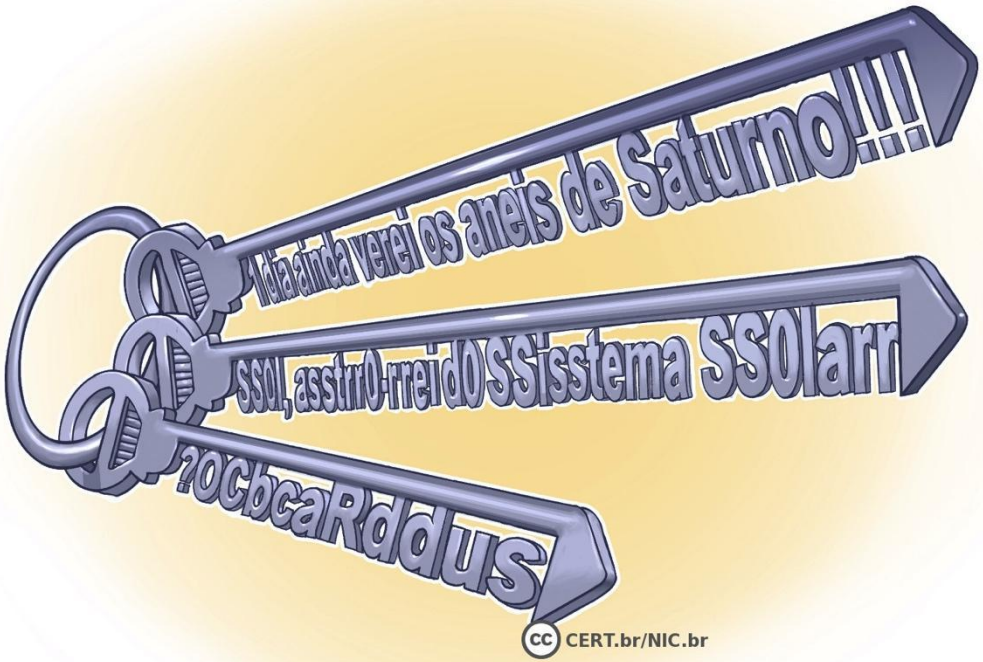
Segurança em Senhas



Roberto Cabral
UFC - Quixadá
rbcabral@ufc.br

Agenda

- Senhas
- Riscos principais
- Cuidados a serem tomados
- Créditos

Senhas (1/2)

- **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:**
  - **é o segredo das suas senhas que garante a sua identidade, ou seja, que você é o dono das suas contas de usuário**

Senhas (2/2)

- **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**

Riscos principais

Riscos principais (1/4)

- 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 contendo:
      - *spam*
      - boatos
      - *phishing*
      - códigos maliciosos
    - pedir o reenvio de senhas de outras contas
      - e assim conseguir acesso a elas
    - trocar a sua senha
      - dificultando que você acesse novamente a sua conta

Riscos principais (2/4)

- De posse da sua senha um invasor pode:
  - acessar o seu computador e:
    - apagar seus arquivos
    - obter informações sensíveis, inclusive outras senhas
    - instalar códigos e serviços maliciosos
    - usar seu computador para:
      - desferir ataques contra outros computadores
      - esconder a real identidade desta pessoa (o invasor)

Riscos principais (3/4)

- De posse da sua senha um invasor pode:
  - acessar a sua rede social e:
    - denegrir a sua imagem
    - explorar a confiança de seus amigos/seguidores
    - enviar mensagens em seu nome, contendo:
      - *spam*
      - boatos
      - *phishing*
      - códigos maliciosos
    - alterar as configurações feitas por você
      - tornando públicas informações privadas
    - trocar a sua senha
      - dificultando que você acesse novamente seu perfil

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

Riscos principais (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 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

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

Cuidados a serem tomados

Elaboração de senhas (1/3)

- 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

Elaboração de senhas (2/3)

- **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**

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

Elaboração de senhas (3/3)

- **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"

Uso de senhas (1/3)

- 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
- Use conexões seguras quando o acesso envolver senhas

Uso de senhas (2/3)

- 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 assuntos pessoais (e vice-versa)
  - respeite os contextos

Uso de senhas (3/3)

- **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**

Alteração de senhas

- **Altere suas senhas:**
  - **imediatamente, se desconfiar que elas tenham sido:**
    - **descobertas ou usadas em computadores invadidos ou infectados**
  - **rapidamente:**
    - **se perder um computador onde elas 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**

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

Recuperação de senhas (1/2)

- **Configure opções de recuperação de senhas:**
  - **um endereço de *e-mail* alternativo**
  - **uma pergunta de segurança**
  - **uma 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**

Recuperação de senhas (2/2)

- Ao usar dicas de segurança, escolha aquelas que sejam:
  - vagas o suficiente para que ninguém consiga descobri-las, e
  - claras o bastante para que você consiga entendê-las
- Ao solicitar o envio de suas senhas por *e-mail*:
  - procure alterá-las o mais rápido possível
  - cadastre um *e-mail* que você acesse regularmente
    - para não esquecer a senha desta conta também

Phishing e códigos maliciosos

- **Desconfie de mensagens recebidas:**
  - **mesmo que enviadas por conhecidos**
    - **elas podem ter sido enviadas de contas falsas ou invadidas**
- **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**
- **Seja cuidadoso ao acessar *links* reduzidos:**
  - **use complementos que permitam expandir o *link* antes de clicar sobre ele**

Privacidade

- **Procure reduzir a quantidade de informações que possam ser coletadas sobre você**
  - **elas podem ser usadas para adivinhar as suas senhas**

- **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**

Computador (1/2)

- **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**

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

Computador (2/2)

- Crie contas individuais para todos os usuários
  - assegure-se de que todas as contas tenham senhas
- Configure seu computador para solicitar senha na tela inicial
- Nunca compartilhe a senha de administrador
  - use-a o mínimo necessário
- Ative o compartilhamento de recursos:
  - apenas quando necessário, e
  - usando senhas bem elaboradas

Dispositivos móveis

- **Cadastre uma senha de acesso bem elaborada**
  - **se possível, configure-o para aceitar senhas complexas (alfanuméricas)**
- **Em caso de perda ou furto:**
  - **altere as senhas que possam estar nele armazenadas**

Computadores de terceiros

- Certifique-se de fechar a sua sessão (*logout*) ao acessar *sites* que requeiram o uso de senhas
- Procure, sempre que possível, utilizar opções de navegação anônima
- Evite efetuar transações bancárias e comerciais
- Ao retornar ao seu computador, procure alterar as senhas que, por ventura, você tenha utilizado

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

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 (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

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

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

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

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

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

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

- Cuidados a serem tomados:
  - 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

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

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

Mantenha-se informado (1/2)

Cartilha de Segurança para Internet

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

RSS

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

Twitter

httphttp://twitter.com/certbr

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

Mantenha-se informado (2/2)

Antispam.br

http://antispam.br/

INTERNET SEGURA.BR

Internet Segura

http://internetsegura.br/

Créditos

- **Fascículo Senhas**

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