SEGURANÇA DA INTERNET

Bruno Brito

Carlos Roberto

Felipe Ricardo

Rodrigo Galdino

**Introdução**

A segurança informática cria métodos, procedimentos e normas que buscam identificar e eliminar as vulnerabilidades das informações e dos equipamentos físicos, como os computadores.

Este tipo de segurança conta com bases de dados, arquivos e aparelhos que fazem com que as informações importantes não caiam em mãos de pessoas erradas.

Uma das melhores formas de se manter seguro na internet é usando [**antivírus**](https://edu.gcfglobal.org/pt/virus-e-antivirus/o-que-e-um-virus/1/) nos computadores, por isso sempre recomendamos ter um instalado nos seus equipamentos.

**O que é segurança da Internet?**

Segurança da Internet é um termo que descreve a segurança de atividades e transações feitas pela Internet. Trata-se de um componente particular de ideias maiores, como segurança virtual e segurança do computador, envolvendo tópicos que incluem segurança do navegador, comportamento on-line e segurança de rede. Passamos grande parte de nossas vidas on-line, e algumas das ameaças à segurança da Internet que podemos encontrar incluem:

* Hackeamento, quando usuários não autorizados obtêm acesso a sistemas de computador, contas de e-mail ou sites.
* Vírus ou software malicioso (conhecidos como malware), que podem danificar dados ou tornar sistemas vulneráveis a outras ameaças.
* Roubo de identidade, em que criminosos podem roubar informações pessoais e financeiras.

Indivíduos e organizações podem se proteger desses tipos de ameaças praticando segurança da Internet.

## Quais são as ameaças mais comuns à segurança na Internet?

Para garantir a privacidade e segurança na Internet, é importante conhecer os diferentes tipos de ataques. As ameaças comuns à segurança na Internet incluem:

### **Phishing**

[Phishing](https://www.kaspersky.com.br/resource-center/preemptive-safety/phishing-prevention-tips) é um ataque virtual envolvendo e-mails enganosos. Os hackers tentam enganar os remetentes dos e-mails para que acreditem que uma mensagem é genuína e relevante, uma solicitação do seu banco ou uma nota de um colega de trabalho, por exemplo, de forma que cliquem em um link ou abram um anexo. O objetivo é enganar as pessoas para que entreguem informações pessoais ou baixem malware.

Phishing é uma das ameaças mais antigas à segurança na Internet, remontando aos anos 1990. É popular até hoje, pois é uma das maneiras mais baratas e fáceis de os criminosos roubarem informações. Recentemente, as técnicas e mensagens de phishing tornaram-se cada vez mais sofisticadas.

### **Hackeamento e acesso remoto**

Os hackers estão sempre procurando explorar uma rede privada ou vulnerabilidades do sistema, de forma que possam roubar informações e dados confidenciais. A tecnologia de acesso remoto dá a eles outro alvo a ser explorado. Os softwares de acesso remoto permitem que os usuários acessem e controlem um computador remotamente e, desde a pandemia, com mais pessoas trabalhando remotamente, sua utilização aumentou.

O protocolo que permite aos usuários controlar um computador conectado à Internet remotamente é chamado de Remote Desktop Protocol, ou RDP. Como empresas de todos os tamanhos usam amplamente o RDP, as chances de uma rede estar inadequadamente protegida são relativamente altas. Os hackers usam diferentes técnicas para explorar vulnerabilidades de RDP até que tenham total acesso a uma rede e aos seus dispositivos. Eles mesmos podem roubar dados ou vender as credenciais na dark web.

### **Malware e malvertising**

[Malware](https://www.kaspersky.com.br/resource-center/threats/malware-protection) é a combinação dos termos "malicious" (malicioso) e "software". É um termo amplo relacionado a vírus, worms, cavalos de Troia e outros programas danosos que os hackers usam para causar estragos e roubar informações confidenciais. Qualquer software criado para danificar um computador, servidor ou rede pode ser descrito como malware.

Malvertising é uma combinação de "malicious" (maliciosa) e "advertising" (publicidade). O termo refere-se à publicidade on-line que distribui malware. Publicidade on-line é um ecossistema complexo que envolve sites de editores, trocas de anúncios, servidores de anúncios, redes de redirecionamento e redes de entrega de conteúdo. Os malvertisers exploram essa complexidade para implantar código malicioso em locais que editores e redes de anúncios nem sempre detectam. Os usuários de Internet que interagem com um anúncio malicioso podem baixar malware em seus dispositivos ou ser redirecionados a sites maliciosos.

### **Ransomware**

[Ransomware](https://www.kaspersky.com.br/resource-center/threats/ransomware-examples) é um tipo de malware que impede você de usar o seu computador ou acessar arquivos específicos no seu computador se um resgate não for pago. Geralmente, ele é distribuído como um cavalo de Troia, ou seja, malware disfarçado de software legítimo. Após instalado, ele bloqueia a tela do seu sistema ou alguns arquivos até que você pague.

Devido ao seu aparente anonimato, os operadores de ransomware normalmente especificam o pagamento em criptomoedas como [Bitcoin](https://www.kaspersky.com.br/resource-center/definitions/what-is-bitcoin). Os preços dos resgates variam, dependendo da variante de ransomware e do preço ou da taxa de câmbio das moedas digitais. Nem sempre os criminosos liberam os arquivos criptografados depois que você paga.

Os ataques de ransomware estão crescendo, e novas variantes de ransomware continuam a surgir. As variantes mais conhecidas de ransomware são: [Maze](https://www.kaspersky.com.br/resource-center/definitions/what-is-maze-ransomware), Conti, GoldenEye, Bad Rabbit, Jigsaw, Locky e [WannaCry](https://www.kaspersky.com.br/resource-center/threats/ransomware-wannacry).

### Botnets

O termo [botnet](https://www.kaspersky.com.br/resource-center/threats/botnet-attacks) é uma contração de "robot network" (rede de robôs). Uma botnet é uma rede de computadores intencionalmente infectados por malware, de forma que possam realizar tarefas automatizadas na Internet sem a permissão ou o conhecimento dos proprietários dos computadores.

Quando o proprietário de uma botnet controla o seu computador, ele pode usá-lo para realizar atividades maliciosas. Entre elas:

* Gerar tráfego falso na Internet em sites de terceiros para ganho financeiro.
* Usar o poder da máquina para auxiliar ataques de negação de serviço distribuído (DDoS, Distributed Denial of Service) para derrubar sites.
* Enviar e-mails de spam a milhões de usuários da Internet.
* Cometer fraudes e roubos de identidade.
* Atacar computadores e servidores.

Os computadores tornam-se parte de uma botnet da mesma forma que são infectados por qualquer outro tipo de malware; por exemplo, abrindo anexos de e-mail que baixam malware ou visitando sites infectados com malware. Eles também podem se espalhar de um computador para outro através de uma rede. O número de bots em uma botnet varia e depende da capacidade do proprietário da botnet de infectar dispositivos desprotegidos.

### **Ameaças a Wi-Fi, público ou doméstico**

O [Wi-Fi público apresenta riscos](https://www.kaspersky.com.br/resource-center/preemptive-safety/public-wifi-risks) porque a segurança dessas redes, em cafeterias, shoppings, aeroportos, hotéis, restaurantes, entre outros, costuma ser relaxada ou inexistente. Falta de segurança significa que criminosos virtuais e ladrões de identidade podem monitorar o que você está fazendo on-line e roubar suas senhas e informações pessoais. Outros perigos do Wi-Fi incluem:

* **Packet sniffing** – os invasores monitoram e interceptam dados.

descriptografados enquanto transitam em uma rede desprotegida.

* **Ataques "man-in-the-middle"** – os invasores comprometem um hotspot Wi-Fi para se inserir nas comunicações entre a vítima e o hotspot para interceptar e modificar os dados em trânsito.
* **Redes de Wi-Fi criminosas** – os invasores estabelecem um [honeypot](https://www.kaspersky.com.br/resource-center/threats/what-is-a-honeypot) na forma de Wi-Fi gratuito para colher dados valiosos. O hotspot do invasor torna-se o veículo para todos os dados trocados na rede.

## Como proteger seus dados on-line

Se você está se perguntando como garantir proteção na Internet e como proteger seus dados on-line, confira estas dicas úteis de segurança na Internet:

### **Ative a autenticação multifatorial sempre que puder**

Autenticação multifatorial (MFA) é um método de autenticação que pede aos usuários que forneçam dois ou mais métodos de verificação para acessar uma conta on-line. Por exemplo, em vez de simplesmente perguntar um nome de usuário e senha, a autenticação multifatorial solicita informações adicionais, como:

* Uma senha única extra que os servidores de autenticação do site enviam ao telefone ou endereço de e-mail do usuário.
* Respostas a perguntas de segurança pessoais.
* Uma impressão digital ou outra informação biométrica, como [reconhecimento facial](https://www.kaspersky.com.br/resource-center/definitions/what-is-facial-recognition) ou de voz.

A autenticação multifatorial diminui a probabilidade de um ataque virtual bem-sucedido. Para tornar suas contas on-line mais seguras, é uma boa ideia implementar a autenticação multifatorial quando possível. Você também pode considerar usar um aplicativo autenticador de terceiros, como Google Authenticator e Authy, para ajudar na segurança da Internet.

### **Use um firewall**

Um [firewall](https://www.kaspersky.com.br/resource-center/definitions/firewall) funciona como uma barreira entre seu computador e outra rede, como a Internet. Os firewalls bloqueiam tráfego indesejado e também podem ajudar a impedir que software malicioso infecte o seu computador. Normalmente, o seu sistema operacional e sistema de segurança vêm com um firewall pré-instalado. Para maximizar a segurança na Internet, é uma boa ideia certificar-se de que esses recursos estejam ativados, com suas configurações definidas para executar atualizações automaticamente.

### Escolha seu navegador com cuidado

Nossos navegadores são a porta de entrada principal para a web e por isso desempenham um papel fundamental na segurança na Internet. Um bom navegador da web deve ser seguro e ajudar a proteger você de violações de dados. A Freedom of the Press Foundation compilou [um guia detalhado aqui, explicando os prós e contras da segurança em relação aos navegadores da web no mercado](https://freedom.press/training/-depth-guide-choosing-web-browser/).

### **Crie senhas fortes e use um gerenciador de senhas seguro**

[Uma senha forte](https://www.kaspersky.com.br/resource-center/threats/how-to-create-a-strong-password) ajudará você a manter a segurança na Internet. Uma boa senha é:

* Longa – composta de até 12 ou mais caracteres.
* Uma combinação de caracteres – ou seja, letras minúsculas e maiúsculas, além de símbolos e números.
* Evita o óbvio – como usar números em sequência (“1234”) ou informações pessoais que alguém que conhece você possa adivinhar, como sua data de nascimento ou o nome do seu animal de estimação.
* Evite caminhos no teclado que sejam fáceis de memorizar.

Hoje em dia, substituir letras e números por caracteres parecidos não é mais suficiente; por exemplo, "S3nh@" para "senha", pois os hackers estão atentos a isso. Quanto mais complexa for sua senha, mais difícil de descobri-la. Um [gerenciador de senhas](https://www.kaspersky.com.br/password-manager) pode ajudar – gerando, armazenando e gerenciando todas as suas senhas em uma conta on-line segura.

Mantenha suas senhas privadas – evite compartilhá-las com outras pessoas ou anotá-las. Tente evitar usar a mesma senha para todas as suas contas e lembre-se de mudá-las regularmente.

### Mantenha um programa de segurança atualizado instalado nos seus dispositivos

Ter um antivírus de segurança na Internet é fundamental para garantir a privacidade e a segurança on-line. O melhor software de segurança na Internet protege você de diferentes tipos de ataques na Internet e protege seus dados on-line. É importante manter o software antivírus atualizado – a maioria dos programas modernos é atualizada automaticamente para ficar à frente das ameaças à segurança na Internet.

## Segurança de rede

Segurança de rede refere-se a qualquer atividade criada para proteger a usabilidade e a integridade da sua rede e dos seus dados. Destina-se a uma variedade de ameaças e as impede de entrar ou se espalhar na sua rede.

### **Como configurar o seu roteador Wi-Fi com segurança**

O seu roteador Wi-Fi é um aspecto essencial da segurança na Internet. Ele verifica todo o tráfego de entrada e saída e controla o acesso à sua rede Wi-Fi e, por meio dela, seus telefones, computadores e outros dispositivos. A segurança do roteador melhorou nos últimos anos, mas ainda há etapas que você pode seguir para aprimorar a proteção na Internet.

Alterar as configurações padrão do seu roteador, como o nome e os detalhes de login do seu roteador padrão, é um primeiro passo importante. Isso pode ajudar a diminuir o potencial de que sua rede Wi-Fi seja um alvo para hackers, pois indica que o roteador está sendo ativamente gerenciado.

Há vários recursos e configurações que você pode desativar para aumentar a segurança do seu roteador Wi-Fi. Programas de malware podem tirar vantagem de recursos como acesso remoto, plug and play universal e configuração de Wi-Fi protegido. Embora possam ser práticos, desativá-los torna sua rede doméstica mais segura.

### **Considere usar uma VPN, principalmente ao acessar Wi-Fi público**

A melhor maneira de proteger seus dados on-line ao acessar Wi-Fi público é usar uma [rede privada virtual (VPN)](https://www.kaspersky.com.br/vpn-secure-connection). Uma VPN cria um túnel criptografado entre você e um servidor remoto operado por um serviço de VPN. Todo o seu tráfego de Internet é roteado através desse túnel, o que torna seus dados mais seguros. Se você se conectar a uma rede pública usando VPN, outras pessoas nessa rede não poderão ver o que você está fazendo. Isso fornece maior proteção na Internet.

### **Segurança da rede e Internet das Coisas**

[Internet das Coisas (IoT)](https://www.kaspersky.com.br/resource-center/threats/internet-of-things-security-risks) é um termo usado para descrever dispositivos físicos que não sejam computadores, telefones e servidores, que se conectam à Internet e podem coletar e compartilhar dados. Entre os exemplos de dispositivos IoT, encontram-se monitores de fitness vestíveis, geladeiras inteligentes, relógios inteligentes e assistentes de voz, como o Amazon Echo e o Google Home. Estima-se que, em 2026, [haverá 64 bilhões de dispositivos IoT instalados em todo o mundo](https://www.businessinsider.com/internet-of-things-devices-examples?r=US&IR=T).

Todos esses dispositivos conectados à Internet criam novas oportunidades para as informações serem comprometidas. Não só o volume de dados compartilhados via IoT nunca foi tão grande como a natureza desses dados é com frequência altamente confidencial. Isso destaca a necessidade de conhecer as ameaças à segurança da Internet e de praticar uma boa higiene de segurança virtual.

## Segurança para dispositivos móveis na Internet

Segurança para dispositivos móveis refere-se às técnicas usadas para proteger dados em dispositivos móveis, como smartphones e tablets, e é outro aspecto da proteção na Internet.

### **Como saber se o seu telefone foi grampeado**

O seu smartphone pode estar vulnerável a grampeamento, especialmente se tiver sido desbloqueado por [jailbreak](https://www.kaspersky.com.br/resource-center/definitions/what-is-jailbreaking) ou por raiz. O grampeamento de telefone pode permitir que terceiros ouçam suas chamadas ou leiam suas mensagens. Se estiver preocupado com a possibilidade do seu telefone ter sido hackeado, você pode buscar sinais como ruídos de fundo incomuns em chamadas, a bateria do seu telefone descarregando mais rápido do que o normal ou se comportando de maneira estranha.

Se o seu telefone parecer que está ligando ou desligando sozinho, ou se aparecerem aplicativos que você não se lembra de ter instalado, isso pode indicar que outra pessoa está acessando seu telefone. Receber mensagens SMS estranhas, contendo uma série de letras e números truncados, ou receber uma conta de telefone com o valor mais alto do que o normal também pode indicar grampeamento do telefone.

### **O que é spoofing de telefone e como você pode evitá-lo?**

O [spoofing](https://www.kaspersky.com.br/resource-center/definitions/spoofing) geralmente envolve criminosos virtuais tentando convencer você de que as informações estão vindo de uma fonte confiável. O spoofing de telefone ocorre quando os golpistas falsificam deliberadamente as informações que aparecem no ID do autor da chamada para esconder sua identidade. Eles fazem isso para que as vítimas pensem que uma chamada está vindo de sua área local ou de um número que reconhecem.

Para evitar spoofing de telefone, verifique se a sua operadora de telefonia possui um serviço ou aplicativo que ajuda a identificar e evitar chamadas de spam. Você também pode procurar aplicativos de terceiros, como o RoboKiller ou Nomorobo, para examinar chamadas, mas saiba que esses aplicativos exigem que você compartilhe dados privados com eles.

Normalmente, se você recebe uma chamada de um número desconhecido, a melhor coisa a fazer é não atender. Atender chamadas de golpes é uma má ideia porque os golpistas entendem que você é um alvo em potencial.

### Como remover software espião do seu telefone

Se você estiver vendo sinais de que o seu smartphone contém spyware, verifique os aplicativos instalados no dispositivo. Remova qualquer aplicativo do qual você não esteja seguro a respeito ou não tenha instalado.

Atualizar o sistema operacional do seu telefone pode ajudar, assim como medidas extremas, como redefinir seu telefone para as configurações de fábrica. Embora isso possa ser inconveniente, pode valer a pena fazer isso se você estiver preocupado com o comprometimento da segurança do seu telefone.

## Dicas de segurança na Internet: como se proteger on-line

Então, quais são os melhores métodos de proteção na Internet? Siga estas práticas recomendadas para se proteger contra ameaças à segurança na Internet e diferentes tipos de ataques na Internet:

### **Você precisa de um software de segurança na Internet que proteja você o tempo todo**

O melhor software de segurança na Internet protegerá você de várias ameaças à segurança na Internet, incluindo hackeamento, vírus e malware. Um produto de segurança na Internet abrangente deve conseguir localizar vulnerabilidades do dispositivo, bloquear ameaças virtuais antes que elas atuem e isolar e remover perigos imediatos.

### **Bloqueie o acesso à webcam, de forma que sua privacidade na Internet seja assegurada**

O hackeamento da webcam ocorre quando os hackers acessam a câmera do seu dispositivo móvel e computador e gravam você. Essa ameaça à segurança na Internet é conhecida como "camfecting". A quantidade de ataques gravados é relativamente baixa, embora a maioria ocorra sem que a vítima jamais tenha percebido que foi comprometida, passando despercebidos.

Uma maneira simples de bloquear o acesso à câmera é usando fita adesiva, mas em um mundo em que muitas pessoas usam videoconferência todos os dias para trabalhar ou se comunicar, isso não é algo prático. Um método de prevenção muito melhor é usar uma solução antivírus que ofereça proteção para a webcam.

### **Um bloqueador de anúncios pode proteger você de malvertising**

Os bloqueadores de anúncios limpam os anúncios das páginas da web e, ao bloquear a exibição de anúncios, você remove o risco de ver e clicar em um que possa ser danoso. Os bloqueadores de anúncios também possuem outros benefícios. Por exemplo, eles podem reduzir a quantidade de cookies armazenados na sua máquina, aumentar a privacidade da sua Internet, reduzindo o rastreamento, economizar largura de banda, ajudar as páginas a carregar mais rapidamente e prolongar a vida útil da bateria em dispositivos móveis.

Alguns bloqueadores de anúncios são gratuitos, enquanto outros são pagos. Tenha em mente que nem todos os bloqueadores de anúncios bloqueiam todos os anúncios on-line, e alguns sites podem não abrir adequadamente se o seu bloqueador de anúncios estiver ativado. Você pode, no entanto, habilitar bloqueadores de anúncios para permitir anúncios on-line de sites específicos.

### **Cuide de toda a família com o controle de pais**

Controle de pais refere-se às configurações que permitem que você controle o conteúdo que o seu filho pode ver na Internet. Usado em conjunto com configurações de privacidade, o controle de pais pode ajudar a aumentar a segurança na Internet para crianças. A configuração do controle de pais varia de acordo com a plataforma e o dispositivo.

### **Proteção entre plataformas**

Hoje em dia, a proteção na Internet precisa dar conta de todos os dispositivos que usamos on-line – notebooks, desktops, smartphones e tablets. O melhor software de segurança na Internet permitirá que você instale o programa antivírus em vários dispositivos, oferecendo proteção entre plataformas contra as ameaças à segurança na Internet.

### **Transações bancárias e compras on-line seguras**

As dicas de segurança de compras on-line a serem lembradas incluem:

* Certifique-se de estar fazendo transações com um site seguro – a URL deve começar com https:// em vez de http:// – o "s" significa "seguro" e indica que o site possui um [certificado de segurança](https://www.kaspersky.com.br/resource-center/definitions/what-is-a-ssl-certificate). Deve haver também um ícone de cadeado à esquerda da barra de endereço.
* Verifique a URL com atenção. Os criminosos podem criar sites falsos com URLs semelhantes aos legítimos. Normalmente, eles mudam uma ou duas letras na URL para enganar as pessoas.
* Evite enviar informações financeiras ao usar Wi-Fi público.

**Conclusão**

Para usuários básicos de tecnologia é muito difícil se proteger desses tipos de ataques, ainda mais que não se tem um conhecimento técnico em relação a esse tipo de perigo. Todos nós já tivemos algum tipo de problema relacionado a ataques cibernético, mesmo que tenha sido o menor deles e pelo menos uma vez.

O que podemos fazer é minimizar os danos, e proteger com segurança máxima todos dados importantes que temos, usar softwares licenciados e não piratas, acessar sites de alta confiabilidade, um bom antivírus e seguir a cartilha acima assim teremos um pouco mais de confiança em utilizar a internet com segurança.

**Fonte:**

<https://www.kaspersky.com.br/resource-center/definitions/what-is-internet-security>

<https://edu.gcfglobal.org/pt/seguranca-na-internet/controle-parental-em-celulares-android/1/>

<https://www.eset.com/br/artigos/dicas-de-seguranca-na-internet/>