

# SUMÁRIO

LÍNGUA PORTUGUESA.....	9
■ <b>COMPREENSÃO E INTERPRETAÇÃO DE TEXTOS DE GÊNEROS VARIADOS</b> .....	9
■ <b>RECONHECIMENTO DE TIPOS E GÊNEROS TEXTUAIS</b> .....	11
■ <b>DOMÍNIO DA ORTOGRAFIA OFICIAL</b> .....	19
■ <b>DOMÍNIO DOS MECANISMOS DE COESÃO TEXTUAL</b> .....	20
EMPREGO DE ELEMENTOS DE REFERENCIAÇÃO, SUBSTITUIÇÃO E REPETIÇÃO, DE CONECTORES E DE OUTROS ELEMENTOS DE SEQUENCIAÇÃO TEXTUAL .....	20
EMPREGO DE TEMPOS E MODOS VERBAIS .....	24
■ <b>DOMÍNIO DA ESTRUTURA MORFOSSINTÁTICA DO PERÍODO</b> .....	24
EMPREGO DAS CLASSES DE PALAVRAS .....	28
RELAÇÕES DE COORDENAÇÃO ENTRE ORAÇÕES E ENTRE TERMOS DA ORAÇÃO.....	54
RELAÇÕES DE SUBORDINAÇÃO ENTRE ORAÇÕES E ENTRE TERMOS DA ORAÇÃO .....	55
EMPREGO DOS SINAIS DE PONTUAÇÃO.....	58
CONCORDÂNCIA VERBAL E NOMINAL.....	60
REGÊNCIA VERBAL E NOMINAL.....	66
EMPREGO DO SINAL INDICATIVO DE CRASE.....	68
COLOCAÇÃO DOS PRONOMES ÁTONOS .....	69
■ <b>REESCRITA DE FRASES E PARÁGRAFOS DO TEXTO</b> .....	69
SIGNIFICAÇÃO DAS PALAVRAS .....	71
SUBSTITUIÇÃO DE PALAVRAS OU DE TRECHOS DE TEXTO.....	74
Reorganização da Estrutura de Orações e de Períodos do Texto .....	74
■ <b>REESCRITA DE TEXTOS DE DIFERENTES GÊNEROS E NÍVEIS DE FORMALIDADE</b> .....	74
LEGISLAÇÃO.....	83
■ <b>CONSTITUIÇÃO FEDERAL DE 1988</b> .....	83
■ <b>LEI DE DIRETRIZES E BASES DA EDUCAÇÃO – LEI FEDERAL Nº 9.394, DE 1996 E SUAS ALTERAÇÕES</b> .....	84
■ <b>ESTATUTO DA CRIANÇA E DO ADOLESCENTE – LEI FEDERAL Nº 8.069, DE 1990 E SUAS ALTERAÇÕES</b> .....	86

■ LEI BRASILEIRA DE INCLUSÃO LEI FEDERAL Nº13.146, DE 2015 E SUAS ALTERAÇÕES.....	108
■ DIRETRIZES CURRICULARES NACIONAIS PARA O ENSINO FUNDAMENTAL DE 9 ANOS – RESOLUÇÃO CNE-CEB Nº 07, DE 2010.....	121
■ AS DIRETRIZES CURRICULARES NACIONAIS PARA O ENSINO MÉDIO – RESOLUÇÃO CNE/CEB Nº 03, DE 2018.....	124
■ DIRETRIZES OPERACIONAIS PARA A EDUCAÇÃO DE JOVENS E ADULTOS NOS ASPECTOS RELATIVOS AO SEU ALINHAMENTO À POLÍTICA NACIONAL DE ALFABETIZAÇÃO (PNA) E À BASE NACIONAL COMUM CURRICULAR (BNCC) .....	127
■ LEI Nº 13.415, DE 2017 - REFORMA DO ENSINO MÉDIO.....	129
■ LEI Nº 15.533, DE 23 DE JUNHO DE 2015 – PLANO ESTADUAL DE EDUCAÇÃO.....	132
■ LEI 6.123 DE 20 DE JULHO DE 1968 E SUAS ALTERAÇÕES – ESTATUTO SERVIDOR PÚBLICO ESTADUAL .....	133
 NOÇÕES DE DIREITO ADMINISTRATIVO.....	 145
■ ESTADO, GOVERNO E ADMINISTRAÇÃO PÚBLICA.....	145
CONCEITOS.....	145
ELEMENTOS, PODERES E ORGANIZAÇÃO, NATUREZA E FINS .....	145
PRINCÍPIOS.....	147
■ ORGANIZAÇÃO ADMINISTRATIVA DO ESTADO.....	149
ADMINISTRAÇÃO DIRETA E INDIRETA.....	149
■ AGENTES PÚBLICOS .....	156
ESPÉCIES E CLASSIFICAÇÃO.....	156
Servidores.....	156
CARGO, EMPREGO E FUNÇÃO PÚBLICOS .....	157
PODERES E PRERROGATIVAS .....	159
DEVERES .....	163
■ PODERES ADMINISTRATIVOS.....	167
■ ATOS ADMINISTRATIVOS.....	172
CONCEITOS.....	172
REQUISITOS .....	172
ATRIBUTOS .....	173
CLASSIFICAÇÃO.....	174

ESPÉCIES .....	175
INVALIDAÇÃO .....	176
■ CONTROLE E RESPONSABILIZAÇÃO DA ADMINISTRAÇÃO.....	177
CONTROLE ADMINISTRATIVO .....	179
CONTROLE JUDICIAL.....	179
CONTROLE LEGISLATIVO .....	180
RESPONSABILIDADE CIVIL DO ESTADO.....	182
USO DE TECNOLOGIA NA EDUCAÇÃO E INFORMÁTICA BÁSICA .....	187
■ SEGURANÇA DA INFORMAÇÃO .....	187
NOÇÕES DE VÍRUS E PRAGAS VIRTUAIS, PROCEDIMENTOS DE BACKUP) .....	187
■ CONHECIMENTO DA PLATAFORMA GOOGLE (GOOGLE SALA DE AULA, GOOGLE DOCUMENTOS, GOOGLE PLANILHA).....	209
■ SISTEMA OPERACIONAL E AMBIENTE WINDOWS (EDIÇÃO DE TEXTOS, PLANILHAS E APRESENTAÇÕES EM AMBIENTE WINDOWS).....	229
■ CONCEITOS BÁSICOS, FERRAMENTAS, APLICATIVOS E PROCEDIMENTOS DE INTERNET.....	260
■ CONCEITOS DE ORGANIZAÇÃO E DE GERENCIAMENTO DE INFORMAÇÕES, ARQUIVOS, PASTAS E PROGRAMAS.....	273
TEMAS EDUCACIONAIS E PEDAGÓGICOS .....	279
■ PLANEJAMENTO E ORGANIZAÇÃO DO TRABALHO PEDAGÓGICO .....	279
PROCESSO DE PLANEJAMENTO: CONCEPÇÃO, IMPORTÂNCIA, DIMENSÕES E NÍVEIS .....	279
PLANEJAMENTO PARTICIPATIVO: CONCEPÇÃO, CONSTRUÇÃO, ACOMPANHAMENTO E AVALIAÇÃO .....	280
Planejamento Escolar: Planos da Escola, do Ensino e da Aula .....	280
■ CURRÍCULO.....	280
DO PROPOSTO À PRÁTICA.....	280
■ TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO NA EDUCAÇÃO .....	283
■ EDUCAÇÃO PARA A DIVERSIDADE, A CIDADANIA E EDUCAÇÃO EM E PARA OS DIREITOS HUMANOS.....	284
■ EDUCAÇÃO INTEGRAL .....	285
■ EDUCAÇÃO DO CAMPO .....	286

■ EDUCAÇÃO DE JOVENS E ADULTOS.....	288
■ EDUCAÇÃO AMBIENTAL .....	291
■ FUNDAMENTOS LEGAIS DA EDUCAÇÃO ESPECIAL/INCLUSIVA E O PAPEL DO PROFESSOR.....	292
■ EDUCAÇÃO, SOCIEDADE E PRÁTICA ESCOLAR.....	294
■ TENDÊNCIAS PEDAGÓGICAS NA PRÁTICA ESCOLAR .....	296
ASPECTOS PEDAGÓGICOS E SOCIAIS DA PRÁTICA EDUCATIVA, SEGUNDO AS TENDÊNCIAS PEDAGÓGICAS.....	296
■ DIDÁTICA E PRÁTICA HISTÓRICO-CULTURAL .....	298
■ A DIDÁTICA NA FORMAÇÃO DO PROFESSOR .....	300
■ PROCESSO ENSINO-APRENDIZAGEM .....	302
■ RELAÇÃO PROFESSOR/ALUNO.....	303
■ COMPROMISSO SOCIAL E ÉTICO DO PROFESSOR.....	305
■ COMPONENTES DO PROCESSO DE ENSINO .....	306
OBJETIVOS; CONTEÚDOS; MÉTODOS; ESTRATÉGIAS PEDAGÓGICAS E MEIOS.....	306
■ INTERDISCIPLINARIDADE E TRANSDISCIPLINARIDADE DO CONHECIMENTO .....	307
■ AVALIAÇÃO ESCOLAR E SUAS IMPLICAÇÕES PEDAGÓGICAS.....	310
■ O PAPEL POLÍTICO-PEDAGÓGICO E ORGANICIDADE DO ENSINAR, APRENDER E PESQUISAR .....	312
FUNÇÃO HISTÓRICO-CULTURAL DA ESCOLA .....	314
ESCOLA .....	316
Comunidade Escolar e Contextos Institucional e Sociocultural .....	316
■ PROJETO POLÍTICO PEDAGÓGICO DA ESCOLA.....	317
CONCEPÇÃO, PRINCÍPIOS E EIXOS NORTEADORES .....	317
■ POLÍTICAS PÚBLICAS PARA A EDUCAÇÃO BÁSICA .....	319
■ GESTÃO DEMOCRÁTICA .....	333
■ PARTE INTRODUTÓRIA DO CURRÍCULO DE PERNAMBUCO DO ENSINO FUNDAMENTAL E PARTE INTRODUTÓRIA, ENSINO MÉDIO E ITINERÁRIO FORMATIVO DO CURRÍCULO DE PERNAMBUCO DO ENSINO MÉDIO .....	335

# USO DE TECNOLOGIA NA EDUCAÇÃO E INFORMÁTICA BÁSICA

## SEGURANÇA DA INFORMAÇÃO

### NOÇÕES DE VÍRUS E PRAGAS VIRTUAIS, PROCEDIMENTOS DE BACKUP

Sabe-se que ameaças e riscos de segurança estão presentes no mundo virtual. Assim como existem pessoas boas e más no mundo real, existem usuários com boas ou más intenções no mundo virtual.

Os criminosos virtuais são genericamente denominados como *hackers*, porém o termo mais adequado seria *cracker*. Um *hacker* é um usuário que possui muitos conhecimentos sobre tecnologia, podendo ser nomeado como *White Hat* – hacker ético que usa suas habilidades com propósitos éticos e legais –, *Gray Hat* – aquele que comete crimes, mas sem ganho pessoal (geralmente, para exposição de falhas nos sistemas) – e *Black Hat* – aquele que viola a segurança dos sistemas para obtenção de ganhos pessoais.

Amadores ou inexperientes, profissionais ou experientes, todo usuário está sujeito aos riscos inerentes ao uso dos recursos computacionais. São riscos de segurança digital:

- **Ameaças:** vulnerabilidades que existem e podem ser exploradas por usuários;
- **Falhas:** vulnerabilidades existentes nos sistemas, sejam elas propositalmente ou acidentais;
- **Ataques:** ação que procura denegrir ou suspender a operação de sistemas.

Devido à crescente integração entre as redes de comunicação, conexão com novos e inusitados dispositivos (IoT – *Internet* das Coisas) e criminosos com acesso de qualquer lugar do mundo, as redes de informações tornaram-se particularmente difíceis de se proteger. Profissionais altamente qualificados são formados e contratados pelas empresas com a única função de proteger os sistemas informatizados.

Em concursos públicos, as ameaças e os ataques são os itens mais questionados.

### Dica

Você conhece a Cartilha de Segurança CERT? Disponível gratuitamente na *Internet*, ela é a fonte oficial de informações sobre ameaças, ataques, defesas e segurança digital. Ela pode ser acessada pelo link: <<https://cartilha.cert.br/>>. (Acesso em: 13 nov. 2020).

### Ameaças

As ameaças são identificadas como aquelas que possuem potencial para comprometer a oferta ou existência dos ativos computacionais, tais como:

informações, processos e sistemas. Um *ransomware* – *software* que sequestra dados, utilizando-se de criptografia e solicita o pagamento de resgate para a liberação das informações sequestradas – é um exemplo de ameaça.

É importante entender que, apesar de a ameaça existir, se não ocorrer uma ação deliberada para sua execução ou se medidas de proteção forem implementadas, ela é eliminada e não se torna um ataque. As ameaças à segurança da informação podem ser classificadas como:

- **Tecnológicas:** quando ocorre mudança no padrão ou tecnologia, sem a devida atualização ou *upgrade*;
- **Humanas:** intencionais ou acidentais, que exploram vulnerabilidades nos sistemas;
- **Naturais:** não intencionais, relacionadas ao ambiente, como as catástrofes naturais.

As empresas precisam fazer uma avaliação das ameaças que possam causar danos ao ambiente computacional dela mesma (Gerenciamento de Risco), implementar sistemas de autenticação (Controlar o Acesso), definir os requisitos de senha forte (Política de Segurança), manter um inventário e realizar o rastreamento de todos os ativos (Gerenciamento de Recursos), além de utilizar sistemas de *backup* e restauração de dados (Gerenciamento de Continuidade de Negócios).

### Falhas

As falhas de segurança nos sistemas de informação poderão ser propositalmente ou involuntárias. Se o programador insere, no código do sistema, uma falha que produza danos ou permita o acesso sem autenticação, temos um exemplo de falha proposital. Já se uma falha for descoberta após a implantação do sistema, sem que tenha sido uma falha proposital, mas sim explorada por invasores, tem-se um exemplo de falha involuntária, inerente ao sistema.

Quando identificadas, as falhas são corrigidas pelas empresas que desenvolveram o sistema por meio da distribuição de notificações e correções de segurança. O Windows Update, serviço da Microsoft para atualização do Windows, distribui, mensalmente, os *patches* (pacotes) de correções de falhas de segurança.

### Ataques

Sem dúvidas, o assunto de maior destaque, tanto em concursos como no mundo real, são os ataques. Coordenados ou isolados, os ataques procuram romper as barreiras de segurança definidas na Política de Segurança, com o objetivo de anular o sistema ou capturar dados.

Os ataques podem ser classificados como:

- **Baixa complexidade:** exploram falhas de segurança de forma isolada e são facilmente identificados e anulados;
- **Média complexidade:** combinam duas ou mais ferramentas e técnicas, para obter acesso aos dados, sendo de média complexidade para a solução, gerando impactos na operação dos sistemas, como a indisponibilidade;
- **Alta complexidade:** refinados e avançados, os ataques combinam o acesso às falhas do sistema, novos códigos maliciosos desconhecidos e a distribuição do ataque com redes zumbis, tornando difícil a resolução do problema.

## Dica

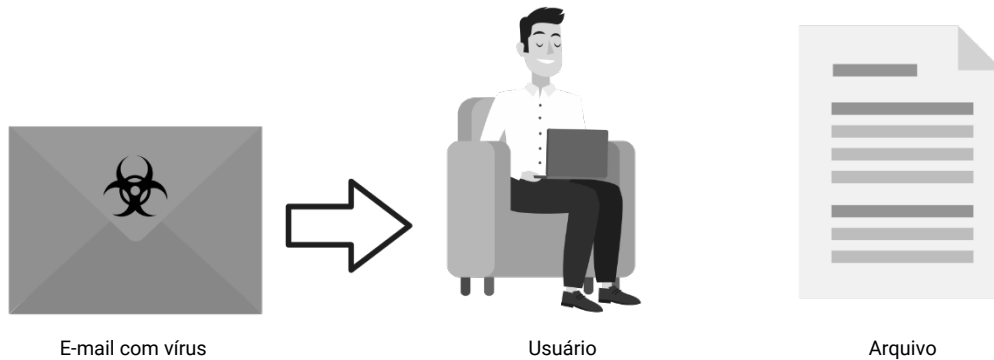
- Ameaças existem e podem afetar ou não os sistemas computacionais;
- Falhas existem e podem ser exploradas ou não pelos invasores;
- Ataques são realizados todo o tempo contra todos os tipos de sistemas.

## Vírus de Computador

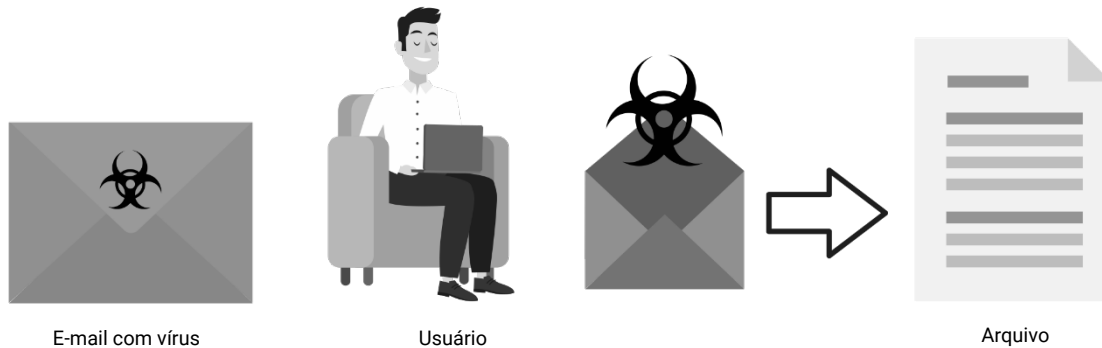
O vírus de computador é a ameaça digital mais popular. Tem esse nome por se assemelhar a um vírus orgânico ou biológico. O vírus biológico é um organismo que possui um código viral que infecta uma célula de outro organismo. Quando a célula infectada é acionada, o código viral é duplicado e se propaga para outras células saudáveis do corpo. Quanto mais vírus existirem no organismo, menor será o seu desempenho, fazendo com que recursos vitais sejam consumidos, podendo levar o hospedeiro à morte.

O vírus de computador é um código malicioso que infecta arquivos em um dispositivo. Quando o arquivo é executado, o código do vírus é duplicado, propagando-se para outros arquivos do computador. Quanto mais vírus existirem no dispositivo, menor será o seu desempenho, fazendo com que recursos computacionais sejam consumidos, podendo levar o hospedeiro a uma falha catastrófica.

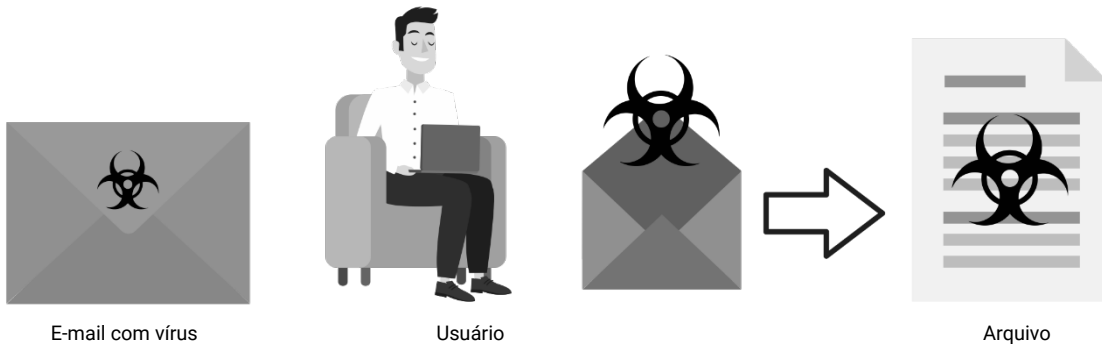
1. E-mail com vírus de computador é enviado para o usuário



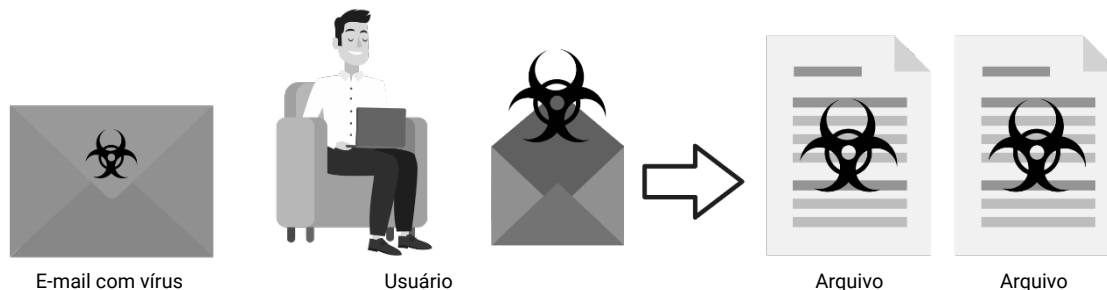
2. E-mail é aberto e o arquivo anexo infectado é executado.



3. O código do vírus é copiado para arquivos do computador



4. Ao executar o arquivo infectado, novos arquivos serão infectados



O vírus de computador poderá entrar no dispositivo do usuário por meio de um arquivo anexado em uma mensagem de *e-mail*, ou por cópia de arquivos existentes em uma mídia removível, como o *pen drive*, recebidos por alguma rede social, baixados de *sites* na *Internet*, entre outras formas de contaminação.

VÍRUS DE COMPUTADOR	CARACTERÍSTICAS
<b>Vírus de boot</b>	<ul style="list-style-type: none"> <li>● Infectam o setor de <i>boot</i> do disco de inicialização</li> <li>● Cada vez que o sistema é iniciado, o vírus é executado</li> </ul>
<b>Vírus de script</b>	Armazenados em <i>sites</i> na <i>Internet</i> , são carregados e executados quando o usuário acessa a página, usando um navegador de <i>Internet</i>
<b>Vírus de macro</b>	<ul style="list-style-type: none"> <li>● As macros são desenvolvidas em linguagem <i>Visual Basic for Applications</i> (VBA) nos arquivos do Office, para a automatização de tarefas</li> <li>● Quando desenvolvido com propósitos maliciosos, é um vírus de macro</li> </ul>
<b>Vírus do tipo mutante</b>	O vírus "mutante" ou "polimórfico", a cada nova multiplicação, o novo vírus mantém traços do original, mas é diferente dele
<b>Vírus time bomb</b>	São programados para agir em uma determinada data, causando algum tipo de dano no dia previamente agendado
<b>Vírus stealth</b>	<ul style="list-style-type: none"> <li>● Um vírus <i>stealth</i> é um código malicioso muito complexo, que se esconde depois de infectar um computador</li> <li>● Ele mantém cópias dos arquivos que foram infectados para si e, quando um <i>software</i> antivírus realiza a detecção, apresenta o arquivo original, enganando o mecanismo de proteção</li> </ul>
<b>Vírus Nimda</b>	<ul style="list-style-type: none"> <li>● O vírus <i>Nimda</i> explora as falhas de segurança do sistema operacional</li> <li>● Ele se propaga pelo correio eletrônico e, também, pela <i>web</i>, em diretórios compartilhados, pelas falhas de servidor Microsoft IIS e nas trocas de arquivos</li> </ul>

Todos os sistemas operacionais são vulneráveis aos vírus de computador. Quando um vírus de computador é desenvolvido por um *hacker*, este procura elaborá-lo para um *software* que tenha uma grande quantidade de usuários iniciantes, o que aumenta as suas chances de sucesso.

O Windows, por exemplo, possui muitos usuários e a maioria deles não tem preocupações com segurança. Por isso, grande parte dos vírus de computadores são desenvolvidos para atacarem sistemas Windows.

O Linux, por sua vez, tem poucos usuários, se comparado ao Windows, e a maioria deles possui muito conhecimento sobre Informática, tornando a ação de vírus nesse sistema uma ocorrência rara.

Já o Android, *software* operacional dos *smartphones* populares, é uma variação do sistema Linux original. Apesar de possuir essa origem nobre, é alvo de milhares de vírus, por causa dos seus usuários, que, na maioria das vezes, não têm rotinas de proteção e segurança de seus aparelhos.

Um vírus de computador poderá ser recebido por *e-mail*, transferido de *sites* na *Internet*, compartilhado em arquivos, através do uso de mídias removíveis infectadas, nas redes sociais e por mensagens instantâneas. Vale lembrar, no entanto, que um vírus necessita ser executado para que entre em ação, pois ele tem um hospedeiro definido e um alvo estabelecido. Ele se propaga, inserindo cópias de si em outros arquivos, alterando ou removendo arquivos do dispositivo para propagação e autoproteção, a fim de não ser detectado pelo antivírus.

### Worms

O *worm* é um verme que explora de forma independente as vulnerabilidades nas redes de dispositivos. Geralmente, eles deixam a comunicação na rede lenta, por ocuparem a conexão de dados ao enviarem cópias de seu código malicioso.

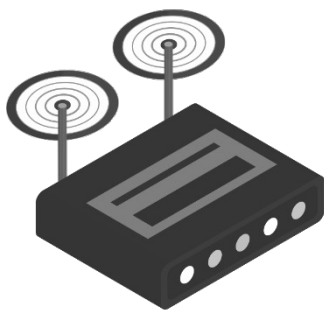
Um verme biológico parasita um organismo, consumindo seus recursos e deixando o corpo debilitado. Um verme tecnológico parasita um dispositivo, consumindo seus recursos de memória e conexão de rede, deixando o aparelho e a rede de dados lentos.

Os worms não precisam ser executados pelo usuário como os vírus de computador e a sua propagação será rápida caso não existam barreiras de proteção que os impeçam.

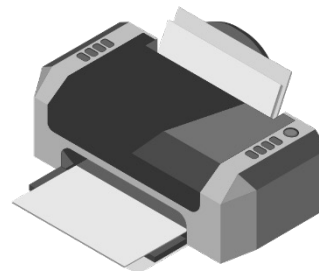
1. Dispositivo infectado se conecta na rede do usuário



Smartphone com worm



Roteador do Usuário



Impressora

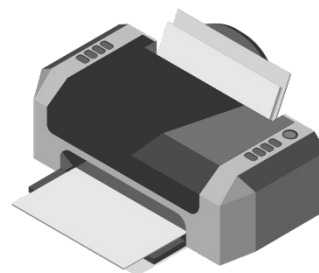
2. Roteador infectado envia o worm para a impressora



Smartphone com worm



Roteador do Usuário

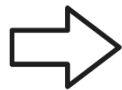


Impressora

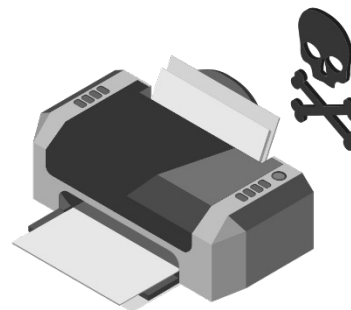
3. Impressora infectada demora muito para imprimir



Smartphone com worm



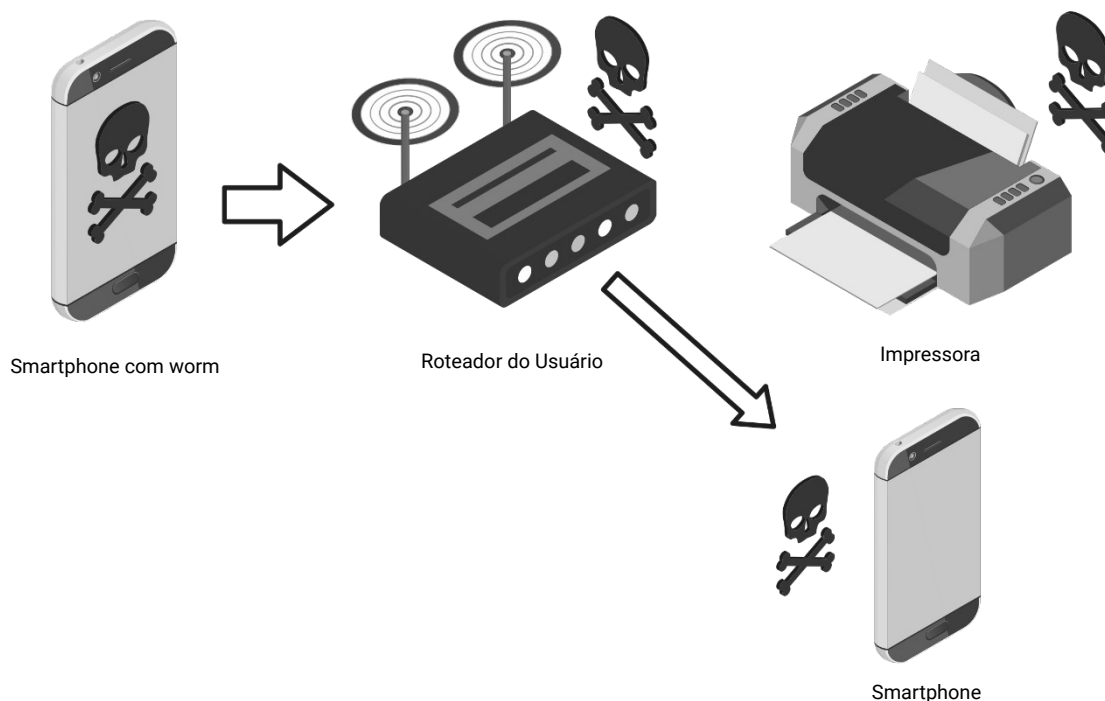
Roteador do Usuário



Impressora



#### 4. Um novo dispositivo se conecta e é infectado



### Dica

Os *worms* infectam dispositivos e propagam-se para outros dispositivos de forma autônoma, sem interferência do usuário.

Os *worms* podem ser recebidos automaticamente pela rede, inseridos por um invasor ou por ação de outro código malicioso. Assim como os vírus, ele poderá ser recebido por *e-mail*, transferido de *sites* na *Internet*, compartilhado em arquivos, por meio do uso de mídias removíveis infectadas, nas redes sociais e por mensagens instantâneas.

Com o objetivo de explorar as vulnerabilidades dos dispositivos, os *worms* enviam cópias de si mesmos para outros dispositivos e usuários conectados. Por serem autoexecutáveis, costumam consumir grande quantidade de recursos computacionais, promovendo a instalação de outros códigos maliciosos e iniciando ataques na *Internet* em busca de outras redes remotas.

### Pragas Virtuais

As diversas pragas virtuais são, genericamente, chamadas de *malwares* (*softwares* maliciosos), por apresentarem características semelhantes: oferecem alguma vantagem para o usuário, mas realizam ações danosas que acabarão prejudicando-o.

#### ● Cavalo de Troia ou *Trojan*

É um código malicioso que realiza operações mal-intencionadas enquanto realiza uma operação desejada pelo usuário, como um jogo *on-line* ou reprodução de um vídeo. Ele é enviado com o conteúdo desejado e, ao ser executado, desativa as proteções do dispositivo, para que o invasor tenha acesso aos arquivos e dados.

Esse nome está, justamente, relacionado com a história do presente dado pelos gregos aos troianos, consistindo em um cavalo de madeira, com soldados em seu interior. Após entrar nas fortificações de Troia, os gregos desativaram as defesas e permitiram o acesso do seu exército.

### Importante!

O *Trojan* ou Cavalo de Troia é apresentado, no enunciado de algumas questões de concursos, como um tipo de vírus de computador.