NURAP

NÚCLEO DE APRENDIZAGEM PROFISSIONAL E ASSISTÊNCIA SOCIAL

Diversidade e Inclusão

Cibersegurança - Tipos De Virus Virtuais

Os avanços tecnológicos na sociedade contemporânea trouxeram diversas formas de lidar com as situações do dia-a-dia, como por exemplo, formas de comunicação de fácil acesso com pessoas de qualquer lugar do país ou a praticidade de pagar uma conta e pedir comida de forma prática e rápida.

Entretanto, com tais avanços tecnológicos surgiram também á necessidade de segurança no âmbito da tecnologia. É normal usarmos um celular ou até mesmo um computador, para guardarmos informações e dados pessoais. Ou seja, um verdadeiro “tesouro” para pessoas más intencionadas, e brechas para possíveis vírus.

Quantos dados você fornece às empresas em compras online?

Pense em endereço, senhas, números de cartão de crédito e mais.

Todas são informações sigilosas e que devem ser protegidas com cuidado, longe de pessoas mal-intencionadas na internet.

O mesmo acontece com as informações de negócios das empresas e governos: investimentos, balancetes financeiros e planejamentos devem ser guardados a sete chaves.

É aí que entra a cibersegurança, para garantir que tais dados só estejam acessíveis a quem possui autorização para isso.

Cibersegurança e Tipos de Vírus Virtuais

- O que é Cibersegurança?
- Como funciona?
- O papel da Cibersegurança;
- Importância da Cibersegurança;
- Crimes Virtuais;
- Tipos de Cibersegurança;
- O que é virus?
- Fases de um vírus virtual;
- Tipos de Vírus virtuais;
- Como se proteger?

O que é Cibersegurança?

A cibersegurança é um conjunto de ações e técnicas para proteger sistemas, programas, redes e equipamentos de invasões.
Dessa forma, é possível garantir que dados valiosos não vazem ou sejam violados em ataques cibernéticos.

Esses ataques podem ter a intenção de acessar servidores, roubar senhas, sequestrar dados ou até mesmo fraudar transações financeiras.

Casos como vazamentos ou ataques de dados vem sendo cada vez mais comum. E infelizmente ninguém está livre de ataques cibernéticos. Temos Empresas grandes por exemplo, que muitas vezes já foram alvos de tais ataques

O que é Cibersegurança

A segurança cibernética deve ser trabalhada em vários níveis desde a segurança das redes físicas e dos aplicativos até a educação do usuário final.

Segundo levantamento da empresa de segurança cibernética Fortinet, em 2020 o Brasil sofreu mais de 8,4 bilhões de tentativas e ameaças de ataques cibernéticos.

O que é Cibersegurança

Se antes da pandemia de Covid-19 já vivíamos em um mundo conectado, o salto digital entre 2020 e 2021 acelerou todas as estimativas sobre a produção e troca de dados cibernéticos. O home office e outras práticas de trabalho a distância vieram para ficar, e empresas de todo o planeta já manifestaram intenção de incorporar novos modelos de atendimento e de manter seus colaboradores.

Por outro lado, também cresceram vertiginosamente os crimes e as ameaças virtuais. Os hackers se aproveitam das vulnerabilidades de nossos dispositivos eletrônicos e das redes que utilizamos para realizar ataques que podem gerar prejuízos incalculáveis.

Cibersegurança- Como funciona

Ciberataques

Segundo uma pesquisa da Netscout, publicada no **portal da Agência EFE**, o Brasil ostenta o preocupante posto de **2º país do mundo em que mais ocorrem Ciberataques**.

São mais de 439 mil tentativas de invasões e de ataques de negação de serviço distribuído (DDoS) registrados, o que nos deixa apenas atrás dos Estados Unidos nesse ranking.

Cibersegurança- Como funciona

Como revela uma matéria no portal Valor Investe, mais da metade das empresas brasileiras pretendem investir em cibersegurança.

Para isso, elas precisam elaborar todo um planejamento, que contemple um orçamento específico para a área de TI, de maneira a definir políticas e medidas de segurança de dados.

Cibersegurança- Como funciona

Entre as possíveis ações a serem realizadas, destacam-se:

- Testes de intrusão automáticos com análise de vulnerabilidades;
- Implementação de plataformas de segurança centralizadas para controle, monitorização e neutralização de ameaças na rede, endpoints e distração de eventuais atacantes;
- Proteção para dispositivos Bluetooth e Wi-Fi;
- Blindagem de dados confidenciais.

O Papel da Cibersegurança

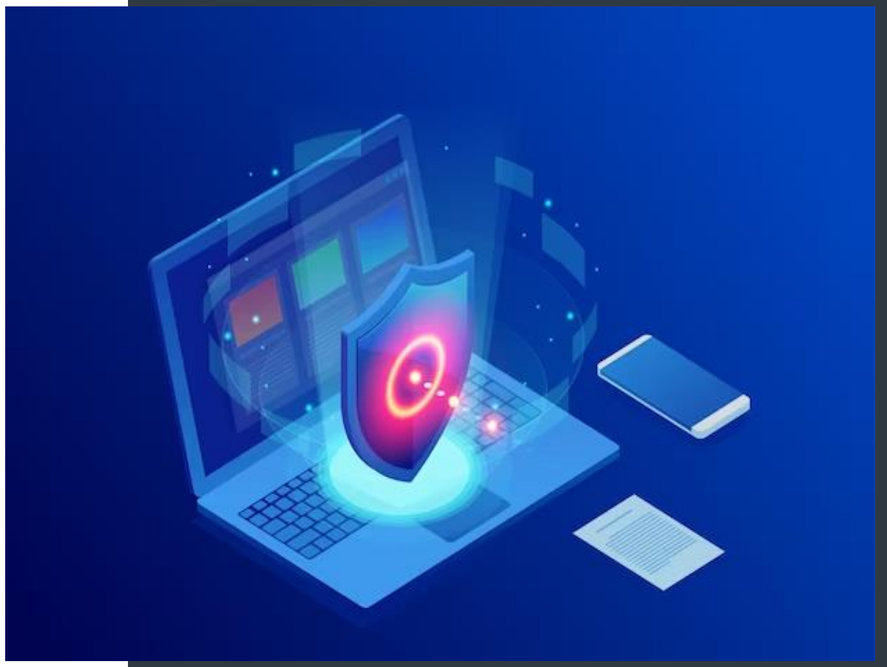
A cibersegurança é voltada para softwares, hardwares e redes. Ou seja, cuida para que o sistema da empresa não permita ataques cibernéticos.

Ela previne problemas com a gestão de informações que é feita pelas máquinas, no trânsito e armazenamento de dados entre elas. Dessa forma, protege a informação digital armazenada ali.

Para isso, algumas das medidas tomadas são: aplicar antivírus nas máquinas, ter cópias de segurança do que está nos servidores, criptografar dados e oferecer uma tecnologia de assinatura digital.

Na era da Indústria 4.0 a cibersegurança é fundamental, já que tudo está conectado e, mais que nunca, é necessário desenvolver práticas e mecanismos capazes de eliminar e/ou reduzir riscos e falhas para se defender de hackers e criminosos virtuais.

E é preciso um conjunto de estratégias para atuar nos vários momentos da cadeia de valor, sendo capaz de prevenir, monitorar e defender as empresas, organizações governamentais e cidadãos contra os ataques à segurança cibernética.

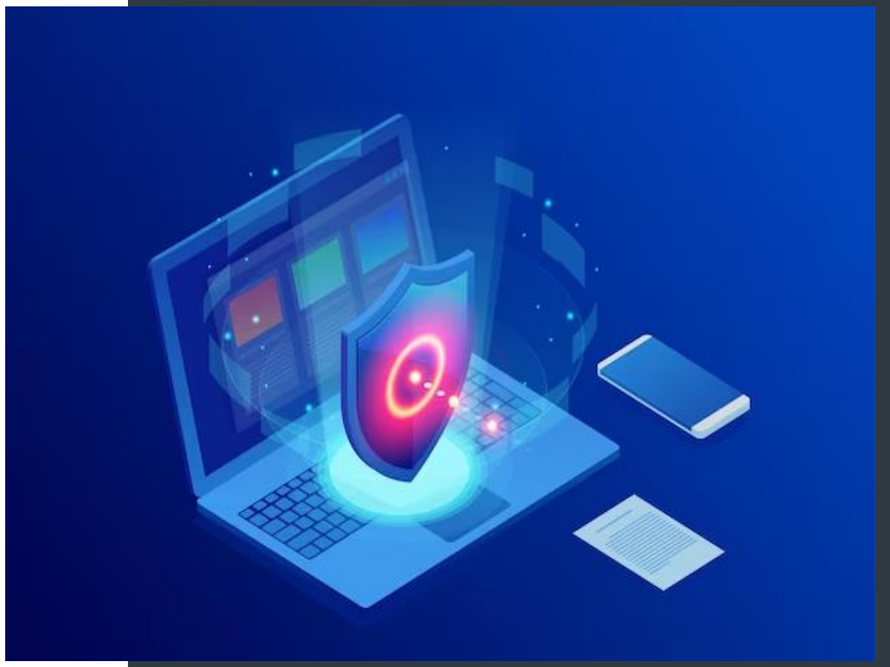


Importância da Cibersegurança

A perda de determinados dados e informações pode comprometer profundamente os processos de trabalho e o funcionamento da empresa.

Nesse cenário, a cibersegurança vem se tornando uma das grandes prioridades no mundo dos negócios. Além disso, à medida que as empresas e a sociedade em geral se tornam mais digitalizadas, cresce também o uso da internet para fins escusos.

É importante ter em mente que as técnicas cibercriminosas têm sido cada vez mais frequentes e vão se aprimorando com o tempo para encontrar brechas nos sistemas e, assim, se tornarem mais danosas.



Importância da Cibersegurança

Os ataques virtuais são realizados por diferentes motivos e mostram que qualquer um está suscetível a esses crimes digitais.

Um hacker pode invadir uma rede com intenções que vão desde o ganho financeiro até o terrorismo de Estado.

Crimes Virtuais

Algumas motivações são:

- Extorquir dinheiro por meio de ameaças de divulgação de dados confidenciais, o chamado sequestro de dados;
- Interromper processos produtivos ou comerciais, paralisando negócios e arranhando a reputação de empresas;
- Alterar ou destruir alguma informação de processos e de bancos de dados;
- Roubar dados do perfil, dos hábitos de consumo ou do histórico de saúde de pessoas;
- Objetivos políticos;
- Protesto;

Crimes Virtuais

Tipos de Cibersegurança

Genericamente, cibersegurança é toda medida pela qual pessoas físicas e empresas se habilitam a proteger seus dispositivos e arquivos da ameaça de hackers mal-intencionados.

Aliás, cabe ressaltar que o termo hacker, em si, não designa um criminoso, tanto que há quem use o termo cracker para se referir a quem pratica delitos virtuais.

Assim como existem diversos tipos de hacker, há também modalidades variadas de cibersegurança.

Tipos de Cibersegurança

Segurança Operacional

Esse tipo de controle é parte das rotinas de segurança operacional, na qual a empresa decide como vai proteger seus dados definindo quem os acessa e como os acessa.

Segurança De Rede

É o conjunto de estratégias, processos e tecnologias desenvolvidos para proteger a rede de uma empresa contra danos e acesso não autorizado.

Ameaças típicas contra dados e infraestrutura de rede incluem hackers, malware e vírus.

Tipos de Cibersegurança

Segurança Da Nuvem

Assim como a segurança de rede, a da nuvem se dedica a antecipar as ameaças que cercam um conjunto de dispositivos que compartilham acesso a plataformas nesse ambiente.

Ela visa a prevenir o vazamento de dados sem autorização, além de blindar a nuvem contra eventuais fragilidades e suscetibilidades.

O que é vírus de computador

O vírus de computador é um programa ou parte de um código malicioso que é capaz de se autorreplicar e se infiltrar em dispositivos sem o conhecimento ou permissão do usuário.

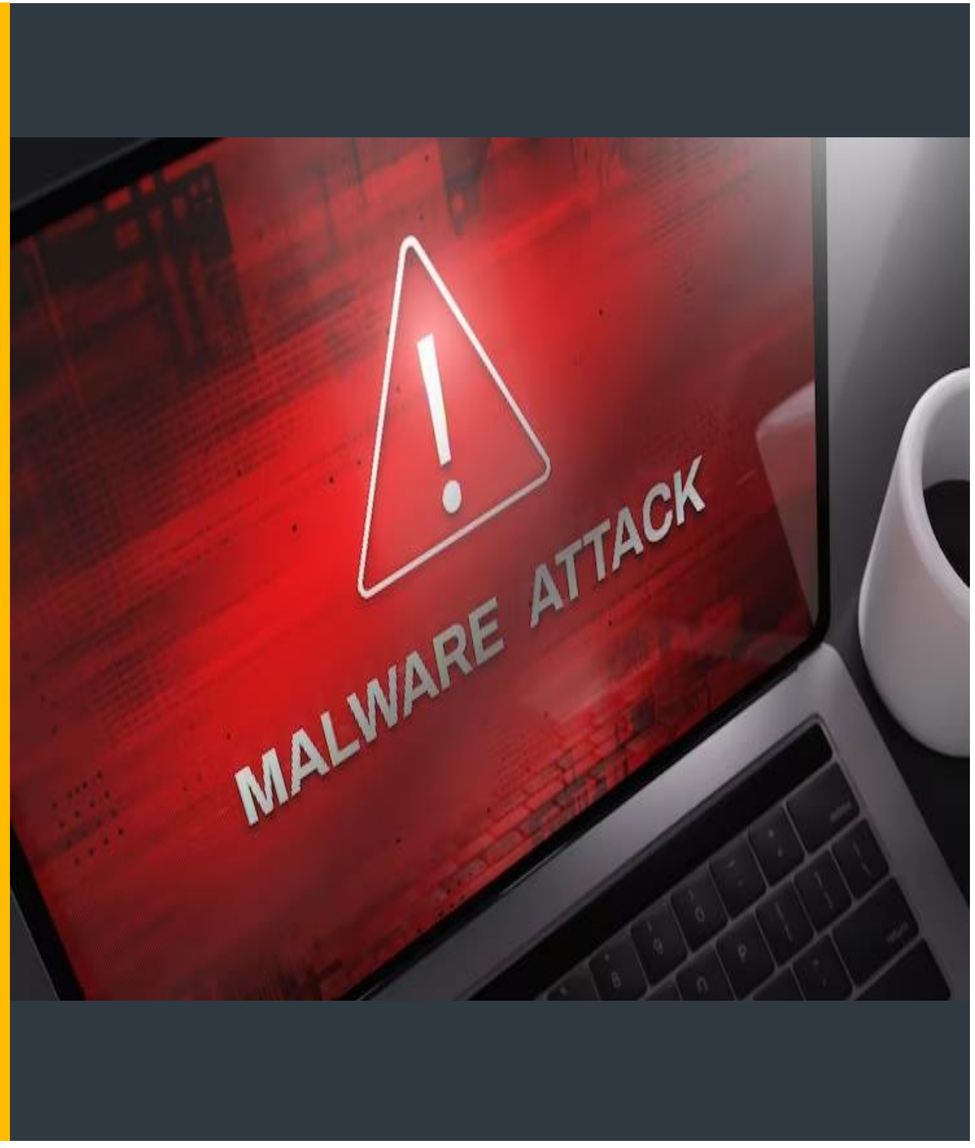
Enquanto alguns vírus são meramente irritantes, a grande maioria é destrutiva e designada a infectar e controlar os dispositivos.

O que é vírus de computador

Eles podem se alastrar por vários computadores e redes ao criar cópias de si mesmos, assim como um vírus biológico que passa de uma pessoa para outra.

Apesar de muitas pessoas utilizarem o termo “vírus” para fazer referência a qualquer tipo de programa perigoso, o vírus é apenas uma categoria de malware, que inclui todos os tipos de códigos criados com o intuito de serem prejudiciais.

Fases de um vírus virtual



Podemos definir os vírus de computador em duas categorias diferentes: aqueles que começam a infectar e se replicar assim que entram na máquina e os que ficam inativos, esperando que o usuário os ative sem querer.

Fases de um vírus virtual

Os vírus de computador possuem 4 fases inspiradas na classificação dos biólogos do ciclo de vida de um vírus real. São elas:

1. Fase dormente: quando o vírus permanece oculto no sistema, aguardando ser ativado sem querer pelo usuário;

2. Fase de propagação: quando o vírus começa a se tornar viral, ou seja, quando ele se replica, escondendo cópias de si mesmo em arquivos, programas e outras partes do disco. Esses clones podem ser levemente alterados na tentativa de evitar detecção e também se autorreplicam e criam mais clones que continuam se copiando e assim por diante;

Fases de um vírus virtual

3) Fase de ativação: quando uma ação específica aciona e ativa o vírus. Pode ser uma ação do usuário, como clicar em um ícone ou abrir um aplicativo. Contudo, outros vírus são programados para ganhar vida após um período de tempo, como após a reinicialização do computador 10 vezes (uma tática utilizada para ofuscar a origem do vírus);

4) Fase de execução: é quando o vírus libera a sua carga, ou seja, o código malicioso que tem como objetivo prejudicar o dispositivo.

Tipos de vírus virtuais

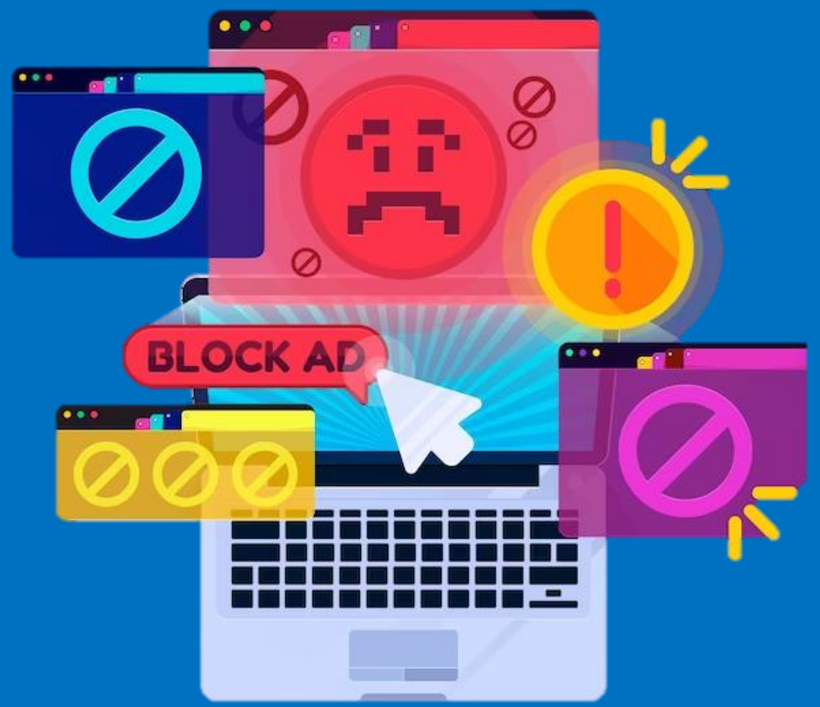
Quando o assunto é vírus de computador, muita gente se lembra do Cavalo de Troia, mas este é apenas um dos tipos de ameaça que pode danificar suas máquinas.

Cavalo de Troia

O Cavalo de Troia (Trojan) é um dos maiores problemas para o computador. Ele não é um vírus propriamente dito, mas abre uma “porta” no computador, deixando todo o sistema vulnerável a outros vírus. O maior problema não é o Cavalo de Troia em si, mas a vulnerabilidade do seu sistema com a presença dele.

Esse tipo de vírus se esconde no seu dispositivo, podendo, entre outros danos, decodificar mensagens e descobrir senhas de bancos e redes sociais. Ele é instalado quando fazemos o download de algum arquivo ou abrimos algum link infectado.

Tipos de vírus virtuais



Ransomware

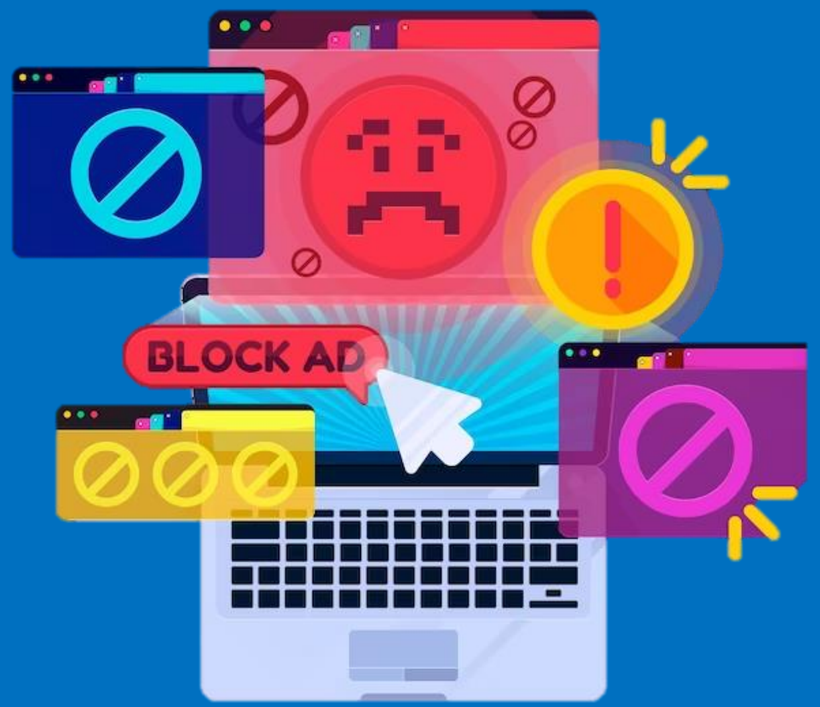
Através dele, são executados ataques que podem causar grandes prejuízos para as empresas, que vão desde a perda de dados críticos até a valores financeiros.

Outro prejuízo causado pelo ransomware é que, enquanto o ataque estiver sendo executado, o estabelecimento não consegue efetuar suas atividades diárias que dependem do sistema de informática.

Os ataques de ransomware são feitos através de um processo complexo de engenharia social que leva à infecção. Hackers enviam mensagens para usuários de um sistema corporativo, simulando um conteúdo real e incentivando o download de um arquivo infectado.

Após a abertura do arquivo, o ransomware começa a fazer uma varredura pela rede da empresa, buscando brechas que permitam acesso aos sistemas internos e à dados privados. Os hackers entram em contato com a empresa e exigem um pagamento (geralmente em bitcoin) de valor variável para liberar o acesso aos dados.

Tipos de vírus virtuais



Autorun

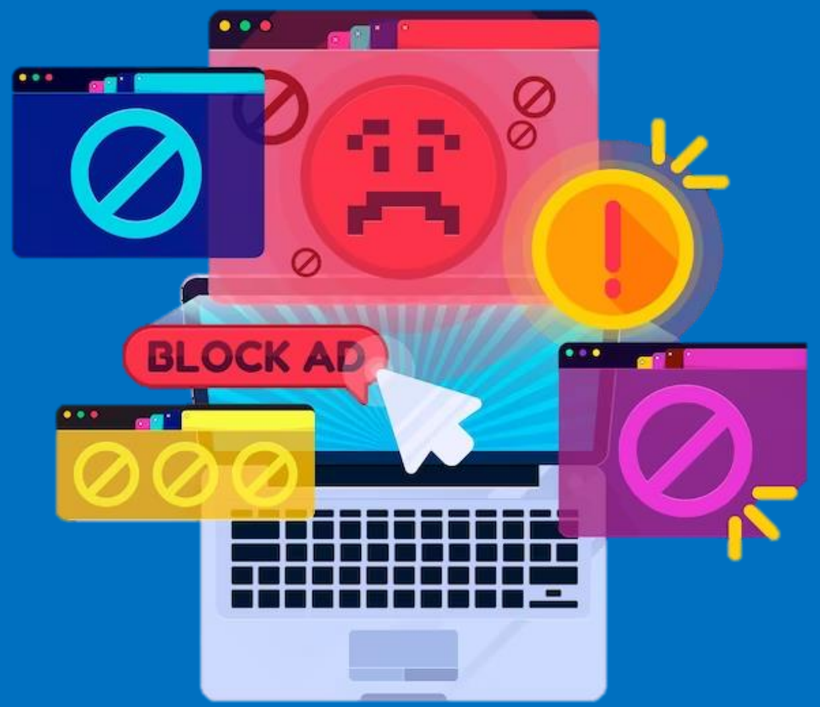
A infecção pelo Autorun acontece, principalmente, pela conexão de pendrives e HD externos ao seu computador.

Esse tipo de vírus utiliza um arquivo de instalação automática aparentemente normal, que se instala no computador e infecta todos os outros programas e arquivos.

Com a Transformação Digital e o armazenamento cada vez maior de informações, os dispositivos estão cada vez mais vulneráveis a esse tipo de vírus.

Para se proteger, além de cuidar do armazenamento de seus dados, ter um cuidado especial ao abrir arquivos desconhecidos também é um caminho. Antes de instalar qualquer arquivo ou programa em seus dispositivos, utilize um antivírus.

Tipos de vírus virtuais



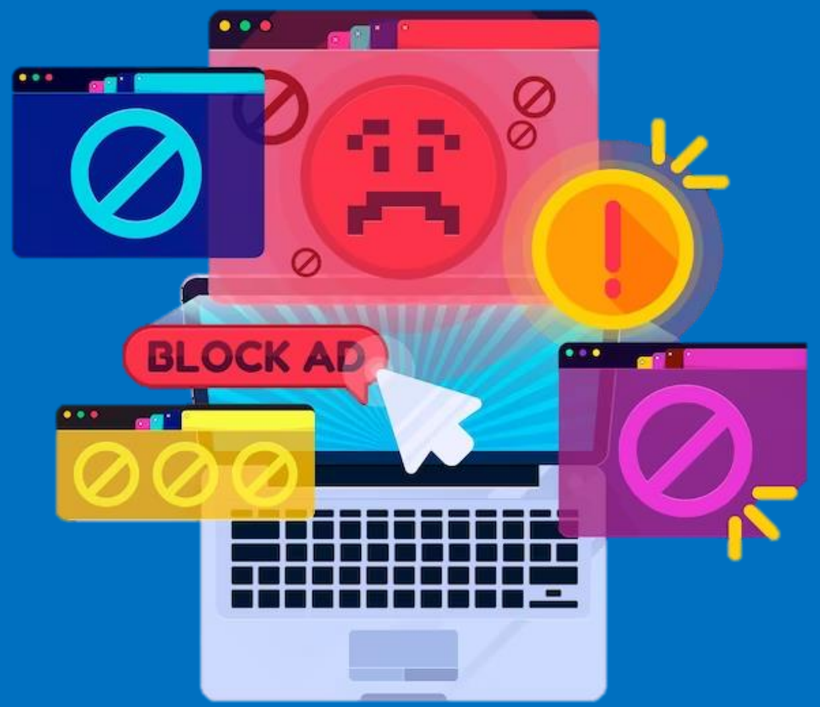
Kilim

O vírus Kilim é um dos que mais têm trazido prejuízos nos últimos tempos. Ele é capaz de realizar ações remotas dentro de redes sociais e outros aplicativos que estão instalados no dispositivo do usuário.

Com cada vez mais pessoas utilizando o Facebook, por exemplo, esse tipo de vírus se tornou ainda mais comum.

Nessa rede social, ele é responsável pelo envio de mensagens e até mesmo por curtidas não executadas pelo usuário. As senhas também podem ser acessadas, o que pode dificultar a recuperação da conta.

Tipos de vírus virtuais



Keylogger

Os Keyloggers são softwares maliciosos que têm como principal objetivo interceptar informações que são digitadas pelo usuário em determinado computador.

Ou seja, todas as informações que são digitadas acabam sendo monitoradas, armazenadas e enviadas para terceiros através deste tipo de vírus.

Além de ter informações confidenciais espionadas, esse tipo de vírus torna vulnerável também informações como senhas, logins e e-mails.

A maneira mais eficiente de bloquear a ação de Keyloggers é mantendo antimalwares e softwares antivírus atualizados.

Tipos de vírus virtuais

Spyware

Os Spywares, por sua vez, são softwares que possuem como principal objetivo capturar informações de usuários sem que eles tenham conhecimento. Sendo distribuído por emails, sites falsos etc.

De maneira geral, esse vírus rastreia os passos de uma pessoa na internet e modifica o conteúdo de páginas para exibição de publicidade que leva ao download de outros tipos de vírus no computador.

Por isso, essa é uma característica que faz com que os Spywares sejam de um nível maior quando comparados aos keyloggers.

Além de capturar informações importantes, como senhas e números de cartão de crédito, os spyware também podem modificar configurações do computador e acionar softwares adicionais.

Tipos de vírus virtuais

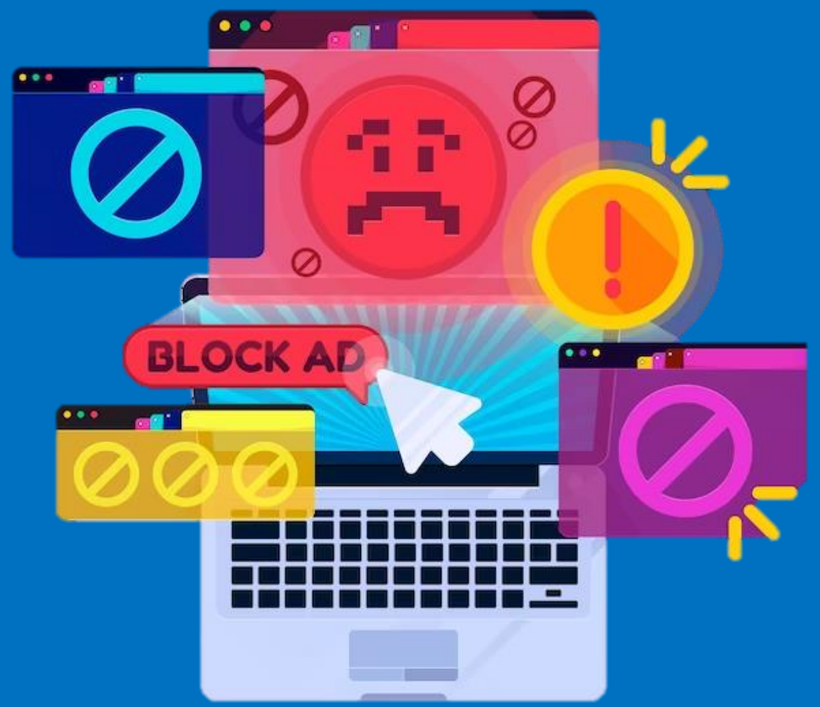
Worms

Os Worms são um dos tipos de vírus mais perigosos. Por ser também um tipo de malware autorreplicador, ele consegue se instalar no computador e se multiplicar sozinho, explorando vulnerabilidades que encontra na rede.

Além de afetar a máquina no qual se infiltrou, esse tipo de malware tem potencial de se espalhar de um computador para outro, podendo causar prejuízo a sistemas em diversos locais.

Sua propagação pode ocorrer por meio da internet, conexões locais, dispositivos USB, arquivos e mensagens. O principal objetivo desse programa malicioso é roubar dados de usuários ou de empresas.

Tipos de vírus virtuais



Adware

Por fim, o adware é um software malicioso facilmente identificado, pois nada mais é do que aqueles anúncios pop-up que aparecem em páginas, ou seja, são publicidades indesejadas.

Existem adwares que tem como objetivo apenas causar incômodo aos usuários, enquanto outros servem para coletar informações e exibir anúncios direcionados.

Como se proteger?

1. Instale um antivírus

O primeiro passo para manter o seu computador protegido contra vírus de computador é instalar um antivírus de qualidade.

Esse programa irá evitar que qualquer arquivo malicioso tente acessar o seu dispositivo e emite notificações sempre que algo suspeito acontecer.

Como se proteger?

3. Atualize sempre o computador

Por fim, uma dica de ouro para se manter protegido contra os vírus de computador é atualizar o seu dispositivo sempre que necessário.

As atualizações oferecidas pelos sistemas operacionais servem não somente para consertar bugs e outros problemas, mas também para atualizar o sistema de forma a deixar certos tipos de vírus obsoletos.

Portanto, sempre que necessário, faça a atualização do sistema do seu computador.

FONTES BIBLIOGRAFICAS

https://www.portaldaindustria.com.br/industria-de-a-z/ciberseguranca/

https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security

https://blog.peduti.com.br/a-importancia-da-ciberseguranca/

https://fia.com.br/blog/ciberseguranca/

https://br.norton.com/blog/malware/what-is-a-computer-virus/

blog.algartelecom.com.br/conheca-os-5-tipos-de-virus-mais-comuns-na-internet-2/