O que é segurança na internet?

Podemos entender como Segurança na Internet todas os cuidados que devemos ter para proteger as coisas que fazem parte da internet como a infraestrutura, que podem ser nossos [computadores](https://edu.gcfglobal.org/pt/informatica-basica/o-que-sao-os-computadores/1/) e as informações, que são as mais atacadas pelos [cibercriminosos](https://edu.gcfglobal.org/pt/seguranca-na-internet/proteja-seu-computador-de-ameacas-na-internet/1/" \t "_blank).

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.

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

### 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.

### 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.

[Ransomware](https://www.kaspersky.com.br/resource-center/threats/ransomware-examples)

[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 peços 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.

### 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 peços 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.

### 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.

### 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 impedir esses ataques?

* Não clique em mensagens de redes sociais como o Twitter ou Facebook que pareçam suspeitas ou onde tiver muitas pessoas marcadas. Se você for marcado em alguma, pergunte para a pessoa que supostamente fez a marcação, se realmente foi ela quem criou o conteúdo da mensagem.
* Quando você não conhecer o remetente de um e-mail, não abra os anexos que essa pessoa lhe enviar. Confirme primeiro e só depois faça o download de qualquer anexo.
* Não entre em sites suspeitos ou nos que oferecem ganhar coisas clicando em determinados sites.
* Evite baixar músicas, vídeos, filmes ou séries on-line de forma ilegal na internet. A grande maioria desses sites que oferecem download de arquivos, contêm vírus que podem infectar seu computador.
* Não clique em propagandas suspeitas que estão nos sites ou que chegam no seu e-mail.
* Analise as memórias USBs, DVDs ou CDs antes de executá-los em seu computador. Não importa se é de um amigo ou conhecido, talvez ele nem saiba que alguns destes elementos possa estar infectado com vírus.
* O mais importante: mantenha atualizado e ativo os antivírus em todos os dispositivos que você usa para navegar na internet

Links

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

<https://edu.gcfglobal.org/pt/seguranca-na-internet/o-que-e-cyberbullying-e-como-evitalo/1/>