nic.br cgi.br | cert.br

Ciclo de Palestras – Segurança na Internet

03 de setembro de 2015

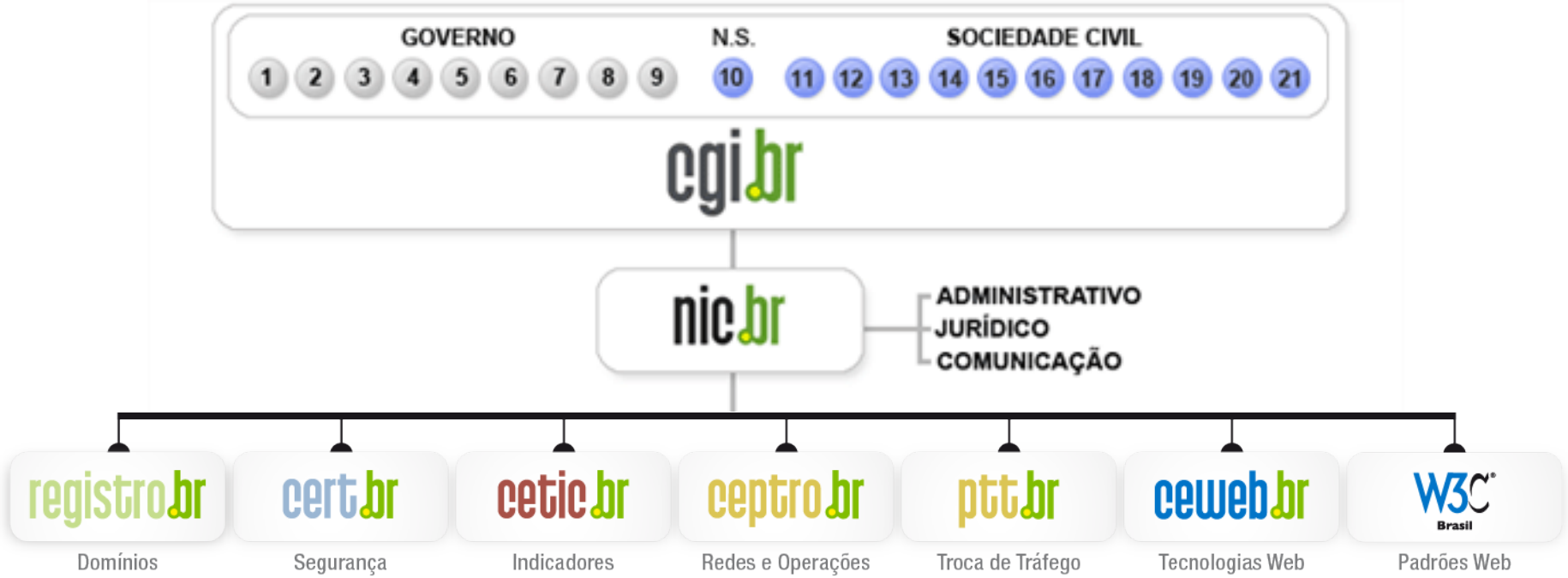
Campinas, SP

Realizando Operações Bancárias e Comerciais com Segurança na Internet

Miriam von Zuben
miriam@cert.br

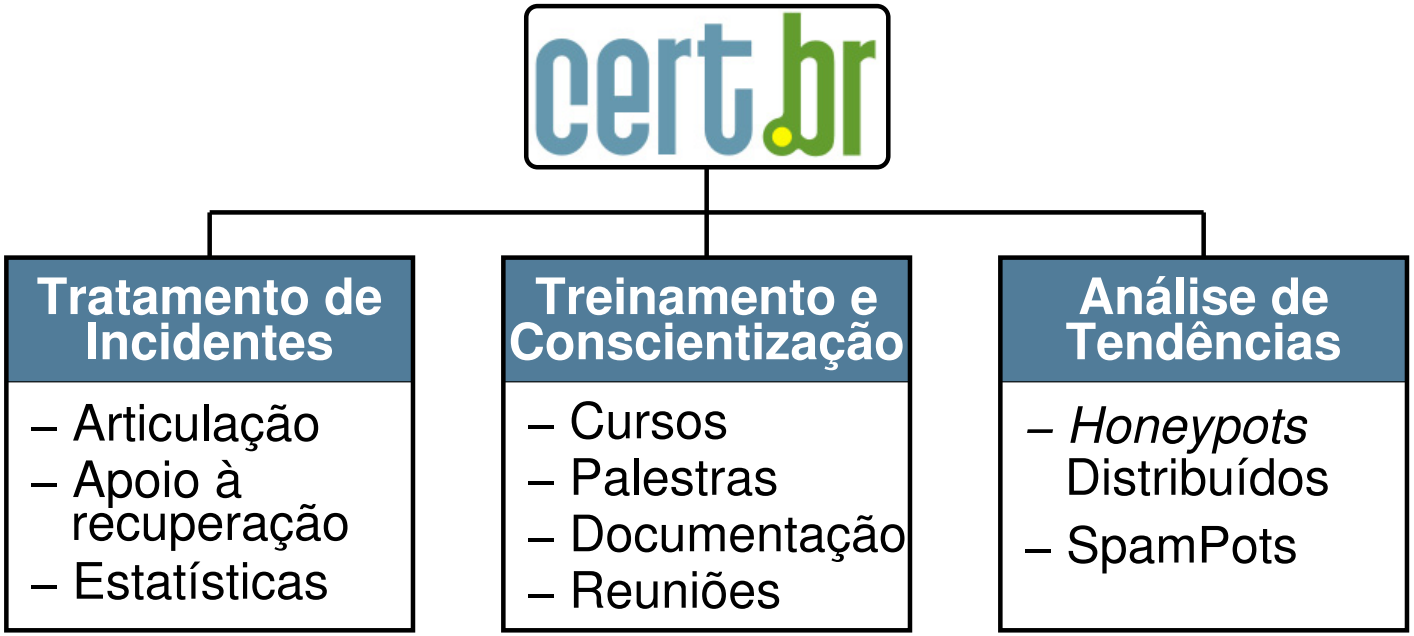
cert.br nic.br cgi.br

Estrutura do CGI.br e NIC.br



1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Cons. Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nac. de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet

11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

Criado em 1997 para:

- **Ser um ponto de contato nacional para notificação de incidentes**
- **Prover a facilitação e o apoio necessários no processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**
- **Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades**

Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil
http://www.nic.br/grupo/historico-gts.htm | http://www.cert.br/sobre/

Internet Banking e Comércio eletrônico

Vantagens

- **Realizar transações bancárias e comprar/vender produtos:**
  - sem sair de casa ou do trabalho
  - sem enfrentar filas ou engarrafamentos
  - sem ficar restrito aos dias e horários de atendimento
  - receber tudo em casa
  - pedir para entregar diretamente onde desejar

Comércio eletrônico

Comércio eletrônico – Riscos principais (1/2)

- **Não receber o produto**
- **Receber o produto, porém:**
  - com atraso
  - totalmente ou parcialmente danificado
  - com características ou especificações diferentes do esperado
  - de origem ilícita ou criminosa
    - como contrabando ou roubo de carga
- **Enfrentar dificuldades de contato com o *site*/loja**
  - a fim de resolver problemas

Comércio eletrônico – Riscos principais (2/2)

- **Ter a privacidade invadida**
  - via o compartilhamento indevido de dados pessoais
- **Ter dados pessoais ou financeiros:**
  - indevidamente obtidos, por meio:
    - do uso de computadores invadidos ou infectados
    - do acesso a *sites* fraudulentos e falsos
    - da interceptação de tráfego
      - caso o *site*/loja não use conexão segura
- **Ter os dados financeiros repassados para outras empresas e indevidamente usados para outros fins**
- **Recebimento de *spam***

Comércio eletrônico – Golpes

- **Golpistas procuram explorar a relação de confiança entre as partes envolvidas na transação comercial**
- **Principais tipos de golpes:**
  - *site* falso (*phishing*)
    - um golpista cria um *site* falso, similar ao original, e tenta induzir os clientes a fornecerem dados pessoais e financeiros
  - *site* fraudulento
    - um golpista cria um *site* fraudulento e, após os clientes efetuarem os pagamentos, não recebem as mercadorias
  - *site* de leilão e venda de produtos
    - um golpista vende produtos que nunca serão entregues ou compra mercadorias que nunca serão pagas
    - também pode usar os dados pessoais e financeiros envolvidos na transação para outros fins

Internet Banking

Internet Banking – Riscos principais

- **Perdas financeiras**
  - conta bancária pode ser usada em ações maliciosas
    - transferências indevidas de dinheiro
    - pagamento de contas de outras pessoas
- **Invasão de privacidade**
  - acesso a informações pessoais
- **Violação de sigilo bancário**
- **Participação em esquemas de fraude**
  - conta bancária pode ser usada como intermediária para:
    - aplicar golpes
    - cometer fraudes

Internet Banking – Golpes (1/3)

- **Dificuldade em fraudar dados em um servidor de uma instituição bancária**

- **Golpistas procuram persuadir as potências vítimas a:**
  - fornecerem informações sensíveis
  - realizarem ações:
    - executar códigos maliciosos
    - acessar páginas falsas (*phishing*)

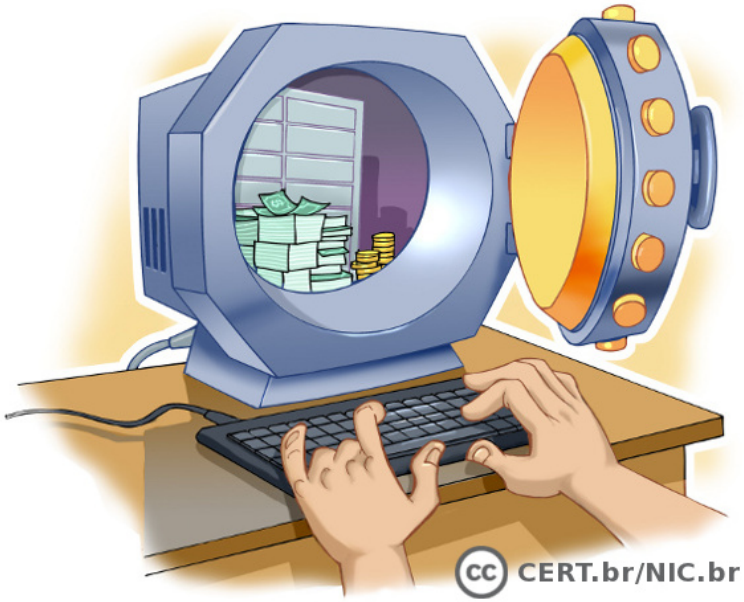
Internet Banking – Golpes (2/3)

- **Principais temas usados em golpes:**
  - atualização de cadastro e de cartão de senhas
  - sincronização de *tokens*
  - lançamento e atualização de módulos de proteção
  - comprovante de transferência e depósito
  - cadastro/recadastro de computadores
  - suspensão de acesso
  - novas campanhas
    - lançamento de produtos
    - unificação de bancos e contas

Internet Banking – Golpes (3/3)

- **Outras formas de golpes:**
  - golpe do boleto bancário
  - disponibilizar aplicativos maliciosos que podem coletar dados
  - efetuar ligações telefônicas
    - tentando se passar pelo gerente do banco e solicitar dados
  - coletar informações sensíveis trafegando sem criptografia
  - explorar possíveis vulnerabilidades em:
    - equipamentos de rede, como senhas fracas ou padrão
    - computadores/dispositivos móveis para instalar códigos maliciosos

Cuidados a serem tomados



Proteja seus equipamentos (1/2)

- **Mantenha seu computador e dispositivos móveis seguros:**
  - com as versões mais recentes dos programas instalados
  - com todas as atualizações aplicadas
  - com mecanismos de segurança instalados e atualizados
    - *antimalware*, antivírus, *antispam* e *firewall* pessoal

- **Ao instalar aplicativos desenvolvidos por terceiros**
  - seja cuidadoso ao permitir que acessem dados pessoais
  - verifique se permissões de instalação/execução são coerentes
  - seja seletivo ao escolher os aplicativos, prefira aqueles:
    - bem avaliados
    - com grande quantidade de usuários

Proteja seus equipamentos (2/2)

- **Dispositivos móveis:**
  - mantenha controle físico sobre eles
    - principalmente em locais de risco
    - procure não deixá-los sobre a mesa
    - cuidado com bolsos e bolsas
  - em caso de perda ou furto:
    - revogue autorizações concedidas para aplicativos instalados
    - cadastre um novo número de celular
    - se tiver configurado a localização remota:
      - apague remotamente os dados armazenados

Proteja seus dados

- **Cuidado com telefonemas solicitando dados pessoais**
  - como senhas e números de cartão de crédito
- **Não responda mensagens de instituições com as quais você não se relacione**
- **Procure reduzir a quantidade de informações que possam ser obtidas sobre você**
  - isso pode impedir a criação de contas fantasma em seu nome
- **Verifique periodicamente seu extrato bancário e do seu cartão de crédito**
  - entre em contato com o seu banco ou com a operadora do seu cartão de crédito caso detecte lançamentos suspeitos

Mantenha seus cadastros atualizados

- **Dados pessoais podem ser solicitados aleatoriamente para checar a sua identidade**

- **Seu endereço de correspondência pode ser usado para o envio de tokens e cartões de segurança**

- **Dados pessoais e perguntas de segurança podem ser solicitados**

Proteja suas senhas

- **Procure usar senhas com:**
  - grande quantidade de caracteres
  - diferentes tipos de caracteres
- **Não utilize:**
  - dados pessoais, como nome, sobrenome e datas
  - dados que possam ser facilmente obtidos sobre você
- **Evite reutilizar suas senhas**
- **Troque periodicamente suas senhas**
- **Não informe senhas via *e-mails* ou telefonemas**

Ao acessar os *sites*

- **Use computadores e dispositivos móveis seguros**
- **Digite o endereço do *site* diretamente no navegador *Web***
  - evite clicar/seguir *links* recebidos via mensagens eletrônicas
    - *e-mails*, mensagens SMS, redes sociais, etc.
  - não utilize sites de busca para localizar o *site*
    - geralmente o endereço é bastante conhecido
- **Evite usar:**
  - redes Wi-Fi públicas
  - computadores e dispositivos móveis de terceiros
    - *lan houses*, Internet cafés, etc.

Ao acessar os *sites*

- **Certifique-se de usar conexões seguras:**
  - alguns indícios apresentados pelo navegador *Web* são:
    - o endereço começa com https://
    - o desenho de um “cadeado fechado” é mostrado na barra de endereço
      - ao clicar sobre ele são exibidos detalhes sobre a conexão e certificado digital em uso
    - um recorte colorido (branco ou azul) com o nome do domínio do *site* é mostrado ao lado da barra de endereço (à esquerda ou à direita)
      - ao passar o *mouse* ou clicar sobre o recorte são exibidos detalhes sobre a conexão e certificado digital em uso
    - a barra de endereço e/ou recorte são apresentados em verde e no recorte é colocado o nome da instituição dona do *site*

Ao acessar os *sites*

Ao acessar os *sites*

- **Existem casos onde a instituição utiliza uma conexão mista (parte da conexão é segura e parte não é)**
  - neste caso verifique com a instituição:
    - se o tipo de conexão utilizada é realmente mista ou
    - se poderia ser um *site* falso
- **Use sempre a opção de "sair"**
- **Seja cuidadoso com mensagens sobre promoções**

Comércio eletrônico – Antes de comprar (1/2)

- **Verifique se o *site*/loja é confiável**
  - pesquise na Internet para ver a opinião de outros clientes
    - principalmente em redes sociais e sites de reclamação
  - escolha lojas que você conheça pessoalmente e/ou que tenha boas referências
  - observe:
    - as políticas de privacidade, garantia, troca, cancelamento, arrependimento e devolução
    - se há reclamações referentes a empresa
      - avalie se elas foram tratadas adequadamente
    - se são disponibilizados canais de atendimento
      - como *e-mai*l, *chat* e telefone de contato
    - se a empresa disponibiliza informações como endereço, telefone e CNPJ
  - valide os dados de cadastro da empresa no site da Receita Federal:
    - http://www.receita.fazenda.gov.br/

Comércio eletrônico – Antes de comprar (2/2)

- **Verifique as condições de compra:**
  - faça uma pesquisa de mercado, comparando o preço do produto desejado com o preço médio obtido na pesquisa
    - desconfie caso esteja muito barato
  - observe:
    - as condições do produto (novo, usado, defeituoso)
    - a descrição detalhada ou especificação técnica
      - tenha certeza do que você está comprando
    - o prazo de entrega
      - sempre compre com antecedência para evitar transtornos
- **Verifique a reputação/qualificação do vendedor**
- **Não compre caso desconfie de algo**

Comércio eletrônico – Ao comprar (1/2)

- **Verifique as opções de pagamento oferecidas pelo site/ loja**
  - escolha aquela que considerar mais segura
- **Ao fornecer dados sensíveis via *e-mail* certifique-se de criptografar a mensagem**
- **Guarde as informações da compra**
  - como comprovantes e número de pedido
  - documente outros contatos que você venha a ter
  - essas informações podem ser importantes em caso de problemas

Comércio eletrônico – Ao comprar (2/2)

- **Utilize sistemas de gerenciamento de pagamentos**
  - além de dificultarem a aplicação dos golpes, também podem impedir que seus dados pessoais e financeiros sejam enviados aos golpistas

- **Caso tenha alguma dúvida entre em contato com a central de relacionamento da empresa**

Comércio eletrônico – Ao receber o produto

- **Marque encontros em locais públicos**
  - caso a entrega seja feita pessoalmente
- **Não confie apenas no código de rastreamento dos Correios**
  - até ter o produto em mãos não há nenhuma garantia de que ele foi realmente enviado
- **Antes de abrir a embalagem:**
  - verifique se ela não está danificada
- **Certifique-se de que o produto está de acordo com o que foi comprado**
- **Comente sobre a compra no *site***

Comércio eletrônico – Em caso de problemas

- **Entre em contato com a empresa e verifique o ocorrido**
- **Se houver problemas de contato com o site/loja:**
  - utilize sites de reclamações
- **Utilize o Código de Defesa do Consumidor**
  - denuncie o ocorrido ao PROCON da sua cidade, que poderá orientá-lo sobre a melhor forma de agir

Internet Banking – Ao acessar os *sites* (1/4)

- **Antes de instalar um módulo de proteção, certifique-se de que o autor é realmente a instituição em questão**
- **Utilize um endereço terminado em "b.br", se disponível**
  - verifique se seu banco oferece essa opção
  - domínios terminados em "b.br":
    - são de uso exclusivo de instituições bancárias
    - oferecem recursos adicionais de segurança
- **Acesse a conta usando a página ou aplicativo fornecido pela própria instituição**

Internet Banking – Ao acessar os *sites* (2/4)

- **Ao usar códigos de verificação:**
  - mantenha seus dados para recebimento sempre atualizados
    - números de telefones celulares alternativos podem ser cadastrados, caso o seu principal não esteja disponível
  - tenha certeza de estar de posse de seu telefone celular, caso tenha configurado o envio via SMS

Internet Banking – Ao acessar os *sites* (3/4)

- **Ao usar cartões de segurança:**
  - guarde seu cartão em um local seguro
  - nunca forneça os códigos do cartão por *e-mail* ou telefone
  - forneça apenas uma posição do seu cartão a cada acesso
  - verifique se o número de identificação do cartão apresentado pelo serviço corresponde ao que está no seu cartão
    - caso sejam diferentes entre em contato com o serviço
  - desconfie caso, em um mesmo acesso, seja solicitada mais de uma posição do cartão

Internet Banking – Ao acessar os *sites* (4/4)

- **Ao usar *tokens*:**
  - guarde seu token em um local seguro
  - nunca informe o código mostrado no *token* por *e-mail* ou telefone
  - caso perca seu *token* ou ele seja furtado:
    - avise imediatamente o responsável pelo serviço no qual ele é usado

- **Ao cadastrar um dispositivo confiável:**
  - não esqueça de excluir seus dispositivos confiáveis caso eles sejam trocados ou você perca o acesso a eles

Internet Banking – Boleto bancário

- **Verifique os dados impressos no boleto**
  - número do banco
    - 3 primeiros dígitos
    - lista dos códigos disponível no *site* da Febraban
  - número do código de barras
    - deve ser igual ao corresponde ao parte superior fatura
  - CNPJ da empresa emissora do boleto
  - data de vencimento
  - dados do beneficiário
  - valor cobrado corresponde ao devido pelo consumidor

Internet Banking – Outros cuidados

- **Evite acessar a central de atendimento do seu banco por meio de celulares de terceiros**
  - os dados digitados podem ficar armazenados
- **A maioria dos bancos não envia *e-mails* sem autorização**
  - desconsidere mensagens recebidas, caso não tenha autorizado
  - principalmente de instituições com as quais não tenha relação
- **Em caso de dúvidas ou problemas:**
  - entre em contato imediatamente com:
    - a central de relacionamento do seu banco
    - diretamente com o seu gerente
    - a operadora do seu cartão de crédito

Referências

cert.br nic.br cgi.br

Educação de Usuários:
Cartilha de Segurança para Internet

Livro (PDF e ePub) e conteúdo no *site* (HTML5)
Dica do dia no site, via *Twitter* e RSS
http://cartilha.cert.br/

Cartilha de Segurança para Internet
Fascículos

Organizados de forma a facilitar a difusão de conteúdos específicos:

- **Redes Sociais**
- **Senhas**
- **Comércio Eletrônico**
- **Privacidade**
- **Dispositivos Móveis**
- ***Internet Banking***
- **Computadores**
- **Códigos Maliciosos**
- **Verificação em Duas Etapas**
- **Redes**

Acompanhados de *Slides* de uso livre para:

- **ministrar palestras e treinamentos**
- **complementar conteúdos de aulas**

Outros Materiais para Usuários Finais

Portal Internet Segura

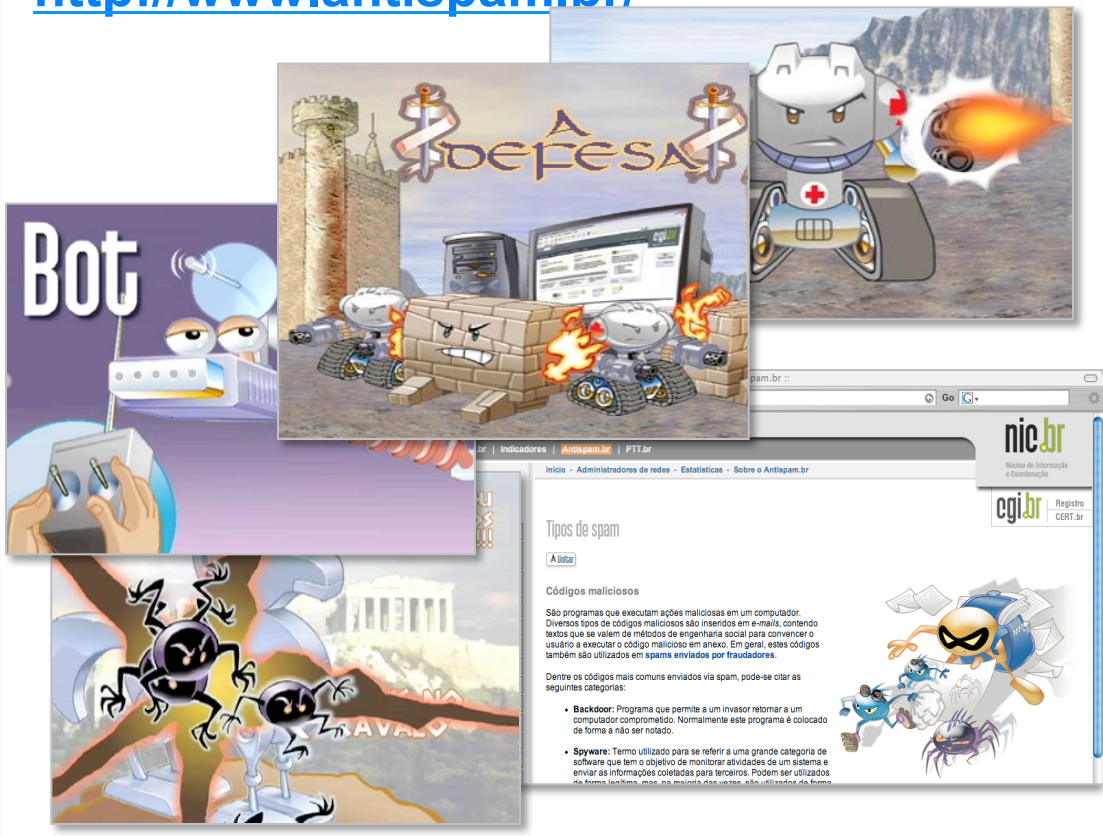
- **Reúne todas as iniciativas conhecidas de educação de usuários no Brasil**

http://www.internetsegura.br/

INTERNET SEGURA.BR

Site e vídeos do Antispam.br

http://www.antispam.br/



Obrigada

www.cert.br

miriam@cert.br

@certbr

03 de setembro de 2015

nic.br cgi.br

www.nic.br | www.cgi.br