



Segurança em Senhas



USP



EESC - USP



STI
SEÇÃO TÉCNICA DE INFORMÁTICA
EESC - USP

sti.seguranca@eesc.usp.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



CC CERT.br/NIC.br





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



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



Cuidados a serem tomados



CC CERT.br/NIC.br





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**



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 SSistema 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



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



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**



Mantenha-se informado (1/2)

Cartilha de Segurança para Internet

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



RSS

<http://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

⇒ Fascículo Senhas

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

⇒ Cartilha de Segurança para Internet

<http://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

egi.br

Comitê Gestor da
Internet no Brasil

