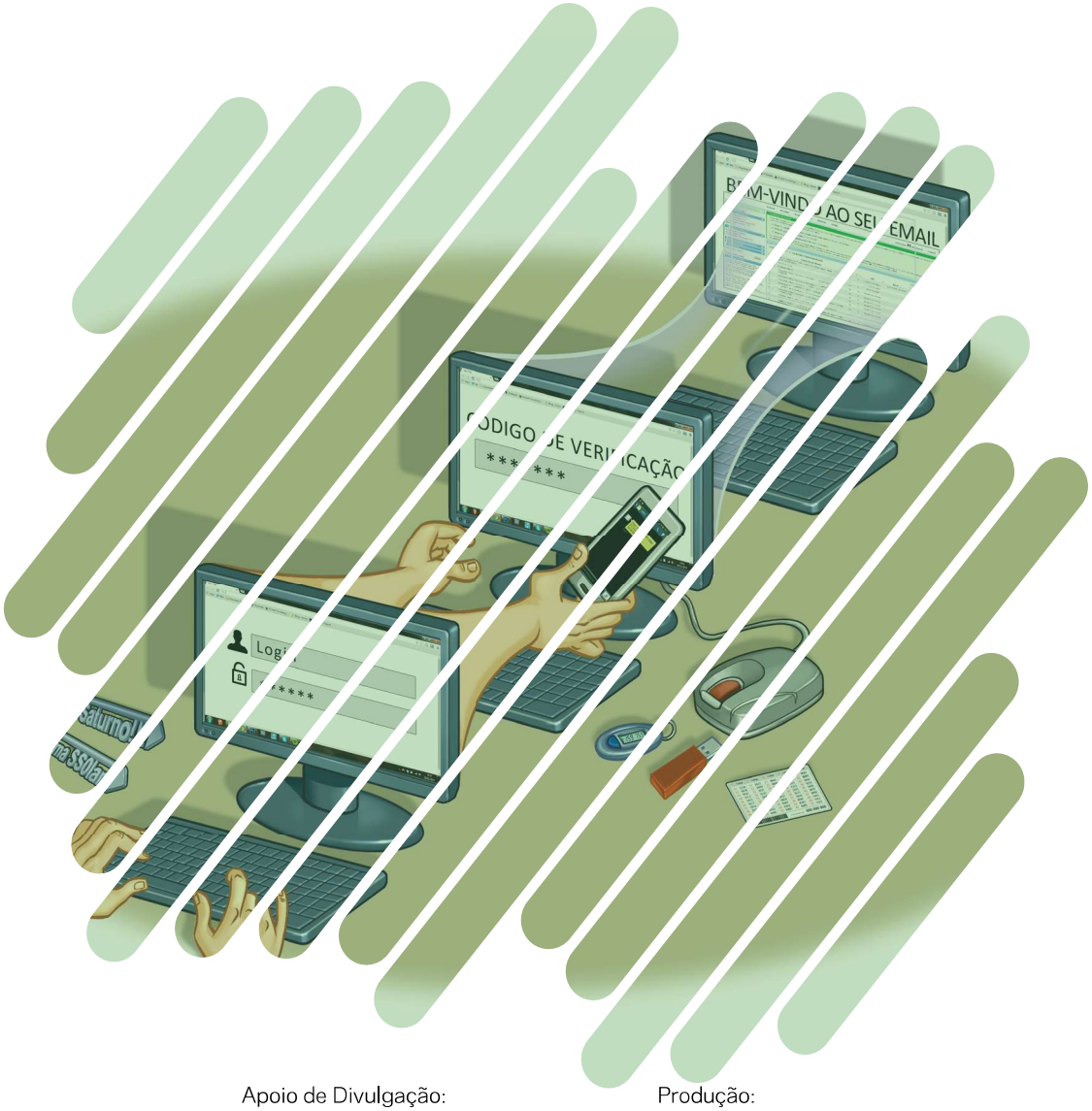
Cartilha de Segurança para Internet

FASCÍCULO

VERIFICAÇÃO EM DUAS ETAPAS



Apoio de Divulgação:

UFPE

STI SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Produção:

cert.br nic.br cgi.br

USAR APENAS SENHAS PODE NÃO SER SUFICIENTE PARA PROTEGER SUAS CONTAS NA INTERNET

Senhas são simples e bastante usadas para autenticação em *sites* na Internet. Infelizmente elas podem não ser suficientes para garantir a sua identidade.

Senhas podem ser facilmente descobertas por meio de técnicas de engenharia social, por observação, se não forem bem elaboradas, se usadas em páginas falsas *(phishing)* ou em computadores infectados/invadidos ou, ainda, se trafegarem na rede sem criptografia.

Por isso, é importante que a verificação da identidade do usuário baseie-se em informações adicionais, além do uso único da senha.

[1]Verificação em duas etapas também é chamada de:
- *two-factor authentication*
- aprovação de *login*
- verificação ou autenticação em dois fatores
- verificação ou autenticação em dois passos

Com a verificação em duas etapas[1] fica mais difícil da sua conta de acesso ser invadida pois, para que isso ocorra, é necessário que o atacante saiba a sua senha (primeira etapa) e também realize com sucesso uma segunda etapa, a qual pode envolver algo que:

» apenas você sabe
- outra senha, pergunta de segurança, número PIN, alguma informação pessoal

» apenas você possui
- código de verificação, cartão de senhas bancárias, *token* gerador de senhas, acesso a um determinado computador ou dispositivo móvel

» você é
- informações biométricas, como impressão digital, palma da mão, rosto, voz e olho.

VERIFICAÇÃO EM DUAS ETAPAS: CONTAS DE ACESSO MAIS SEGURAS

PRINCIPAIS TIPOS E CUIDADOS A SEREM TOMADOS

A verificação em duas etapas é um recurso opcional oferecido por diversos serviços de Internet, como *webmail*, redes sociais, *Internet Banking* e de armazenamento em nuvem. Ao habilitá-la você estará aumentando a segurança de sua conta e, caso não deseje mais utilizá-la, basta que você a desabilite.

O tipo de verificação usado pode variar de acordo com o serviço acessado mas, por facilidade, a maioria costuma utilizar-se de algo que apenas você sabe ou possui.

Alguns dos tipos mais comuns e os cuidados que você deve tomar ao usá-los são:

CÓDIGO DE VERIFICAÇÃO

é um código individual criado pelo serviço e enviado de forma que apenas você possa recebê-lo, por exemplo, por *e-mail*, chamada de voz ou mensagem de texto (SMS) para o telefone celular que você cadastrou. Também pode ser gerado por um aplicativo autenticador, instalado em seu dispositivo móvel.

- Mantenha seus dados para recebimento sempre atualizados
  - números de telefones celulares alternativos também 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 ou gerado pelo aplicativo autenticador
- Recomenda-se o uso do aplicativo autenticador em casos onde não é possível receber mensagens SMS
  - por exemplo, se você estiver viajando ou em uma área sem cobertura de celular
- Tarifas de recebimento de SMS podem ser aplicadas por sua operadora

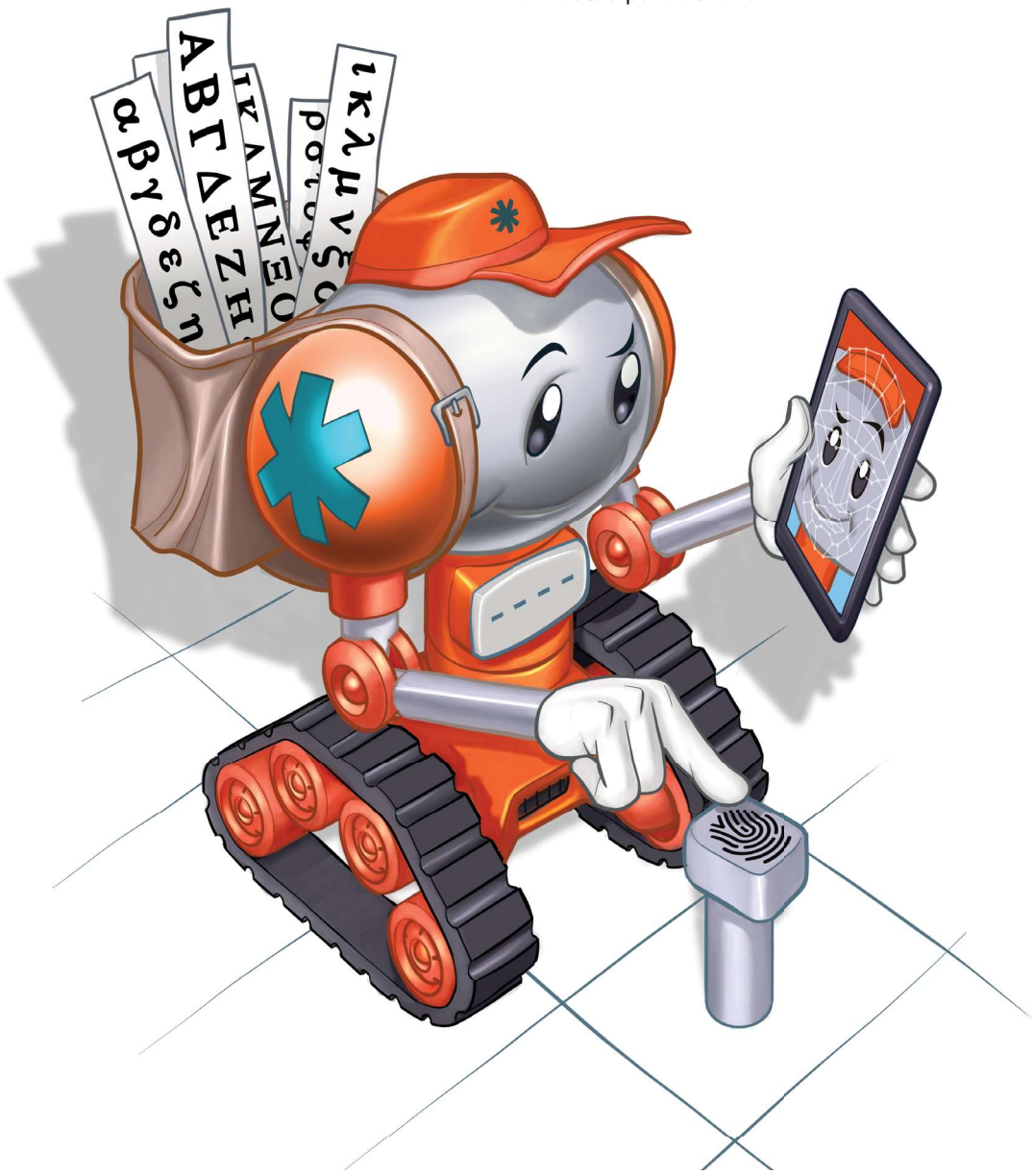
CÓDIGO DE VERIFICAÇÃO ESPECÍFICO

é um código gerado para aplicativos que não suportam a verificação em duas etapas.

» Caso perca o acesso ao seu dispositivo móvel, revogue os códigos específicos gerados para os acessos realizados por meio dele

TOKEN GERADOR DE SENHAS (OU CHAVE ELETRÔNICA)

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



- 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

é um cartão com diversos códigos numerados e que são solicitados quando você acessa a sua conta.

- 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 que é 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 CONFIÁVEL (OU DE CONFIANÇA)

é um computador ou dispositivo móvel que você frequentemente usa para acessar suas contas. Pode ser necessário inserir um código de segurança no primeiro acesso. Ele não será necessário nos demais, pois seu dispositivo será "lembrado", caso você assim o configure.

- Não esqueça de excluir seus dispositivos confiáveis caso eles sejam trocados ou você perca o acesso a eles
- Pode ser necessário que você habilite a opção de *cookies* em seu navegador *web* para que seu dispositivo seja memorizado

LISTA DE CÓDIGOS RESERVA/*BACKUP*

é uma lista de códigos que devem ser usados de forma sequencial e uma única vez.

- 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

é um 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.

- 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

MANTENHA SEU CADASTRO ATUALIZADO

» Dados pessoais, como data de aniversário, podem ser solicitados aleatoriamente para checar a sua identidade

» É importante manter seu endereço de correspondência atualizado, para o recebimento de *tokens* e cartões de segurança

» Dados pessoais e perguntas de segurança podem ser solicitados, caso você desabilite a verificação em duas etapas

SEJA CUIDADOSO AO ELABORAR SUAS SENHAS

» Evite usar:

- dados que possam ser obtidos em redes sociais e páginas *web*
- dados pessoais, como nomes, sobrenomes e contas de usuário
- sequências de teclado, como "1qaz2wsx" e "QwerTAsdfG"
- palavras que fazem parte de listas publicamente conhecidas

» Use:

- números aleatórios
- grande quantidade e diferentes tipos de caracteres

SEJA CUIDADOSO AO USAR SUAS SENHAS

» Certifique-se de utilizar conexão segura

» Evite utilizar computadores de terceiros

» Somente acesse os serviços digitando o endereço diretamente no navegador *web*, nunca clicando em um *link* existente em uma página ou em uma mensagem

PROTEJA SEUS DISPOSITIVOS MÓVEIS

» Cadastre uma senha de acesso que seja bem elaborada e, se possível, configure-os para aceitarem senhas complexas (alfanuméricas)

» Se disponível, instale um programa antivírus

» Mantenha o sistema operacional e as aplicações instaladas sempre com a versão mais recente e com todas as atualizações aplicadas

» Mantenha controle físico sobre eles, principalmente em locais de risco

- procure não deixá-los sobre a mesa
- cuidado com bolsos e bolsas quando estiver em ambientes públicos

» Em caso de perda ou furto:

- revogue todas as autorizações concedidas para os aplicativos neles instalados
- remova-os da lista de dispositivos confiáveis
- cadastre um novo número de celular para continuar a receber códigos de verificação
- se tiver configurado a localização remota, você pode ativá-la e, se achar necessário, apagar remotamente todos os dados neles armazenados

PROTEJA SEU COMPUTADOR

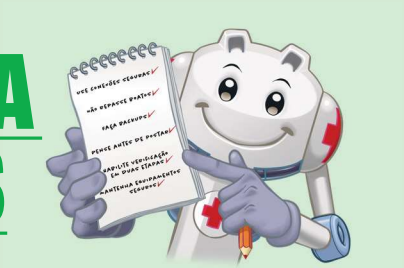
» Mantenha o seu computador seguro

- com a versão mais recente de todos os programas instalados
- com todas as atualizações aplicadas

» Utilize e mantenha atualizados mecanismos de segurança, como *antispam*, antivírus e *firewall* pessoal

» Configure-o para solicitar senha na tela inicial

SAIBA MAIS



» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **cartilha.cert.br**

» Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **internetsegura.br**

cert.br

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 **www.cert.br.**

nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

cgi.br

O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento 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 do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br.**

cartilha.cert.br/cc

outubro / 2020