

nic.br egi.br

cert.br

VI Fórum da Internet no Brasil
11 a 13 de julho de 2016
Porto Alegre, RS

Navegar é preciso, arriscar-se não!

Dicas de uso seguro da Internet

Lucimara Desiderá
lucimara@cert.br

cert.br nic.br cgi.br

Agenda

- **Introdução**
 - CGI.br, NIC.br e CERT.br
- **Segurança na Internet**
- **Riscos no uso da Internet**
- **Prevenção**



1 2 3 4 5 6 7 8 9

GOVERNO

10 11 12 13 14 15 16 17 18 19 20 21

SOCIEDADE CIVIL

e

Representantes do Governo:

- 1 Ministério da Ciência, Tecnologia e Inovação (coordenador)
- 2 Casa Civil da Presidência da República
- 3 Ministério das Comunicações
- 4 Ministério da Defesa
- 5 Ministério do Desenvolvimento, Indústria e Comércio Exterior
- 6 Ministério do Planejamento, Orçamento e Gestão
- 7 Agência Nacional de Telecomunicações
- 8 Conselho Nacional de Desenvolvimento Científico e Tecnológico
- 9 Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

Representantes da Sociedade Civil:

- 10 Notório saber em assunto da Internet
- 11 a 14 Representantes do setor empresarial
 - provedores de acesso e conteúdo da Internet
 - provedores de infra-estrutura de telecomunicações
 - indústria de bens de informática, de bens de telecomunicações e de software
 - setor empresarial usuário
- 15 a 18 Representantes do terceiro setor
- 19 a 21 Representantes da comunidade científica e tecnológica

Comitê Gestor da Internet no Brasil – CGI.br

Tem a missão de estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil

Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03 de setembro de 2003, destacam-se:

- a proposição de normas e procedimentos relativos à regulamentação das atividades na internet;
- a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;
- o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;
- a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;
- a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;
- a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.
- ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;

<http://www.cgi.br/sobre/>

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

registro.br

Domínios

cert.br

Segurança

cetic.br

Indicadores

ceptro.br

Redes e Operações

ceweb.br

Tecnologias Web

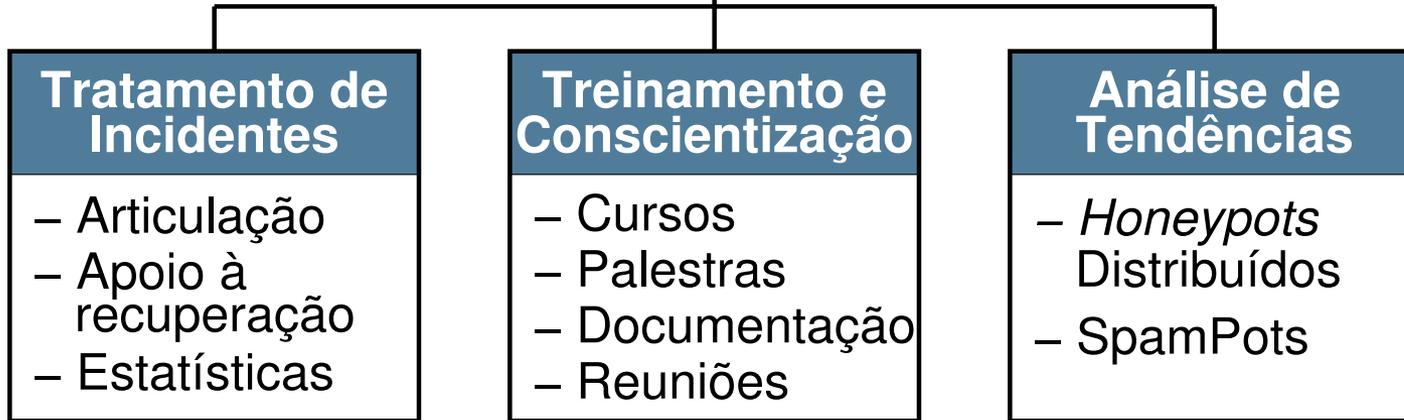
ix.br

Troca de Tráfego

W3C
Brasil

Padrões Web

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



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/>

Segurança na Internet



Segurança na Internet

Internet está presente no cotidiano de grande parte da população

- **Alguns usos:**
 - *Internet Banking*
 - comércio eletrônico
 - redes sociais
 - estudo a distância
 - governo eletrônico
- **Aproveitar esses benefícios de forma segura requer que alguns cuidados sejam tomados**
 - ter consciência de que a Internet não é um mundo “virtual”
 - importante estar informado dos riscos a que está exposto para poder tomar medidas preventivas / postura preventiva

Riscos no uso da Internet



Riscos no uso da Internet (1/5)

- **Acesso a conteúdos impróprios ou ofensivos**
- **Contato com pessoas mal-intencionadas**
- **Furto de identidade**
- **Furto e perda de dados**
- **Invasão de privacidade**
- **Divulgação de boatos**
- **Uso excessivo**
- **Plágio e violação de direitos autorais**
- **Dificuldade de:**
 - exclusão
 - manter sigilo
 - detectar e expressar sentimentos

Riscos no uso da Internet (2/5)

- **Achar que não corre riscos, supondo que:**
 - seu computador dificilmente será localizado
 - ninguém possui interesse em:
 - acessar seus dados
 - usar seu computador
- **Tipo de pensamento explorado pelos atacantes**
 - ao se sentir seguro você pode achar que não precisa se prevenir
- **Atacantes interessados em acessar muitos computadores**
 - independente de quais são
 - podem efetuar varreduras na rede, localizar grande parte dos computadores conectados à Internet

INCLUSIVE O SEU

- **Ilusão termina quando os primeiros problemas aparecem**

Riscos no uso da Internet (3/5)

- **Um problema de segurança em seu computador pode:**
 - torná-lo indisponível
 - colocar em risco a confidencialidade e a integridade dos dados nele armazenados / processados
- **Ao ser comprometido, seu computador pode ser usado para a prática de atividades maliciosas como:**
 - servir de repositório para dados fraudulentos
 - lançar ataques contra outros computadores
 - propagar códigos maliciosos
 - disseminar *spam*

Riscos no uso da Internet (4/5)

- **Se um invasor tiver acesso as suas senhas ele pode:**
 - **acessar a sua conta de correio eletrônico e:**
 - ler e/ou apagar seus *e-mails*
 - furtar sua lista de contatos e enviar *e-mails* em seu nome
 - enviar mensagens contendo:
 - *spam*, boatos, *phishing*, códigos maliciosos
 - pedir o reenvio de senhas de outras contas
 - e assim conseguir acesso a elas
 - trocar a sua senha
 - **acessar a sua rede social e:**
 - denegrir a sua imagem
 - explorar a confiança de seus amigos/seguidores
 - enviar mensagens em seu nome
 - alterar as configurações feitas por você
 - tornando públicas informações privadas
 - trocar a sua senha

Riscos no uso da Internet (5/5)

- **Se um invasor tiver acesso as suas senhas ele pode (cont.):**
 - **acessar a sua conta bancária e:**
 - verificar o seu extrato e seu saldo bancário
 - **acessar o seu *site* de comércio eletrônico e:**
 - alterar informações de cadastro
 - fazer compras em seu nome
 - verificar informações sobre suas compras anteriores
 - **acessar o seu dispositivo móvel e:**
 - furtar sua lista de contatos e suas mensagens
 - acessar e/ou copiar fotos e vídeos
 - bloquear o acesso ao dispositivo
 - apagar os dados armazenados no dispositivo
 - lançar ataques contra outros computadores

Golpes na Internet



CC CERT.br/NIC.br

Golpes na Internet (1/3)

- Não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária ou comercial
- Golpistas concentrando esforços na exploração de fragilidades dos usuários
 - engenharia social
 - procuram enganar e persuadir as potenciais vítimas a:
 - fornecerem informações sensíveis
 - realizarem ações, como executar *malware* e acessar páginas falsas
- Vários dos golpes aplicados na Internet podem ser considerados crimes contra o patrimônio, tipificados como estelionato
 - golpista → estelionatário

Golpes - Furto de identidade

- **Ato pelo qual uma pessoa tenta se passar por outra**
 - atribuindo-se uma falsa identidade
 - objetivo de obter vantagens indevidas
- **Como ocorre:**
 - criação de contas falsas
 - invasão de contas
 - falsificação de *e-mails*
- **Quanto mais informação você disponibiliza sobre sua vida e rotina**
 - mais fácil para um golpista roubar sua identidade

Golpes - Fraude de antecipação de recursos

- **Golpista procura induzir uma pessoa a:**
 - fornecer informações confidenciais, ou
 - realizar um pagamento adiantado
- **Promessa de futuramente receber algum tipo de benefício**
- **Exemplos:**
 - golpe da Nigéria
 - crédito fácil
 - oferta de emprego
 - loteria internacional
 - doação de animais
 - noiva russa

Golpes – *Phishing scam*

- **Usado por golpistas para tentar obter dados pessoais e financeiros de um usuário**
 - utilização combinada de meios técnicos e engenharia social
- **Ocorre via mensagens eletrônicas que:**
 - tentam se passar pela comunicação oficial de uma instituição conhecida
 - procuram atrair a atenção do usuário
 - por curiosidade, caridade ou possibilidade de vantagem financeira
 - exploram campanhas de publicidade, serviços, imagem de pessoas, assuntos em destaque no momento
 - informam que a não execução dos procedimentos pode acarretar sérias consequências
 - tentam induzir o usuário a fornecer dados pessoais e financeiros
 - acesso a páginas falsas
 - instalação de códigos maliciosos, projetados para coletar informações
 - preenchimento de formulários contidos na mensagem ou em páginas Web

Golpes – Exemplos de *phishing scam*

- **Páginas falsas de:**
 - comércio eletrônico
 - *Internet Banking*
 - redes sociais
 - companhias aéreas
 - programas de milhagem
- **Mensagens contendo formulários:**
 - recadastramento de conta
 - grupo de suporte
- **Mensagens contendo links para códigos maliciosos**
 - “Clique aqui”
 - ações judiciais
 - imposto de renda
 - reality shows
 - regularização de débitos

Ataques na Internet



Ataques na Internet

- **Qualquer serviço, computador ou rede que seja acessível via Internet pode:**
 - ser alvo de um ataque
 - participar de um ataque
- **Motivação dos atacantes:**
 - demonstração de poder
 - prestígio
 - financeira
 - ideológica
 - comercial

Ataques na Internet – tipos

- Exploração de vulnerabilidades
- Varredura em redes (*scan*)
- Falsificação de e-mail (*e-mail spoofing*)
- Interceptação de tráfego (*sniffing*)
- Força bruta (*brute force*)
- Negação de serviço (DoS e DDoS)
- Desfiguração de página (*defacement*)
 - *sites* de grandes instituições
 - hospedagem de *malware*

Códigos Maliciosos (*Malware*)



Códigos maliciosos

- **Programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador**
- **Infectam também dispositivos móveis**
 - *tablets, celulares, smartphones, etc.*
- **Uma vez instalados:**
 - **passam a ter acesso aos dados armazenados no computador**
 - **ou bloquear o acesso a eles**
 - **podem executar ações em nome dos usuários**
 - **de acordo com as permissões de cada usuário**
- **Vírus, worm, bot, spyware, backdoor, trojan, rootkit, ransomware**

Códigos maliciosos

- **Um computador pode ser infectado ou comprometido:**
 - pela exploração de vulnerabilidades nos programas instalados
 - pela auto-execução de mídias removíveis infectadas
 - pelo acesso a páginas *Web* maliciosas, via navegadores vulneráveis
 - pela ação direta de atacantes
 - pela instalação de aplicativos maliciosos
 - pela execução de arquivos previamente infectados, obtidos:
 - anexos em mensagens eletrônicas
 - via mídias removíveis
 - em páginas *Web*
 - diretamente de outros computadores
- **São usados como intermediários, possibilitam:**
 - prática de golpes, realização de ataques, disseminação de spam

Outros Riscos



Outros riscos

- **Boatos**
- ***Spam***
- ***Cookies***
- **Códigos móveis**
- **Janelas de *pop-up***
- ***Plug-ins*, complementos e extensões**
- ***Links* patrocinados**
- ***Banners* de propaganda**
- **Programas de distribuição de arquivos (P2P)**
- **Compartilhamento de recursos**

Prevenção



Prevenção

- **Internet não tem nada de “virtual”**
 - tudo o que ocorre ou é realizado por meio dela é real
 - os riscos aos quais você está exposto ao usá-la são os mesmos presentes no seu dia a dia
 - os golpes que são aplicados por meio dela são similares àqueles que ocorrem na rua ou por telefone
- **É preciso levar para a Internet os mesmos cuidados e as mesmas preocupações que você tem no seu dia a dia**
 - visitar apenas lojas confiáveis, não deixar públicos dados sensíveis
 - ficar atento quando “for ao banco” ou “fizer compras”
 - não passar informações a estranhos
 - não deixar a porta da sua casa aberta, etc.

Prevenção

- **Atenção com a segurança deve ser hábito incorporado a rotina, independente de questões como;**
 - local
 - tecnologia
 - meio usado
- **Necessário aliar:**
 - postura preventiva
 - mecanismos técnicos de segurança

Mecanismos de segurança (1/2)

- Política de segurança
- Notificação de incidentes e abusos
- Cópia de segurança (*backups*)
- Registro de eventos (*logs*)
- Filtros:
 - *antispam*
 - *antiphishing*
 - janelas de *pop-up*
 - códigos móveis
 - bloqueio de propagandas
- Teste de reputação de sites
- Programa para verificação de vulnerabilidades
- Sites e complementos para verificação de links curtos
- Anonymizer

Mecanismos de segurança (2/2)

- **Contas e senhas**
 - **Senhas servem para autenticar um usuário**
 - asseguram que você é realmente quem diz ser, e
 - que possui o direito de acessar o recurso em questão
 - **Um dos principais mecanismos de autenticação usados na Internet**
- **Criptografia**
- ***Firewall* Pessoal**
- **Ferramentas antimalware**
 - **antivírus, *antispyware*, *antirookit*, *antitrojan***

Protegendo-se de golpes na Internet

- **Mantenha sua privacidade**
 - quanto mais informação você disponibiliza maiores são as chances de alguém se passar por você
- **Fique atento a indícios**
 - problemas com órgãos de proteção ao crédito, retorno de e-mails, notificações de acessos indevidos, lançamentos estranhos no extrato bancário
- **Saiba como identificar mensagens**
 - quantias astronômicas, pedido de sigilo, urgência
 - erros de linguagem
 - por que você foi escolhido?
 - use a sabedoria popular
 - quando a esmola é demais o Santo desconfia
 - tudo que vem fácil vai fácil
- **NUNCA RESPONDER**

Protegendo-se de ataques na Internet (1/2)

- **O que define as chances de um ataque ser ou não bem sucedido é o conjunto de medidas preventivas tomadas por:**
 - usuários
 - desenvolvedores de aplicações
 - administradores dos computadores, serviços e equipamentos envolvidos
- **Se cada um fizer a sua parte, muitos dos ataques realizados via Internet podem ser evitados ou, ao menos, minimizados**
- **A você cabe:**
 - proteger os seus dados
 - proteger suas contas e senhas
 - fazer uso dos mecanismos de proteção disponíveis
 - manter o seu computador atualizado e livre de códigos maliciosos

Protegendo-se de ataques na Internet (2/2)

- **Faça sua parte e contribua para a segurança da Internet, incluindo a sua própria!**
 - quanto menor a quantidade de vulnerabilidades existentes em seu computador, menores serão as chances de ele ser invadido ou infectado
 - quanto menor a quantidade de computadores infectados, menor será a potência das *botnets* e menos eficazes serão os ataques de negação de serviço
 - quanto melhores forem as suas senhas, menores serão as chances de sucesso de ataques de força bruta e, conseqüentemente, de suas contas serem invadidas (e usadas para fraudes)
 - quanto mais os usuários usarem criptografia para proteger os dados, menores serão as chances de tráfego em texto claro ser interceptado por atacantes (e usados para fraudes)

Protegendo suas contas e senhas (1/8)

Elaboração de senhas:

- **Evite usar:**
 - **dados pessoais**
 - nome, sobrenome
 - contas de usuário
 - datas
 - números de documentos, de telefones ou de placas de carros
 - **dados disponíveis em redes sociais e páginas *Web***
 - **sequências de teclado**
 - “1qaz2wsx”, “QwerTAsdfG”
 - **palavras presentes em listas publicamente conhecidas**
 - músicas, times de futebol
 - personagens de filmes
 - dicionários de diferentes idiomas

Protegendo suas contas e senhas (2/8)

Elaboração de senhas:

- **Use:**
 - **números aleatórios**
 - **quanto mais ao acaso forem os números melhor**
 - principalmente em sistemas que aceitem exclusivamente caracteres numéricos
 - **grande quantidade de caracteres**
 - **quanto mais longa for a sua senha melhor**
 - **diferentes tipos de caracteres**
 - **quanto mais “bagunçada” for a sua senha melhor**

Protegendo suas contas e senhas (3/8)

Elaboração de senhas:

- **Dicas práticas para elaborar boas senhas:**

- **escolha uma frase e selecione a primeira, a segunda ou a última letra de cada palavra**

Frase: “O Cravo brigou com a Rosa debaixo de uma sacada”

Senha: “?OCbcaRddus”

- **escolha uma frase longa, fácil de ser memorizada e com diferentes tipos de caracteres**

Senha: “1 dia ainda verei os aneis de Saturno!!!”

- **invente um padrão de substituição próprio**

Padrão: substituir “o” por “0” e duplicar as letras “s” e “r”

Frase: “Sol, astro-rei do Sistema Solar”

Senha: “SS0l, asstrr0-rrei d0 SSistema SS0larr”

Protegendo suas contas e senhas (4/8)

- **Não exponha suas senhas**
 - certifique-se de não estar sendo observado ao digitá-las
 - não as deixe anotadas em locais onde outros possam ver
 - um papel sobre sua mesa ou colado em seu monitor
 - evite digitá-las em computadores e dispositivos móveis de terceiros
- **Não forneça suas senhas para outras pessoas**
 - cuidado com *e-mails*/telefonemas pedindo dados pessoais
 - não compartilhe
- **Use conexões seguras quando o acesso envolver senhas e dados sensíveis**

Protegendo suas contas e senhas (5/8)

- **Evite:**
 - salvar as suas senhas no navegador *Web*
 - usar opções, como:
 - “Lembre-se de mim”
 - “Continuar conectado”
 - usar a mesma senha para todos os serviços que acessa
 - basta ao atacante conseguir uma senha para ser capaz de acessar as demais contas onde ela seja usada
- **Não use senhas de acesso profissional para acessar contas pessoais (e vice-versa)**
 - respeite os contextos

Protegendo suas contas e senhas (6/8)

- **Crie grupos de senhas, de acordo com o risco envolvido:**
 - **crie senhas:**
 - únicas, fortes, e use-as onde haja recursos valiosos envolvidos
 - únicas, um pouco mais simples, e use-as onde o valor dos recursos protegidos é inferior
 - simples e reutilize-as para acessos sem risco
- **Armazene suas senhas de forma segura:**
 - anote-as em um papel e guarde-o em local seguro
 - grave-as em um arquivo criptografado
 - use programas gerenciadores de contas/senhas

Protegendo suas contas e senhas (7/8)

- **Altere suas senhas:**

- **imediatamente, se desconfiar que elas tenham sido:**
 - descobertas ou usadas em computadores invadidos ou infectados
- **rapidamente:**
 - **se perder um computador/dispositivo móvel onde estejam gravadas**
 - **se usar:**
 - um padrão de formação e desconfiar que alguma tenha sido descoberta
 - uma mesma senha em mais de um lugar e desconfiar que ela tenha sido descoberta em algum deles
 - **ao adquirir equipamentos acessíveis via rede**
 - eles podem estar configurados com senha padrão
- **regularmente:**
 - **nos demais casos**

Protegendo suas contas e senhas (8/8)

- **Recuperação de senhas**

- **Configure opções de recuperação de senhas:**

- um endereço de *e-mail* alternativo
 - uma pergunta /dica de segurança
 - um número de telefone celular

- **Ao usar perguntas de segurança:**

- evite escolher questões cujas respostas sejam facilmente adivinhadas
 - procure criar suas próprias questões
 - de preferência com respostas falsas

- **Ative verificação em duas etapas quando disponível**

Verificação em duas etapas (1/3)

- Também chamada de:
 - *two-factor authentication*
 - verificação ou autenticação em dois fatores
 - verificação ou autenticação em dois passos
- Fatores de autenticação:
 - algo que apenas você sabe
 - uma senha
 - perguntas de segurança
 - número PIN
 - alguma informação pessoal
 - algo que apenas você possui
 - código de verificação
 - cartão de senhas bancárias
 - *token* gerador de senhas
 - acesso a um determinado computador ou dispositivo móvel
 - algo que você é
 - informações biométricas
 - impressão digital, palma da mão, rosto, olho

Verificação em duas etapas (2/3)

- **Torna mais difícil o acesso indevido às contas de usuário**
 - Para ter acesso é necessário realizar com sucesso duas etapas:
 - primeira etapa: senha do usuário
 - segunda etapa: informações adicionais
- **Segundo fator de autenticação: código único**
 - criado pelo serviço
 - enviado de forma que apenas você possa recebê-lo
 - *e-mail*
 - chamada de voz
 - mensagem SMS para o telefone cadastrado
 - pode ser gerado por um aplicativo instalado em dispositivo móvel
- **Recurso opcional oferecido por diversos serviços**
 - *Webmail*
 - redes sociais
 - *Internet Banking*
 - armazenamento em nuvem

Verificação em duas etapas (3/3)

- **Cuidados a serem tomados:**

- **guarde seu *token/cartão* em um local seguro**
- **nunca informe o código mostrado no *token/cartão* por *e-mail* ou telefone**
- **forneça apenas uma posição do seu cartão a cada acesso ou operação**
 - **desconfie caso, em um mesmo acesso/operação, seja solicitada mais de uma posição do cartão**
- **configure opções secundárias e mantenha seus dados para recebimento sempre atualizados**
- **caso perca ou tenha seu *token* furtado:**
 - **avise imediatamente o responsável pelo serviço no qual ele é usado**

Protegendo-se de *phishing* e *malware* (1/4)

- **Desconfie de mensagens recebidas:**
 - mesmo que enviadas por conhecidos
 - elas podem ter sido enviadas de contas falsas ou invadidas
 - elas podem ter sido forjadas
- **Fique atento a mensagens que tentem induzi-lo a:**
 - fornecer informações
 - instalar/executar programas
 - clicar em *links*
- **Questione-se por que instituições com as quais você não tem contato estão lhe enviando mensagens**
- **Fique atento a mensagens que apelativas**
 - pela sua atenção
 - que ameacem caso você não execute os procedimentos descritos

Protegendo-se de *phishing* e *malware* (2/4)

- **Evite:**
 - clicar/seguir *links* recebidos via mensagens eletrônicas
 - procure digitar a URL diretamente no navegador
 - usar *sites* de busca para acessar serviços que requeiram senhas, como seu *Webmail* e sua rede social
- **Verifique o *link* apresentado na mensagem**
 - golpistas podem ofuscar o *link* real para o *phishing/malware*
- **Seja cuidadoso ao acessar *links* reduzidos:**
 - use complementos que expandam o *link* antes de clicar sobre ele

Protegendo-se de *phishing* e *malware* (3/4)

- **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 sobre o 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 o recorte são apresentados em verde e no recorte é colocado o nome da instituição dona do site

Protegendo-se de *phishing* e *malware* (4/4)



Protegendo seu computador

- **Mantenha seu computador seguro, com:**
 - todos os programas instalados nas versões mais recentes
 - todas as atualizações aplicadas, principalmente as de segurança
- **Utilize e mantenha atualizados mecanismos de segurança**
 - *antispam, antimalware, firewall* pessoal
- **Crie contas individuais para todos os usuários**
 - assegure-se de que todas as contas tenham senhas
 - não usar no dia-a-dia, conta com privilégio de administrador
- **Configure seu computador para solicitar senha na tela inicial**
- **Nunca compartilhe a senha de administrador**
 - use-a o mínimo necessário

Protegendo dispositivos móveis (1/5)

- **Instale e mantenha atualizados mecanismos de segurança (*antimalware*)**
- **Mantenha seu dispositivo sempre atualizado:**
 - com a versão mais recente do sistema e dos aplicativos instalados
- **Configure-o previamente, se possível, para que:**
 - seja localizado/rastreado e bloqueado remotamente, por meio de serviços de geolocalização
 - os dados sejam apagados após um determinado número de tentativas de desbloqueio sem sucesso
- **Não faça *jailbreak* nem adquira um dispositivo nesta condição**
 - violação dos termos de garantia
 - comprometimento da segurança
 - comprometimento do funcionamento

Protegendo dispositivos móveis (2/5)

- **Proteja seus dados**

- **configure:**

- **senha de bloqueio na tela inicial**
 - bloqueio automático
 - **código PIN**
 - **criptografia no dispositivo**
 - **se disponível, autenticação por biometria**

- **faça backups periódicos**

- **use conexão segura quando a comunicação envolver dados confidenciais**

- **senhas**
 - **número de cartão de crédito**

Protegendo dispositivos móveis (3/5)

- **Seja cuidadoso na instalação de aplicativos**
 - **Só instale aplicativos de fontes confiáveis**
 - lojas oficiais
 - *site* do fabricante
 - **Avalie a reputação do aplicativo:**
 - desenvolvedor
 - bem avaliado
 - quantidade de usuários
 - **Observe as permissões para execução**
 - elas devem ser coerentes com a finalidade do aplicativo
 - um aplicativo de jogos, por exemplo, não precisa ter acesso a sua lista de chamadas ou SMS
- **Não siga *links* recebidos via mensagens eletrônicas**
 - **SMS, e-mails, redes sociais, etc.**

Protegendo dispositivos móveis (4/5)

- **Seja cuidadoso ao usar redes Wi-Fi públicas**
 - desabilite a opção de conexão automática
 - remova as redes que não for mais acessar
- **Mantenha interfaces de comunicação desativadas**
 - *bluetooth*, infravermelho e Wi-Fi
 - somente as habilite quando necessário
- **Configure a conexão *bluetooth* para que seu dispositivo não seja identificado (ou “descoberto”) por outros aparelhos**
- **Mantenha controle físico**
 - especialmente em locais públicos e de risco

Protegendo dispositivos móveis (5/5)

- **Em caso de perda ou furto**

- **Informe:**

- **a sua operadora**

- solicite o bloqueio do seu número (chip)

- **a empresa onde você trabalha**

- caso haja dados e senhas profissionais nele armazenadas

- **Altere as senhas que possam estar nele armazenadas**

- e-mail, redes sociais, etc

- **Bloqueie cartões de crédito cujo número esteja nele armazenado**

- **Ative a localização remota, caso você a tenha configurado**

- se necessário, apague remotamente os dados nele gravados

- **Ao se desfazer do seu dispositivo**

- **Apague todas as informações nele contidas**

- **Restaure as configurações de fábrica**

Protegendo-se de *Ransomware* (1/2)

- ***Ransomware* é um tipo de código malicioso que impede o usuário de ter acesso ao sistema infectado e/ou seus dados, até que seja paga a quantia exigida, no prazo especificado**
 - não há garantia que pagando recobrará acesso
 - normalmente usa criptografia forte
 - *alguns mudam o boot do sistema (tela de bloqueio)*
 - ***Alguns exemplos***
 - CryptoLocker, CryptoWall, Cerber, Locky, Petya, TeslaCrypt
 - só há ferramentas de recuperação para algumas poucas famílias e versões:
 - <https://noransom.kaspersky.com/>
 - <http://www.trendmicro.com/tools/us/#ransomware>

Protegendo-se de *Ransomware* (2/2)

- **Medidas preventivas**

- todos os cuidados anteriores

- **com o computador e dispositivos móveis**

- ferramentas *antimalware* e atualizações

- não usar conta com privilégios de administrador

- **com *phishing*, arquivos anexos, sites suspeitos, mensagens de texto**

- e mais:

- **desabilitar execução de *scripts***

- *javascript* em navegadores (ex: No-Script)

- "Windows Script Host" no Windows

- **NÃO habilitar macros em arquivos Office suspeitos**

- *bad guys* vão tentar persuadí-lo do contrário

- ***BACKUP, BACKUP, BACKUP!!!***

- **manter as cópias desconectadas do sistema**

- *ransomwares costumam buscar outros dispositivos conectados, locais ou em rede, e criptografá-los também!*

Preserve a sua privacidade (1/3)

- **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
- **Mantenha seu perfil e seus dados privados**
- **Restrinja o acesso ao seu endereço de e-mail**
- **Cuidado ao confirmar sua presença em eventos públicos organizados via redes sociais**

Preserve a sua privacidade (2/3)

- **Seja seletivo:**
 - ao aceitar seus contatos
 - ao se associar a grupos
- **Não acredite em tudo que você lê**
 - Verifique sempre a fonte das informações
 - Não repasse boatos nem, mensagens que possam gerar pânico ou ódio
- **Não confie na promessa de anonimato oferecida por algumas redes sociais e aplicativos**
 - de acordo com as informações divulgadas é possível inferir:
 - a sua identidade
 - a identidade de outras pessoas

Respeite a privacidade alheia

- **Evite falar sobre as ações, hábitos e rotina de outras pessoas**
- **Não divulgue, sem autorização:**
 - imagens em que outras pessoas apareçam
 - mensagens ou imagens copiadas do perfil de usuários que restrinjam o acesso
- **Tente imaginar como a outra pessoa se sentiria ao saber que aquilo está se tornando público**
 - e se fosse o contrário?

Proteja os seus filhos (1/2)

- **Informe-os sobre os riscos de uso das redes sociais**
- **Respeite os limites de idade estipulados pelos *sites***
- **Não exponha excessivamente seus filhos:**
 - **muitos pais criam perfis em nome dos filhos e postam sobre eles ou como se fossem eles**
 - **isso pode confundir e desagradar as crianças**
 - **evite constranger seus filhos divulgando fotos ou comentários que possam embaraçá-los**
 - **seja cuidadoso ao divulgar imagens de seus filhos**
 - **o que para você pode ser algo inocente, para outras pessoas pode ter uma conotação diferente**

Proteja os seus filhos (2/2)

- **Oriente-os:**

- para não se relacionarem com estranhos e nunca fornecerem informações pessoais
 - nem enviarem fotos ou vídeos
- para não divulgarem informações sobre:
 - hábitos familiares
 - localização geográfica (atual ou futura)
- para não marcarem / irem a encontros desacompanhados
- sobre os riscos de uso da *webcam*
 - ela não deve ser usada para se comunicar com estranhos
- para usar opções como silenciar, bloquear e denunciar, caso alguém os esteja incomodando

Proteja a sua vida profissional (1/2)

- **Cuide da sua imagem profissional**
- **Ao usar redes sociais profissionais:**
 - procure ser formal
 - evite tratar de assuntos pessoais
- **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

Proteja a sua vida profissional (2/2)

- **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**

Proteja a sua empresa

- **Crie um código de conduta**
- **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

Protegendo sua privacidade

- **Procure reduzir a quantidade de informações que possam ser coletadas sobre você**
 - elas podem ser usadas para:
 - adivinhar as suas senhas
 - criar perfis falsos
- **Seja cuidadoso com as informações que você divulga em *blogs* e redes sociais**
 - elas podem ser usadas por invasores para tentar:
 - confirmar os seus dados cadastrais
 - descobrir dicas de segurança
 - responder perguntas de segurança
 - tentar se passar por você

Mantenha-se Informado

Iniciativas de Conscientização

Portal Internet Segura

<http://www.internetsegura.br/>



Campanha Antispam.br

<http://www.antispam.br/>



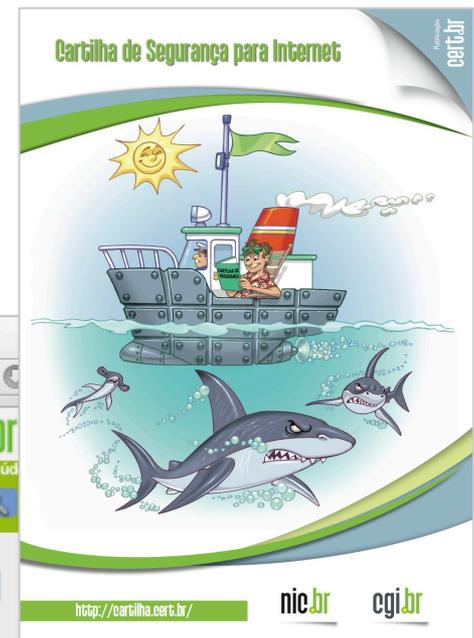
Educação de Usuários: Cartilha de Segurança para Internet

Livro (PDF e ePub) e conteúdo no *site* (HTML5)

Dica do dia no site, via *Twitter* e RSS

<http://cartilha.cert.br/>

The screenshot shows the website's main page. At the top, there's a navigation bar with 'Inicio', 'Livro', 'Fasciculos', and 'Sobre' tabs. A search bar is also present. The main content area features a large heading 'Cartilha de Segurança para Internet' with a sub-heading 'Navegar é preciso, arriscar-se não!'. Below this, there's a paragraph of text and a small illustration of a boat. To the right, there's a 'Dica do dia' section with a tip about backing up passwords. Below that, a 'Veja também' section recommends other resources like 'INTERNETSEGURABR', 'antispam.br', and 'SIACT'.



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

Obrigada

www.cert.br

© lucimara@cert.br © @certbr

12 de julho de 2016

nic.br **cgi.br**

www.nic.br | www.cgi.br