

Cartilha de Segurança para Internet

Fascículo **Senhas**





Contas e senhas são os mecanismos de autenticação mais utilizados na Internet atualmente.

Por meio de contas e senhas os sistemas conseguem saber quem você é, confirmar sua identidade e definir as ações que você pode realizar.

A sua conta de usuário em um determinado sistema normalmente é de conhecimento público, já que é por meio dela que as pessoas e serviços conseguem identificar quem você é. Desta forma, **proteger sua senha é essencial** para se prevenir dos riscos envolvidos no uso da Internet, pois **é o segredo dela que garante a sua identidade**, ou seja, que você é o dono da sua conta de usuário.

Se uma outra pessoa souber a sua conta de usuário e tiver acesso à sua senha, ela poderá usá-las para se passar por você na Internet e realizar ações em seu nome. Algumas das formas como sua senha pode ser indevidamente descoberta são:

- ✓ quando usada em computadores infectados
- ✓ quando usada em computadores invadidos
- ✓ quando usada em *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 ou dos cliques do *mouse* em teclados virtuais

Preserve suas senhas,
proteja sua identidade

Riscos principais



Proteger suas senhas é fundamental para se prevenir dos riscos que o uso da Internet pode representar. Algumas das ações que um invasor pode realizar, caso tenha acesso às suas senhas, e os riscos que estas ações podem representar são:

- ✓ **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 de spam e/ou contendo *phishing* e códigos maliciosos
 - pedir o reenvio de senhas de outras contas (e assim conseguir acesso a elas)
 - trocar sua senha, dificultando que você acesse novamente sua conta
- ✓ **acessar o seu computador e:**
 - apagar seus arquivos e obter informações sensíveis, inclusive outras senhas
 - instalar códigos e serviços maliciosos
 - usá-lo para desferir ataques contra outros computadores
- ✓ **acessar redes sociais e:**
 - denegrir a sua imagem e explorar a confiança de seus amigos/seguidores
 - enviar mensagens de *spam* ou contendo boatos e códigos maliciosos
 - alterar as configurações feitas por você, tornando públicas informações privadas
 - trocar sua senha, dificultando que você acesse novamente sua conta
- ✓ **acessar sua conta bancária e:**
 - verificar seu extrato e seu saldo bancário
- ✓ **acessar seu site de comércio eletrônico e:**
 - alterar informações de cadastro
 - fazer compras em seu nome e verificar informações sobre suas compras anteriores

Cuidados a serem tomados



Seja cuidadoso ao elaborar suas senhas:

- ✓ Evite usar:
 - dados pessoais, como nomes, sobrenomes, contatos de usuário, datas, números de documentos, placas de carros e números de telefones
 - dados que possam ser obtidos em redes sociais e páginas *Web*
 - sequências de teclado, como "1qaz2wsx" e "QwerTAsdfg"
 - palavras que fazem parte de listas publicamente conhecidas, como nomes de músicas, times de futebol, personagens de filmes e dicionários de diferentes idiomas
- ✓ Use:
 - números aleatórios
 - grande quantidade de caracteres
 - diferentes tipos de caracteres

Dicas práticas para elaborar boas senhas:

- ✓ Escolha uma frase e selecione a primeira, a segunda ou a última letra de cada palavra: com a frase "O Cravo brigou com a Rosa debaixo de uma sacada" você pode gerar a senha **"?OCbcaRddus"**
- ✓ Escolha uma frase longa, que seja fácil de ser memorizada e que, se possível, tenha diferentes tipos de caracteres: se quando criança você sonhava em ser astronauta, pode usar como senha **"1 dia ainda verei os aneis de Saturno!!!"**
- ✓ Invente um padrão de substituição baseado, por exemplo, na semelhança visual ou de fonética entre os caracteres: duplicando as letras "s" e "r", substituindo "o" por "0" (número zero) e usando a frase "Sol, astro-rei do Sistema Solar" você pode gerar a senha **"SS0l, asstr0-rrei d0 SSistema SS0lar!"**

Seja cuidadoso ao usar suas senhas:

- ✓ **não exponha suas senhas**
 - certifique-se de não estar sendo observado ao digitá-las
 - não as deixe anotadas em locais onde outras pessoas possam vê-las (por exemplo, em um papel colado no monitor do seu computador)
 - evite digitá-las em computadores e dispositivos móveis de terceiros

- ✓ **não forneça as suas senhas para outra pessoa, em hipótese alguma**
 - fique atento a ligações telefônicas e *e-mails* pelos quais alguém, geralmente falando em nome de alguma instituição, solicita informações pessoais sobre você, inclusive senhas

- ✓ **certifique-se de usar conexões seguras sempre que o acesso envolver senhas**

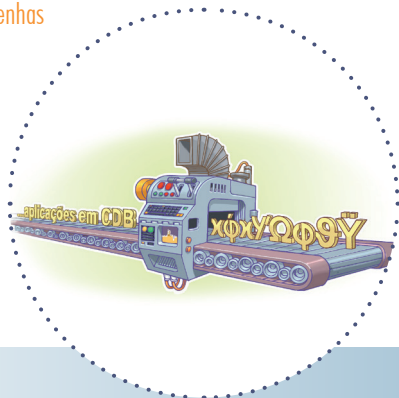
- ✓ **evite salvar as suas senhas no navegador *Web***

- ✓ **evite usar opções como “Lembre-se de mim” e “Continuar conectado”**

- ✓ **evite usar a mesma senha para todos os serviços que você acessa**
 - basta ao atacante conseguir uma senha para ser capaz de acessar as demais contas onde ela seja usada

- ✓ **crie grupos de senhas, de acordo com o risco envolvido**
 - crie senhas únicas, bastante fortes, e use-as onde haja recursos valiosos envolvidos
 - crie senhas únicas, um pouco mais simples, e use-as onde o valor dos recursos protegidos é inferior
 - crie senhas simples e reutilize-as para acessos sem risco
 - não use senhas de acesso a assuntos pessoais para acessar assuntos profissionais, e vice-versa (respeite os contextos)

- ✓ **armazene suas senhas de forma segura. Por exemplo:**
 - anote suas senhas em um papel e guarde-o em local seguro
 - grave suas senhas em um arquivo criptografado
 - use programas gerenciadores de contas/senhas



Altere suas senhas:

- ✓ **imediatamente:**
 - se desconfiar que elas tenham sido descobertas ou que o computador no qual você as usou tenha sido invadido ou infectado
- ✓ **rapidamente:**
 - se alguém furtar ou você perder um computador onde elas estejam gravadas
 - se usar um padrão para a formação de senhas e desconfiar que uma delas tenha sido descoberta (altere também o padrão e as demais senhas elaboradas com ele)
 - se usar uma mesma senha em mais de um lugar e desconfiar que ela tenha sido descoberta em algum deles (altere-a em todos os lugares nos quais é usada)
 - ao adquirir equipamentos acessíveis via rede, como roteadores Wi-Fi e *modems* ADSL (eles podem estar configurados com senha padrão, facilmente obtida na Internet)
- ✓ **regularmente:**
 - nos demais casos

Seja cuidadoso ao usar mecanismos de recuperação:

- ✓ certifique-se de configurar opções de recuperação de senha, como um endereço de *e-mail* alternativo, uma pergunta de segurança e um número de telefone celular
- ✓ ao usar perguntas de segurança evite escolher questões cujas respostas possam ser facilmente adivinhadas (crie suas próprias questões com respostas falsas)
- ✓ 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 possa entendê-las
- ✓ ao solicitar o envio de suas senhas por *e-mail* altere-as o mais rápido possível e certifique-se de cadastrar um *e-mail* de recuperação que você acesse regularmente (para não esquecer a senha desta conta também)

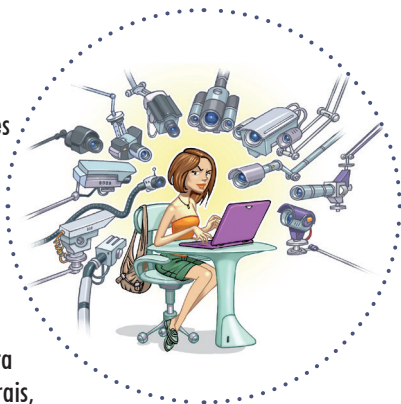
Proteja-se de *phishing* e códigos maliciosos:

- ✓ desconfie de mensagens recebidas, mesmo que enviadas por conhecidos
- ✓ evite seguir *links* recebidos em mensagens eletrônicas
- ✓ não utilize um *site* 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 que você expanda o *link* antes de clicar sobre ele



Preserve a sua privacidade:

- ✓ procure reduzir a quantidade de informações que possam ser coletadas sobre você, pois elas podem ser usadas para adivinhar as suas senhas
- ✓ seja cuidadoso com as informações que você disponibiliza em *blogs* e redes sociais (elas podem ser usadas por invasores para tentar confirmar os seus dados cadastrais, descobrir dicas e responder perguntas de segurança)



Proteja seu 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*, *anti-malware* e *firewall* pessoal
- ✓ configure seu computador para solicitar senha na tela inicial
- ✓ ative o compartilhamento de recursos de seu computador apenas quando necessário e usando senhas bem elaboradas
- ✓ nunca compartilhe a senha de administrador e use-a o mínimo necessário
- ✓ crie contas individuais para todos aqueles que usam seu computador e assegure que todas elas tenham senha

Proteja seus dispositivos móveis:

- ✓ cadastre uma senha de acesso que seja bem elaborada e, se possível, configure-o para aceitar senhas complexas (alfanuméricas)
- ✓ em caso de perda ou furto altere as senhas que possam estar nele armazenadas

Seja cuidadoso ao usar computadores de terceiros:

- ✓ certifique-se de fechar a sua sessão (*logout*) ao acessar *sites* que usem 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 você tenha usado



Consulte a **Cartilha de Segurança** para a Internet para mais detalhes sobre os cuidados a serem tomados ao utilizar senhas:

<https://cartilha.cert.br/senhas/>



INTERNET
SEGURA
BR

Precisa conversar sobre o uso seguro da Internet com **crianças e adolescentes**? O **Portal Internet Segura** apresenta uma série de iniciativas e de recomendações sobre esse assunto, confira!

<http://internetsegura.br/>

cert.br

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

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em <https://www.cert.br/>.

nic.br

Núcleo de Informação
e Coordenação do
Ponto BR

O Núcleo de Informação e Coordenação do Ponto BR - NIC.br (<http://www.nic.br/>) é uma entidade civil, sem fins lucrativos, que implementa as decisões e projetos do Comitê Gestor da Internet no Brasil. São atividades permanentes do NIC.br coordenar o registro de nomes de domínio - Registro.br (<http://www.registro.br/>), estudar e tratar incidentes de segurança no Brasil - CERT.br (<https://www.cert.br/>), estudar e pesquisar tecnologias de redes e operações - CEPTRO.br (<http://www.ceptro.br/>), produzir indicadores sobre as tecnologias da informação e da comunicação - CETIC.br (<http://www.cetic.br/>) e abrigar o escritório do W3C no Brasil (<http://www.w3c.br/>).

cgi.br

Comitê Gestor da
Internet no Brasil

O Comitê Gestor da Internet no Brasil coordena e integra todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios de multilateralidade, transparência e democracia, o CGI.br representa um modelo de governança multissetorial da Internet com efetiva participação de todos os setores da sociedade nas suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (<http://www.cgi.br/principios>). Mais informações em <http://www.cgi.br/>.