Verificação em duas etapas

<Nome>
<Instituição>
<e-mail>

Agenda

- Senhas
- Verificação em duas etapas
- Principais tipos e cuidados a serem tomados
- Outros cuidados
- Créditos

Senhas (1/4)

- **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**
- **Proteger suas senhas é essencial para se prevenir dos riscos envolvidos no uso da Internet**
  - **se usadas isoladamente podem não ser suficientes para garantir a identidade de um usuário**

Senhas (2/4)

- **Sua senha pode ser descoberta:**
  - **quando usada em:**
    - **computadores infectados**
    - **computadores invadidos**
    - ***sites* falsos (*phishing*)**
  - **por meio de tentativas de adivinhação**
  - **ao ser capturada enquanto trafega na rede**
  - **por meio do acesso ao arquivo onde foi armazenada**
  - **com o uso de técnicas de engenharia social**
  - **pela observação da movimentação:**
    - **dos seus dedos no teclado**
    - **dos cliques do *mouse* em teclados virtuais**

Senhas (3/4)

- De posse da sua senha um invasor 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 com *spam,* boatos, *phishing* e *malware*
    - trocar a sua senha
    - pedir o reenvio de senhas de outras contas
  - acessar o seu *site* de comércio eletrônico e:
    - alterar informações de cadastro
    - fazer compras em seu nome
    - verificar informações sobre suas compras anteriores

Senhas (4/4)

- De posse da sua senha um invasor pode:
  - **acessar a sua conta bancária e:**
    - **verificar o seu extrato e seu saldo bancário**
  - **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**
    - **trocar a sua senha**

Verificação em duas etapas (1/3)

- **Também chamada de:**
  - ***two-factor authentication***
  - **aprovação de *login***
  - **verificação ou autenticação em dois fatores**
  - **verificação ou autenticação em dois passos**

- **Recurso opcional oferecido por diversos serviços:**
  - ***Webmail***
  - **redes sociais**
  - **Internet *Banking***
  - **armazenamento em nuvem**

Fonte - https://cartilha.cert.br/

Verificação em duas etapas (2/3)

- **Ao ser habilitada**
  - **permite aumentar a segurança de sua conta**
  - **pode ser desabilitada caso não seja mais desejada**
- **Torna mais difícil o acesso indevido de contas de usuário**
- **Para que o acesso ocorra é necessário que o atacante realize com sucesso duas etapas**
  - **primeira etapa: senha do usuário**
  - **segunda etapa: informações adicionais**

Verificação em duas etapas (3/3)

- **Segunda etapa pode envolver:**
  - **algo que apenas você sabe**
    - **outra 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**

Principais tipos e cuidados a serem tomados

Código de verificação (1/2)

- **Código individual**
  - **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 autenticador instalado em seu dispositivo móvel**

Código de verificação (2/2)

- **Cuidados a serem tomados:**
  - **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**
    - **o uso do aplicativo autenticador**
  - **aplicativo autenticador deve ser usado em casos onde não é possível receber mensagens SMS**
    - **se você estiver viajando ou em área sem cobertura de celular**
  - **tarifas de recebimento de SMS podem ser aplicadas por sua operadora**

Código de verificação específico

- **Código gerado para aplicativos que não suportam a verificação em duas etapas**

- **<u>Cuidados a serem tomados:</u>**
  - **caso perca o acesso ao seu dispositivo móvel:**
    - **revogue os códigos específicos gerados para os acessos realizados por meio dele**

Token gerador de senhas (1/2)

- Chave eletrônica
- Tipo de dispositivo eletrônico que gera códigos usados na verificação da sua identidade
- Cada código é válido por um determinado período
  - geralmente alguns segundos
  - após esse tempo um novo código é gerado
  - código pode ser gerado automaticamente ou necessitar que você clique em um botão para ativá-lo

Token gerador de senhas (2/2)

- **Cuidados a serem tomados:**
  - **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**

Cartão de segurança

- **Cartão com diversos códigos numerados e que são solicitados quando você acessa a sua conta**

- **<u>Cuidados a serem tomados:</u>**
  - **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**

Dispositivo confiiável

- **Computador ou dispositivo móvel usado para acessar suas contas**
- **No primeiro acesso:**
  - **pode ser necessário inserir um código de segurança**
  - **ele não será necessário nos demais, pois seu dispositivo será "lembrado", caso você assim o configure**

- **<u>Cuidados a serem tomados:</u>**
  - **não esqueça de excluir seus dispositivos confiáveis caso eles sejam trocados ou você perca o acesso a eles**
  - **pode ser necessário habilitar a opção de *cookies* em seu navegador *Web* para que seu dispositivo seja memorizado**

Lista de códigos reserva/*backup*

- **Lista de códigos que devem ser usados de forma sequencial e uma única vez**

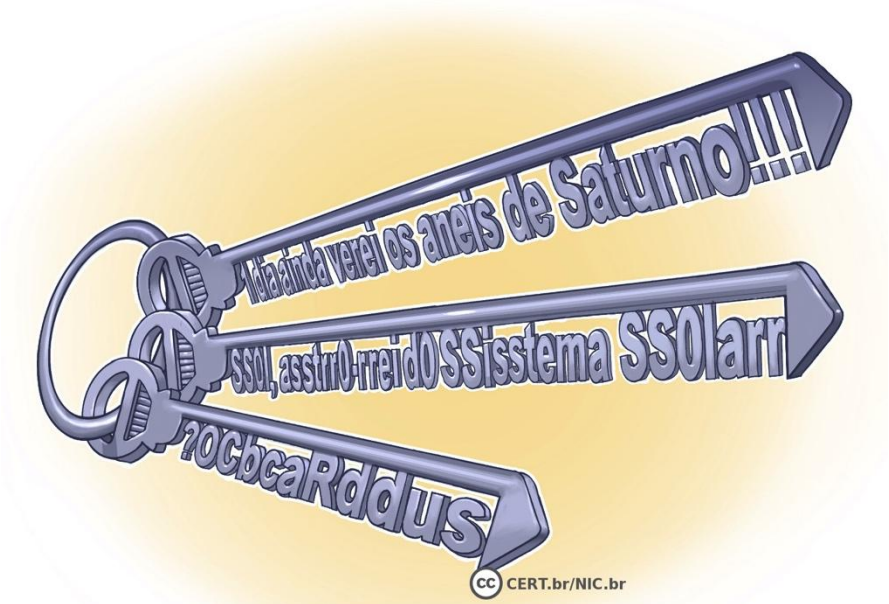
- **<u>Cuidados a serem tomados:</u>**
  - **anote ou imprima a lista e a mantenha em um local seguro**
  - **não a armazene em seu dispositivo confiável pois ela poderá vir a ser acessada por atacantes**
    - **caso não esteja criptografada**
  - **caso perca a lista ou desconfie que alguém a acessou você deve gerá-la novamente ou revogá-la**
    - **anulando assim a anterior**

Chave de recuperação

- **Número gerado pelo serviço quando você ativa a verificação em duas etapas**
- **Permite que você acesse o serviço mesmo que perca sua senha ou seus dispositivos confiáveis**

- **<u>Cuidados a serem tomados:</u>**
  - **anote ou imprima a chave e a mantenha em um local seguro**
  - **não a deixe anotada em seu dispositivo confiável pois ela poderá vir a ser acessada por atacantes**
    - **caso não esteja criptografada**
  - **caso perca ou desconfie que alguém acessou a sua chave você deve gerá-la novamente**
    - **substituindo assim a anterior**

Outros cuidados



Dados pessoais

- **Mantenha seu cadastro atualizado**
  - **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**
    - **caso você desabilite a verificação em duas etapas**

Senhas (1/4)

- **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**

Senhas (2/4)

- **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**

Senhas (3/4)

- **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 SSisstema SS0larr”

Senhas (4/4)

- **Seja cuidadoso ao usar suas senhas**
  - **certifique-se de utilizar conexão segura**
  - **não forneça suas senhas para outra pessoa**
    - **em hipótese alguma**
  - **certifique-se de não estar sendo observado ao digitá-las**
  - **altere as suas senhas sempre que julgar necessário**
  - **evite utilizar computadores de terceiros**
  - **somente acesse os serviços digitando o endereço diretamente no navegador *Web***
    - **nunca clicando em *links* existentes em páginas ou mensagens**

Dispositivos móveis (1/2)

- **Cadastre uma senha de acesso que seja bem elaborada**
  - **configure-os para aceitarem senhas complexas (alfanuméricas)**
- **Instale um programa antivírus**
- **Mantenha o sistema operacional e as aplicações instaladas sempre:**
  - **com a versão mais recente**
  - **com todas as atualizações aplicadas**

Dispositivos móveis (2/2)

- **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:**
  - **remova-os da lista de dispositivos confiáveis**
  - **revogue autorizações concedidas para aplicativos instalados**
  - **cadastre um novo número de celular**
  - **se tiver configurado a localização remota:**
    - **apague remotamente os dados armazenados**

Computador

- **Mantenha o seu computador seguro**
  - **com a versão mais recente de todos os programas instalados**
  - **com todas as atualizações aplicadas**
- **Utilize e mantenha atualizados mecanismos de segurança, como *antispam*, antivírus e *firewall* pessoal**
- **Configure-o para solicitar senha na tela inicial**

Mantenha-se informado (1/2)

Cartilha de Segurança para Internet

https://cartilha.cert.br/

RSS

https://cartilha.cert.br/rss/cartilha-rss.xml

Twitter

http://twitter.com/certbr

Mantenha-se informado (2/2)

Antispam.br

http://antispam.br/

INTERNET SEGURA.BR

Internet Segura

http://internetsegura.br/

Créditos

- **Fascículo Verificação em duas etapas**

  https://cartilha.cert.br/fasciculos/

- **Cartilha de Segurança para Internet**

  https://cartilha.cert.br/

cert.br

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

nic.br

Núcleo de Informação e Coordenação do Ponto BR

cgi.br

Comitê Gestor da Internet no Brasil