

Input
TECNOLOGIA



www.input.com.vc



***Proteja-se:
Verificação em
duas etapas***

Segurança da Informação



➤ **Proteja-se:** **Verificação em duas etapas**



Usar apenas senhas pode não ser suficiente para proteger suas contas na internet.

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, com a chamada **verificação em duas etapas**.

Contas de acesso mais seguras

Com a verificação em duas etapas, 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 (íris).

Fonte: www.cert.br

Proteja-se: Verificação em duas etapas



Principais tipos



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 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.



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.

Fonte: www.cert.br

Proteja-se: Verificação em duas etapas



Principais tipos



Dispositivo móvel 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.



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).

Fonte: www.cert.br

➤ **Proteja-se:** **Verificação em duas etapas**



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 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.

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;
- caracteres especiais (*&#@);
- grande quantidade e diferentes tipos de caracteres.

Fonte: www.cert.br

➤ **Proteja-se:** *Verificação em duas etapas*



Outros cuidados

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;

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 receber códigos de verificação;
- se tiver configurado a localização remota, você pode ativá-la e 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.



Fonte: www.cert.br



www.input.com.vc

+55 (11) 3976.8000

