nic.br cgi.br | cert.br

4ª Semana de Segurança da Informação da Itaipu Binacional

02 de dezembro de 2021

Evento *Online*

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 Político

Filiações e Parcerias:

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

Criação:

Agosto/1996: CGI.br publica o relatório "Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil"[1]

Junho/1997: CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório[2]

[1] https://cert.br/sobre/estudo-cgibr-1996.html | [2] https://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 administrados pelo NIC.br

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

Governança

Mantido pelo **NIC.br** – Núcleo de Informação e Coordenação do .br

- todas as atividades são sustentadas pelo registro de domínios .br

O NIC.br é o **braço executivo do CGI.br** – Comitê Gestor da Internet no Brasil

- entidade multissetorial
- responsável por coordenar e integrar as iniciativas e serviços da Internet no País

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

Phishing: Dicas de como Proteger seus Dados e suas Contas

Miriam von Zuben
Analista de Segurança
miriam@cert.br

cert.br nic.br cgi.br

Riscos
Uso da Internet

- Exploram:
  - vulnerabilidades em sistemas
  - fragilidades de usuários (engenharia social)

- Engenharia social
  - prática de má-fé
  - usada por golpistas para tentar persuadir alguém, a fim de:
    - aplicar golpes
    - ludibriar, ou
    - obter informações sigilosas e importantes
  - explora sentimentos humanos para persuasão:
    - automatismo, urgência, obediência à autoridade
    - mentalidade de manada, distração, desejo
    - desonestidade, medo, orgulho
    - ganância, curiosidade, preguiça, caridade, gentileza

Riscos
Engenharia Social

- Principais objetivos:
  - obtenção de dados e senhas
  - invadir contas e criar contas falsas
  - servir de ponto de entrada para outros golpes e ataques
    - como furto de identidade e *ransomware*
- Dados podem ser:
  - comercializados
  - usados pelo próprio atacante
- Exemplos:
  - códigos maliciosos (*malware*)
    - vírus, *trojan*, *ransomware*, RAT, etc
  - aplicativos maliciosos
  - golpes (antecipação de recursos)
  - páginas falsas (*phishing*)

Phishing, *Phishing-scam*, *Phishing/Scam*: **Definição**

- Tipo de fraude em que um golpista:
  - tenta obter dados pessoais e financeiros de um usuário pela utilização combinada de meios técnicos e engenharia social
- Origem da palavra *phishing*:
  - do inglês "*fishing*"
  - analogia criada pelos golpistas:
    - "iscas" são usadas para "pescar" senhas e dados financeiros
- Ocorre por intermédio do envio de mensagens eletrônicas que:
  - procuram atrair a atenção do usuário
  - informam que a não execução dos procedimentos pode trazer sérias consequências
  - tentam:
    - se passar pela comunicação oficial de uma instituição conhecida
    - induzir o usuário a fornecer seus dados por meio:
      - do acesso a páginas falsas
      - da instalação de códigos maliciosos
      - do preenchimento de formulários

Tipos de *Phishing*

Tradicional	Mensagens enviadas de forma massificada
Spear phishing	Explora tópicos e temas relativos a uma pessoa ou grupo específico
Whaling	Direcionado a alvos chave das organizações. Normalmente posições que movimentam grandes somas de dinheiro ou tem acesso a informações importantes
Watering hole attack	Direcionado a *sites* acessados pelos alvos reais dos golpistas
Pharming	Redireciona a navegação do usuário para *sites* falsos, por meio de alterações no serviço de DNS
Smishing	Enviado via SMS e direcionado a usuários de dispositivos móveis

Cenário atual

cert.br nic.br cgi.br

Phishing Scam Aims to Hijack TikTok 'Influencer' Accounts

Author:
Elizabeth Montalbano
November 17, 2021 / 8:44 am

FEATURE

Business email compromise (BEC) attacks take phishing to the next level

Business email compromise (BEC) remains a popular, skillfully crafted, and continually effective phishing attack vector for cybercriminals.

By Michael Hill
UK Editor, CSO | JUL 15, 2021 2:00 AM PDT

NOTÍCIAS SEGURANÇA E PRIVACIDADE

Usuários do Instagram são alvos de novo ataque de phishing; proteja-se

Luiz Nogueira | 27/08/2019 14h44

Home › Segurança

Campanha de phishing no Facebook faz 480 mil vítimas em apenas 13 dias

Por Felipe Demartini | 10 de Fevereiro de 2021 às 10h41

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
https://www.csoonline.com/article/3624674/business-email-compromise-bec-attacks-take-phishing-to-the-next-level.html

Top 200 most common passwords

Findings

Brazil

Get the 2020 password list

RANK	PASSWORD	TIME TO CRACK IT	COUNT
1	123456	< 1 Second	1,003,925
2	123456789	< 1 Second	326,815
3	Brasil	< 1 Second	154,075
4	12345	< 1 Second	143,513
5	102030	< 1 Second	106,217
6	senha	10 Seconds	103,500
7	12345678	< 1 Second	85,937
8	1234	< 1 Second	85,158
9	10203	< 1 Second	62,649
10	123123	< 1 Second	54,441
11	123	< 1 Second	51,725
12	1234567	< 1 Second	49,286
13	654321	< 1 Second	45,459

Findings

Brazil

Get the 2020 password list

RANK	PASSWORD	TIME TO CRACK IT	COUNT
14	1234567890	< 1 Second	42,703
15	gabriel	5 Seconds	42,532
16	abc123	< 1 Second	40,939
17	q1w2e3r4t5y6	< 1 Second	40,244
18	101010	< 1 Second	38,013
19	159753	< 1 Second	37,380
20	123321	< 1 Second	34,061
21	senha123	17 Minutes	33,801
22	mirantte	3 Hours	33,027
23	flamengo	3 Hours	32,770
24	felicidade	12 Days	30,901
25	qwerty	< 1 Second	30,789

https://nordpass.com/most-common-passwords-list/

Cenário Atual:
Causas Mais Comuns de Invasões e Comprometimento de Dados

Ataques mais reportados e mais observados em sensores do CERT.br

- Acesso indevido via **senhas fracas** ou **comprometidas/vazadas**
  - senhas expostas no Github/Pastebin pelos próprios donos/desenvolvedores dos sistemas
  - força bruta de senhas em serviços protegidos só com conta e senha. Exemplos:
    - *e-mails* e serviços em nuvem
    - acesso remoto (VPN, SSH, RDP, Winbox, etc)
    - gestão remota de ativos de rede e servidores
- Exploração de vulnerabilidades antigas
  - para invasão e/ou movimentação lateral
  - falta de aplicação de correções - erros de configuração
  - falta/falha de processos

Veja também: Principais Ataques na Internet: Dados do CERT.br
https://youtu.be/nHh8hHaomFE?t=714
https://cert.br/stats/

Mais de 80% dos incidentes seriam evitados se
- todas as correções (*patches*) fossem aplicadas
- todos os serviços tivessem 2FA / MFA
- houvesse mais atenção a erros e configurações

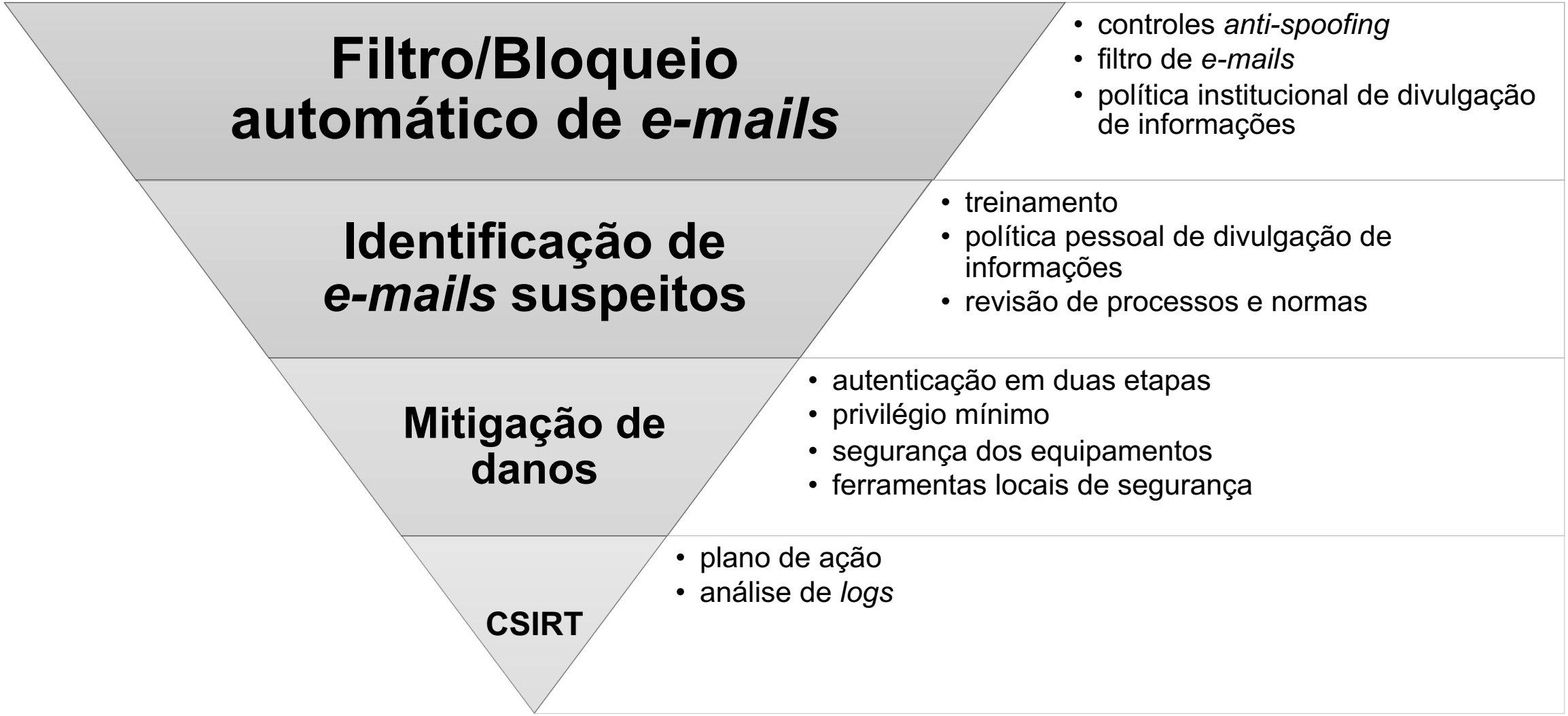
Barreiras: formação dos profissionais e priorização por gestores

Estudo Setorial Segurança digital: uma análise de gestão de risco em empresas brasileiras
https://cetic.br/pt/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/

Prevenção/Mitigação

cert.br nic.br cgi.br

Prevenção/Mitigação – *Phishing*
Tecnologia, Processos e Conscientização



Identificação de *E-mails* Suspeitos
Treinamento

- Desenvolva o pensamento crítico
  - verifique as informações (atenção aos detalhes)
    - porque você está recebendo a mensagem?
    - o que está sendo solicitado?
    - quem está enviando o *e-mail*?
    - algo parece estranho?
    - quais URLs e anexos estão presentes?
    - o que diz o cabeçalho da mensagem?

- Não confie na mensagem baseado apenas em quem a enviou
- Acesse os *sites* digitando o endereço diretamente no navegador
- Esclareça as dúvidas por um canal alternativo

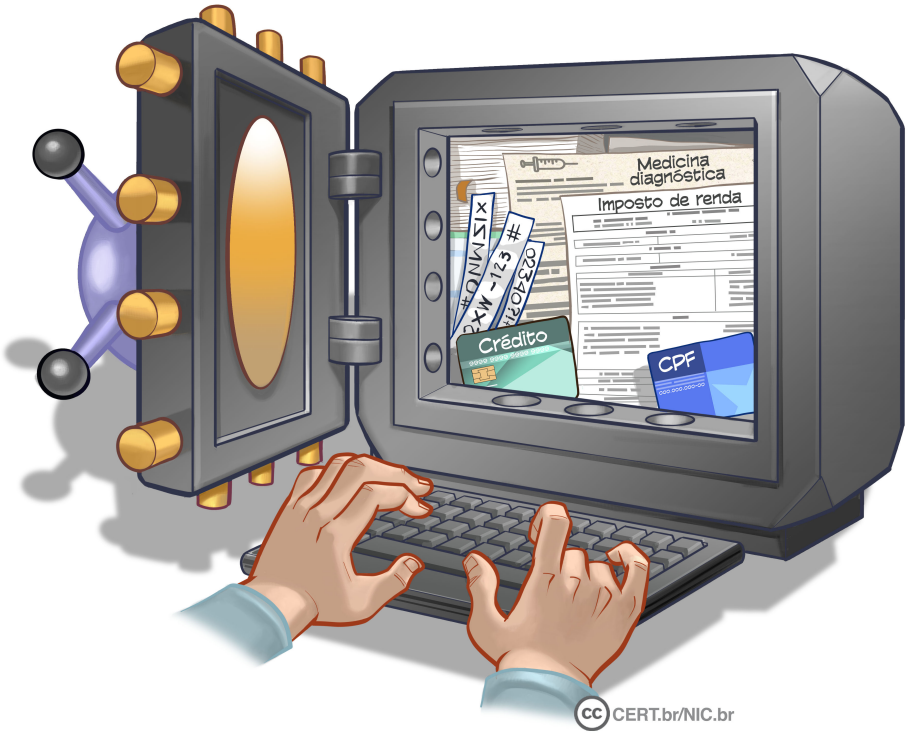
Identificação de *E-mails* Suspeitos
Política de Divulgação de Informações

- Procure restringir as informações que você divulga
  - páginas *web*, redes sociais, *blogs*
- Pense bem antes de divulgar algo
  - considere que você está em um local público
- Sempre que solicitarem dados reflita se eles são realmente necessários
- Use as opções de privacidade oferecidas pelos *sites*
  - mantenha seu perfil e seus dados privados
- Seja seletivo ao aceitar seus contatos

Identificação de *E-mails* Suspeitos
Revisão de Processos e Normas

- Conheça os processos e normas de sua empresa
  - política de confidencialidade
  - papéis dos gestores e como é o fluxo de informações
  - quem pode solicitar o que e de que forma
  - como os incidentes devem ser reportados

- Se desconfiar de algo, reporte o ocorrido
  - envie o *e-mail* completo, incluindo os cabeçalhos (*headers*)



Mitigação de Danos
Dicas de Como Minimizar os Danos (1/2)

- Proteja suas contas:
  - ative a verificação em duas etapas
  - use contas com poucos privilégios
  - use senhas bem elaboradas
  - não reuse suas senhas
  - fique atento a notificações referentes a atividades de *login*

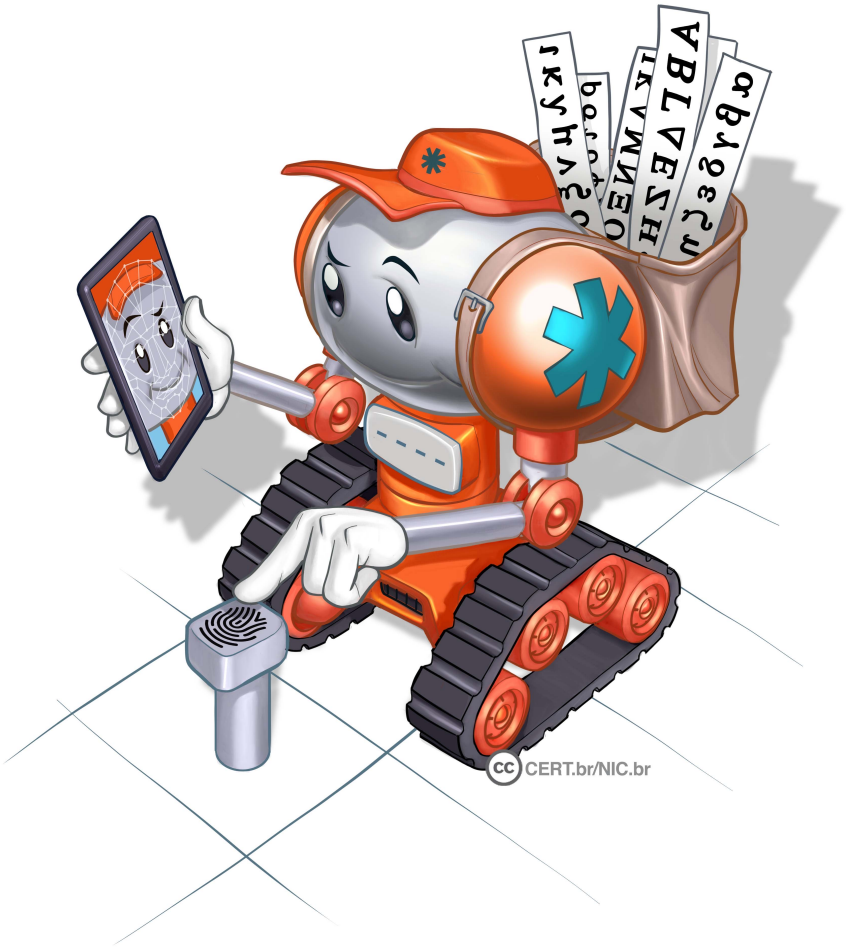
- Conheça as formas de comunicação dos serviços que usa
  - não faz parte da política da maioria das empresas o envio de mensagens, de forma indiscriminada, a seus usuários

- Mantenha seus equipamentos seguros
  - mantenha-os atualizados
  - use ferramentas de segurança

Mitigação de Danos
Dicas de Como Minimizar os Danos (2/2)

- O que fazer se for vítima de *phishing*
  - troque sua senha na página oficial
  - ative a verificação em duas etapas, caso ainda não tenha feito
  - troque a senha em todos os lugares onde é usada
  - monitore os acessos e ative notificações de *login*

- Reporte o ocorrido:
  - internamente
  - aos responsáveis pelo serviço

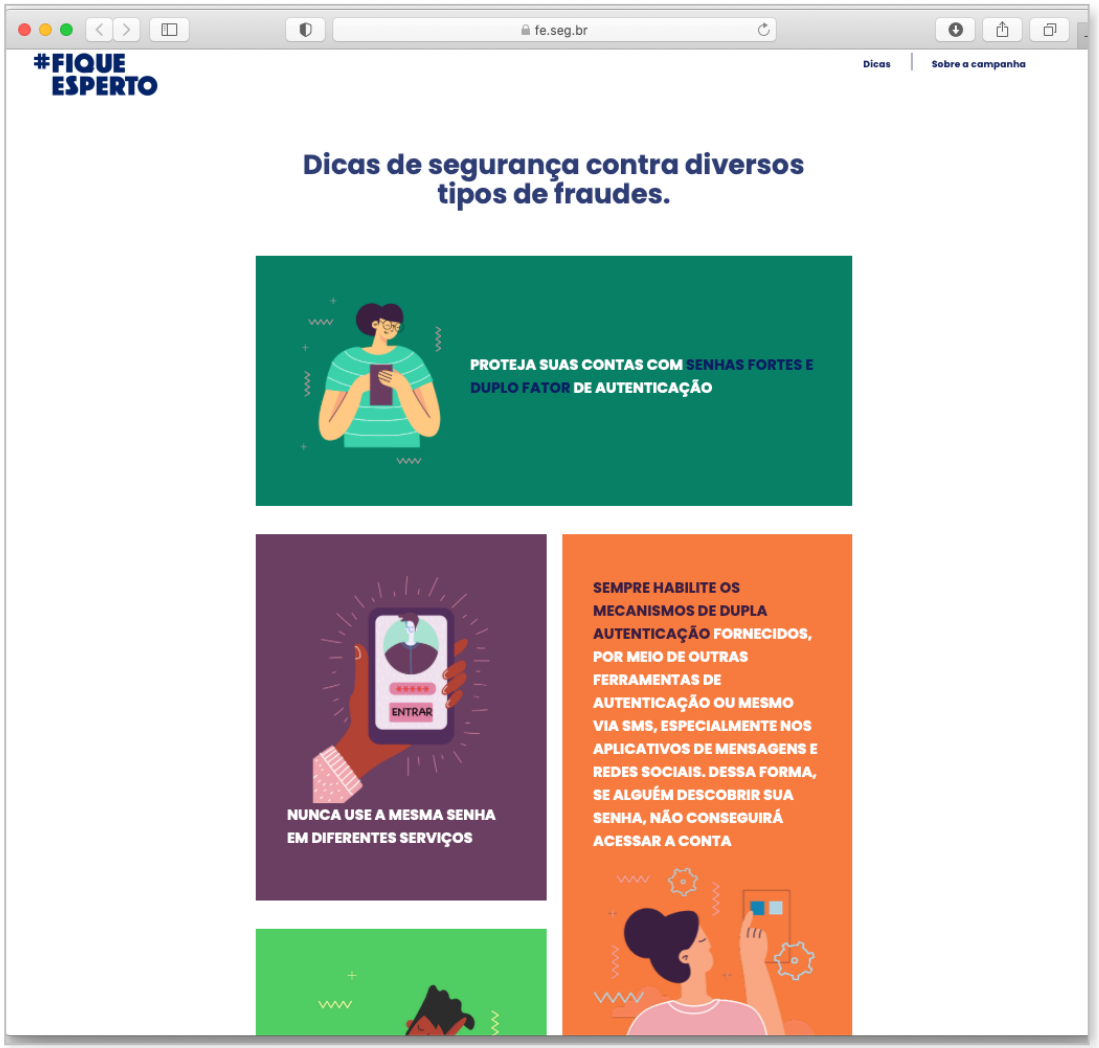


Prevenção
Mantenha-se Informado

Senhas seguras

Não clique em tudo que receber

Tome cuidado com as informações que você compartilha



https://internetsegura.br/ | https://cartilha.cert.br/ | https://cidadaonarede.nic.br/ | https://fe.seg.br/

Obrigada

miriam@cert.br

Notificações para: cert@cert.br @certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br