

CONSCIOUS YOUTH BEHAVIOURS.
IN EMERGING REALITIES

Práticas de educação não-formal:

Doxing

R2 CYBER TOOLKIT



Co-funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

#15	Táticas Anti-Doxing: Manter a Vida Privada em Privado
Ameaça(s)	Doxing
	O doxing, no âmbito das ciberameaças aos jovens, consiste na prática maliciosa de recolher e publicar informações privadas ou identificáveis de alguém, sem o seu consentimento, tipicamente através da Internet. Este ato visa, frequentemente, intimidar, ameaçar, assediar, humilhar ou exercer poder sobre a vítima. O doxing pode acarretar repercussões graves para os jovens, designadamente sofrimento psicológico, perda de privacidade e, em certos casos, danos à integridade física. Esta prática aproveita a acessibilidade das informações pessoais na era digital, violando o direito dos indivíduos à privacidade e segurança online.
Tipologia	Exercícios de simulação
Duração	110 minutos/1 hora e 50 Minutos (pode ser adaptado em função da intensidade das atividades)
Modalidade	Presencialmente [contexto de sala de aula]
Finalidade	O objetivo desta prática é dotar os participantes dos conhecimentos e competências necessários para salvaguardar a sua privacidade online, compreender o comportamento ético online e responder, de forma eficaz, ao doxing e outras ciberameaças associadas.
Objetivos de Aprendizagem	<p>Estratégias de Proteção da Privacidade: Aptidão para empregar estratégias de proteção da sua própria privacidade e informações sensíveis online, minimizando o risco de se tornar uma vítima de doxing.</p> <p>Conduta Ética Online: Demonstrar compreensão do comportamento ético nos espaços online, comprometendo-se a respeitar a privacidade e dignidade dos demais.</p> <p>Análise Crítica ao Cyberbullying: Desenvolver competências para responder adequadamente ao cyberbullying e ao assédio, o que engloba as ações a tomar caso os próprios ou conhecidos sejam vítimas de doxing.</p> <p>Mitigação do Risco de Roubo de Identidade: Aplicar noções sobre como salvaguardar informações pessoais e financeiras, de modo a evitar o roubo de identidade e fraude.</p> <p>Literacia Jurídica Referente ao Doxing: Compreender os direitos e potenciais ações legais que podem ser tomadas contra os autores de doxing, bem como as implicações legais do envolvimento em doxing.</p>
Perfil do formando	<p>Faixa Etária: 15-17 anos</p> <p>Formação Escolar: Estudantes do ensino secundário</p> <p>Pré-requisitos: Conhecimento básico da navegação na Internet e nas plataformas de redes sociais</p>
nº de participantes	20-25

Materiais	<p>Dispositivos com acesso à Internet (computadores portáteis/tablets)</p> <p>Projetor e ecrã para apresentações</p> <p>Quadro branco e marcadores</p> <p>Folhetos impressos sobre estratégias de proteção da privacidade e direitos legais</p> <p>Cartões com cenários para exercícios de simulação</p> <p>Cadernos e canetas para os participantes</p>
Preparação	<p>Preparar o Local: Dispor os assentos da sala de aula de forma a facilitar as discussões em grupo e a visualização do ecrã do projetor.</p> <p>Preparar os Materiais: Preparar os computadores/tablets com o software necessário e acesso à Internet. Imprimir e organizar os folhetos e os cartões de cenário.</p>
Implementação	<p><i>Introdução (10 minutos):</i></p> <p>Acolher os participantes e apresentar o tema do doxing.</p> <p>Esclarecer a finalidade da sessão e os objetivos de aprendizagem.</p> <p><i>Visão Geral do Doxing (10 minutos):</i></p> <p>Apresentar um breve enquadramento do doxing, incluindo exemplos reais e potenciais impactos.</p> <p>Discutir a razão pela qual constitui uma ameaça significativa, em particular para os jovens.</p> <p><i>Estratégias de Proteção da Privacidade (15 minutos):</i></p> <p>Distribuir folhetos e expor diversas estratégias para a proteção das informações pessoais online (opcional).</p> <p>Envolver os participantes num debate à volta da importância das definições de privacidade em plataformas de redes sociais.</p> <p><i>Exercício de Simulação: Identificar Vulnerabilidades (20 minutos):</i></p> <p>Dividir os participantes em pequenos grupos.</p> <p>Fornecer a cada grupo um cenário fictício (ver anexo), no qual devem identificar potenciais vulnerabilidades em matéria de privacidade e propor medidas de proteção.</p> <p>Os grupos apresentam as suas observações e sugestões.</p>

	<p><i>Conduta Ética Online (10 minutos):</i></p> <p>Debater os comportamentos éticos online e a importância de respeitar a privacidade de terceiros.</p> <p>Salientar as consequências de comportamentos pouco éticos como o doxing.</p> <p><i>Resposta Crítica ao Cyberbullying (15 minutos):</i></p> <p>Apresentar de forma sucinta estratégias para dar resposta ao cyberbullying e ao doxing.</p> <p>Conduzir um exercício de role-playing, através do qual os participantes praticam a reação a um incidente de doxing.</p> <p><i>Mitigação do Risco do Roubo de Identidade (10 minutos):</i></p> <p>Explicar como proteger as informações pessoais e financeiras.</p> <p>Fornecer sugestões e exemplos práticos.</p> <p><i>Literacia Jurídica Referente ao Doxing (10 minutos):</i></p> <p>Discutir os aspetos jurídicos do doxing, nomeadamente eventuais ações judiciais, assim como os direitos das vítimas.</p> <p>Dar resposta às questões colocadas pelos participantes no que concerne às implicações legais.</p> <p><i>Q&A e Conclusão (10 minutos):</i></p> <p>Abrir espaço para questões adicionais.</p> <p>Recapitular os pontos-chave e distribuir os formulários de feedback (opcional).</p>
<p>Dicas e sugestões</p>	<p>Incentivar o debate aberto e assegurar que todos os participantes possuem a oportunidade de contribuir.</p> <p>Supervisionar as atividades do grupo, com vista a fornecer orientações e manter os debates no caminho certo.</p> <p>Recorrer a exemplos reais para tornar a sessão mais relevante e impactante.</p>
<p>Medidas de segurança</p>	<p>Garantir a segurança na Internet no decorrer das atividades online.</p> <p>Promover um ambiente de suporte, no qual os participantes se sintam seguros para partilhar e debater.</p> <p>Estar preparado para lidar com qualquer angústia ou desconforto entre os participantes em virtude da natureza delicada do tópico.</p>

Valor acrescentado	<p>Conhecimentos Práticos: Estratégias e técnicas concretas para proteger a privacidade e informações confidenciais online.</p> <p>Consciência Ética: Compreensão alargada do comportamento ético online e da importância em preservar a privacidade dos demais.</p> <p>Capacidade de Resposta: Reforço eficaz da capacidade de resposta a incidentes de cyberbullying e doxing, incluindo conhecer as ações a tomar e quem contactar para obter auxílio.</p> <p>Mitigação do Risco: Competências aprimoradas em matéria de proteção de informações pessoais e financeiras para prevenir a usurpação de identidade e fraude.</p> <p>Conhecimento Jurídico: Compreensão clara dos direitos legais no que diz respeito ao doxing e às eventuais ações legais contra os autores.</p>
Feedback e avaliação	<p>Encorajar os participantes a transmitirem feedback no final da sessão, com vista a aperfeiçoar práticas futuras.</p>
Conclusão	<p>Esta prática educa, de forma eficaz, os jovens quanto aos aspetos fundamentais da privacidade online, conduta ética e resposta ao cyberbullying. Esta prática, para além de aprimorar o entendimento dos direitos e responsabilidades legais, promove um ambiente online respeitador e seguro. Em suma, a prática capacita os jovens a navegar no mundo digital com confiança, mitigando os riscos associados ao doxing e a outras ameaças cibernéticas e reforçando a importância de preservar a privacidade e o comportamento ético online.</p>

Anexo. Exercício de Role-Playing: Responder a um Incidente de Doxing

<p>Objetivo: Permitir que os participantes pratiquem a resposta a um incidente de doxing eficazmente, dotando-os das competências necessárias para lidar com tais situações no mundo real.</p>
<p>Duração: 15 minutos</p>
<p>Etapas:</p> <p>Introdução ao Exercício:</p> <p>Esclarecer o objetivo do exercício de role-playing.</p> <p>Sublinhar a importância de praticar a resposta, de modo a estar devidamente preparado em contextos reais.</p> <p>Distribuição dos Cartões de Cenário:</p> <p>Dividir os participantes em pequenos grupos de 4-5 pessoas.</p> <p>Distribua um cartão de cenário por grupo.</p> <p>Preparação do Grupo:</p> <p>Conceder tempo a cada grupo para a leitura do seu cenário e discussão de como responder.</p>

Incentivar os participantes a consultar os folhetos sobre estratégias de resposta e direitos legais.

Role-Playing:

Cada grupo representa o seu cenário, com os membros do grupo a assumirem diferentes papéis (ex., a vítima, o amigo, o doxer, o espetador).

Os moderadores observam e orientam, conforme necessário.

Apresentações de Grupo:

Cada grupo apresenta o seu cenário e revela a sua resposta.

Após cada apresentação, reserve tempo para que os moderadores e os colegas transmitam feedback.

Avaliação e Discussão:

Conduzir um breve debate sobre o conhecimento adquirido com o exercício.

Destacar estratégias eficazes e identificar as áreas que devem ser aperfeiçoadas.

Anexo. Exemplos de Cartões de Cenário

Cartão de Cenário 1: Divulgação da Informação Pessoal

Descrição: Um participante constata que a sua informação pessoal (morada, número de telefone) foi publicada online por um utilizador anónimo.

Tarefa: Determinar medidas imediatas para proteger as contas, comunicar o incidente e alertar adultos de confiança ou autoridades.

Cartão de Cenário 2: Amigo em Apuros

Descrição: O amigo de um participante está a ser alvo de doxing, após uma acesa discussão online. O amigo encontra-se desanimado e não sabe que atitude tomar.

Tarefa: Prestar apoio emocional ao amigo, auxiliá-lo na denuncia do incidente e aconselhá-lo sobre a melhor forma de proteger as suas informações.

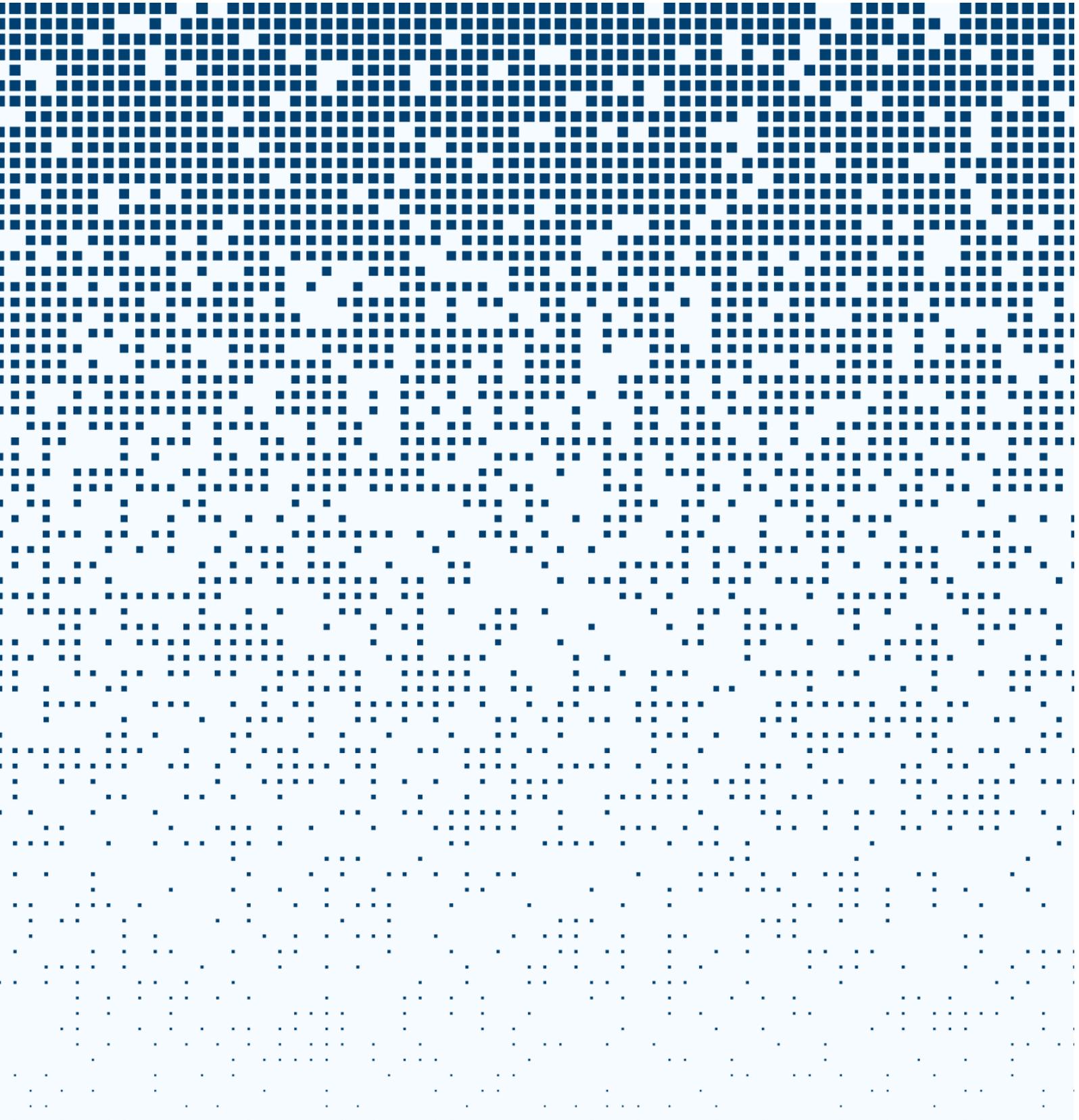
Cartão de Cenário 3: Colega Sob Ameaça

Descrição: Um participante testemunha um colega a ser vítima de doxing numa conversa de grupo. O doxer é conhecido de ambos.

Tarefa: Determinar se deve confrontar o doxer, depois comunicar o incidente ao administrador do grupo e às autoridades e apoiar a vítima.



This Document is published under an [Attribution-NonCommercial 4.0](https://creativecommons.org/licenses/by-nc/4.0/) International license [CC BY-NC].



Conscious Youth Behaviours in Emerging Realities

Erasmus+ KA2 Cooperation Partnerships in School Education

[Reference n. 2023-1-EL01-KA220-SCH-000156982]



**Co-funded by
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.