nic.br cgi.br | cert.br

Tarde de Conscientização em Segurança Cibernética

Anatel

21 de outubro de 2021 – Evento *Online*

Dicas de Como se Proteger Contra *Phishing*

Miriam von Zuben
Analista de Segurança
miriam@cert.br

cert.br nic.br cgi.br

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
- Sentimentos humanos usados para persuasão:
  - automatismo, urgência, obediência à autoridade, mentalidade de manada, distração, desejo, desonestidade, medo, orgulho, ganância, curiosidade, preguiça, caridade, gentileza
- Origem da palavra *phishing*:
  - do inglês "*fishing*"
  - analogia criada pelos golpistas:
    - "iscas" (mensagens eletrônicas) são usadas para ...
    - ... "pescar" senhas e dados financeiros

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

Phishing, *Phishing-scam*, *Phishing/Scam*: **Como Ocorre**

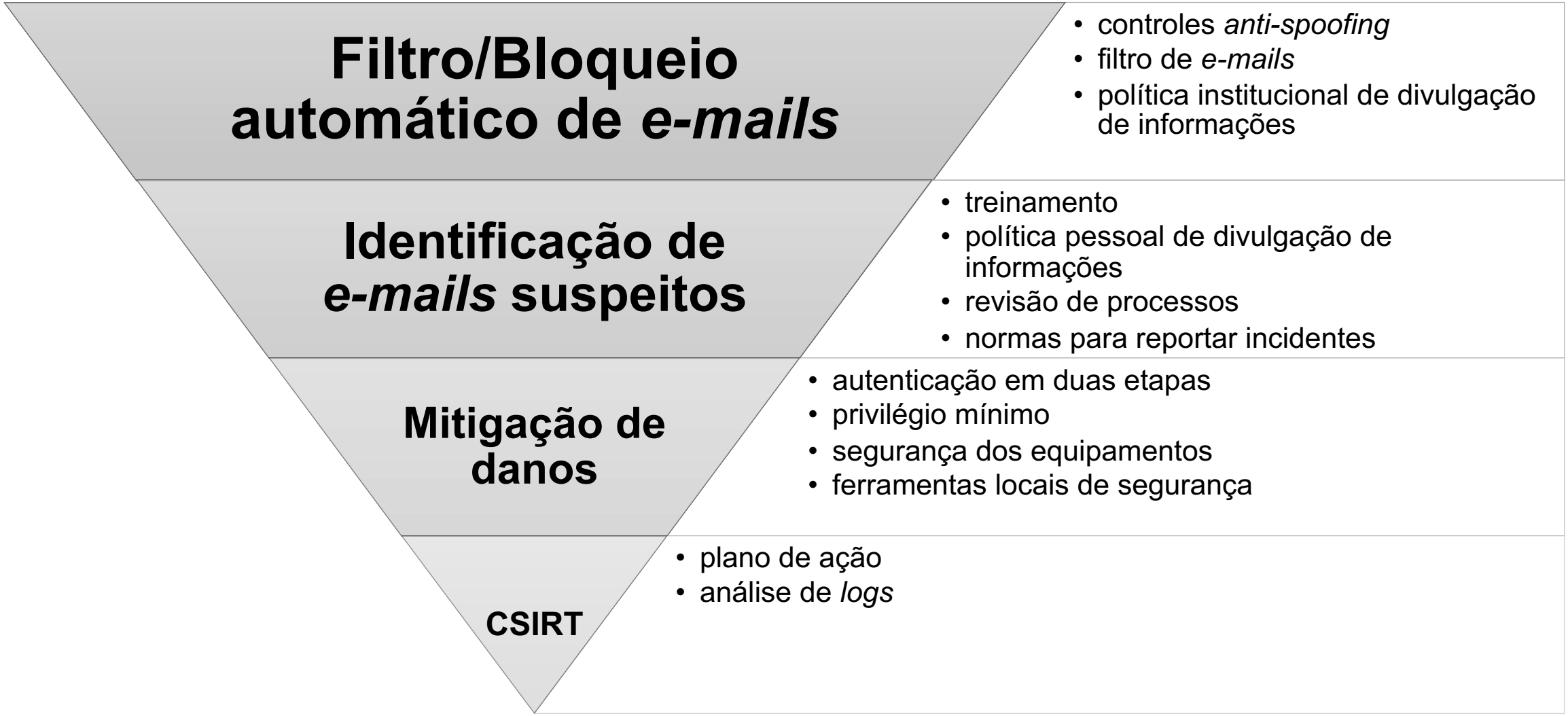
- Por intermédio do envio de mensagens eletrônicas que:
  - procuram atrair a atenção do usuário
  - tentam se passar pela comunicação oficial de uma instituição conhecida
  - informam que a não execução dos procedimentos pode trazer sérias consequências
  - tentam induzir o usuário a fornecer seus dados por meio:
    - do acesso a páginas falsas
    - da instalação de códigos maliciosos
    - do preenchimento de formulários

- Dados coletados são:
  - comercializados
  - usados para invadir contas e criar contas falsas
  - ponto de entrada para outros ataques
    - como *ransomware*

Prevenção/Mitigação

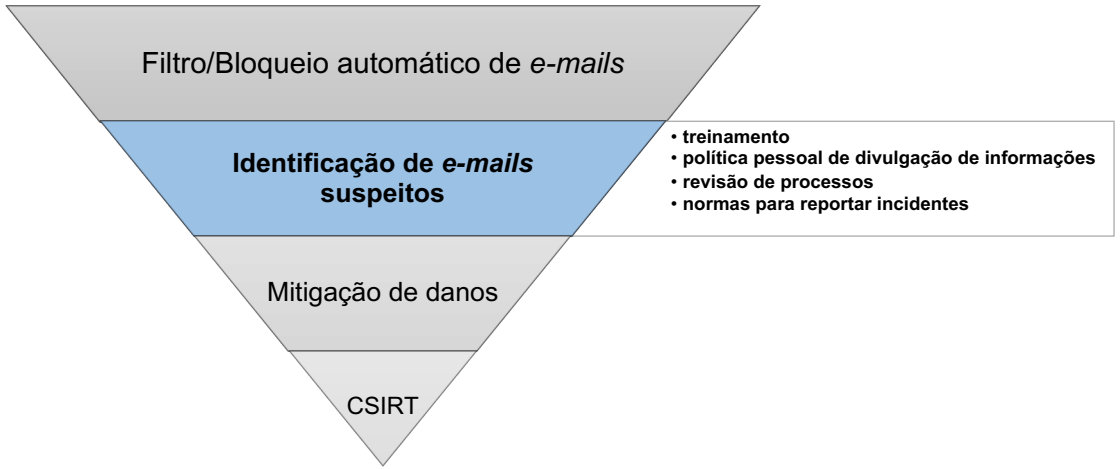
cert.br nic.br cgi.br

Prevenção/Mitigação
Tecnologia, Processos e Conscientização



Dicas de Como Identificar um *Phishing*
Ao Receber uma Mensagem

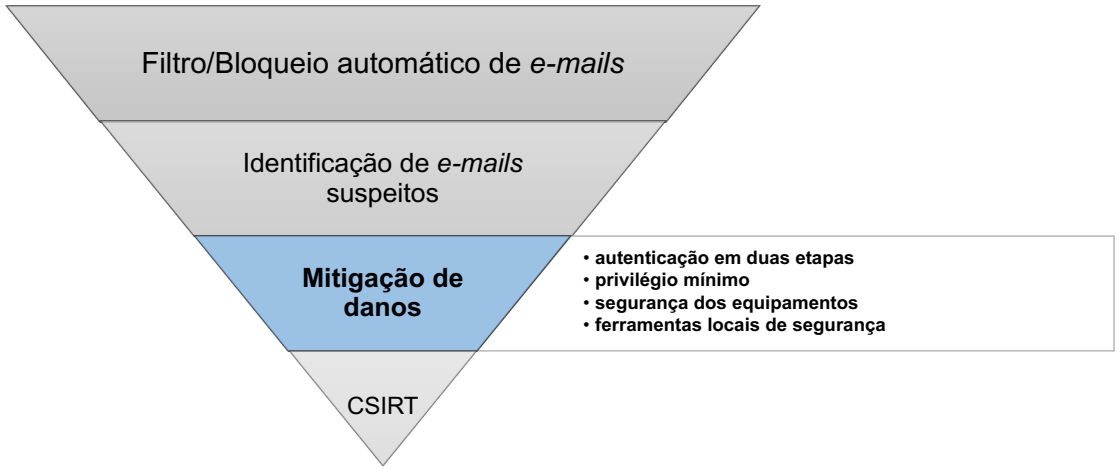
- Desenvolva o pensamento crítico
  - verifique as informações (atenção aos detalhes)
    - porque você está recebendo a mensagem?
    - o que está sendo solicitado?
    - quem está enviando o *e-mail*?
    - algo parece estranho?
    - quais URLs e anexos estão presentes?
    - o que diz o cabeçalho 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
- Reporte o ocorrido
  - envie o *e-mail* completo, incluindo os cabeçalhos (*headers*)

Prevenção/Mitigação
Dicas de Como Minimizar os Danos

- Ative a verificação em duas etapas
- Use contas com poucos privilégios
- Não reuse suas senhas
- Mantenha seus equipamentos seguros
  - mantenha-os atualizados
  - use ferramentas de segurança

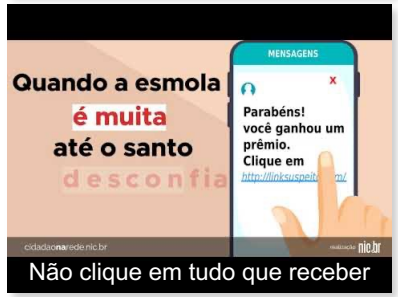


- O que fazer se for vítima de *phishing*
  - troque sua senha na página oficial
  - ative a verificação em duas etapas, caso ainda não tenha feito
  - troque a senha em todos os lugares onde é usada
  - monitore os acessos e ative notificações de *login*

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

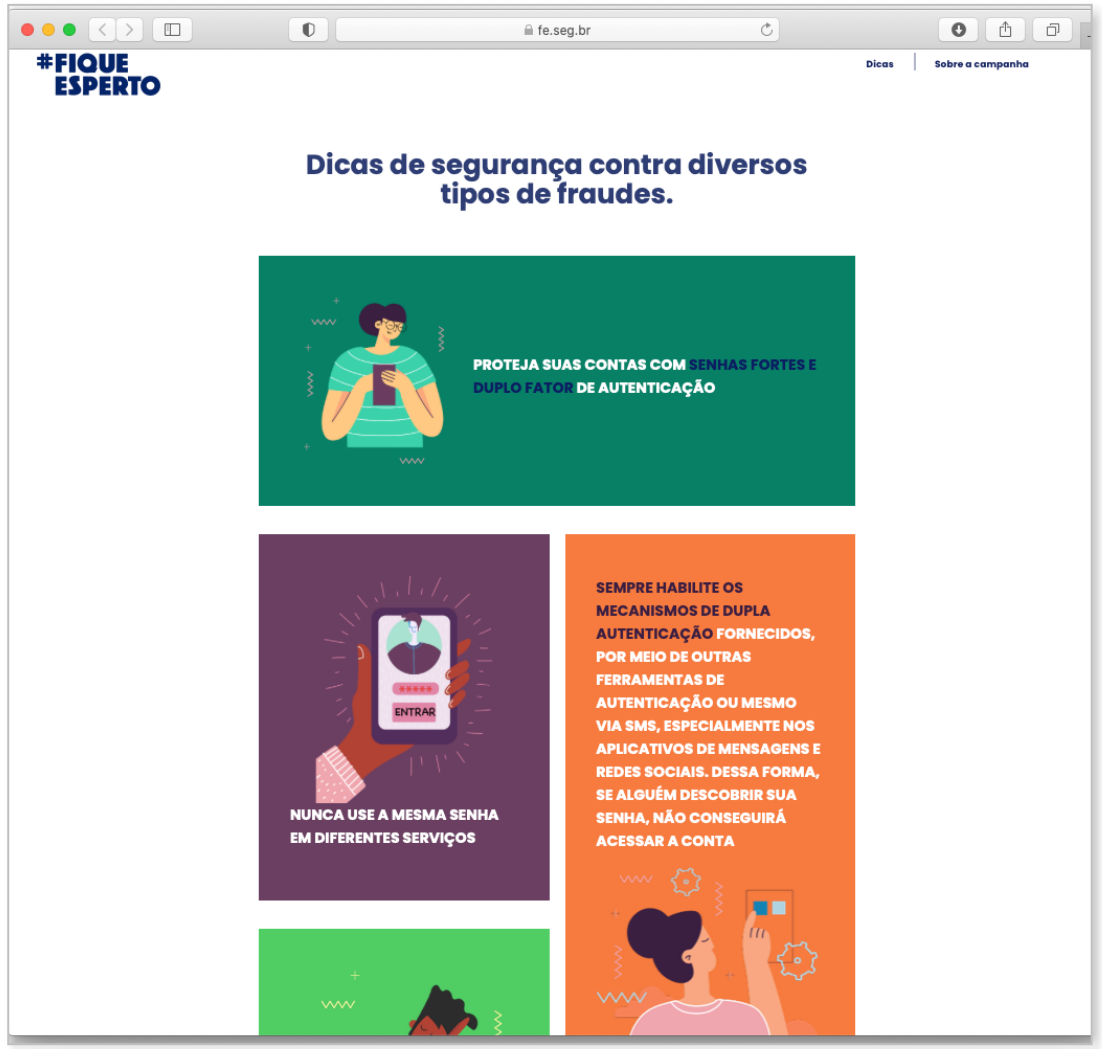
Prevenção
Mantenha-se Informado

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