Autenticação:
Senhas e
Verificação em Duas Etapas

Miriam von Zuben
CERT.br / NIC.br
miriam@cert.br

Agenda

- Autenticação
- Grupos de mecanismos de autenticação
- Cuidados a serem tomados
- Outros cuidados
- Créditos

Segurança da Informação

- **Controle de acesso**

- **Autenticação: processo que**
  - permite verificar a sua identidade assegurando que você é quem diz ser
  - garante que seus equipamentos e contas sejam usados só por você

- **Autorização: garante que você só tenha acesso aos recursos autorizados**

- **Auditoria: coleta de informações sobre o uso dos recursos feito por você**

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

Grupos de mecanismos de autenticação

- **Aquilo que apenas você sabe (conhecimento)**
  - senha, pergunta de segurança, padrão (desenho)
  - número PIN, alguma informação pessoal
- **Aquilo que apenas você possui (posse)**
  - cartão de senhas bancárias
  - *token* gerador de senhas
  - pulseiras / anéis / relógios
  - acesso a um determinado equipamento, celular e *tablet*
  - código de verificação
- **Aquilo que você é (existência)**
  - informações biométricas: impressão digital, palma da mão, rosto, olho
- **Onde você está (localização)**
  - localização geográfica / rede Wi-Fi / som ambiente
- **Quando está ocorrendo o acesso (horário)**
  - período

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

Grupos de mecanismos de autenticação

- **Qual usar?**
  - depende de questões como:
    - facilidade de uso pelo usuário
    - “valor” da informação
    - custo de implementação e manutenção
    - confiabilidade
  - podem ser usados sozinhos ou em conjunto

Verificação em duas etapas (1/2)

- ***Two-factor authentication* (2FA)**
  - aprovação de *login*
  - verificação ou autenticação em dois fatores
  - verificação ou autenticação em dois passos

- ***Three-factor authentication* (3FA)**

- ***Multi-factor authentication* (MFA)**

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

Verificação em duas etapas (2/2)

- **Recurso oferecido/exigido por diversos serviços:**
  - *Webmail*, redes sociais, *Internet Banking*, nuvem
  - permite aumentar a segurança de sua conta
  - quando opcional, pode ser desabilitada se não 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 ou mais etapas

Aquilo que apenas você sabe

Senhas (1/3)

- **Um dos principais mecanismos usados na Internet**
  - facilidade de implementação
- **Como podem ser descobertas:**
  - quando usadas em:
    - computadores infectados e/ou invadidos
    - *sites* falsos (*phishing*)
  - tentativas de adivinhação (força bruta)
  - capturadas enquanto trafegam na rede, sem criptografia
  - acesso ao arquivo onde foram armazenadas
  - técnicas de engenharia social
  - observação da movimentação:
    - dos seus dedos no teclado
    - dos cliques do *mouse* em teclados virtuais

Senhas (2/3)

- **De posse da sua senha um invasor pode:**
  - acessar a sua conta de *e-mail* e:
    - ler e/ou apagar suas mensagens
    - furtar sua lista de contatos e enviar mensagens em seu nome
    - enviar mensagens contendo *spam*, boatos, *phishing* e *malware*
    - pedir reenvio de senhas de outras contas (e assim conseguir acesso a elas)
    - trocar a sua senha (dificultando que você acesse novamente a sua conta)
  - acessar seus equipamentos e:
    - apagar seus arquivos
    - furtar sua lista de contatos e suas mensagens
    - obter informações sensíveis, inclusive outras senhas, fotos e vídeos
    - instalar códigos e serviços maliciosos
    - usá-lo para desferir ataques contra outros equipamentos
    - bloquear o acesso ao equipamento

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

Senhas (3/3)

- **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* e *malware*
    - alterar configurações feitas por você (tornando públicas informações privadas)
    - trocar a sua senha (dificultando que você acesse novamente seu perfil)
  - acessar o seu *site* de comércio eletrônico e:
    - alterar informações de cadastro
    - fazer compras em seu nome
    - verificar informações sobre suas compras anteriores

Elaboração de senhas (1/2)

- **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
- **Use:**
  - números aleatórios
    - quanto mais ao acaso forem os números melhor
  - 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 (2/2)

- **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 (1/2)

- **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 equipamentos 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**
- **Não use senhas profissionais para acessos pessoais (e vice-versa)**
  - respeite os contextos

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

Uso de senhas (2/2)

- **Evite:**
  - salvar as suas senhas no navegador Web
  - usar opções como: “Lembre-se de mim” e “Continuar conectado”
  - usar a mesma senha para todos os serviços que acessa
    - basta ao atacante conseguir uma senha para acessar as demais contas onde é usada
- **Crie grupos de senhas, de acordo com o risco envolvido:**
  - únicas e fortes: use-as onde haja recursos valiosos envolvidos
  - únicas e mais simples: use-as onde o valor dos recursos protegidos é inferior
  - simples: 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 ou até mesmo sem senha
  - regularmente: nos demais casos

Recuperação de senhas

- **Configure opções de recuperação de senhas:**
  - endereço de *e-mail* alternativo, pergunta ou dica de segurança, número de celular
- **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

Perguntas de Segurança

- **Usadas para recuperação de senhas**

- **<u>Cuidados a serem tomados</u>**
  - evite escolher questões cujas respostas sejam facilmente adivinhadas
  - procure criar suas próprias questões
    - de preferência com respostas falsas

Aquilo que apenas você possui

Token gerador de senhas (chave eletrônica)

- **Dispositivo eletrônico ou aplicativo que gera códigos**
- **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

- **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**

- **Cuidados a serem tomados:**
  - 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

Chave de segurança

- **Dispositivo que se conecta ao equipamento**
  - USB, Bluetooth, NFC
- **Utiliza padrão de *token* de autenticação U2F (*Universal 2nd Factor*)**
- **Suportado por alguns navegadores Web**
- **Em dispositivos móveis pode necessitar de aplicativo específico**

- **<u>Cuidados a serem tomados:</u>**
  - tenha cuidado para não perder o dispositivo
  - caso perca sua chave de segurança ou ela seja furtado, revogue o acesso aos serviços onde ela está sendo usada

Dispositivo confiável

- **Equipamento 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

Código de verificação

- **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 equipamento

- **Cuidados a serem tomados:**
  - mantenha seus dados para recebimento sempre atualizados
    - números de telefones celulares alternativos podem ser cadastrados
  - tenha certeza de estar de posse de seu equipamento cadastrado
    - com bateria e conexão à Internet
  - aplicativo autenticador deve ser usado em casos onde não é possível receber SMS

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

Como faço se estou sem acesso aos meus equipamentos?

Chave de recuperação

- **Número gerado quando a verificação em duas etapas é ativada**
- **Permite o acesso ao serviço mesmo que perca a senha ou 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

Lista de códigos reserva/*backup*/extra

- **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

Aquilo que você é

Biometria

- **Não há necessidade de:**
  - lembrar de algo
  - carregar algo
- **Deixada em diversos lugares**
- **Segurança depende diretamente de como as informações são armazenadas**
- **Não há como revogar ou alterar**
- **Ainda cara**
- **Diversos estudos sendo feitos**
  - reconhecimento de fala
  - uso de *selfies*

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

Outros cuidados

Dados pessoais

- **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
    - caso você desabilite a verificação em duas etapas

Privacidade

- **Procure reduzir a quantidade de informações que possam ser coletadas sobre você**

- **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
    - adivinhar senhas
    - descobrir dicas de segurança
    - responder perguntas de segurança

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

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

Proteja seus equipamentos

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

Equipamentos 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:**
  - 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

Equipamentos de terceiros

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

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

Conclusão

Conclusão

- Não confunda quantidade com qualidade
- Não é somente a quantidade de fatores usados que torna a autenticação mais segura
- Mas sim a soma dos cuidados tomados com cada um deles

HABILITE A VERIFICAÇÃO EM DUAS ETAPAS

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)

Portal Internet Segura

http://www.internetsegura.br/

Campanha Antispam.br

http://www.antispam.br/

Créditos

- **Fascículos**

  Senhas

  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

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

Obrigada

www.cert.br

miriam@cert.br

@certbr

08 de novembro de 2017

20 anos cert.br

nic.br cgi.br

www.nic.br | www.cgi.br