**Segurança na internet: saiba como se proteger**

O meio digital encurta distâncias e torna nosso dia a dia mais prático. Mas, assim como cuidamos da nossa segurança no mundo real, a **segurança na internet**precisa ser redobrada, dada a crescente sofisticação dos golpes virtuais. Quem nunca ouviu falar de um conhecido que teve uma conta clonada ou caiu em um golpe online, não é verdade?

Usamos a internet para interagir com amigos, estudar, fazer compras e pagar contas. Mas, com essa conveniência, surgiram também novas preocupações. Nesse cenário, é importante conhecer algumas dicas de**segurança na internet** para ter uma experiência positiva. E é por isso que preparamos este guia especial para você.

Queremos te ajudar a navegar mais com tranquilidade, mostrando como identificar e evitar essas ameaças para que sua experiência online seja sempre positiva e segura. Fique conosco para entender os detalhes e**aprender a se proteger**!

## **O que é segurança na internet?**

Segurança na internet tem a ver com uma série de **boas práticas que adotamos para usar a rede com mais cuidado**. Afinal, assim como no mundo físico, onde tomamos precauções para nos proteger, a segurança na internet se refere ao conjunto de cuidados e boas práticas que adotamos ao utilizar a rede.

Por exemplo, quando você atravessa a rua, geralmente procura a faixa de pedestres, certo? Isso porque ela indica o ponto mais seguro para ir de um lado a outro da via.

**No caso da internet, é igualmente importante se preocupar por onde você circula.**Então, surgem recomendações como evitar sites suspeitos e nunca clicar em links estranhos.

É importante termos essa atenção, pois as ameaças online evoluíram bastante. Se antes nos preocupávamos mais com vírus simples, **hoje enfrentamos golpes elaborados**, muitas vezes utilizando técnicas de engenharia social para nos enganar.

Mas fique tranquilo, entender o que é segurança na internet é o primeiro passo para navegarmos de forma mais protegida.

## **O que é engenharia social? A base de quase todos os golpes**

Antes de conhecer os tipos de golpes, é importante entender a tática que a maioria deles utiliza: a **engenharia social**. Ela é a base de quase todas as fraudes, pois consiste em manipular psicologicamente a vítima, explorando sentimentos como a confiança, a curiosidade ou o senso de urgência.

Um golpista não precisa de sistemas complexos de invasão se conseguir te convencer, por exemplo, a fornecer sua senha ou fazer uma transferência por conta própria. **Eles se aproveitam do fator humano para quebrar as barreiras de segurança.**

O cibercriminoso pode se passar por um familiar em perigo, um funcionário de banco solicitando uma confirmação ou até mesmo informando um prêmio que você acabou de “ganhar”. Em todos esses casos, o objetivo é o mesmo: fazer com que você, sem pensar, tome uma atitude que vai favorecê-lo.

Com a engenharia social, os golpes ganharam novas roupagens. Os criminosos usam a tecnologia a seu favor para criar armadilhas cada vez mais sofisticadas e convincentes. Por isso, **a melhor defesa é a informação.**

## **Principais perigos que você corre na internet**

Existem diversos riscos para quem não se protege na rede. Entre os mais danosos, podemos citar:

### **Furto de informações pessoais**

Dados como nome completo, data de nascimento e CPF podem ser roubados e até vendidos para outros bandidos. Eles usam esse conteúdo para realizar fraudes, como fazer compras caríssimas em nome de outra pessoa.

### **Roubo de identidade**

Alguns golpistas podem invadir sua conta no WhatsApp. Fingindo ser você, eles entram em contato com seus amigos e pedem dinheiro emprestado para uma emergência. Depois somem com a grana, obviamente.

### **Exposição da intimidade**

Já imaginou ter suas mensagens privadas ou fotos íntimas vazadas para o mundo inteiro ver? Desconhecidos saberiam onde você mora, com quem você se relaciona e o que faz quando ninguém está olhando. É para acabar com o sono de qualquer um!

### **Perda de arquivos**

A invasão ao dispositivo pessoal também compromete os documentos ali armazenados. Vírus, malwares e outros softwares maliciosos são capazes de corromper os arquivos, ou até mesmo apagá-los completamente do sistema.

## **Ataques virtuais mais comuns: como os criminosos agem e como se proteger**

A criatividade dos golpistas não tem limites, mas as táticas se repetem. Conhecer os tipos de golpes mais comuns e seus sinais de alerta é o que vai te ajudar a evitar prejuízos.

### **Golpe do Pix e do WhatsApp: táticas do falso familiar e do número clonado**

O **golpe do Pix** é uma das fraudes mais comuns hoje em dia. Em sua forma mais conhecida, o golpista se passa por um familiar ou amigo em apuros e, usando um número de telefone novo com a foto da pessoa, pede uma transferência urgente via Pix.

Outra tática, ainda mais perigosa, é o sequestro ou a clonagem do WhatsApp. Nesse caso, o criminoso tem acesso à sua conta e pede dinheiro a todos os seus contatos.

* **Sinal de alerta:** o pedido de dinheiro é urgente e a pessoa não pode atender a uma ligação ou chamada de vídeo.
* **Como se proteger:** sempre **desconfie** de pedidos de dinheiro. Ligue ou faça uma chamada de vídeo para o contato em seu número original para confirmar a identidade antes de fazer qualquer transferência.

### **Phishing, smishing e vishing: o ataque da isca digital**

O **[phishing](https://blog.cresol.com.br/o-que-e-phishing-como-se-proteger-desse-golpe/" \t "_blank)** (“pescaria digital”) é uma técnica de engenharia social em que o criminoso se passa por uma instituição confiável ([**instituição financeira**](https://blog.cresol.com.br/quais-as-vantagens-de-optar-por-uma-instituicao-financeira-cooperativa/), loja, empresa de e-commerce) para roubar seus dados. Ele envia um e-mail ou SMS (**smishing**) com um link falso que te direciona para uma página idêntica à original. Quando você preenche seus dados (senha, número do cartão, CPF), os criminosos roubam as informações.

Já o **vishing** é o mesmo golpe, mas por meio de uma ligação telefônica.

* **Sinal de alerta:** e-mails com erros de português, links com endereços estranhos e mensagens que pedem para você “confirmar seus dados” ou “regularizar uma situação urgente”.
* **Como se proteger:** nunca clique em links suspeitos. Vá diretamente ao site oficial da instituição ou utilize o aplicativo para verificar qualquer informação.

### **Golpe da falsa central de atendimento e do falso suporte técnico**

Nesse tipo de golpe, **o criminoso entra em contato com você se passando por representante de alguma instituição ou empresa** — seja um banco, uma operadora de [**cartão de crédito**](https://blog.cresol.com.br/cartao-de-credito-debito-cresol/) ou até mesmo o suporte técnico de uma grande empresa de tecnologia. O golpista afirma que há um problema na sua conta e que você precisa fornecer dados para “solucioná-lo” ou, ainda, baixar um aplicativo para que ele tenha acesso remoto ao seu dispositivo.

* **Sinal de alerta:** as instituições financeiras jamais pedem sua senha ou dados de segurança por telefone. Nenhum suporte técnico legítimo vai te pedir para baixar um app para ter acesso remoto ao seu celular ou computador.
* **Como se proteger:** encerre a ligação e, caso tenha dúvidas, entre em contato com a instituição por um canal oficial que você já conhece (o número de telefone que está no seu cartão ou no site oficial).

### **Falso boleto e falso leilão: armadilhas com documentos**

Os golpes que utilizam documentos falsos são muito comuns. No caso do **falso boleto**, o criminoso envia um boleto com informações falsas para que você pague por uma dívida que não existe. A vítima, na pressa de pagar, não confere os dados do beneficiário e acaba caindo na armadilha.

Já no **falso leilão**, o golpista cria sites falsos que imitam leiloeiros para vender produtos (geralmente carros) com preços muito abaixo do mercado.

* **Sinal de alerta:** em boletos, verifique o nome do beneficiário (o pagador deve ser a empresa real, e não um CPF). Em leilões, desconfie de preços muito baixos e verifique se o site é o oficial, consultando os órgãos reguladores.
* **Como se proteger:** antes de pagar um boleto, confira todas as informações do documento. Para leilões, verifique a reputação da empresa e as condições de venda com atenção.

### **Falso site de vendas e clonagem de cartão**

O **falso site de vendas** é uma tática de phishing. O criminoso cria um e-commerce falso — geralmente, muito parecido com grandes varejistas, ou seja, empresas que o público confia — para roubar os dados do seu cartão de crédito.

Outra forma de roubo de dados é a **clonagem de cartão**, que pode ocorrer em maquininhas adulteradas em lojas, restaurantes ou postos de gasolina. Quando isso acontece, o criminoso tem acesso aos seus dados e pode fazer compras no seu nome.

* **Sinal de alerta:** desconfie de sites com preços “imperdíveis”, endereços eletrônicos estranhos e layouts amadores.
* **Como se proteger:** verifique sempre se o site tem um cadeado de segurança na URL. Para grandes varejistas, certifique-se de que o endereço do site não contém erros de digitação ou caracteres adicionais (ex: “mercadolivree.com.br” em vez de “mercadolivre.com.br”). Ao usar a maquininha, nunca a perca de vista e verifique se não há nenhum dispositivo estranho acoplado.

### **Malvertising: publicidade que esconde perigo**

Malvertising é o termo em inglês para **publicidade maliciosa**. Os golpistas exibem anúncios em sites confiáveis, mas escondem um malware ali. Se você clica no banner, acaba infectando seu dispositivo. A partir daí, o malware pode criar brechas que comprometem sua **segurança na internet**.

* **Sinal de alerta:** o anúncio parece legítimo, mas o leva para uma página suspeita ou inicia um download sem sua permissão.
* **Como se proteger:** evite clicar em anúncios, mesmo em sites confiáveis, e mantenha um bom software de segurança (antivírus, firewall).

### **Malware: programas que comprometem sua segurança**

**Malware** é um termo geral para programas maliciosos (como vírus, worms, trojans, spywares e keyloggers) que se instalam no seu computador ou celular sem você perceber. Eles podem roubar informações confidenciais, monitorar suas atividades, registrar senhas e dados bancários ou simplesmente deixar seu dispositivo lento.

* **Sinal de alerta:** lentidão inesperada no dispositivo, exibição excessiva de anúncios ou o surgimento de novos programas desconhecidos.
* **Como se proteger:** instale um bom antivírus e o mantenha sempre atualizado. Tenha cuidado com anexos de e-mail e baixe aplicativos apenas de lojas oficiais.

### **Ransomware: o sequestro de seus arquivos**

O **ransomware** é um tipo de malware que “sequestra” seus dados, criptografando seus arquivos importantes e exigindo um resgate, geralmente em criptomoedas, para devolvê-los. Esse tipo de golpe pode atingir tanto grandes empresas quanto usuários domésticos, causando grande transtorno e perda de informações valiosas.

* **Sinal de alerta:** você perde acesso aos seus arquivos e uma mensagem pedindo pagamento aparece na sua tela.
* **Como se proteger:** a melhor forma de se proteger é manter backups regulares de todos os seus arquivos importantes. Nunca pague o resgate, pois não há garantia de que os dados serão devolvidos.

### **Pirâmide financeira e roubo de identidade**

A [**pirâmide financeira**](https://blog.cresol.com.br/piramide-financeira/) é uma fraude antiga que continua fazendo vítimas. Nesse esquema, o golpista promete altos lucros em investimentos que não existem, usando o dinheiro de novos investidores para pagar os antigos. O sistema só se mantém enquanto há novas pessoas entrando. No entanto, quando não há mais ninguém, o golpe desmorona e os fundadores somem com o dinheiro de todos.

Já o **roubo de identidade** acontece quando um criminoso rouba seus dados pessoais para fazer empréstimos ou abrir contas em seu nome, deixando um rastro de dívidas para você.

* **Sinal de alerta:** desconfie de promessas de “dinheiro fácil” e de retornos muito acima do mercado.
* **Como se proteger:** nunca invista em algo que pareça bom demais para ser verdade e não compartilhe seus dados pessoais em sites ou aplicativos que você não conhece. Lembre-se também de monitorar seu CPF regularmente, por meio de serviços de monitoramento de crédito, que alertam sobre qualquer atividade suspeita em seu nome.

## **12 dicas de segurança na internet para você se proteger**

Além de conhecer os golpes, é fundamental ter hábitos e atitudes que fortaleçam a sua **segurança digital**. A melhor forma de se proteger é agindo preventivamente.

### **Proteja seus dados e senhas com inteligência**

1. **Nunca revele senhas:** as instituições financeiras jamais solicitam esses dados. Use senhas fortes e exclusivas para cada conta. Se precisar anotá-las, mantenha-as em local seguro, fora da internet.
2. **Ative a autenticação de dois fatores (2FA):** esse recurso confirma sua identidade e eleva a proteção das suas contas online.
3. **Tenha cuidado com o que compartilha:** evite divulgar informações pessoais e financeiras em redes sociais.
4. **Revise as permissões de apps:** fique atento às permissões que você concede a aplicativos em seu celular, como acesso à câmera, microfone ou contatos.
5. **Use apenas seu dispositivo pessoal:** faça operações financeiras online apenas em seu celular ou computador. Evite dispositivos de terceiros.

### **Use apenas canais e redes seguras**

1. **Acesse sites e aplicativos oficiais:** prefira lojas e serviços conhecidos. Verifique o endereço eletrônico e o símbolo de cadeado no navegador, que indica um site seguro.
2. **Tenha atenção ao usar Wi-Fi público:** evite fazer transações financeiras em redes Wi-Fi abertas, pois elas são mais vulneráveis a ataques. Prefira sua rede particular ou dados móveis.
3. **Use softwares de segurança:** instale antivírus e firewall em seus dispositivos e mantenha-os sempre atualizados para bloquear programas maliciosos.
4. **Desconfie de software pirata:** evite instalar softwares piratas, pois eles podem conter brechas de segurança que facilitam a invasão da sua máquina.

### **Fique alerta para não cair em golpes**

1. **Desconfie sempre:**mensagens que criam senso de urgência, promessas de dinheiro fácil ou ofertas muito vantajosas são grandes sinais de alerta.
2. **Atenção a links e anexos:** nunca clique em links suspeitos ou baixe anexos de e-mails de remetentes desconhecidos.
3. **Monitore suas contas:**revise regularmente seu CPF e o extrato da sua conta para identificar qualquer transação suspeita.