

Proteja seus dados

Cartilha de boas práticas de
uso do computador para
mantê-lo mais rápido e seguro

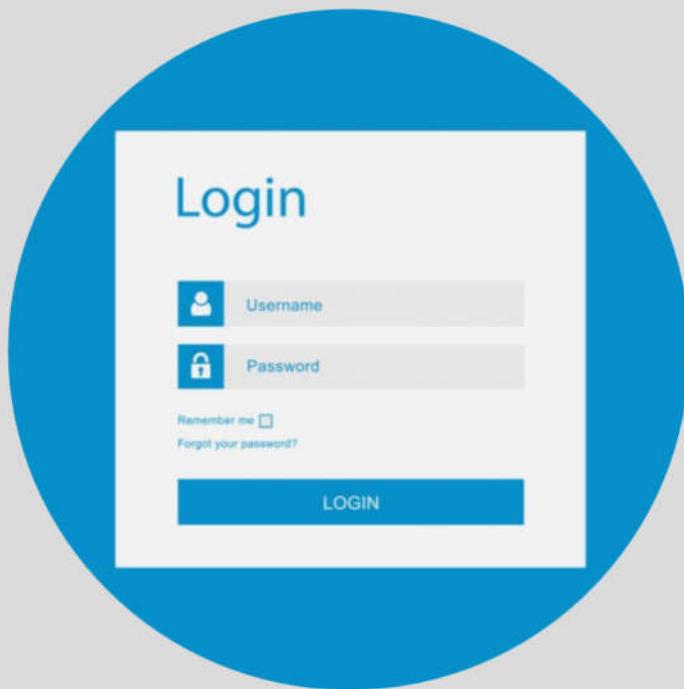
Investigue o site antes de inserir os dados



O primeiro e principal sinal para saber se um site é seguro é observar se ele possui o certificado de segurança SSL

(Secure Socket Layer). Para isso, basta observar a url (endereço do site) e garantir que ela possui o formato HTTPS e se a barra de busca exibe o ícone de um cadeado para sinalizar que o site é seguro.

Fique atento a suas senhas



Com tantas informações para lembrar, muitas pessoas optam por usar a mesma senha para diversos serviços. No entanto, essa prática não é recomendada. Isso porque, caso o fraudador descubra essa senha, ele pode ter acesso a todas as suas contas pessoais de uma só vez.

Para evitar que isso ocorra, utilize senhas diferentes e para não esquecer guarde-as anotadas em um local seguro. Além disso, ao escolher suas senhas, certifique-se de que elas sejam fortes, contendo números, letras e caracteres especiais, se for possível. Evite datas de aniversário ou números sequenciais que são facilmente descobertos.

Mantenha o sistema operacional atualizado

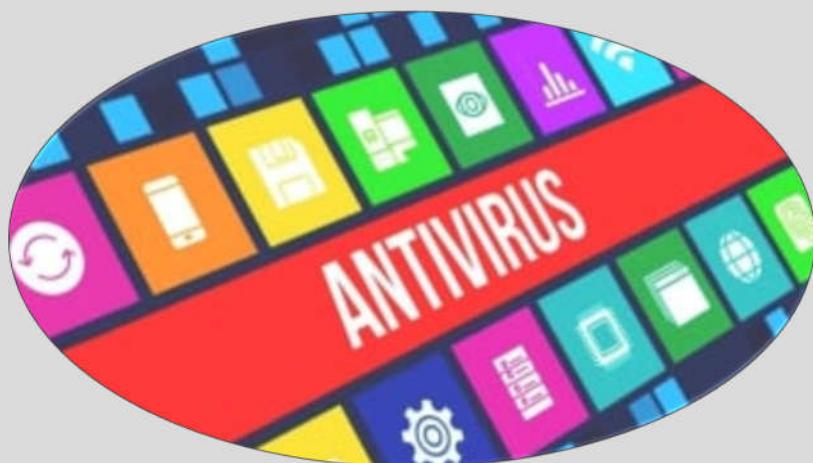


Sempre surgem novas atualizações do sistema operacional e

mantê-las em dia é essencial. A cada mudança são inseridas novas formas de proteção que ajudam a manter os invasores longe e as vulnerabilidades são corrigidas.

Quem não se atenta a esse detalhe, pode deixar a configuração para que a atualização seja automática, pois assim não será preciso se preocupar com isso e o computador estará mais seguro.

Mantenha um antivírus atualizado



O antivírus é um importante aliado da segurança na internet.

Existem opções pagas e gratuitas que podem identificar ameaças durante a navegação ou mesmo bloquear o acesso a sites suspeitos.

Outra dica importante é não realizar downloads de fontes desconhecidas. Sempre que decidir baixar um aplicativo ou arquivo, certifique-se de que trata-se de uma fonte confiável

Evite instalar softwares suspeitos



Sabe quando um site manda você instalar um software antes de baixar um filme ou música? Ou até aquela barra de ferramentas que promete organizar a sua vida e o seu computador? Desconfie.

Diversos softwares são responsáveis por vigiar os seus passos no computador, reconhecer e gravar suas senhas e dados e também controlar a sua webcam.

Evitar clicar ou baixar os anexos de e-mails desconhecidos



Cuidado ao abrir e-mails de pessoas ou fontes

desconhecidas, especialmente quando eles não são solicitados.

Clicar em links ou fazer download de anexos pode infectar seu computador com vírus ou sujeitar você a fraude, malware ou fraude. Alguns vírus danificam seu computador, enquanto outros têm a capacidade de roubar suas informações pessoais e, finalmente, sua identidade.

Tenha cuidado ao repassar informações pessoais pela internet



Pense antes de publicar qualquer coisa online ou compartilhar informações em e-mails. O que você publica online pode ser visto por qualquer

pessoa.

Compartilhar informações pessoais com outras pessoas que você não conhece pessoalmente é um dos seus maiores riscos online.

Considere remover seu nome de sites que compartilham suas informações pessoais obtidas de registros públicos (incluindo seu número de telefone, endereço, avatares de mídia social e fotos) com qualquer pessoa na Internet

Tenha cuidado ao repassar informações pessoais pela internet



no equipamento.

Existem diferentes maneiras de fazer isso. Há a possibilidade de salvar os dados em um disco rígido externo fazendo a transferência manual. Outra possibilidade é usar o backup em nuvem em serviços especializados. Neles há a possibilidade de salvar os arquivos manualmente ou fazer o backup automático periodicamente.

Manter o computador seguro é uma necessidade para não ter os dados expostos e manter a privacidade. Seguir dicas de especialistas e manter os softwares atualizados é a melhor maneira de conseguir isso.

O backup não é uma forma de manter o computador seguro, mas pode garantir que não perca informações importantes no caso de uma invasão ou problema