



MATERIAL DO PROFESSOR

Segurança cibernética: práticas para
proteção digital - Parte 1





1

Introdução

O Material do Professor é um instrumento que oferece o suporte e o embasamento necessários para a condução dos estudantes nesta jornada de aprendizagem.



Aqui, você encontrará orientações pedagógicas para o trabalho com cada unidade, bem como os objetivos de aprendizagem, os conteúdos e habilidades, as estratégias didáticas utilizadas na construção da unidade e, por fim, materiais aula a aula que servirão de apoio ao seu planejamento e durante o processo avaliativo dos estudantes. Utilize o Material do Professor como guia durante o planejamento das aulas, adaptando as estratégias de acordo com as necessidades e interesses dos seus estudantes.

Este material é digital e pode sofrer atualizações periódicas. Certifique-se de verificar regularmente a plataforma para baixar as versões mais recentes e garantir que você tenha acesso às informações mais atualizadas e relevantes para suas aulas.

2

Conteúdo programático

Olá, professor(a)!

Nesta unidade, os estudantes aprenderão sobre os principais riscos e ameaças do ambiente digital — como malwares, phishing, engenharia social e desinformação — de forma prática e conectada ao seu cotidiano online. Eles serão convidados a refletir sobre os rastros digitais que deixam na internet, além de compreender como proteger suas informações e também a manter um comportamento empático e responsável no ambiente virtual.

Temática da unidade: Linguagem de blocos

Ferramentas utilizadas: plataforma de compartilhamento de arquivos

Formato de entrega do projeto: StartLab

Quantidade de aulas: 4

Objetivos de aprendizagem:

1. Identificar diferentes tipos de ameaças digitais (malwares, phishing, engenharia social, desinformação) e seus impactos.
2. Explicar, com suas próprias palavras, como os dados pessoais são usados na internet e por que isso pode representar um risco.
3. Avaliar situações reais ou fictícias de ameaças digitais e apontar estratégias de prevenção adequadas.

Habilidades:

- (EF07CO07) Identificar problemas de segurança cibernética e experimentar formas de proteção.
- (EF07CO08) Demonstrar empatia sobre opiniões divergentes na web.

2

Conteúdo programático

AULA	CONTEÚDO	OBJETIVO DE APRENDIZAGEM
1	<ul style="list-style-type: none">• Diferença entre dados e informações digitais.• Como interações online geram perfis pessoais.• Introdução ao conceito de segurança digital e rastros deixados na internet.	<ul style="list-style-type: none">• Compreender a diferença entre dados e informações no contexto digital.• Identificar práticas inseguras no uso da internet que podem comprometer dados pessoais.• Refletir sobre os próprios rastros digitais e como eles podem ser utilizados por terceiros.
2	<ul style="list-style-type: none">• Tipos de ameaças digitais: malware e phishing.• Estratégias utilizadas por golpistas para obter dados pessoais.• Dicas práticas de prevenção e segurança na internet.	<ul style="list-style-type: none">• Analisar como dados pessoais podem ser usados em golpes digitais.• Relacionar ameaças cibernéticas a comportamentos inseguros online.• Identificar formas seguras de agir frente a mensagens e links suspeitos.
3	<ul style="list-style-type: none">• Ameaças digitais: engenharia social e desinformação (fake news).• Desinformação (fake news) e manipulação de conteúdo (imagens, áudios).• Riscos do compartilhamento de dados e imagens na internet.	<ul style="list-style-type: none">• Analisar como a engenharia social e a desinformação ameaçam a segurança digital.• Reconhecer riscos associados à exposição de dados pessoais na internet.• Propor estratégias de proteção contra golpes que utilizam dados e imagens pessoais.

AULA**CONTEÚDO****OBJETIVO DE APRENDIZAGEM****4**

- Ações individuais e sua relação com a segurança digital.
- Empatia, respeito e convivência saudável na internet.
- Riscos da disseminação de conteúdos ofensivos ou falsos.

- Refletir sobre atitudes pessoais que impactam a segurança e o respeito no ambiente digital.
- Reconhecer a importância da empatia e do respeito nas interações online.
- Avaliar os riscos de compartilhamentos impulsivos e conteúdos prejudiciais.

3

Orientações pedagógicas

Pensando em prepará-lo(a) para a condução das aulas, construímos uma formação, em vídeo, sobre esta unidade com o objetivo de fornecer mais insumos para sua prática docente. Você pode acessá-la na plataforma Start clicando aqui. A seguir, temos um resumo, em texto, das orientações didáticas que você encontrará nas videoaulas da formação.

Inicie a unidade convidando os estudantes a refletirem sobre o que são dados e informações no cotidiano digital. Apresente exemplos concretos, como cliques, buscas e localização, e conduza a turma a perceber como esses registros brutos podem ser transformados em interpretações sobre hábitos e preferências. Utilize situações próximas da realidade dos alunos, incentive a troca de ideias e valorize opiniões diferentes, criando um ambiente seguro para o diálogo.

Avance para a etapa de identificação das ameaças digitais, explorando diferentes tipos de ataques de forma contextualizada. Apresente casos práticos de vírus, phishing e outros golpes comuns, analisando como dados pessoais podem ser usados de maneira indevida. Proponha atividades de leitura e interpretação de mensagens suspeitas, destacando sinais de alerta e estratégias utilizadas por golpistas. Incentive que os estudantes discutam riscos, expressem empatia diante de opiniões divergentes na web e construam entendimentos coletivos sobre segurança online.

Na sequência, conduza os alunos à etapa de compreensão das formas de proteção, utilizando analogias simples, como a ideia da casa como um espaço seguro. Relacione medidas físicas de proteção (portas, fechaduras e câmeras) com práticas digitais, como manter dispositivos atualizados, usar antivírus, evitar downloads suspeitos e acessar apenas sites confiáveis. Estimule a turma a listar e justificar ações de proteção digital, sempre conectando teoria e prática, para que percebam como pequenas atitudes impactam a segurança no dia a dia.

Finalize a unidade sintetizando o que aprenderam sobre segurança cibernética. Planeje momentos de debates, revisão e questionamento com os estudantes, apoiando o uso consciente de ferramentas da web. Incentive que registrem suas ideias e reflexões de forma clara, reforçando a responsabilidade ética no uso das tecnologias e a empatia a se comunicar. Ao concluir, promova uma roda de conversa sobre os temas abordados, valorize os aprendizados construídos e retome os principais conceitos trabalhados ao longo da unidade.

4

Materiais de apoio

Para auxiliar na condução das aulas desta unidade, disponibilizamos materiais de apoio aula a aula para professores e estudantes. Esses materiais podem ser acessados na plataforma Start, no campo “Material de apoio” de cada aula.

4.1 Professores

O **guião do professor** possui o passo a passo descritivo da aula, bem como os comandos necessários para a construção do projeto. Ele pode ser utilizado para o planejamento e preparação da aula, contando com direcionamentos pedagógicos, dicas para condução das aulas, explicação de conceitos de programação e soluções para possíveis dificuldades que os estudantes possam ter. Ao final de cada guia, há uma explicação para o desafio da aula, contando com a expectativa de resolução por parte dos estudantes.

O **gabarito do professor** possui a resolução comentada dos exercícios que os estudantes devem realizar em cada aula. Essas atividades funcionam como um complemento à prática de programação pela construção de projetos, fornecendo uma devolutiva rápida ao professor sobre a proficiência dos estudantes.

4.2 Estudantes

Os **slides dos estudantes** contêm um passo a passo descritivo, aula a aula, dos comandos que os estudantes deverão realizar para a construção do projeto da unidade. Por se tratar de um direcionamento da aula, ele pode ser disponibilizado individualmente ou projetado para a turma. Ao final de cada slide, há um desafio para aprofundar os conteúdos que foram trabalhados naquela aula, sendo uma ferramenta importante para a prática da programação e para fornecer uma atividade extra para aqueles estudantes que finalizarem mais rapidamente a construção dos códigos.

As **listas de exercícios dos estudantes** são um conjunto de atividades de fixação dos conteúdos que foram trabalhados em aula. É esperado que, a cada aula, os estudantes realizem os exercícios e tirem eventuais dúvidas sobre eles com o professor.

4

Materiais de apoio

4.3 Rubrica de avaliação

Por fim, a rubrica é uma valiosa ferramenta para auxiliar na correção dos projetos que são submetidos pelos estudantes. Elas possuem quatro características a serem avaliadas de acordo com cada projeto da unidade e, para cada característica, há a descrição de quatro níveis de proficiência em que o estudante pode se encaixar. Dessa forma, ao avaliar um projeto, o professor consegue analisar o que é esperado em cada nível, fazendo com que sua correção seja baseada em critérios claros e que o feedback de desenvolvimento para o estudante seja melhor direcionado. Essas rubricas também podem ser acessadas no painel de gestão.

Acesse aqui a rubrica do projeto:

[**Projeto – Segurança digital e convivência responsável na internet**](#)



Minhas anotações

Utilize o seu editor de PDF para realizar anotações neste espaço.



start

by alura

**Contato:**

Suporte

@startbyalura

www.startalura.com.br