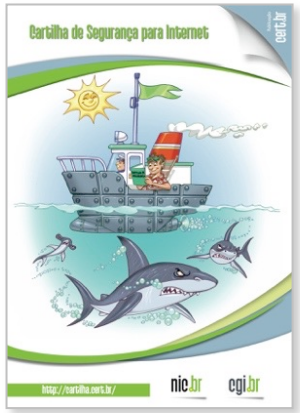






https://internetsegura.br/criancas/

Portal InternetSegura.br:
Outros públicos e Interesse Geral



https://internetsegura.br/ | https://cartilha.cert.br/ | https://antispam.br/ | https://bcp.nic.br/

Projeto Cidadão na Rede:
Vídeos curtos sobre diversos temas

"É direito e dever de cada pessoa ser um bom cidadão, e isso também vale para o mundo digital, usando de forma responsável as Tecnologias de Informação e Comunicação, em particular a Internet."

Cyberbullying: e se fosse com você?

Senhas seguras

Não clique em tudo que receber

Tome cuidado com as informações que você compartilha

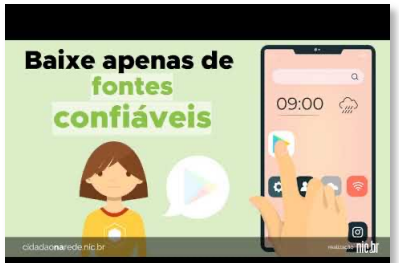
Vazamento de dados

Verificação em dois Fatores

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

Controle Parental

Compras seguras: use cartão virtual!



Cuidado com Aplicativos Falsos

Boatos

Não confie em estranhos na Internet!

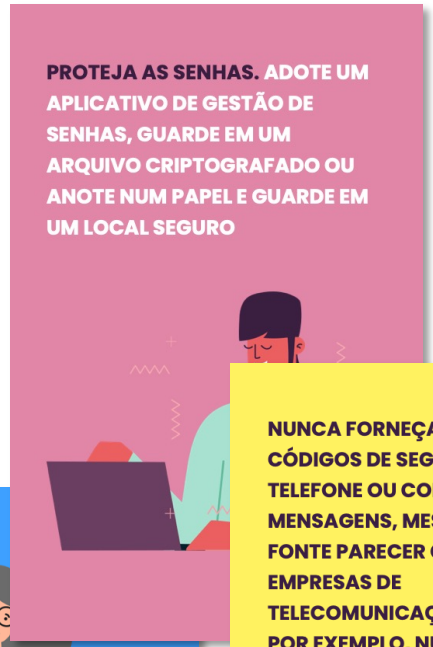
https://cidadaonarede.nic.br/

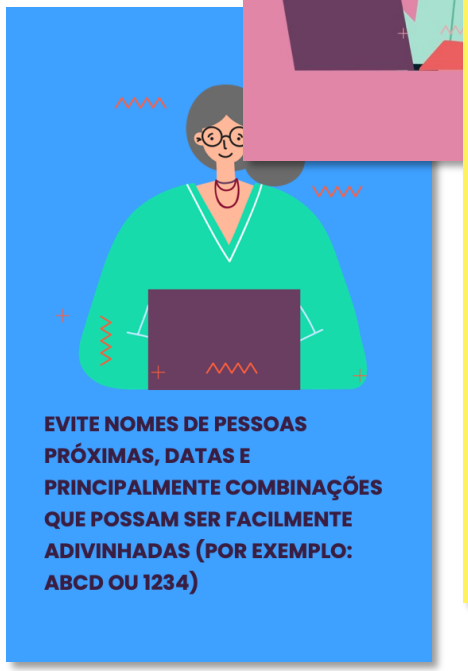
Campanha #FiqueEsperto

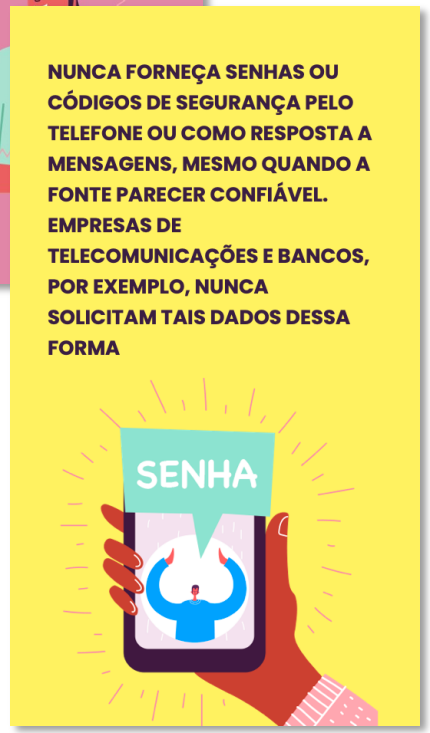
Iniciativa multissetorial em prol do uso seguro da Internet, com o objetivo de disseminar boas práticas

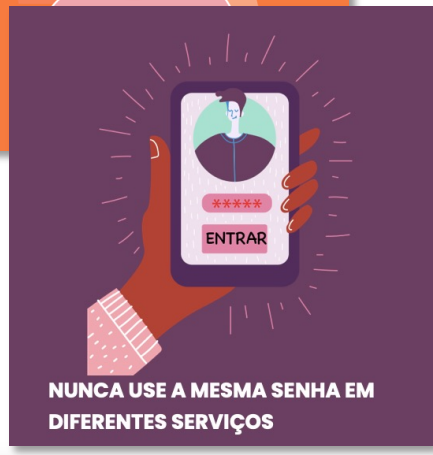
– *Site* com informações, divulgação via *e-mail*, via redes sociais e via mensagens (SMS) pelas operadoras de celular

– Apoiadores:
- ABBC
- Abranet
- Abrint
- Anatel
- Assoc. Neo
- Banco Central
- CACB
- camara-e.net
- Conexis
- CGI.br
- Febraban
- ISOC Brasil
- NIC.br
- Telcomp
- WhatsApp









https://fe.seg.br/

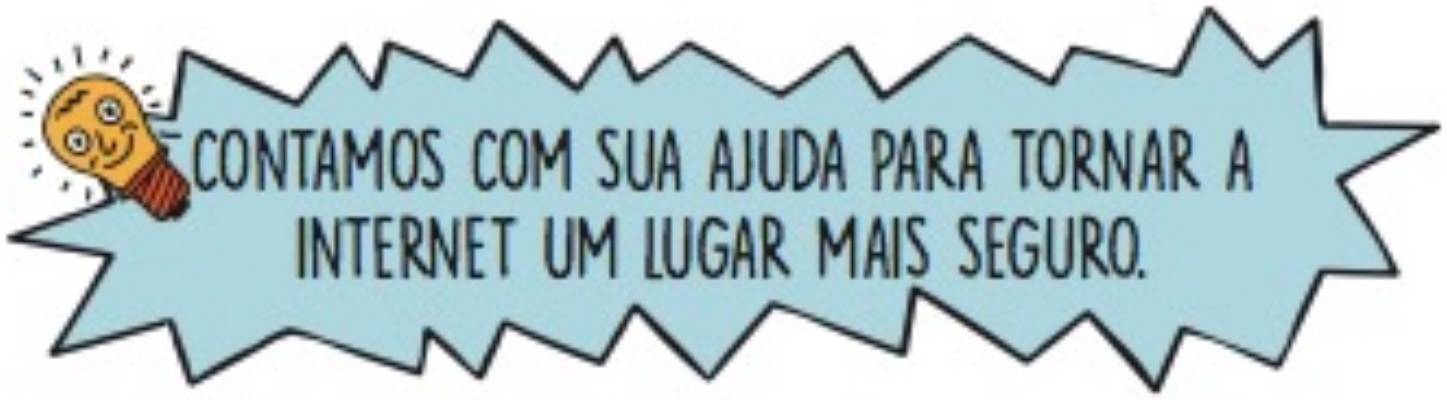
Público Técnico:
Boas Práticas com Base nos Incidentes mais Prevalentes

Objetivo de fomentar a adoção de boas práticas de segurança por profissionais da área técnica:

- Recomendações para Melhorar o Cenário de Ataques DDoS
  https://cert.br/docs/whitepapers/ddos/
- Recomendações para Notificações de Incidentes de Segurança
  https://cert.br/docs/whitepapers/notificacoes/
- Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos
  https://cert.br/docs/whitepapers/dns-recursivo-aberto/
- Práticas de Segurança para Administradores de Redes Internet
  https://cert.br/docs/seg-adm-redes/
- *Honeypots* e *Honeynets*: Definições e Aplicações
  https://cert.br/docs/whitepapers/honeypots-honeynets/
- Boas Práticas para Reduzir *Spam*
  https://antispam.br/admin/

"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

lucimara@cert.br

notificações para: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br