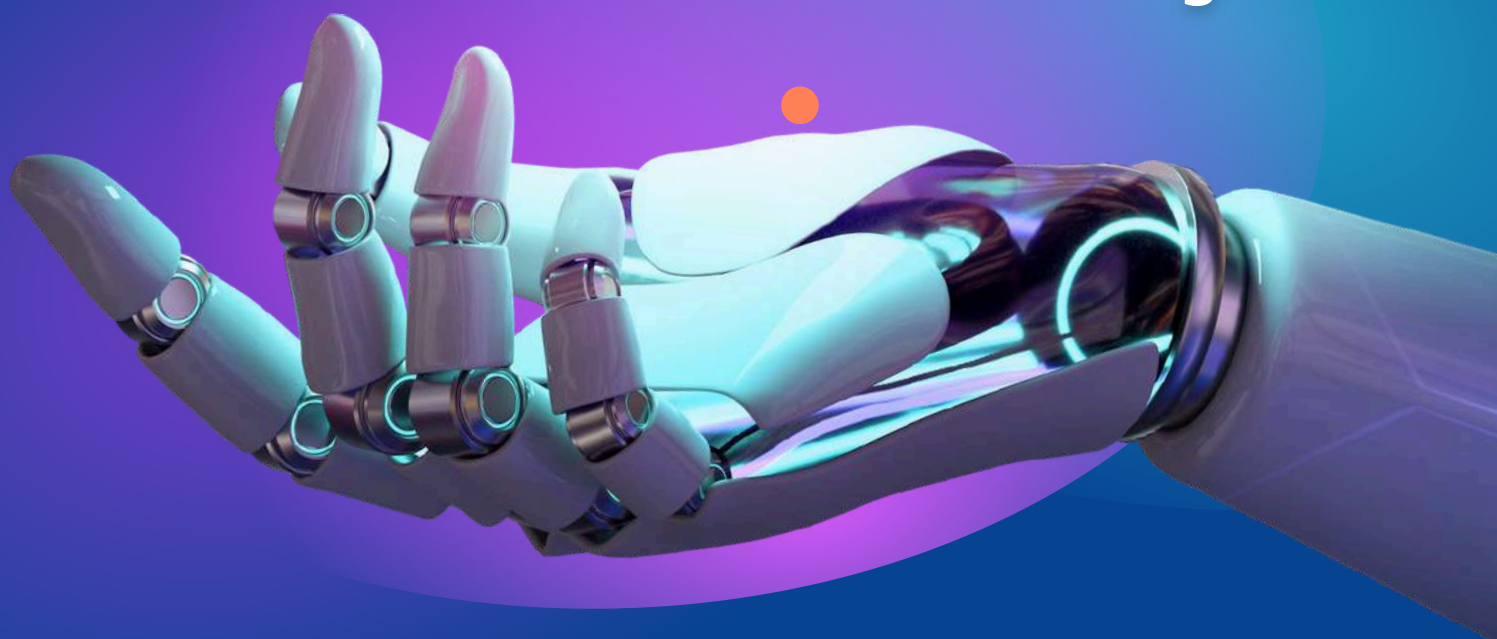




Co-funded by
the European Union



MÉTODOS NÃO FORMAIS SOBRE CIBERSEGURANÇA



2025-1-ES02-KA220-YOU-000358192

**ESCAP(E+) - Educar jovens em segurança através de um
programa de sensibilização e envolvimento em
cibersegurança.**

ESTA OBRA ESTÁ
LICENCIADA SOB A
LICENÇA CC BY-SA 4.0.





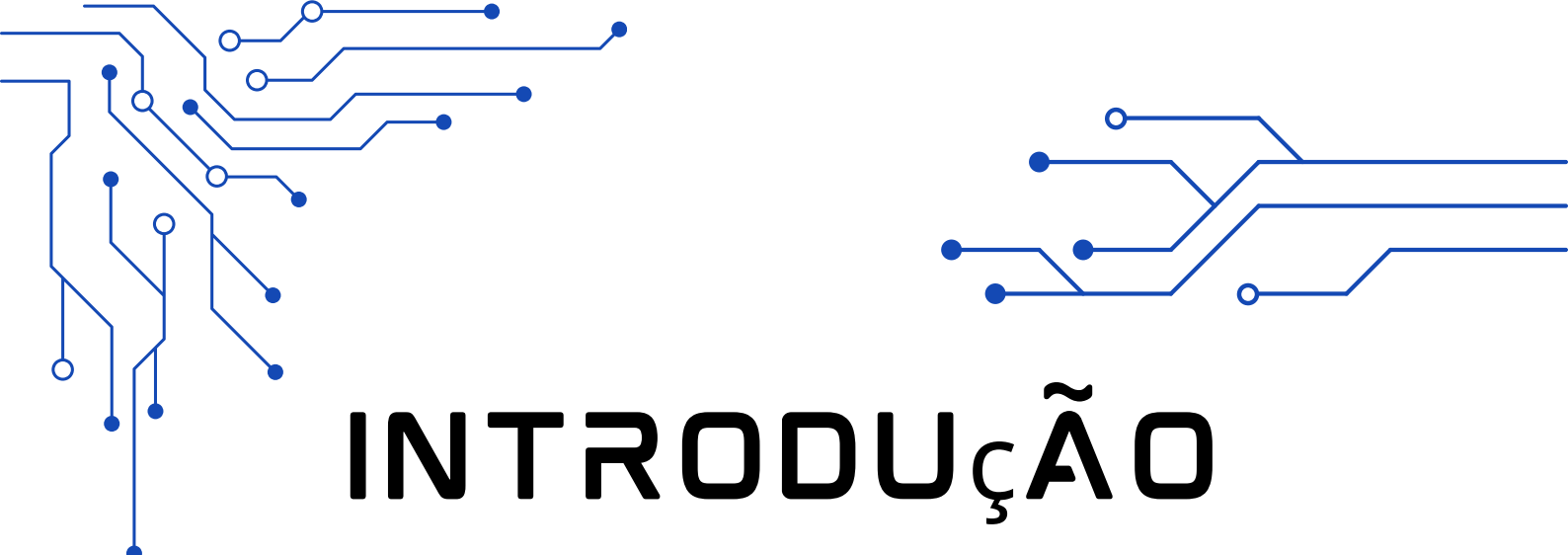
**Co-funded by
the European Union**

Financiado pela União Europeia. As opiniões e pontos de vista expressos são, contudo, da exclusiva responsabilidade do(s) seu(s) autor(es) e não refletem necessariamente os da União Europeia ou da Agência de Execução Europeia da Educação e da Cultura (EACEA). Nem a União Europeia nem a EACEA podem ser responsabilizadas pelos mesmos.

Os materiais desenvolvidos são classificados como Recursos Educativos Abertos (REA) e podem ser descarregados, usados, reutilizados, copiados, adaptados e partilhados livremente pelos utilizadores, sem necessidade de autorização dos seus criadores, desde que seja indicada a respetiva fonte.

ÍNDICE

1. Introdução.....	4
2. Cibersegurança e Juventude.....	8
3. Metodologia da Educação Não Formal.....	13
4. Como usar este Kit de Ferramentas.....	18
5. Atividades de Aprendizagem em Cibersegurança.....	23
6. Métodos de Debriefing e Reflexão.....	71
7. Dicas para técnicos de juventude.....	74
8. Recursos e ferramentas.....	78



INTRODUÇÃO

FINALIDADE DO KIT DE FERRAMENTAS

O **Kit de Ferramentas de Cibersegurança ESCAP(E+)** foi desenvolvido como um recurso prático e fácil de usar para apoiar técnicos de juventude, educadores e organizações na abordagem de temas relacionados com a cibersegurança junto dos jovens. No ambiente digital atual, os jovens interagem constantemente com plataformas online, mas muitas vezes não possuem o conhecimento e a confiança necessários para lidar com os riscos de forma segura. Ao mesmo tempo, muitos técnicos de juventude consideram a cibersegurança um tema demasiado técnico ou complexo para ser integrado nas suas atividades diárias.

Este conjunto de ferramentas responde diretamente a esses desafios, oferecendo abordagens concretas e prontas a utilizar, que simplificam o ensino da cibersegurança e o tornam acessível em contextos de aprendizagem não formal. Em vez de se concentrar em explicações teóricas ou altamente técnicas, o conjunto de ferramentas traduz conceitos-chave em experiências de aprendizagem interativas e envolventes que podem ser facilmente aplicadas em workshops, intercâmbios juvenis ou atividades locais.

O principal objetivo do guia é capacitar os técnicos de juventude para facilitarem discussões e atividades significativas sobre segurança online, comportamento digital e riscos cibernéticos. O guia apoia-os na criação de ambientes de aprendizagem seguros, onde os jovens podem refletir sobre as suas próprias práticas online, desenvolver o pensamento crítico e adquirir competências práticas. Dessa forma, o guia contribui para o fortalecimento da resiliência digital entre os jovens e promove uma utilização mais responsável e informada das tecnologias digitais, em consonância com as prioridades europeias em matéria de transformação digital e educação (Comissão Europeia, 2021).

VISÃO GERAL DO PROJETO – ESCAP(E+)

ESCAP(E+) – Educar Jovens em Segurança através de Programas de Consciencialização e Envolvimento em Cibersegurança – é uma Parceria de Cooperação Erasmus+ com duração de 24 meses, na área da juventude, implementada entre dezembro de 2025 e novembro de 2027. O projeto reúne seis organizações parceiras de Espanha, Portugal, Roménia, Turquia, Estónia e Lituânia, combinando experiência em trabalho juvenil, educação digital, gamificação e inovação tecnológica.

O projeto foi concebido em resposta à crescente exposição dos jovens a ameaças cibernéticas e à falta de ferramentas educativas envolventes e adequadas ao público jovem para lidar com esses riscos. O seu principal objetivo é aumentar a consciencialização sobre cibersegurança e a resiliência digital entre jovens e técnicos de juventude, utilizando métodos de aprendizagem inovadores, interativos e não formais.

Ao longo da sua implementação, o ESCAP(E+) desenvolve uma gama de produtos educativos que tornam a aprendizagem em cibersegurança mais acessível e envolvente. Estes incluem aplicações de escape room em realidade virtual, uma série de infográficos e vídeos animados, e atividades de aprendizagem estruturadas testadas em laboratórios com jovens e ações de formação. Ao integrar gamificação e aprendizagem experiencial, o projeto garante que os participantes não só são informados sobre cibersegurança, mas também se envolvem ativamente em processos de resolução de problemas e tomada de decisões.

Além disso, o projeto dá grande ênfase ao desenvolvimento de capacidades dos técnicos de juventude, fornecendo-lhes ferramentas e metodologias práticas que podem ser diretamente aplicadas no seu trabalho. Através da cooperação internacional e da troca de práticas, o ESCAP(E+) contribui para a melhoria da qualidade e da inovação do trabalho com jovens em toda a Europa, alinhando-se com as prioridades do Erasmus+ relacionadas com a preparação digital, a resiliência e o desenvolvimento de capacidades (Comissão Europeia, Programa Erasmus+).

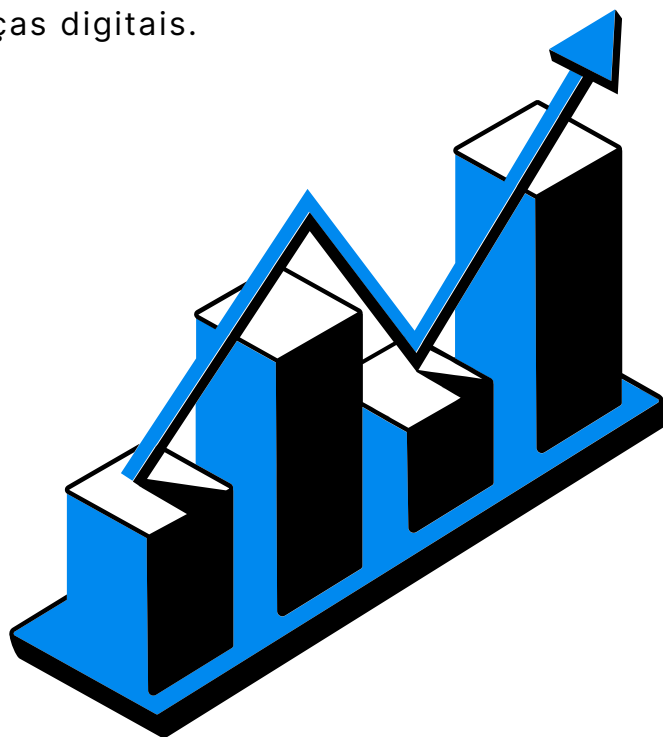
PORQUÊ É QUE A EDUCAÇÃO EM CIBERSEGURANÇA PARA JOVENS É IMPORTANTE?



Os jovens de hoje estão entre os utilizadores mais ativos de tecnologias digitais, passando uma parte significativa das suas vidas diárias online. Redes sociais, plataformas de mensagens, ambientes de jogos e ferramentas digitais são espaços essenciais para a comunicação, a aprendizagem e a autoexpressão. No entanto, esse elevado nível de envolvimento também aumenta a sua exposição a uma ampla gama de riscos de cibersegurança.

Segundo o Eurostat, aproximadamente 97% dos jovens na União Europeia utilizam a internet diariamente, o que evidencia o papel central dos ambientes digitais nas suas vidas (Eurostat, 2024). Ao mesmo tempo, dados e estudos europeus indicam que muitos jovens enfrentam riscos online, como burlas de phishing, roubo de identidade, cyberbullying, desinformação e violações de privacidade. Apesar disso, uma parte significativa não possui as competências necessárias para avaliar criticamente o conteúdo online, proteger os seus dados pessoais ou responder eficazmente a ameaças digitais.

Esta situação é ainda mais complicada pelo facto de que a educação em cibersegurança existente é frequentemente dirigida a públicos técnicos e não corresponde às necessidades ou à realidade dos jovens. Os técnicos de juventude também enfrentam dificuldades para abordar esses temas, pois podem não ter acesso a ferramentas adequadas ou a formação que se enquadre em abordagens de educação não formal.



PORQUÊ É QUE A EDUCAÇÃO EM CIBERSEGURANÇA PARA JOVENS É IMPORTANTE?

A educação em cibersegurança é, portanto, essencial não só para aumentar a consciencialização, mas também para desenvolver competências práticas. Desempenha um papel fundamental na construção da literacia digital, no reforço do pensamento crítico e na promoção de um comportamento online responsável. Contribui ainda para capacitar os jovens a assumirem o controlo das suas vidas digitais, a tomarem decisões informadas e a protegerem-se a si próprios e aos outros em ambientes online.

A importância deste tema reflete-se fortemente nos quadros políticos europeus. O Plano de Ação para a Educação Digital (2021-2027) enfatiza a necessidade de reforçar as competências digitais e a resiliência em todos os setores da educação (Comissão Europeia, 2021), enquanto a Agência da União Europeia para a Cibersegurança destaca a educação e a sensibilização como pilares fundamentais para a construção de uma sociedade digital mais segura (ENISA, 2023).

O ESCAP(E+) responde a essas necessidades oferecendo uma abordagem inovadora que combina educação em cibersegurança com gamificação, realidade virtual e aprendizagem não formal. Ao tornar o processo de aprendizagem interativo, relevante e envolvente, o projeto garante que os jovens não sejam recetores passivos de informação, mas participantes ativos na construção das suas próprias competências em segurança digital.



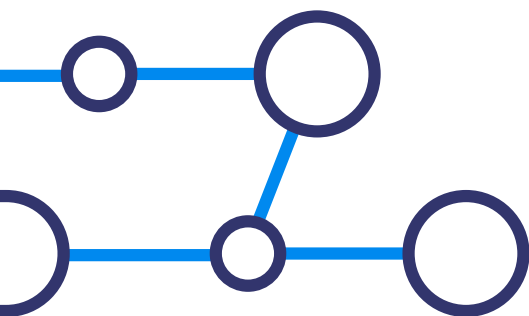


CIBERSEGURANÇA E JUVENTUDE

PRINCIPAIS AMEAÇAS ONLINE PARA JOVENS

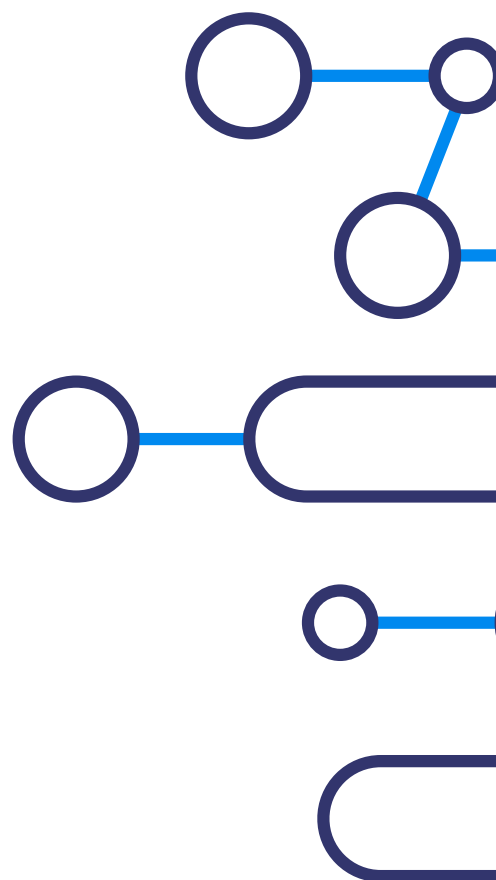
A investigação documental realizada nos países parceiros do ESCAP(E+) revela um panorama de ameaças, apesar das diferenças nos contextos nacionais. As ameaças mais relevantes para os jovens são as manipulações baseadas na confiança ou no comportamento, que exploram a dinâmica social comum do uso quotidiano de plataformas digitais. Quatro plataformas emergem como vetores principais (Email, Instagram, Facebook e TikTok), cada uma com um perfil de ameaça distinto, mas com um mecanismo subjacente em comum: criar um sentido de urgência, apropriar-se de legitimidade institucional ou social e agir antes que o utilizador pare para verificar. Entre os riscos prevalentes, **o phishing e o roubo de credenciais por email** representam a ameaça de maior gravidade documentada. Mensagens fraudulentas fazem-se passar por instituições de confiança, como bancos, universidades, autoridades públicas e serviços de entrega, direcionando os utilizadores para páginas de login falsas onde as credenciais são obtidas. A geração de conteúdo assistida por inteligência artificial aumentou substancialmente a sofisticação dessas mensagens.

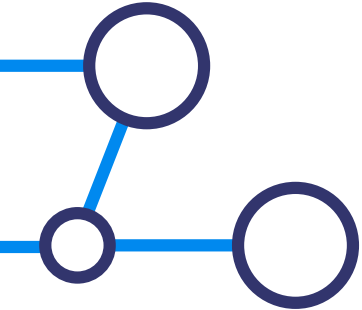
Burlas relacionadas com falsas ofertas de emprego e estágio podem levar as vítimas a burlas com cheques e ao roubo de dados pessoais, com perdas financeiras documentadas que chegam a milhões de euros anualmente. A **usurpação de identidade e o roubo de contas** no Instagram operam através de mensagens diretas elaboradas para despertar curiosidade ou confiança. Campanhas de "verificação de conta" e "aviso de direitos de autor" induzem os administradores de páginas a fornecerem as suas credenciais; transmissões repetidas em direto, fazendo-se passar por celebridades, solicitam "taxas de verificação" a adolescentes. Uma variante qualitativamente mais grave é a sextorsão: redes criminosas organizadas conquistam a confiança das vítimas através de mensagens românticas, solicitam imagens íntimas e, em seguida, extorquem-nas sob ameaça de divulgação.



A burla e a desinformação no Marketplace do Facebook operam através de dois mecanismos distintos, mas igualmente exploradores. Anúncios falsos de telemóveis, bilhetes e jogos direcionam os utilizadores para páginas de pagamento fraudulentas, com os esquemas a redirecionarem frequentemente as vítimas entre plataformas, antes de chegarem a formulários de pagamento clonados. Paralelamente, campanhas coordenadas de desinformação exploram o algoritmo do Facebook, focado no envolvimento, para amplificar conteúdo falso ou emocionalmente carregado; as correções raramente alcançam o mesmo público da alegação falsa original, e a impressão emocional persiste muito tempo depois da retratação.

A desinformação e os redirecionamentos fraudulentos no TikTok exploram a velocidade e o apelo emocional dos vídeos curtos. Conteúdo viral que anuncia falsamente bolsas de estudo, pagamentos estatais ou recompensas leva os utilizadores a links maliciosos. O algoritmo da página "Para Ti" do TikTok amplifica o conteúdo com base no envolvimento, e não na precisão, o que significa que vídeos falsos, mas com forte apelo emocional, espalham-se com a mesma eficácia que informações verificadas. Em sociedades pequenas e altamente conectadas, já visadas por operações externas de informação, esta vulnerabilidade estrutural acarreta riscos que vão além do dano individual. Subjacente a estes perfis de ameaça, encontra-se um quinto risco identificado em todos os relatórios dos países parceiros: **a exposição não intencional de dados pessoais através da partilha excessiva e habitual**. Detalhes de identidade, padrões de localização e informações de relacionamento partilhados rotineiramente entre plataformas fornecem a matéria-prima para engenharia social direcionada, sem necessidade de qualquer intrusão técnica.





COMPORTAMENTO DIGITAL DOS JOVENS

Segundo o Eurostat (2025), 97% dos cidadãos da UE com idades entre 16 e 29 anos utilizam a internet diariamente. Os dados dos países parceiros refletem essa intensidade. O uso regular da internet entre jovens dos 16 aos 24 anos atinge 99,6% em Espanha, 99,2% na Lituânia e aproxima-se dos 100% na Estónia, onde 96% se ligam à internet várias vezes ao dia. Os dados romenos mostram que 95,7% dos estudantes do ensino secundário estão online todos os dias; os dados turcos documentam que 95,3% dos jovens dos 16 aos 24 anos utilizam as redes sociais diariamente. É importante salientar que uma elevada competência digital não se traduz automaticamente em resiliência. A Estónia, onde 62,6% da população possui pelo menos competências digitais básicas (acima da média da UE de 55,6%), regista, no entanto, algumas das maiores taxas de exposição de jovens a danos online na UE. Diversas tendências comportamentais repetem-se de forma consistente em todos os resultados dos países parceiros:

A socialização mediada por plataformas como modo padrão: comunicação, validação entre pares, entretenimento e construção de identidade acontecem pelos mesmos canais que veiculam ameaças. Aplicar um modo de envolvimento distinto e cético a conteúdos potencialmente arriscados exigiria a interrupção da participação social normal.



Evitar atritos em decisões de segurança: aceitar todas as permissões, reutilizar palavras-passe e ignorar a autenticação de dois fatores são respostas racionais a sistemas concebidos para tornar o cumprimento o caminho de menor resistência. Mais de dois terços dos jovens dos 16 aos 19 anos já se envolveram em alguma forma de comportamento de risco online, frequentemente sem terem consciência disso.

Poucos hábitos de verificação antes de partilhar/clicar: a velocidade e as estruturas de recompensa social da interação nas plataformas normalizam cliques e partilhas rápidos e frequentes. Quando os verificadores de factos sinalizam conteúdo falso, ele geralmente já alcançou milhões de utilizadores; as retificações raramente compensam essa perda. As diretrizes oficiais de segurança digital em países parceiros alertam consistentemente contra reações a conteúdo "urgente" ou "baseado no medo" — justamente as categorias que os algoritmos das plataformas destacam de forma desproporcional.



Reutilização de credenciais e partilha excessiva habitual: a reutilização de palavras-passe em diferentes contas é comum em todos os países parceiros. Uma única violação cria uma vulnerabilidade em cascata sempre que as mesmas credenciais são utilizadas. Entretanto, 49% dos jovens europeus entre os 16 e os 29 anos relataram ter-se deparado com mensagens online hostis ou abusivas em 2023, com taxas de exposição nos países mais conectados digitalmente a chegarem a 69%, o que reflete os rastros digitais deixados pelo uso rotineiro das plataformas.

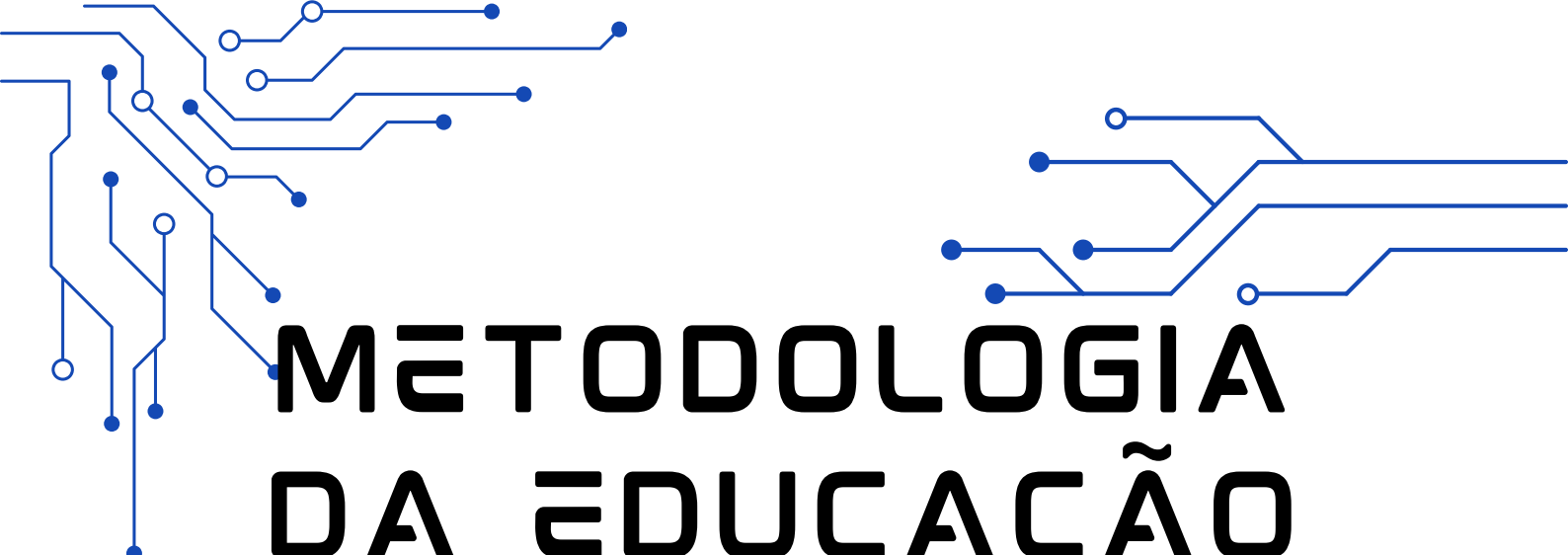
A IMPORTÂNCIA DA RESILIÊNCIA DIGITAL

Uma conclusão comum nos relatórios dos países parceiros é que a consciencialização por si só não garante comportamentos seguros. Jovens que têm uma compreensão geral da existência do phishing ainda clicam em links suspeitos; aqueles que sabem que reutilizar palavras-passe é arriscado ainda mantêm as mesmas credenciais em diversas plataformas. A lacuna entre saber e agir não se deve à falta de informação. Esta lacuna reflete como as decisões são tomadas sob condições de urgência, pressão social, uso habitual da plataforma e design persuasivo.

Superar esta lacuna exige o desenvolvimento ativo da resiliência digital. A resiliência digital, conforme entendida no âmbito do ESCAP(E+), é a capacidade de reconhecer uma ameaça no seu contexto, tomar decisões ponderadas em situações de incerteza, recuperar de um erro e servir de recurso para outros membros da rede. Trata-se de uma competência tanto individual como social — e essa distinção é importante. O vetor mais eficaz tanto para a prevenção de riscos como para a proteção entre os jovens é a própria rede de pares: comportamentos, incluindo comportamentos seguros, propagam-se pelos mesmos canais sociais que as ameaças. As correções entre pares são mais eficazes do que comunicados institucionais; discutir conteúdo suspeito com amigos está entre as defesas mais poderosas contra a desinformação.

A resiliência não é algo que os indivíduos constroem, mas sim algo que as comunidades praticam. Todos os seis relatórios dos países parceiros convergem para a mesma recomendação pedagógica: a educação eficaz em cibersegurança para jovens deve ser prática, baseada em cenários e fundamentada nas plataformas e comportamentos com os quais os jovens realmente interagem. A formação baseada em cenários capacita os alunos com competências de reconhecimento, em vez de regras para memorizar. A "orientação de resposta rápida" (saber o que fazer nos primeiros minutos após um problema) é uma competência específica e ensinável. Hábitos de avaliação crítica são importantes mesmo entre utilizadores tecnicamente proficientes que podem estar demasiado confiantes na sua capacidade de detetar manipulação. Além das competências, há uma dimensão cultural: os jovens precisam de se sentir confiantes para pedir ajuda sem vergonha e de estar inseridos num ambiente entre pares que normalize essa prática. A devastação psicológica documentada em casos de sextorsão e desinformação, em que a ausência dessa confiança se mostrou decisiva, torna isso não apenas uma preferência pedagógica, mas um imperativo de proteção. Abordagens experienciais podem produzir mudanças mais duradouras e transferíveis do que a mera transferência passiva de informação. Conhecimento incorporado e testado, aliado à clareza sobre a quem recorrer quando algo corre mal e a uma cultura entre pares que normaliza a procura de ajuda, é o que a resiliência digital representa na prática.





METODOLOGIA DA EDUCAÇÃO NÃO FORMAL

O QUE É APRENDIZAGEM NÃO FORMAL?

A principal característica da aprendizagem não formal é que se refere a atividades educativas organizadas que ocorrem fora do sistema escolar formal. Estas são concebidas para apoiar o desenvolvimento pessoal, social e profissional. A aprendizagem não formal é flexível, centrada no aluno e, muitas vezes, voluntária. Esta é a sua principal diferença em relação à educação formal, que segue um currículo estruturado, leva à certificação e é ministrada por instituições como escolas e universidades.

A aprendizagem não formal ocorre normalmente em contextos como organizações juvenis, grupos comunitários, workshops, programas de formação ou iniciativas como este projeto ESCAP(E+), cofinanciado pelo programa Erasmus+. Esta aprendizagem centra-se nas necessidades, interesses e participação ativa dos aprendizes. Por isso, privilegia a aprendizagem experiencial, em contraste com a aprendizagem formal tradicional, que se concentra principalmente no conhecimento teórico.

No âmbito da metodologia "aprender fazendo", são promovidas atividades como discussões em grupo, dramatizações, simulações, trocas entre pares e tarefas baseadas em projetos, pois envolvem ativamente os participantes no processo de aprendizagem. Esta abordagem permite que os alunos liguem novos conhecimentos às suas próprias experiências, tornando a aprendizagem mais significativa e relevante para situações da vida real.

Além disso, o papel do facilitador é de grande importância. Enquanto em ambientes de aprendizagem formal os professores tradicionais transmitem conhecimento, em contextos de aprendizagem não formal os facilitadores orientam, apoiam e criam oportunidades para que os alunos explorem ideias, reflitam e colaborem. O processo de aprendizagem é frequentemente horizontal, o que significa que os participantes aprendem uns com os outros, na chamada "aprendizagem entre pares", tanto quanto com o facilitador. Isto fomenta um sentido de pertença, empoderamento e respeito mútuo dentro do grupo.

Além disso, a aprendizagem não formal privilegia o desenvolvimento de competências transversais, frequentemente denominadas "competências interpessoais". Estas incluem comunicação, trabalho em equipa, pensamento crítico, resolução de problemas, criatividade e competência digital. No contexto do mundo atual, em rápida transformação, tais competências são essenciais para a cidadania ativa, a empregabilidade e a aprendizagem ao longo da vida. Por exemplo, no projeto ESCAP(E+), que aborda a consciencialização em cibersegurança, a aprendizagem não formal envolve a análise de cenários online da vida real, a discussão de riscos digitais e a elaboração colaborativa de estratégias para um comportamento online mais seguro. Todos estes tópicos são abordados no conjunto de ferramentas do ESCAP(E+).

Além disso, os programas de aprendizagem não formal caracterizam-se pela sua flexibilidade, uma vez que podem ser adaptados a diferentes faixas etárias, contextos e níveis de aprendizagem. São particularmente eficazes para alcançar públicos diversos, incluindo jovens com menos oportunidades, pois podem ser personalizados para serem inclusivos e acessíveis. Normalmente, não há avaliação ou classificação formal. Em vez disso, a reflexão e o feedback construtivo são utilizados para apoiar tanto a aprendizagem como o crescimento pessoal.

Importa salientar que a aprendizagem não formal complementa tanto a aprendizagem formal como a informal. Enquanto a educação formal proporciona conhecimento estruturado e qualificações, e a aprendizagem informal ocorre naturalmente através de experiências quotidianas, a aprendizagem não formal preenche essa lacuna, oferecendo oportunidades de aprendizagem intencionais, porém flexíveis. Por outras palavras, cria espaços onde os indivíduos podem experimentar, expressar-se e desenvolver autoconfiança num ambiente acolhedor.

Em suma, a aprendizagem não formal é uma abordagem dinâmica e participativa que capacita os indivíduos a envolverem-se ativamente no seu próprio processo de aprendizagem. Ao centrar-se na experiência, na colaboração e na aplicação prática, desempenha um papel crucial no fomento do desenvolvimento pessoal, da inclusão social e da participação ativa na sociedade.

PORQUÊ É QUE A GAMIFICAÇÃO FUNCIONA NO TRABALHO COM JOVENS?

Para começar, vamos esclarecer o que é a gamificação. Em primeiro lugar, a gamificação refere-se ao uso de elementos de jogos, como pontos, desafios, narrativas, recompensas e competição, em contextos não lúdicos, com o objetivo de aumentar o envolvimento e a aprendizagem. Especialmente no trabalho com jovens, a gamificação tem-se mostrado particularmente eficaz, pois se alinha perfeitamente com a forma como os jovens aprendem, interagem e se mantêm motivados de forma natural.

Sem dúvida, a gamificação funciona no trabalho com jovens por muitos motivos. Em primeiro lugar, aumenta a motivação e o envolvimento. As abordagens tradicionais de aprendizagem podem, por vezes, parecer passivas ou desligadas dos interesses dos jovens. Em contrapartida, as atividades gamificadas introduzem elementos de diversão, desafio e curiosidade. Quando os jovens são apresentados a missões, níveis ou tarefas de resolução de problemas, tornam-se participantes ativos em vez de recetores passivos. Este sentido de envolvimento incentiva a atenção sustentada e um envolvimento mais profundo.

Em segundo lugar, a gamificação apoia a aprendizagem experiencial, um princípio fundamental do trabalho com jovens e da aprendizagem não formal, como analisámos na secção anterior. Em vez de simplesmente receberem informação, os participantes aprendem fazendo através de simulações, dramatizações ou desafios interativos. Isto está intimamente ligado às ideias de David Kolb, que enfatizou que o conhecimento é construído através da experiência e da reflexão. Num ambiente gamificado, os jovens podem testar decisões, cometer erros num ambiente seguro e ver imediatamente as consequências das suas ações. Isto torna a aprendizagem mais significativa e mais fácil de reter.

Em terceiro lugar, a gamificação promove a motivação intrínseca, pois geralmente inclui recompensas como distintivos ou pontos. No entanto, a sua verdadeira força reside em fomentar a satisfação interna, como a sensação de realização, progresso ou domínio. Elementos como objetivos claros, feedback instantâneo e progresso visível ajudam os alunos a compreender como estão a melhorar. Isto está alinhado com as teorias motivacionais que sugerem que autonomia, competência e relacionamento são essenciais para um envolvimento significativo.

Por fim, a gamificação é altamente eficaz no desenvolvimento de competências transversais e interpessoais, visto que muitas atividades gamificadas exigem trabalho em equipa, comunicação, resolução de problemas e pensamento crítico. Por exemplo, desafios colaborativos ou missões em equipa incentivam a aprendizagem entre pares e a interação social. Estas são competências essenciais no trabalho com jovens, particularmente em áreas relacionadas com o projeto ESCAP(E+), ou seja, literacia digital e consciencialização em cibersegurança, em que os jovens precisam de lidar com situações complexas da vida real.

Por fim, importa salientar que a gamificação cria um espaço seguro para a experimentação, é flexível e inclusiva, e está em sintonia com a cultura digital dos jovens. Muitos já estão familiarizados com ambientes baseados em jogos, seja através de videojogos ou aplicações para telemóvel. Trazer dinâmicas semelhantes para o trabalho com jovens cria uma sensação de familiaridade e relevância, preenchendo a lacuna entre a aprendizagem e a vida quotidiana.

Em resumo, a gamificação funciona no trabalho com jovens porque transforma a aprendizagem numa experiência ativa, envolvente e significativa. Ao combinar motivação, participação e aplicação prática, apoia não apenas a aquisição de conhecimento, mas também o desenvolvimento pessoal e a inclusão social.





FACILITAR A APRENDIZAGEM INTERATIVA

A educação não formal desempenha um papel crucial na facilitação da aprendizagem interativa, colocando a participação, a experiência e a colaboração no centro do processo de aprendizagem. Como analisámos em 3.1, ao contrário das abordagens tradicionais que muitas vezes se baseiam na transmissão unilateral de conhecimento, a educação não formal cria ambientes dinâmicos onde os alunos se envolvem ativamente com o conteúdo, os facilitadores e uns com os outros.

O processo de aprendizagem torna-se uma experiência partilhada. Deixa de ser uma tarefa individual. Através de métodos como discussões em grupo, simulações, dramatizações e atividades entre pares, os alunos são incentivados a contribuir com as suas próprias perspetivas e experiências. Esta interação não só torna a aprendizagem mais envolvente, como também aprofunda a compreensão, à medida que os participantes refletem, questionam e aplicam o conhecimento em contextos da vida real.

Além disso, a educação não formal promove um espaço seguro e inclusivo onde os alunos se sentem à vontade para expressar ideias, cometer erros e experimentar novas abordagens. Esta sensação de segurança psicológica é essencial para uma interação significativa, pois fomenta a abertura, a confiança e o respeito mútuo dentro do grupo.

Por último, mas não menos importante, como também mencionámos em 3.1, o papel do facilitador, que orienta o processo em vez de o dominar, é de grande importância. Ao incentivar o diálogo e a colaboração, os facilitadores ajudam os aprendizes a assumirem o controlo da sua jornada de aprendizagem. Isto capacita os participantes a tornarem-se colaboradores ativos, fortalecendo tanto a sua confiança como a sua capacidade de aprender com os outros.

Em suma, a educação não formal facilita a aprendizagem interativa, transformando os alunos de recetores passivos em participantes ativos. Incentiva o diálogo, a reflexão e a cooperação, resultando em experiências de aprendizagem mais envolventes, relevantes e impactantes. É isso que o conjunto de ferramentas ESCAP(E+) visa alcançar.



COMO USAR ESTE KIT DE FERRAMENTAS

Este guia foi concebido como um recurso prático que auxilia os utilizadores a navegar, selecionar e aplicar atividades de cibersegurança não formal de forma estruturada e flexível. Destina-se principalmente a técnicos de juventude, formadores, educadores, facilitadores e organizações que trabalham com jovens, especialmente em contextos de aprendizagem não formal. O seu objetivo é tornar a educação em cibersegurança mais acessível, envolvente e aplicável, oferecendo atividades prontas a utilizar que podem ser implementadas em workshops, laboratórios para jovens, cursos de formação, sessões escolares e atividades comunitárias.

Em vez de ser um documento que deve ser seguido do início ao fim, o guia deve ser usado como um recurso de aprendizagem flexível. Os utilizadores podem escolher atividades individuais, combinar várias atividades numa sessão temática ou usar o guia como parte de um processo educativo mais amplo sobre literacia digital, cibersegurança ou segurança online. O guia foi concebido para apoiar a prática, não para impor um método fixo. Isto permite que facilitadores e organizações o utilizem de formas que se adaptem aos seus próprios contextos de aprendizagem, prioridades e participantes.

PARA QUEM SE DESTINA ESTE CONJUNTO DE FERRAMENTAS?

O conjunto de ferramentas foi desenvolvido principalmente para profissionais e especialistas que trabalham com jovens em contextos de aprendizagem e participação. Isto inclui técnicos de juventude, formadores de jovens, facilitadores, professores, líderes juvenis, voluntários, mentores e organizações que atuam na área da educação juvenil ou da literacia digital.

As atividades em si são destinadas principalmente a jovens com idades entre os 15 e os 30 anos, aproximadamente. No entanto, o conjunto de ferramentas também pode ser relevante em ambientes de aprendizagem mistos, onde outros grupos estejam envolvidos, como estudantes, educadores de pares, voluntários da comunidade ou adultos que apoiam o bem-estar digital dos jovens. A sua força reside no facto de poder ser usado numa ampla variedade de contextos, mantendo-se prático e fácil de aplicar.

COMO ESTÁ ESTRUTURADO O KIT DE FERRAMENTAS

O guia foi organizado para ajudar os utilizadores a progredirem da compreensão do tema geral para a aplicação de atividades concretas. Inclui secções introdutórias que explicam o tema e a metodologia, seguidas de atividades práticas, elementos de reflexão e recursos de apoio adicionais. Isto significa que os utilizadores não precisam de o ler numa ordem rígida. Podem começar pelas secções introdutórias se desejarem uma compreensão conceptual ou ir diretamente para as atividades se precisarem de material prático para uma sessão.

Cada atividade segue uma estrutura consistente para que os utilizadores possam compreender rapidamente como aplicá-la. Em geral, as atividades incluem um título, objetivos de aprendizagem, público-alvo, duração, tamanho do grupo, materiais necessários, instruções passo a passo, questões de reflexão e principais mensagens de aprendizagem. Isto facilita a comparação entre as atividades e a escolha daquela que melhor se adapta ao tempo disponível, aos objetivos de aprendizagem e ao perfil do grupo.

FORMATO DE SESSÃO RECOMENDADO

O conjunto de ferramentas funciona melhor quando as atividades são utilizadas num formato interativo. Como os métodos são baseados na aprendizagem não formal, os participantes devem envolver-se ativamente através de discussões, trabalho em equipa, reflexão, resolução de problemas, dramatizações ou tarefas baseadas em cenários. O objetivo não é apenas fornecer informação, mas também ajudar os participantes a explorar, questionar e aplicar o que aprendem.

Um formato simples e recomendado para usar uma atividade é o seguinte:

1. Abertura

Comece com uma breve introdução ao tema e ao objetivo da sessão. Isto ajudará os participantes a compreenderem por que razão o tema é importante e o que será explorado.

2. Implementação da atividade

Execute a atividade selecionada seguindo as instruções fornecidas no guia. Dependendo do formato, isto pode envolver trabalho em pares, trabalho em pequenos grupos, discussão plenária ou resolução de tarefas práticas.

3. Reflexão

Após a atividade, convide os participantes a refletirem sobre o que aconteceu, o que observaram e o que aprenderam. A reflexão é importante porque ajuda a transformar a experiência num resultado de aprendizagem significativo.

4. Mensagens-chave

Encerre a sessão destacando os principais pontos e lições práticas que os participantes devem recordar e aplicar.

Como diretriz geral, o conjunto de ferramentas pode ser utilizado em sessões curtas de 30 a 45 minutos, workshops padrão de 60 a 90 minutos ou sessões mais longas que combinam diversas atividades em torno de um mesmo tema. Os facilitadores também podem utilizar várias atividades ao longo de uma série de sessões, caso desejem construir um processo de aprendizagem mais abrangente ao longo do tempo.

GRUPOS-ALVO

Embora o conjunto de ferramentas seja usado principalmente por facilitadores e profissionais da área da juventude, as atividades são dirigidas principalmente aos jovens. O perfil principal dos participantes inclui jovens que são ativos online e podem estar expostos a riscos como phishing, burlas, roubo de identidade, perfis falsos, desinformação, manipulação, violações de privacidade ou hábitos digitais inseguros.

Ao mesmo tempo, o conjunto de ferramentas também pode ser usado com participantes que tenham menor confiança digital ou conhecimento prévio mais limitado. Algumas atividades podem ser particularmente úteis para grupos mistos, incluindo participantes com diferentes níveis de experiência, confiança ou acesso à tecnologia.

Ao escolher atividades, os utilizadores devem considerar:

- a idade dos participantes;
- a sua familiaridade com plataformas online e ferramentas digitais;
- os seus conhecimentos prévios sobre tópicos de cibersegurança;
- a sua confiança no trabalho em grupo e na discussão;
- o ambiente de aprendizagem, como um centro juvenil, escola, curso de formação ou workshop local.

Isto ajuda a garantir que a atividade selecionada seja apropriada, relevante e realista para o grupo específico.

ADAPTAR AS ATIVIDADES A DIFERENTES GRUPOS

O conjunto de ferramentas foi concebido para ser adaptável. As atividades não precisam de ser implementadas exatamente da mesma maneira todas as vezes. Os utilizadores são encorajados a ajustar o nível, os exemplos, o ritmo e o formato de acordo com as necessidades dos participantes.

Para grupos mais jovens ou participantes com menor familiaridade com o mundo digital, as atividades podem ser simplificadas com exemplos mais comuns, instruções mais concisas e tarefas práticas mais claras. Para grupos mais velhos ou com mais experiência, a mesma atividade pode ser expandida com cenários mais complexos, análises mais aprofundadas ou tarefas de reflexão adicionais. Em alguns casos, as atividades podem precisar de ser encurtadas, divididas em etapas ou complementadas com explicações mais detalhadas.

A adaptação pode incluir:

- simplificar a linguagem usada nas instruções;
- adaptar os exemplos para que reflitam as plataformas e situações que os participantes conhecem;
- reduzir o número de etapas ou perguntas de discussão;
- prolongar a fase de reflexão para grupos preparados para uma análise mais aprofundada;
- substituir elementos digitais por alternativas em papel ou baseadas em discussões quando o acesso a dispositivos for limitado.

Esta flexibilidade é importante porque diferentes grupos aprendem de maneiras diferentes, e nem todos os participantes têm as mesmas experiências, confiança ou hábitos digitais. Um conjunto de ferramentas é mais útil quando pode ser ajustado sem perder a sua função principal.



COMO ESCOLHER A ATIVIDADE CERTA

Os utilizadores devem selecionar as atividades de acordo com o objetivo da sessão. Algumas atividades são mais adequadas para introduzir um tópico, enquanto outras são mais úteis para praticar a tomada de decisões, discutir situações online da vida real ou refletir sobre o comportamento digital pessoal.

O conjunto de ferramentas pode ser usado:

- para apresentar conceitos básicos de cibersegurança;
- para explorar um tópico específico, como phishing, burlas, privacidade, perfis falsos, segurança de palavras-passe ou desinformação;
- para incentivar o trabalho em equipa e a resolução de problemas;
- para apoiar a reflexão após um workshop ou laboratório para jovens;
- para complementar atividades mais amplas sobre cidadania digital, participação ou literacia mediática.

Escolher a atividade certa também significa ser realista quanto ao tempo, ao tamanho do grupo e à capacidade de atenção dos participantes. Muitas vezes, é melhor aproveitar bem uma atividade, com tempo suficiente para reflexão, do que realizar várias atividades à pressa, sem uma aprendizagem significativa.

Este guia deve ser usado como um recurso flexível e fácil de usar que apoia o planeamento e a execução da aprendizagem não formal em cibersegurança. Ajuda os utilizadores a identificar atividades adequadas, a compreender como elas são estruturadas e a adaptá-las a diferentes contextos e perfis de participantes. Ao combinar métodos práticos com temas digitais relevantes, proporciona experiências de aprendizagem envolventes e significativas que ajudam os jovens a compreender melhor os riscos online e a responder aos mesmos com mais confiança.



The background is a solid dark blue. On the left side, there is a large, light blue silhouette of a human head in profile, facing right. Inside the head, there are intricate white circuit-like patterns, including lines, dots, and concentric arcs, suggesting a neural or technological theme. In the top right corner, there are some faint, thin white lines forming a partial circular shape. In the middle right, there are some thin white lines forming a zigzag or circuit-like pattern. In the bottom right corner, there are some thin white lines forming a partial circular shape, similar to the one in the top right.

ATIVIDADES DE APRENDIZAGEM

ESCAP(E+): EDIÇÃO DA EQUIPA DE DETETIVES DA DESINFORMAÇÃO

OBJETIVOS DE APRENDIZAGEM

Objetivo 1	Desenvolver a capacidade de identificar informação errada e conteúdo enganoso.
Objetivo 2	Compreender como as informações podem ser verdadeiras, falsas ou tiradas de contexto.
Objetivo 3	Aprimorar o pensamento crítico, o trabalho em equipa e as competências de tomada de decisão.

GRUPO-ALVO

Público	Jovens (16-30 anos), técnicos de juventude e educadores
Conhecimento prévio	Experiência básica no uso de redes sociais e conteúdo online.

DURAÇÃO

Tempo total	90 minutos
Discriminação	Introdução: 15 min Atividade principal: 55-60 min Debriefing: 15-20 min

TAMANHO DO GRUPO

Mín. / Máx.	10-20
-------------	-------

MATERIAIS NECESSÁRIOS

Físico	Nenhum
Digital	Kahoot, telemóveis/computadores, ecrã/projetor https://kahoot.it/challenge/04208904?challenge_id=36d2f2fd-bdf0-447c-96fb-149651d2390a_1775577027740
Preparação	Criar um questionário no Kahoot. Preparar explicações. Selecionar perguntas-chave para discussão.

GUIA DE FACILITAÇÃO PASSO A PASSO

Etapa 1: Introdução (15 min) - Apresente o conceito de desinformação.

Explique as ideias principais:

- Nem toda a informação online é precisa.
- Alguns conteúdos são enganosos, e não completamente falsos.
- Importância de verificar a informação e pensar criticamente.

Etapa 2: Explicação da atividade (10 min) - Explique que os participantes farão um questionário gamificado usando o Kahoot. Para cada pergunta, devem:

- Decidir se o conteúdo é verdadeiro, falso ou enganoso.
- Responder dentro de um tempo limitado.
- Refletir sobre as suas escolhas.

Etapa 3: Questionário Kahoot (30-35 min) - Os participantes respondem a uma série de perguntas usando o Kahoot.

Para cada pergunta, os participantes devem:

- Analisar o conteúdo.
- Selecionar a resposta correta dentro do limite de tempo.

Cada questão segue o mesmo formato: os participantes devem decidir se o conteúdo é verdadeiro, falso ou enganoso.

Etapa 4: Revelação e discussão das respostas (20-25 min)

Após cada pergunta:

- Verifique a resposta correta exibida no Kahoot.
- Pergunte brevemente aos participantes por que razão escolheram essa resposta.
- Explique por que é que o conteúdo é verdadeiro, falso ou enganoso.

Para as questões previamente selecionadas, permita uma breve discussão para explorar o raciocínio com mais profundidade.

Destaque:

- O que torna o conteúdo credível?
- O que sinaliza a desinformação?

Etapa 5: Debriefing final (15-20 min) - Resuma os principais pontos de aprendizagem.

Discuta como os participantes podem:

- Verificar a informação.
- Evitar espalhar informações falsas.
- Aplicar essas competências no dia a dia.

PERGUNTAS PARA O DEBRIEFING

- 1 Qual foi o caso mais difícil de avaliar?
- 2 O que fazia com que certas informações parecessem credíveis?
- 3 Porque é que informações enganosas são perigosas?
- 4 De que forma o trabalho em equipa influenciou as suas decisões?
- 5 Que estratégias pode usar para verificar informações?

MENSAGENS PRINCIPAIS DE CIBERSEGURANÇA

- ✓ Mensagem principal 1: Nem toda a informação online é completamente verdadeira ou falsa.
- ✓ Mensagem-chave 2: Alguns conteúdos são enganosos ou foram retirados do contexto.
- ✓ Mensagem-chave 3: Verifique sempre as fontes e confirme as informações.
- ✓ Mensagem-chave 4: Pense criticamente antes de partilhar conteúdo.

ESCAP(E+): ARMADILHA DIGITAL - ESCAPE DA BURLA!

OBJETIVOS DE APRENDIZAGEM

Objetivo 1	Desenvolva a capacidade de identificar táticas comuns de burlas online.
Objetivo 2	Entenda como as burlas usam a urgência, a manipulação e o engano.
Objetivo 3	Aprimore o pensamento crítico e a tomada de decisões seguras online.

GRUPO-ALVO

Público	Jovens (16-30 anos), técnicos de juventude e educadores
Conhecimento prévio	Conhecimento básico de redes sociais e comunicação online.

DURAÇÃO

Tempo total	90 minutos
Discriminação	Introdução: 15 min Atividade principal: 55-60 min Debriefing: 15-20 min

TAMANHO DO GRUPO

Mín. / Máx.	10-20
-------------	-------

MATERIAIS NECESSÁRIOS

Físico	Nenhum
Digital	Computador portátil, projetor e formulários do Google (sala de fuga)
Preparação	Crie e teste a sala de fuga do Google Forms. Configure as secções e a navegação baseada em respostas (corretas/incorrectas). Prepare as instruções para os participantes. Prepare perguntas para discussão posterior.

GUIA DE FACILITAÇÃO PASSO A PASSO

Etapa 1: Introdução (15 min) - Apresente o tema das burlas online.

Explique brevemente os conceitos-chave:

- Burlas online
- Urgência e manipulação
- Sites falsos e ofertas enganosas

Envolve os participantes perguntando sobre as suas experiências com burlas.

Etapa 2: Explicação da atividade (5 min) - Apresente a sala de fuga como uma missão.

Explique que os participantes devem:

- Completar os desafios.
- Responder corretamente para prosseguir.
- Identificar táticas de burla.

Etapa 3: Atividade de sala de fuga (15-20 min) - Os participantes completam individualmente o formulário do Google para a sala de fuga.

Enfrentam diferentes desafios relacionados com:

- Mensagens de burla.
- Sites falsos.
- Ofertas enganosas.
- Segurança de dados pessoais.

Etapa 4: Discussão em grupo (20-25 min) - Analise os desafios com o grupo. Peça aos participantes que expliquem as suas respostas e o seu raciocínio.

Destaque as principais táticas de burlas:

- Urgência.
- Manipulação emocional.
- Informações enganosas.

Etapa 5: Atividade em grupo - criar um desafio de burla (20-25 min) - Divida os participantes em pequenos grupos. Cada grupo cria um pequeno cenário de burla e transforma-o num minidesafio (semelhante a uma sala de fuga).

Devem incluir:

- Uma situação curta.
- Uma pergunta.
- Múltiplas opções.

Os grupos apresentam o seu desafio e os outros grupos tentam identificar a burla.

PERGUNTAS PARA O DEBRIEFING

- 1 Qual foi o desafio mais difícil e porquê?
- 2 Qual tática de burla achou mais convincente?
- 3 Porque é que as pessoas caem em burlas online?
- 4 O que fará de diferente após esta atividade?
- 5 Como pode ajudar outras pessoas a manterem-se seguras online?

MENSAGENS PRINCIPAIS DE CIBERSEGURANÇA

- ✓ Mensagem principal 1: Burlas online frequentemente parecem realistas e confiáveis.
- ✓ Mensagem-chave 2: A urgência e a pressão emocional são táticas comuns de manipulação.
- ✓ Mensagem-chave 3: Verifiquem sempre links, fontes e solicitações de dados pessoais.
- ✓ Mensagem principal 4: Pense antes de clicar e proteja as suas informações pessoais.

ESCAP(E+): CONFIANÇA OU ARMADILHA? - INVESTIGAÇÃO DE PERFIL FALSO

OBJETIVOS DE APRENDIZAGEM

Objetivo 1	Desenvolva a capacidade de identificar perfis falsos nas redes sociais.
Objetivo 2	Entenda os sinais comuns de engano e falsificação de identidade online.
Objetivo 3	Aprimore suas competências de tomada de decisão e pensamento crítico online.

GRUPO-ALVO

Público	Jovens (16-30 anos), técnicos de juventude e educadores
Conhecimento prévio	Experiência básica no uso de plataformas de redes sociais

DURAÇÃO

Tempo total	90 minutos
Discriminação	Introdução: 15 min Atividade principal: 55-60 min Debriefing: 15-20 min

TAMANHO DO GRUPO

Mín. / Máx.	10-20
-------------	-------

MATERIAIS NECESSÁRIOS

Físico	Nenhum
Digital	<i>Opcional: computador portátil, projetor ou slides para apresentar cenários.</i>
Preparação	Prepare cenários de perfis falsos. Prepare perguntas orientadoras para discussão. Prepare exemplos visuais de perfis falsos (opcional).

GUIA DE FACILITAÇÃO PASSO A PASSO

Etapa 1: Introdução (15 min) - Apresente o tema dos perfis falsos nas redes sociais. Explique os conceitos-chave:

- Perfis falsos.
- Representação.
- Riscos online (burlas, manipulação, roubo de dados).

Etapa 2: Explicação da atividade (5 min) - Explique que os participantes analisarão diferentes situações e decidirão o que fazer. Devem:

- Identificar elementos suspeitos.
- Tomar uma decisão.
- Explicar o seu raciocínio.

Etapa 3: Análise de Cenários (30-35 min) - Apresente cenários de perfis fictícios, um de cada vez. Os participantes devem:

- Analisar a situação.
- Decidir o que fariam.
- Discutir em pares ou pequenos grupos.

Incentive os participantes a justificarem as suas decisões.

Etapa 4: Discussão em grupo (20-25 min) - Discuta cada cenário com todo o grupo. Pergunte:

- Quais são os sinais de alerta?
- O que verificariam?
- Porque é que isso é arriscado?

Etapa 5: Debriefing final (15-20 min) - Resuma os principais pontos de aprendizagem e relacione-os com o comportamento na vida real. Discuta como os participantes se podem proteger de perfis falsos.

Cenários

Cenário 1: Pedido de seguimento suspeito

Recebe pedido para seguir de um perfil com:

- Pouquíssimas fotos.
- Sem biografia.
- Conta criada recentemente.

O que faria? Porquê?

Cenário 2: Mensagem desconhecida

Um perfil envia-lhe uma mensagem: “Olá, acho que já nos encontramos antes. Pode ajudar-me com uma coisa?” Como responderia?

Cenário 3: Perfil profissional, mas suspeito

Um perfil parece profissional, mas:

- As imagens parecem fotos de banco de imagens.
- Tem interação muito baixa.

Este perfil é confiável? Porquê?

Cenário 4: Migração para outra plataforma

Alguém lhe pede para continuar a conversa no WhatsApp ou no Telegram. Porque é que isso poderia ser arriscado?

PERGUNTAS PARA O DEBRIEFING

- 1 O que te deixou desconfiado(a) nos perfis?
- 2 Qual cenário foi o mais difícil de avaliar?
- 3 Porque é que as pessoas confiam em perfis falsos?
- 4 O que verificaria antes de confiar num perfil?
- 5 Como pode proteger-se online?

MENSAGENS PRINCIPAIS DE CIBERSEGURANÇA

- ✓ Mensagem principal 1: Perfis falsos podem parecer realistas e confiáveis.
- ✓ Mensagem principal 2: Nem todas as interações online são seguras ou genuínas.
- ✓ Mensagem-chave 3: Verifique sempre os perfis antes de interagir.
- ✓ Mensagem principal 4: Seja cauteloso ao partilhar informações pessoais.

ESCAP(E+): VIRAL OU MANIPULADO? INTERPRETAÇÃO DE PAPÉIS NAS REDES SOCIAIS

OBJETIVOS DE APRENDIZAGEM

Objetivo 1	Compreenda como o conteúdo das redes sociais pode influenciar opiniões e comportamentos.
Objetivo 2	Identifique táticas comuns de manipulação (clickbait, conteúdo emocional, desinformação).
Objetivo 3	Desenvolva o pensamento crítico ao interagir com conteúdo viral.

GRUPO-ALVO

Público	Jovens (16-30 anos), técnicos de juventude e educadores
Conhecimento prévio	Experiência básica no uso de plataformas de redes sociais

DURAÇÃO

Tempo total	90 minutos
Discriminação	Introdução: 15 min Atividade principal: 60 min Debriefing: 15 min

TAMANHO DO GRUPO

Mín. / Máx.	10-20
-------------	-------

MATERIAIS NECESSÁRIOS

Físico	Nenhum
Digital	Nenhum (uso opcional de telemóveis, caso os participantes queiram simular o uso de redes sociais)
Preparação	Prepare cenários para dramatização. Atribua papéis a cada grupo.

GUIA DE FACILITAÇÃO PASSO A PASSO

Etapa 1: Introdução (15 min) - Apresente o tema da manipulação nas redes sociais.

Explique brevemente os conceitos-chave:

Conteúdo viral.

Manipulação.

Influência emocional.

Etapa 2: Explicação da atividade (5 min) - Explique a dramatização e os objetivos.

Divida os participantes em grupos de 3 e atribua-lhes funções:

Criador de conteúdo, utilizador e observador.

Etapa 3: Distribuição do cenário (5 min) - Dê a cada grupo um cenário e certifique-se de que os participantes compreendem a tarefa: criar uma breve interação nas redes sociais que inclua manipulação.

Etapa 4: Preparação da dramatização (15 min) - Os grupos preparam a sua dramatização.

Devem:

Criar uma publicação curta.

Incluir uma tática de manipulação.

Preparar uma interação curta.

Etapa 5: Dramatização (25 min) - Cada grupo realiza a sua dramatização (1 a 2 minutos cada). Os outros participantes observam e identificam as táticas de manipulação utilizadas.

Etapa 6: Análise em grupo (10-15 min) - Após cada apresentação, pergunte:

Qual é a tática de manipulação?

Porque é que isso é enganoso?

Etapa 7: Debriefing final (15 min) - Facilite a reflexão e relacione-a com o comportamento real nas redes sociais.

Cenários

Cenário 1: Clickbait

Uma publicação é elaborada para atrair atenção através de um título exagerado ou enganoso. O objetivo é criar uma interação breve em que o conteúdo utilize uma mensagem dramática ou exagerada para levar as pessoas a clicarem ou reagirem.

Cenário 2: Manipulação emocional

Uma publicação é disseminada online com o objetivo de provocar fortes emoções nas pessoas e influenciar as suas reações. A tarefa é criar uma breve interação em que o conteúdo utilize medo, raiva ou compaixão para levar as pessoas a acreditarem na publicação e/ou a partilhá-la.

Cenário 3: Informações enganosas

Uma publicação partilha informações parcialmente verdadeiras, mas apresentadas de forma enganosa. A tarefa é criar uma breve interação em que o conteúdo inclua informações incompletas ou distorcidas.

Cenário 4: Promoção por influenciadores

Um influenciador promove um produto ou ideia sem explicar claramente todos os detalhes. O objetivo é criar uma interação curta em que o público seja influenciado sem total transparência.

PERGUNTAS PARA O DEBRIEFING

- 1 Qual foi o papel mais desafiador e por quê?
- 2 Qual tática de manipulação foi a mais convincente?
- 3 Como foi a sensação de ser influenciado ou de influenciar outras pessoas?
- 4 Porque é que o conteúdo manipulado se espalha tão facilmente?
- 5 Como pode proteger-se online?

MENSAGENS PRINCIPAIS DE CIBERSEGURANÇA

- ✓ Mensagem principal 1: Nem tudo que viraliza é verdade.
- ✓ Mensagem-chave 2: O conteúdo das redes sociais é frequentemente concebido para influenciar o comportamento.
- ✓ Mensagem-chave 3: O conteúdo emocional espalha-se mais rapidamente e é mais persuasivo.
- ✓ Mensagem-chave 4: O pensamento crítico é essencial ao consumir conteúdo online.

ESCAP(E+): PRESO OU NÃO?

DESAFIO DE RESOLUÇÃO DE PROBLEMAS DE PHISHING

OBJETIVOS DE APRENDIZAGEM

Objetivo 1	Desenvolva a capacidade de identificar tentativas de phishing em emails, SMS e redes sociais.
Objetivo 2	Compreenda as técnicas que os atacantes usam para enganar as vítimas, incluindo urgência, falsificação de identidade e engenharia social.
Objetivo 3	Aplique estratégias práticas para verificar mensagens suspeitas e proteger dados pessoais.

GRUPO-ALVO

Público	Jovens dos 16 aos 30 anos, técnicos de juventude e educadores.
Conhecimento prévio	Experiência básica no uso de email, aplicações de mensagens e plataformas de redes sociais.

DURAÇÃO

Tempo total	90 minutos
Discriminação	Introdução: 15 min Atividade principal: 55–60 min Debriefing: 15–20 min

TAMANHO DO GRUPO

Mín. / Máx.	10 a 20 participantes (a trabalhar em pequenos grupos de 3 a 5 pessoas)
-------------	---

MATERIAIS NECESSÁRIOS

Físico	Cartões de cenário impressos (um conjunto por grupo), flipchart ou quadro branco para anotações do grupo, marcadores e notas adesivas para votação.
Digital	Computador portátil e projetor para apresentar cenários (opcional), slides de apresentação com vocabulário-chave e recursos visuais dos mesmos.
Preparação	Imprima cartões com cenários para cada grupo. Prepare uma breve apresentação introdutória sobre conceitos de phishing. Elabore perguntas orientadoras para cada cenário. Familiarize-se com os cenários e os seus respectivos sinais de alerta para que possa conduzir as discussões com segurança.

GUIA DE FACILITAÇÃO PASSO A PASSO

Etapa 1: Introdução (15 min)

Introduza o tema do phishing. Explique que o phishing é uma das ameaças cibernéticas mais comuns e que qualquer pessoa pode ser alvo.

Pergunte ao grupo: "Alguém já recebeu um email ou mensagem suspeita? O que fez com que parecesse estranho?"

Use as respostas para iniciar a discussão sem constranger ninguém. Explique brevemente os conceitos-chave:

Phishing – uma tentativa fraudulenta de obter informações confidenciais fingindo ser uma fonte de confiança.

Spear phishing – um ataque de phishing direcionado a uma pessoa ou organização específica.

Smishing – phishing através de mensagens de texto SMS.

Vishing – phishing através de chamadas de voz.

Engenharia social – manipulação de pessoas para obter informações confidenciais.

Etapa 2: Explicação da atividade (5 min)

Explique que os participantes trabalharão em pequenos grupos para analisar cenários realistas de phishing. Para cada cenário, devem: identificar os sinais de alerta e elementos suspeitos, decidir que ações tomariam e preparar uma breve explicação do seu raciocínio para partilhar com todo o grupo. Divida os participantes em grupos de 3 a 5 pessoas e distribua um cartão com um cenário a cada grupo.

Etapa 3: Análise de Cenários (30–35 min)

Os grupos analisam os cenários que lhes foram atribuídos. O facilitador circula entre os grupos para fornecer orientação e fazer perguntas exploratórias.

Após 15 minutos, os grupos trocam os cartões de cenário para que cada grupo analise pelo menos dois cenários diferentes.

Cenários:

Cenário 1 (email urgente do banco): Recebe um email do “seu banco” a informar que a sua conta foi comprometida. O email pede que clique num link e verifique a sua identidade imediatamente, caso contrário, a sua conta será bloqueada. O endereço de email é support@b4nk-secure.com. O link leva a b4nk-secure.com/verify. Sinais de alerta: domínio com erro ortográfico, urgência, saudação genérica.

Cenário 2 (SMS de prémio): Recebe uma mensagem de texto: “Ganhou um vale-presente de 500 euros. Resgate-o agora em bit.ly/fr33prize. A oferta expira dentro de 1 hora!” Sinais de alerta: prémio não solicitado, URL encurtada, pressão de tempo, demasiado bom para ser verdade.

Cenário 3 (Pedido de Amizade nas Redes Sociais): Recebe uma mensagem da conta de um amigo a dizer: “Olá, és tu neste vídeo? Parece muito constrangedor!” com um link. Ao verificar, o perfil do seu amigo parece um pouco diferente e foi criado recentemente. Sinais de alerta: apelo emocional, link suspeito, conta clonada.

Cenário 4 (Email de Oferta de Emprego): Recebe um email com uma oferta de emprego remoto com um salário alto. O nome da empresa parece legítimo, mas o email solicita que forneça o seu documento de identidade, dados bancários e uma “taxa de processamento” antes de começar. Sinais de alerta: solicitação de dados pessoais/financeiros antecipadamente, taxa de processamento, oferta de emprego não solicitada.

Cenário 5 (Pedido do Departamento de TI): Recebe um email do “Suporte de TI” da sua escola ou local de trabalho a solicitar que atualize a sua palavra-passe clicando num link. O endereço do remetente é it-support@yourschool.mail-update.com. Sinais de alerta: truque do subdomínio, urgência, link para domínio externo em vez do site oficial.

Etapa 4: Apresentações e Discussão em Grupo (20–25 min)

Cada grupo apresenta a sua análise de cenário a todo o grupo (2 a 3 minutos por grupo). Após cada apresentação, o facilitador pergunta: Quais são os principais sinais de alerta? O que faria nessa situação?

Que informações estava o atacante a tentar obter? Incentive outros grupos a acrescentarem observações. Destaque padrões comuns entre os cenários: urgência, falsificação de identidade, gatilhos emocionais e pedidos de informações confidenciais.

Etapa 5: Debriefing final (15–20 min)

Resuma os principais pontos de aprendizagem de todos os cenários. Discuta medidas práticas que os participantes podem tomar: verificar sempre cuidadosamente o endereço do remetente, nunca clicar em links em mensagens não solicitadas, contactar as organizações diretamente através dos canais oficiais, ativar a autenticação de dois fatores e denunciar mensagens suspeitas. Relacione a aprendizagem com o comportamento na vida real e peça aos participantes que partilhem uma ação que irão realizar após a sessão.

PERGUNTAS PARA O DEBRIEFING

- 1 Qual cenário de phishing foi o mais convincente e por quê?
- 2 Quais foram os sinais de alerta mais difíceis de identificar?
- 3 Você ou alguém que conhece já caiu numa burla de phishing? O que aconteceu?
- 4 Porque é que os ataques de phishing continuam a ser tão eficazes apesar das campanhas de Consciencialização?
- 5 Que medidas específicas tomará para se proteger contra phishing no futuro?

MENSAGENS PRINCIPAIS DE CIBERSEGURANÇA

- ✓ Mensagem principal 1: O phishing é a forma mais comum de ciberataque e atinge a todos – ninguém está imune, independentemente da idade ou competência técnica.
- ✓ Mensagem-chave 2: Os atacantes exploram a urgência, o medo e a confiança para enganar as pessoas e levá-las a revelar informações confidenciais. Reconhecer esses gatilhos emocionais é a primeira linha de defesa.
- ✓ Mensagem-chave 3: Nunca clique em links nem forneça informações pessoais em resposta a mensagens não solicitadas. Verifique sempre através de canais oficiais.
- ✓ Mensagem principal 4: Denunciar mensagens suspeitas ajuda a proteger não só você, mas toda a sua comunidade. Na dúvida, pare, pense e verifique.

ESCAP(E+): TESTE DE MANIPULAÇÃO DE REDES SOCIAIS - SCROLL CONSCIENTE

OBJETIVOS DE APRENDIZAGEM

Objetivo 1	Reconheça táticas comuns de manipulação nas redes sociais, como clickbait, exploração emocional e envolvimento falso.
Objetivo 2	Compreenda como os algoritmos e o comportamento do utilizador contribuem para a disseminação de conteúdo manipulador online.
Objetivo 3	Desenvolva o pensamento crítico, o trabalho em equipa e as competências de tomada de decisão ao interagir com conteúdo de redes sociais.

GRUPO-ALVO

Público	Jovens dos 16 aos 30 anos, técnicos de juventude e educadores.
Conhecimento prévio	Experiência básica no uso de plataformas de redes sociais (ex.: Instagram, TikTok, X/Twitter, Facebook).

DURAÇÃO

Tempo total	90 minutos
Discriminação	Introdução: 15 min Quiz: 50 min (3 rondas) Debriefing: 25 min

TAMANHO DO GRUPO

Mín. / Máx.	10 a 30 participantes (podem jogar individualmente ou em equipas de 2 a 4 pessoas)
--------------------	--

MATERIAIS NECESSÁRIOS

Físico	Quadro branco ou flipchart para anotações durante o debriefing, cartões impressos com perguntas de reserva (em caso de problemas técnicos).
Digital	O facilitador utiliza um portátil ou tablet ligado a um projetor ou ecrã grande. Os participantes usam telemóveis ou dispositivos com acesso à internet (um por participante ou por equipa). Plataforma: Kahoot! (kahoot.com) – conta gratuita. Os participantes acedem ao site kahoot.it ou a aplicação Kahoot! usando um PIN do jogo.

Preparação

Crie uma conta gratuita no Kahoot! em kahoot.com. Elabore o quiz usando as perguntas e opções de resposta fornecidas no guia de facilitação abaixo. Defina o tempo de cada pergunta para 20 segundos para perguntas padrão e 30 segundos para perguntas baseadas em cenários. Faça um teste no seu próprio dispositivo para confirmar se o sistema de PIN do jogo funciona. Prepare um slide com a agenda da sessão e o vocabulário-chave (clickbait, algoritmo, bot, manipulação emocional, astroturfing). Se o acesso à internet for instável, prepare cartões com perguntas alternativas impressas.

GUIA DE FACILITAÇÃO PASSO A PASSO

Etapa 1: Introdução (15 min) – Apresente a sessão aos participantes e contextualize-a: as redes sociais são uma ferramenta poderosa, mas também são usadas para manipular opiniões, emoções e comportamentos, muitas vezes sem que nos apercebamos disso.

Pergunte ao grupo: “Já partilharam uma publicação e depois descobriram que ela era enganosa? O que a tornou convincente?” Use as respostas para gerar curiosidade sem constranger ninguém.

Explique brevemente a estrutura: três rondas de perguntas e respostas com uma tabela de classificação competitiva, seguidas de uma sessão de discussão em grupo.

Vocabulário essencial para apresentar rapidamente (2 minutos):

- Clickbait – conteúdo criado para atrair cliques usando títulos exagerados ou enganosos.
- Algoritmo – um sistema que decide que conteúdo vê com base no seu comportamento.
- Conta bot/falsa – perfis automatizados ou falsos usados para amplificar conteúdo ou opiniões.
- Manipulação emocional – conteúdo criado para desencadear sentimentos fortes e influenciar reações.
- Astroturfing – fazer uma campanha manipulada parecer um movimento popular.

Etapa 2: Entrar no jogo (5 min) – Mostre o PIN do jogo no ecrã. Peça aos participantes que abram o kahoot.it nos seus telemóveis (ou a aplicação Kahoot) e insiram o PIN. Devem escolher um apelido (para si mesmos ou para a equipa). Se estiverem a jogar em equipas, divida-as em grupos e peça a uma pessoa de cada equipa que entre em nome do grupo.

Etapa 3: Ronda 1 – Questionário de aquecimento (15 min, 5 perguntas) – Inicie a Ronda 1 no Kahoot.

Estas perguntas introduzem conhecimentos básicos de forma lúdica e sem pressão. Após cada pergunta, o Kahoot revela automaticamente a resposta correta.

GUIA DE FACILITAÇÃO PASSO A PASSO

Após cada pergunta, reserve 30 segundos para explicar brevemente o motivo – especialmente para respostas incorretas que revelem equívocos comuns.

Perguntas da Ronda 1:

Q1. O que é "clickbait"?

(a) Um tipo de vírus de computador | (b) Conteúdo com títulos exagerados criado para gerar cliques | (c) Uma configuração de privacidade em redes sociais | (d) Uma ferramenta para bloquear anúncios

→ Correto: B

Q2. Qual das seguintes opções é um sinal de que uma conta de redes sociais pode ser falsa?

(a) Possui foto de perfil | (b) Foi criada recentemente, tem poucos seguidores e publica conteúdo repetitivo | (c) Segue celebridades | (d) Usa hashtags

→ Correto: B

Q3. Porque é que o conteúdo com forte carga emocional se espalha mais rapidamente nas redes sociais?

(a) É sempre mais preciso | (b) Os algoritmos priorizam conteúdo que gera reações fortes | (c) Apenas pessoas emotivas usam redes sociais | (d) É promovido por governos

→ Correto: B

Q4. Verdadeiro ou falso: Se uma publicação tem milhares de gostos e partilhas, as informações nela contidas devem ser verdadeiras.

(a) Verdadeiro | (b) Falso

→ Correto: B

Q5. O que é "astroturfing" no contexto das redes sociais?

(a) Uma tendência de jardinagem popular no Instagram | (b) Criar a falsa impressão de que uma campanha tem amplo apoio popular | (c) Usar filtros verdes em fotos | (d) Plantar árvores como parte de um desafio online

→ Correto: B

Etapa 4: Ronda 2 – Questionário de Cenários (20 min, 5 perguntas) – Estas perguntas apresentam situações realistas. Os participantes devem aplicar o que aprenderam, em vez de apenas lembrar um facto. Defina o cronómetro para 30 segundos.

Após cada cenário, dedique até um minuto à discussão.

Antes de confirmar, peça ao participante que tenha acertado para explicar o seu raciocínio.

Perguntas da Ronda 2 (baseadas em cenários):

Q6. A Lena vê uma publicação com a seguinte mensagem: “ÚLTIMA HORA: Uma grande cidade europeia proíbe o uso de todas as redes sociais para menores de 18 anos”. A publicação não possui link para a fonte e usa linguagem dramática. O que deve fazer?

- (a) Partilhar imediatamente para alertar os seus amigos | (b) Comentar a perguntar se é verdade | (c) Procurar a notícia em sites de confiança antes de reagir | (d) Denunciar a publicação como spam

→ Correto: C

Q7. Marco percebe que uma hashtag em alta está a ser usada por centenas de contas que publicam a mesma mensagem, foram criadas na mesma semana e não têm fotos pessoais. O que provavelmente está a acontecer?

- (a) Um novo desafio popular | (b) Uma campanha coordenada de bots para manipular a opinião pública | (c) Uma falha na plataforma | (d) Uma estratégia de marketing de uma marca conhecida

→ Correto: B

Q8. Sofia segue uma influenciadora que publica sobre um “suplemento milagroso para a saúde”. A influenciadora não revela que está a ser paga pela publicação. Que tática de manipulação está a ser usada?

- (a) Clickbait | (b) Manipulação emocional | (c) Conteúdo patrocinado oculto / publicidade não divulgada | (d) Phishing

→ Correto: C

Q9. Um vídeo viral mostra um político a dizer algo ultrajante. O clipe tem apenas 10 segundos de duração e termina abruptamente no meio da frase. O que deve considerar?

- (a) Políticos dizem sempre coisas absurdas, por isso deve ser verdade | (b) O vídeo pode ter sido retirado do contexto ou editado para mudar o significado | (c) Se viralizou, deve ser verdade | (d) Vídeos curtos são sempre mais fiáveis

→ Correto: B

Q10. Durante a época eleitoral, Amir vê uma publicação emotiva sobre um candidato que inclui estatísticas chocantes, mas sem fonte. Percebe que a publicação é partilhada principalmente por contas sem conteúdo pessoal. Que combinação de táticas de manipulação está em jogo?

- (a) Clickbait e astroturfing | (b) Manipulação emocional e comportamento inautêntico coordenado | (c) Phishing e roubo de identidade | (d) Spam e hacking

→ Correto: B

Etapas 5: Ronda de Desafio e Debriefing (25 min) – A ronda de desafio apresenta perguntas mais difíceis e um tempo limite mais curto (15 segundos). Estas foram elaboradas para desafiar os participantes que acharam as rondas anteriores fáceis. O facilitador deve aumentar a tensão, anunciando que os pontos serão dobrados nesta ronda.

Perguntas da Ronda de Desafio:

Q11. O algoritmo de uma plataforma de redes sociais tem maior probabilidade de mostrar conteúdo que:

(a) É o mais factualmente preciso | (b) Mantém o utilizador a fazer scroll, combinando com os seus interesses e gatilhos emocionais existentes | (c) É o mais recente | (d) Foi verificado por verificadores de factos → Correto: B

Q12. Qual das seguintes opções é a MELHOR estratégia para se proteger da manipulação nas redes sociais?

(a) Seguir apenas contas com muitos seguidores | (b) Verificar informações com múltiplas fontes de confiança, questionar reações emocionais e verificar antes de partilhar | (c) Evitar completamente as redes sociais | (d) Ler apenas conteúdo de pessoas que conhece pessoalmente → Correto: B

Q13. Um amigo envia-lhe um link para uma petição a dizer “Assine agora – 1 milhão de pessoas já assinaram!”. O site parece não ser oficial, pede dados pessoais e a causa é descrita de forma vaga. Qual é o risco mais provável?

(a) É uma campanha legítima | (b) É um esquema de recolha de dados que utiliza pressão social para obter informações pessoais | (c) É uma pesquisa governamental | (d) É um projeto escolar → Correto: B

Exiba a classificação final do Kahoot. Mencione brevemente os melhores classificados. Em seguida, faça a transição para o debriefing: afaste-se do formato do jogo e convide à reflexão. Use as perguntas de debriefing abaixo.

PERGUNTAS PARA O DEBRIEFING

- | | |
|---|--|
| 1 | Qual pergunta mais o surpreendeu e o que aprendeu com ela? |
| 2 | Já foi influenciado por conteúdo manipulador sem perceber? O que o tornou convincente? |
| 3 | Porque é que o conteúdo manipulador se espalha tão facilmente nas redes sociais? Qual o papel dos algoritmos nesse processo? |
| 4 | De que forma o trabalho em equipa influenciou as suas decisões? Mudou de ideia depois de discutir com outras pessoas? |
| 5 | Qual é um hábito específico que irá mudar ao consumir ou partilhar conteúdo nas redes sociais? |

MENSAGENS PRINCIPAIS DE CIBERSEGURANÇA

- ✓ Mensagem principal 1: Nem tudo que viraliza é verdade. O conteúdo das redes sociais é frequentemente criado para despertar emoções e gerar envolvimento, não para informar.
- ✓ Mensagem principal 2: Técnicas de manipulação como clickbait, contas falsas, exploração emocional e astroturfing são generalizadas e muitas vezes difíceis de detetar sem pensamento crítico.
- ✓ Mensagem-chave 3: Sempre verifique as informações consultando diversas fontes confiáveis antes de acreditar ou partilhar qualquer conteúdo. Pare, questione e verifique.
- ✓ Mensagem principal 4: Compreender como os algoritmos funcionam permite ter mais controlo sobre o seu feed e tomar decisões mais informadas sobre o conteúdo que consome e partilha.

QUEM É O DONO DOS SEUS DADOS? (ESTUDO DE CASO SOBRE PRIVACIDADE DE DADOS)

OBJETIVOS DE APRENDIZAGEM

Objetivo 1	Compreender como os dados pessoais são recolhidos, armazenados e usados por plataformas online e aplicações móveis.
Objetivo 2	Identificar cenários em que a privacidade pessoal pode ser comprometida sem o conhecimento do utilizador.
Objetivo 3	Desenvolver estratégias práticas para proteger dados pessoais no dia a dia digital.

GRUPO-ALVO

Público	Jovens dos 16 aos 25 anos, técnicos de juventude e educadores.
Conhecimento prévio	Conhecimento básico de telemóveis e plataformas de redes sociais. Não é necessário conhecimento técnico prévio.

DURAÇÃO

Tempo total	90 minutos
Discriminação	Introdução: 15 min Atividade principal: 60 min Debriefing: 15 min

TAMANHO DO GRUPO

Mín. / Máx.	10 a 30 participantes
-------------	-----------------------

MATERIAIS NECESSÁRIOS

Físico	Fichas de estudo de caso impressas (um conjunto por grupo), notas adesivas, marcadores, flipchart ou quadro branco.
Digital	Computador portátil ou projetor para apresentar instruções e avisos (uso opcional). Os participantes podem usar os seus telemóveis para consultar políticas de privacidade reais.
Preparação	Prepare e imprima os quatro cartões de estudo de caso (um para cada pequeno grupo). Escreva os tópicos de discussão num gráfico ou prepare um slide. Familiarize-se com cada cenário do estudo de caso antes da sessão.

GUIA DE FACILITAÇÃO PASSO A PASSO

Etapa 1: Introdução (15 min) - Comece com uma breve provocação: peça aos participantes que levantem a mão se já leram alguma vez uma política de privacidade ou os termos de serviço completos. Use a resposta (geralmente muito baixa) para orientar a discussão. Explique brevemente o conceito de privacidade de dados e por que razão é importante para os jovens online. Apresente os termos-chave:

- Dados pessoais (nome, localização, hábitos de navegação, contactos)
- Recolha de dados (que aplicações recolhem dados e porquê)
- Partilha com terceiros (quem mais recebe os seus dados)
- Os seus direitos como utilizador (direito de acesso, eliminação e revogação do consentimento)

Etapa 2: Explicação da atividade (5 min) - Divida os participantes em quatro grupos. Explique que cada grupo receberá um estudo de caso diferente, baseado num cenário real. A tarefa do grupo é ler o caso, discuti-lo e responder às perguntas orientadoras presentes no cartão. Em seguida, cada grupo apresentará as suas conclusões ao restante grupo.

Etapa 3: Análise do estudo de caso (25 min) - Distribua um cartão com o estudo de caso por cada grupo. Permita que os grupos leiam e discutam individualmente. Incentive-os a usar as suas próprias experiências. O facilitador circula pela sala para estimular uma reflexão mais profunda, sem revelar as respostas.

Etapa 4: Apresentações em grupo (15 min) - Cada grupo apresenta o seu caso (2 a 3 minutos cada) e partilha o que mais o surpreendeu. Os outros participantes podem reagir ou acrescentar ligações com as suas próprias experiências após cada apresentação.

Etapa 5: Ligação entre os casos (5 min) - Facilite uma breve comparação com todo o grupo: O que os quatro casos têm em comum? Que padrões os participantes observam sobre o fluxo de dados online?

Etapa 6: Debriefing (15 min) - Utilize as perguntas de debriefing abaixo. Encerre a pedir a cada participante que mencione uma ação concreta que irá tomar para proteger melhor os seus dados pessoais.

Estudos de caso

Caso 1: A aplicação gratuita que sabe tudo

Elif descarrega uma aplicação gratuita de flashcards para estudar pouco antes dos exames da faculdade. Para se registar, clica em "Aceitar tudo" no ecrã de permissões sem ler. A aplicação solicita acesso ao seu microfone, contactos, localização e biblioteca de fotos. Três semanas depois, começa a receber anúncios direcionados de serviços de tutoria que nunca procurou, e uma amiga menciona ter recebido uma mensagem promocional "dela".

Sugestões para discussão: Que permissões concedeu Elif? Porque é que uma aplicação precisaria de aceder aos seus contactos ou microfone? Quem pode ter recebido os dados dela e porquê? O que poderia ela ter feito de diferente?

Caso 2: O login social

Mehmet regista-se num novo site de compras online usando o botão "Continuar com o Facebook" porque é mais rápido do que criar uma nova conta. Não repara no pequeno texto que explica que o site de compras terá acesso ao seu perfil público do Facebook, à sua lista de amigos e ao seu endereço de email. Ao longo do mês seguinte, o seu feed do Facebook enche-se de anúncios de produtos que visualizou no site de compras.

Tópicos para discussão: Que dados foram partilhados quando Mehmet clicou em "Continuar com o Facebook"? Quem beneficia dessa configuração e como? Isto representa um risco de segurança, um risco de privacidade ou ambos? Quais são as vantagens e desvantagens da conveniência em comparação com o controlo?

Caso 3: A violação de dados da qual nunca ouviu falar

Zeynep usa o mesmo email e a mesma palavra-passe para cinco contas online desde os 16 anos. Um dia, recebe um email de um remetente desconhecido com a sua palavra-passe no assunto. Mais tarde, descobre que um site menor, no qual se registou há dois anos, sofreu uma violação de dados e as suas credenciais foram vendidas na internet. Nunca recebeu nenhuma notificação oficial do site.

Tópicos para discussão: Como é que os dados de Zeynep acabaram em risco mesmo sem ela ter feito nada obviamente errado? Qual é o perigo de reutilizar palavras-passe em diferentes plataformas? As empresas têm a obrigação de informar os utilizadores quando os seus dados são comprometidos? O que faria se isso acontecesse consigo?

Caso 4: Dados de localização e o percurso que não partilhou

Deniz usa uma aplicação de mapas popular para navegação e mantém o acesso à localização sempre ativado por ser mais conveniente. Mais tarde, lê uma notícia que explica que a empresa responsável pela aplicação vende dados de localização anonimizados a terceiros, incluindo seguradoras e redes de retalho. Descobre também que as fotos do seu telemóvel contêm coordenadas de GPS e que, certa vez, partilhou acidentalmente a morada de casa ao publicar uma foto nas redes sociais.

Sugestões para discussão: Os dados de localização são sensíveis mesmo quando descritos como anonimizados? Quem poderia ter interesse em saber onde vai todos os dias e porquê? Que metadados ocultos podem conter as suas fotos? Como ajustaria as definições do seu telemóvel depois de saber isto?

PERGUNTAS PARA O DEBRIEFING

- 1 Qual estudo de caso pareceu mais semelhante a algo que o/a próprio/a ou alguém que conhece já vivenciou? O que lhe deu essa sensação de familiaridade?
- 2 Algum dos casos o/a surpreendeu? Quais pressupostos sobre privacidade digital esta atividade desafiou?
- 3 Quando as empresas recolham dados, isso é sempre prejudicial? Onde está a linha divisória entre um serviço útil e uma invasão de privacidade?
- 4 Quais são os seus direitos sobre os seus próprios dados? Acha que a maioria dos jovens conhece esses direitos?
- 5 Qual é uma mudança específica e realista que fará esta semana para proteger melhor os seus dados pessoais?

MENSAGENS PRINCIPAIS DE CIBERSEGURANÇA

- ✓ Mensagem principal 1: Os seus dados pessoais têm valor real. Trate cada pedido de permissão e formulário de inscrição como uma decisão, não como uma mera formalidade.
- ✓ Mensagem principal 2: Os serviços "gratuitos" são frequentemente financiados pelos seus dados. Compreender esta troca é o primeiro passo para fazer escolhas informadas online.
- ✓ Mensagem principal 3: Pequenos hábitos fazem grandes diferenças. Usar palavras-passe exclusivas, rever as permissões das aplicações e desativar o acesso desnecessário à localização reduzem significativamente a sua exposição a riscos relacionados com dados.
- ✓ Mensagem-chave 4: Tem direitos. De acordo com o quadro de proteção de dados, pode solicitar acesso, correção ou eliminação dos seus dados pessoais mantidos por organizações.

SUBA DE NÍVEL!

(QUESTIONÁRIO GAMIFICADO SOBRE SEGURANÇA DE SENHAS)

OBJETIVOS DE APRENDIZAGEM

Objetivo 1	Reconhecer as características de palavras-passe fortes e fracas e compreender por que a força da palavra-passe é importante.
Objetivo 2	Identificar ameaças comuns à segurança de palavras-passe, incluindo phishing e credential stuffing, etc.
Objetivo 3	Adotar boas práticas de palavras-passe, como usar padrões exclusivos, ativar a autenticação de dois fatores e considerar o uso de um gestor de palavras-passe.

GRUPO-ALVO

Público	Jovens dos 16 aos 25 anos, técnicos de juventude e educadores. O questionário é adequado para participantes com pouco conhecimento prévio em cibersegurança.
Conhecimento prévio	Não é necessário nenhum requisito. Familiaridade com telemóveis e contas online é suficiente.

DURAÇÃO

Tempo total	75 minutos
Discriminação	Introdução: 10 min Questionário: 45 min (3 partes) Debriefing: 20 min

TAMANHO DO GRUPO

Mín. / Máx.	10 a 30 participantes (podem jogar individualmente ou em equipas de 2 a 4 pessoas)
-------------	--

MATERIAIS NECESSÁRIOS

Físico	Quadro branco ou flipchart para anotações durante o debriefing, cartões impressos com perguntas de reserva (em caso de problemas técnicos).
--------	---

Digital	O facilitador utiliza um portátil ou tablet ligado a um projetor ou ecrã grande. Os participantes utilizam telemóveis ou dispositivos digitais com acesso à internet (um por participante ou por equipa). Plataforma: Kahoot! (kahoot.com) - conta gratuita. Os participantes podem entrar diretamente através do site kahoot.it ou da aplicação Kahoot usando um PIN do jogo.
Preparação	Crie uma conta gratuita no Kahoot! em kahoot.com. Elabore o quiz usando as perguntas e opções de resposta fornecidas no guia de facilitação abaixo. Defina o tempo de cada pergunta para 20 segundos para perguntas padrão e 30 segundos para perguntas baseadas em cenários. Faça um teste no seu próprio dispositivo para confirmar se o sistema de PIN do jogo funciona. Prepare um slide com a agenda da sessão e o vocabulário-chave (palavra-passe, força bruta, autenticação de dois fatores, gestor de palavras-passe). (Caso o acesso à internet seja instável no local do evento, prepare cartões com perguntas impressas como alternativa.)

GUIA DE FACILITAÇÃO PASSO A PASSO

Etapa 1: Introdução (10 min) - Dê as boas-vindas aos participantes e apresente o contexto da sessão: as palavras-passe são a primeira linha de defesa para quase todas as contas online, mas a maioria das pessoas tem hábitos que as colocam em sério risco. Pergunte ao grupo: 'Quantas palavras-passe têm? Reutilizam alguma delas?' Use as respostas para gerar curiosidade sem constranger ninguém. Explique brevemente a estrutura da sessão: três rondas de perguntas e respostas com um ranking competitivo, seguidas de uma discussão em grupo.

Vocabulário essencial para apresentar rapidamente (2 minutos):

- Ataque de força bruta – um programa que tenta milhares de combinações de palavras-passe por segundo.
- Phishing – uma mensagem ou site falso criado para roubar as suas credenciais.
- Credential stuffing – uso de pares de nome de utilizador/palavra-passe expostos numa violação de segurança para aceder a outras contas.
- Autenticação de dois fatores (2FA) – uma segunda etapa de verificação além da palavra-passe.
- Gestor de palavras-passe – uma aplicação encriptada que armazena e gera palavras-passe exclusivas.

Etapa 2: Entrar no jogo (5 min) - Mostre o PIN do jogo no ecrã. Peça aos participantes que abram o kahoot.it nos seus telemóveis (ou a aplicação Kahoot) e insiram o PIN. Devem escolher um apelido (para si mesmos ou para os seus respetivos grupos). Se estiverem a jogar em equipas, divida-as em equipas e peça a uma pessoa de cada equipa que entre em nome do grupo.)

Etapa 3: Ronda 1 – Quiz de aquecimento (15 min, 6 perguntas) - Inicie a Ronda 1 no Kahoot. Estas perguntas introduzem conhecimentos básicos de forma descontraída e divertida. Após cada pergunta, o Kahoot revela automaticamente a resposta correta. Reserve 30 segundos após cada pergunta para explicar brevemente o motivo da resposta – especialmente para respostas incorretas que revelem equívocos comuns. Não faça uma palestra; seja breve e informal.

Perguntas da Ronda 1

- Q1. Qual das seguintes palavras-passe é a mais forte? (a) password123 | (b) MyDog2010! | (c) Tr!4#bQz9@Lm | (d) qwerty → Correto: C
- Q2. Quantos caracteres deve ter, no mínimo, uma palavra-passe forte? (a) 6 | (b) 8 | (c) 12 | (d) 20 → Correto: C
- Q3. Qual destas opções torna uma palavra-passe mais fácil de quebrar? (a) Usar uma mistura de símbolos e números | (b) Usar a sua data de nascimento | (c) Usar mais de 15 caracteres | (d) Usar uma sequência gerada aleatoriamente → Correto: B
- Q4. Verdadeiro ou falso: Usar a mesma palavra-passe em várias contas é seguro, desde que a palavra-passe seja forte. (a) Verdadeiro | (b) Falso → Correto: B
- Q5. O que faz a autenticação de dois fatores (2FA)? (a) Dobra o comprimento da sua palavra-passe | (b) Adiciona uma segunda etapa de verificação após a sua palavra-passe | (c) Gera duas palavras-passe simultaneamente | (d) Permite o login em dois dispositivos ao mesmo tempo → Correto: B
- Q6. Qual NÃO é uma função de um gestor de palavras-passe? (a) Gerar palavras-passe fortes e exclusivas | (b) Armazenar palavras-passe de forma encriptada | (c) Partilhar as suas palavras-passe com contactos de confiança | (d) Preencher formulários de login automaticamente e com segurança → Correto: C

Etapa 4: Ronda 2 – Quiz de cenários (20 min, 5 perguntas) – Estas perguntas apresentam situações realistas. Os participantes devem aplicar o que aprenderam, em vez de simplesmente memorizar um facto. Defina um cronómetro para 30 segundos. Após cada cenário, reserve até um minuto para discussão. Peça a um participante que tenha acertado para explicar o seu raciocínio antes de confirmar a resposta.

Perguntas da Ronda 2 (baseadas em cenários)

- Q7. Selin recebe um email do 'Google Security' a pedir que verifique a sua palavra-passe imediatamente ou a sua conta será eliminada. O link no email parece ligeiramente diferente de google.com. O que deve fazer? (a) Clicar no link e verificar a sua palavra-passe rapidamente | (b) Ignorar o email e eliminá-lo | (c) Verificar o endereço do remetente, não clicar no link e aceder diretamente a google.com para verificar a sua conta | (d) Encaminhar o email para os seus amigos para os alertar → Correto: C

Q8. Ahmet usa 'istanbul2005' como palavra-passe para o seu email, Instagram e conta bancária. O seu fornecedor de email sofre uma violação de dados e as suas credenciais são expostas. Qual é a provável consequência? (a) Apenas o seu email está em risco | (b) Todas as três contas estão em risco porque a mesma palavra-passe foi reutilizada | (c) A sua conta bancária está segura porque os bancos têm melhor segurança | (d) Nada grave, já que a sua palavra-passe contém números → Correto: B

- Q9. Fatma quer criar uma palavra-passe de que se consiga lembrar. Qual método é o mais seguro? (a) O seu apelido de infância seguido do seu ano de nascimento | (b) Uma palavra-passe curta, mas complexa, como 'X@9!' | (c) Uma frase-palavra-passe longa com quatro palavras aleatórias, como 'orange-cloud-bicycle-17' | (d) O seu primeiro nome ao contrário, com letra maiúscula → Correto: C

- Q10. Murat tem a autenticação de dois fatores (2FA) ativada na sua conta via SMS. Um hacker consegue obter a sua palavra-passe. O hacker pode aceder à conta? (a) Sim, a palavra-passe é suficiente | (b) Não, porque a 2FA exige uma segunda etapa que apenas Murat controla | (c) Só se o hacker também souber o seu nome de utilizador | (d) Sim, os códigos SMS são fáceis de intercetar → Correto: B (Nota para o facilitador: reconheça brevemente que a 2FA baseada em SMS é melhor do que nada, mas as aplicações de autenticação são ainda mais seguras)

- Q11. Um site no qual Deniz se registou há anos envia um email a informar que os seus dados foram violados. A palavra-passe que usa para aceder a esse site é a mesma que usa para o seu email profissional. O que deve fazer primeiro? (a) Aguardar para ver se algo de mau acontece | (b) Alterar apenas a palavra-passe do site afetado | (c) Alterar imediatamente a palavra-passe de todas as contas que partilham a mesma palavra-passe | (d) Eliminar a sua conta no site afetado → Correto: C

Etapa 5: Ronda de Desafio (10 min, 3 perguntas) - A ronda de desafio apresenta perguntas mais difíceis e um tempo limite mais curto (15 segundos). Estas perguntas foram concebidas para desafiar os participantes que acharam as rondas anteriores fáceis e para gerar surpresa. O facilitador deve aumentar a tensão, anunciando que os pontos serão dobrados nesta ronda.

Perguntas da Ronda de Desafio

- Q12. Um ataque de força bruta tenta todas as combinações possíveis. Aproximadamente quanto tempo leva para quebrar uma palavra-passe de 8 caracteres, composta apenas por letras minúsculas, atualmente? (a) Vários anos | (b) Algumas semanas | (c) Algumas horas ou menos | (d) É impossível de quebrar → Correto: C (Computadores modernos podem tentar milhares de milhões de combinações por segundo; palavras-passe de 8 caracteres, compostas apenas por letras minúsculas, podem ser quebradas em minutos ou horas)

- Q13. Qual das seguintes práticas de palavra-passe oferece a maior proteção no mundo real? (a) Alterar a sua palavra-passe a cada 30 dias | (b) Usar uma palavra-passe única, gerada aleatoriamente, para cada conta, armazenada num gestor de palavras-passe, com autenticação de dois fatores (2FA) ativada | (c) Anotar as suas palavras-passe num caderno que guarda em casa | (d) Usar uma palavra-

Q14. Encontra um site que afirma verificar se a sua palavra-passe é forte. O site pede que introduza a sua palavra-passe real. O que deve fazer? (a) Usá-lo – é uma ferramenta de segurança útil | (b) Usá-lo apenas se o site parecer profissional | (c) Nunca introduzir a sua palavra-passe real em nenhum verificador de terceiros | (d) Usá-lo, mas alterar primeiro o último carácter → Correto: C

Etapa 6: Classificação e Debriefing (20 min) - Mostre a classificação final do Kahoot aos participantes. Mencione brevemente os melhores classificados. Em seguida, faça a transição para o debriefing: afaste-se do formato de jogo e convide os participantes a refletir. Use as perguntas de debriefing abaixo.

PERGUNTAS PARA O DEBRIEFING

- 1 Qual pergunta mais o surpreendeu e o que aprendeu com ela?
- 2 Quantas das suas palavras-passe atuais consideraria fracas? O que as torna arriscadas?
- 3 Já reutilizou a mesma palavra-passe em várias contas? Como se sente em relação a esse hábito agora?
- 4 O que seria necessário para começar a usar um gestor de palavras-passe? O que considera um obstáculo?
- 5 Qual hábito específico relacionado com palavras-passe irá mudar ou adotar esta semana?

MENSAGENS PRINCIPAIS DE CIBERSEGURANÇA

- ✓ Mensagem principal 1: O comprimento e a singularidade da palavra-passe importam mais do que a complexidade por si só. Uma palavra-passe longa, composta por palavras aleatórias, é ao mesmo tempo memorável e altamente segura.
- ✓ Mensagem principal 2: Reutilizar palavras-passe é um dos hábitos mais comuns e perigosos na internet. Uma única violação de segurança pode comprometer todas as contas que partilham as mesmas credenciais.
- ✓ Mensagem principal 3: A autenticação de dois fatores é uma das formas mais eficazes de proteger uma conta, mesmo que a palavra-passe seja comprometida.
- ✓ Mensagem principal 4: Um gestor de palavras-passe não é um risco (geralmente é uma solução). Pode eliminar a necessidade de memorizar dezenas de palavras-passe, garantindo que cada uma é única e forte.

BURLA EM CURSO: CONSEGUE IMPEDI-LA A TEMPO?

OBJETIVOS DE APRENDIZAGEM

Objetivo 1	Para ajudar os participantes a compreender como as burlas online se desenvolvem em situações digitais da vida real.
Objetivo 2	Desenvolver a capacidade dos jovens de reconhecer táticas de burlas, reagir com segurança e tomar decisões informadas sob pressão.
Objetivo 3	Incentivar o trabalho em equipa, a comunicação e o pensamento crítico na resposta a ameaças online e comportamentos digitais suspeitos.

GRUPO-ALVO

Público	Jovens dos 15 aos 25 anos, especialmente aqueles que usam redes sociais, aplicações de mensagens, plataformas de compras online, plataformas de jogos ou serviços bancários online.
Conhecimento prévio	Não é necessária formação prévia em cibersegurança. Experiência básica com ferramentas digitais é suficiente. É útil que os participantes já utilizem plataformas online e ferramentas de comunicação comuns.

DURAÇÃO

Tempo total	90 minutos (podendo ser reduzido para 75 minutos, se necessário)
Discriminação	Introdução: 15 min Atividade principal: 55 min Debriefing: 20 min

TAMANHO DO GRUPO

Mín. / Máx.	12 a 30 participantes (configuração recomendada: os participantes trabalham em pequenos grupos de resposta de 4 a 6 pessoas).
-------------	---

MATERIAIS NECESSÁRIOS

Físico	• Cartas de cenário impressas • Cartões de função • Folhas de instruções da equipa • Papel para flipchart ou quadro branco • Marcadores • Notas adesivas • Envelopes com “novos desenvolvimentos” ou “atualizações de incidentes”
--------	---

Digital	• Computador • Projetor • Slides com a linha do tempo do cenário de ataque • Temporizador opcional • Efeitos sonoros opcionais ou slides de alerta visual para aumentar a sensação de urgência.
Preparação	O facilitador deve preparar-se com antecedência: • Um cenário fictício, mas realista, de burla online. • Funções ou missões da equipa • 3 a 5 cartões de atualização/agravamento do cenário • Uma ficha de decisão para cada equipa. • Um breve resumo final sobre comportamento seguro e denúncia de burlas online.

GUIA DE FACILITAÇÃO PASSO A PASSO

Etapa 1: Aquecimento – “Burla ou Seguro?”

Comece com uma breve discussão em grupo. Pergunte aos participantes:

- Que tipos de burlas online viram recentemente?
- Onde costumam aparecer as burlas: email, Instagram, WhatsApp, lojas online, jogos, ofertas de emprego?
- Porque é que as pessoas ainda caem em burlas?

Anote as respostas num flipchart. Explique brevemente que as burlas online geralmente funcionam não porque as pessoas são descuidadas, mas porque os burlões são habilidosos na criação de pressão, confiança ou confusão.

Etapa 2: Apresentar o cenário

Diga aos participantes que estão prestes a entrar numa simulação de crise digital.

Apresente a história:

Um grupo de jovens está a preparar-se para um evento internacional. No mesmo dia, várias coisas suspeitas começam a acontecer:

- Aparece uma mensagem falsa sobre o pagamento da inscrição.
- Alguém recebe uma “oferta de viagem com desconto” através das redes sociais.
- Um membro da equipa recebe uma mensagem a pedir a confirmação urgente dos dados da conta.
- Um link suspeito está a ser partilhado no grupo de chat.
- Um participante afirma que pode já ter inserido dados pessoais.

Explique que cada equipa deve agir como uma equipa de resposta digital. A sua tarefa é compreender o que está a acontecer, decidir o que fazer, minimizar os danos e proteger os outros.

Etapa 3: Formação da equipa e Funções

Divida os participantes em equipas de 4 a 6 pessoas. Cada equipa assumirá o papel de uma equipa de resposta cibernética.

Funções opcionais dentro de cada equipa:

- Investigador – verifica pistas e identifica elementos suspeitos.
- Responsável pela tomada de decisão – ajuda o grupo a escolher ações.
- Comunicador – apresenta as decisões da equipa.
- Secretário(a) – redige as respostas da equipa.
- Responsável pela Segurança – verifica se as ações são realistas e seguras.

Explique que o cenário irá evoluir em etapas e que as equipas devem responder após cada atualização.

Etapa 4: Cenário Fase 1 – Os primeiros sinais de alerta

Entregue a cada equipa o cartão do primeiro incidente.

Situação de exemplo:

Um participante do grupo de jovens recebe uma mensagem direta no Instagram de uma página de viagens que oferece "promoções especiais de transporte para eventos" e solicita pagamento imediato através de um link suspeito. Ao mesmo tempo, recebe um email que parece ser dos organizadores do evento e pede aos utilizadores que "reconfirmem os dados de inscrição" iniciando sessão.

Cada equipa deve responder:

- Quais são os sinais de alerta?
- É provável que seja uma burla? Porquê?
- O que o grupo deve fazer imediatamente?
- O que devem evitar fazer?

Reserve de 8 a 10 minutos para discussão e, em seguida, convide todos para apresentações rápidas.

Fase 2 do cenário – agravamento:

Forneça às equipas um segundo cartão de atualização.

Exemplo de agravamento:

Um jovem clicou no link e inseriu o seu nome completo, número de telefone e endereço de email. Outro membro da equipa disse ter recebido uma mensagem de texto do seu "banco" a pedir que verificasse uma transação relacionada com o pagamento falso.

As equipas agora discutem:

- Qual é o nível de risco atual?
- Que medidas imediatas devem ser tomadas?
- Quem deve ser informado?
- O que ainda pode ser feito para reduzir os danos?

Algumas ideias podem incluir:

- Interromper toda e qualquer interação adicional.
- Avisar todo o grupo.
- Alterar palavras-passe, se necessário.
- Verificar a atividade bancária apenas através dos canais oficiais.
- Denunciar páginas/contas falsas.
- Recolher evidências como capturas de ecrã.
- Informar os organizadores ou os adultos/trabalhadores juvenis responsáveis.
- Nunca clicar no mesmo link ou mensagem suspeita.

Fase 3 do cenário – Pressão e Confusão:

Introduza uma terceira reviravolta.

Exemplo:

Aparece uma mensagem no chat em grupo a dizer:

“Caso o pagamento não seja concluído nos próximos 15 minutos, a sua vaga no evento será cancelada.”

Ao mesmo tempo, outro participante insiste que a oferta pode ser real porque a página falsa usa o logótipo e as fotos do evento.

As equipas precisam agora de decidir:

- Como é que os burlões usam pressão e sinais de confiança falsos?
- Como pode o grupo verificar as informações com segurança?
- Como devem comunicar com o grupo maior sem gerar pânico?

Após a discussão, cada equipa apresenta um breve plano de ação.

Missão Final da equipa – Elaborar o Plano de Resposta

Peça a cada equipa que prepare uma estratégia de resposta final numa folha de flipchart, dividida em 4 tópicos:

- O que aconteceu?
- Quais são os sinais de uma burla?
- O que devemos fazer agora?
- Como podemos evitar que isso aconteça novamente?

As equipas apresentam os seus planos. O facilitador compara as respostas e reforça as boas práticas.

Etapa 5: Reflexão final

Resuma o cenário e explique que as burlas online costumam ser rápidas, emocionais e concebidas para levar as pessoas a agir por impulso. Destaque que uma boa cibersegurança não é apenas técnica, mas também social: fazer perguntas, verificar informações, alertar outras pessoas e manter a calma.

PERGUNTAS PARA O DEBRIEFING

- 1 Em que momento do cenário a burla se tornou mais convincente?**
- 2 Que táticas de manipulação usaram os burlões nesse cenário?**
- 3 De que forma a pressão do tempo afetou as decisões da sua equipa?**
- 4 O que deve fazer um jovem se já tiver clicado num link suspeito ou partilhado alguma informação?**
- 5 Que hábitos podem ajudar a prevenir burlas online no dia a dia digital?**

MENSAGENS PRINCIPAIS DE CIBERSEGURANÇA

- ✓ Mensagem principal 1: As burlas online combinam frequentemente urgência, confiança e pressão emocional para fazer com que as pessoas ajam rapidamente.**
- ✓ Mensagem-chave 2: Uma mensagem que parece oficial não é automaticamente autêntica — logótipos, nomes e marcas podem ser copiados.**
- ✓ Mensagem principal 3: Se suspeitar de uma burla, pare, verifique através dos canais oficiais e avise outras pessoas antes que ocorram mais danos.**
- ✓ Mensagem principal 4: Mesmo que alguém cometa um erro, uma ação rápida ainda pode reduzir os danos e proteger contas, dinheiro e dados pessoais.**

CAÇADORES DE PHISHING: IDENTIFIQUEM A BURLA!

OBJETIVOS DE APRENDIZAGEM

Objetivo 1	Ajudar os jovens a compreender o que é phishing e como se manifesta no dia a dia digital.
Objetivo 2	Desenvolver a capacidade dos participantes de identificar sinais de alerta em emails, mensagens, links, sites falsos e interações em redes sociais suspeitas.
Objetivo 3	Fortalecer o pensamento crítico, os hábitos de segurança digital e a confiança para responder com segurança a tentativas de burlas online.

GRUPO-ALVO

Público	Jovens de 14 a 25 anos, especialmente aqueles que usam ativamente email, redes sociais, aplicações de mensagens, plataformas de compras online ou serviços digitais.
Conhecimento prévio	Não é necessário conhecimento avançado em cibersegurança. Basta ter familiaridade básica com o uso de telemóveis, aplicações, email e redes sociais.

DURAÇÃO

Tempo total	75 minutos (podendo ser adaptado entre 60 e 90 minutos, dependendo do tamanho do grupo e da profundidade da discussão)
Discriminação	Introdução: 15 min Atividade principal: 45 min Debriefing: 15 min

TAMANHO DO GRUPO

Mín. / Máx.	10 a 30 participantes (formato recomendado: os participantes trabalham em pequenos grupos de 3 a 5 pessoas)
--------------------	---

MATERIAIS NECESSÁRIOS

Físico	Cartões impressos com cenários de phishing/não phishing; folha de pontuação para cada equipa; canetas ou marcadores; flipchart ou quadro branco; notas adesivas; pequenos itens de recompensa para a equipa vencedora (opcional).
---------------	---

Digital	Computador Projetor ou ecrã Slides do PowerPoint/Canva com rondas de perguntas Ferramentas digitais opcionais para perguntas, como Kahoot, Mentimeter, Quizizz ou Google Forms, com cronómetro.
Preparação	O facilitador deve preparar-se com antecedência: • 12 a 20 perguntas de teste ou cartões com cenários relacionados com phishing. • Uma variedade de exemplos: emails, SMS, páginas de login falsas, burlas de sorteios, mensagens de falsificação de identidade, mensagens de entrega falsas, alertas bancários falsos e burlas em redes sociais. • Um sistema de pontuação simples. • Um slide final ou folheto com dicas essenciais de segurança contra phishing. • Emblemas/nomes de equipa opcionais para tornar a atividade mais divertida.

GUIA DE FACILITAÇÃO PASSO A PASSO

Etapa 1: Quebra-gelo – “Clicaria?”

Comece com uma atividade rápida para energizar o grupo. Mostre 3 a 4 exemplos curtos no ecrã, como:

- “A sua encomenda está atrasada, clique aqui agora.”
- “Ganhou um iPhone grátis!”
- “A sua conta escolar será bloqueada hoje.”

Peça aos participantes que se movam para um lado da sala para a opção “Eu clicaria” e para o outro lado para a opção “Eu não clicaria”.

Após cada exemplo, incentive uma ou duas reações rápidas. Isto cria curiosidade e mostra que o phishing, por vezes, pode parecer convincente.

Etapa 2: Mini-informação – O que é phishing?

Dê uma breve explicação interativa sobre phishing. Evite um formato de palestra e, em vez disso, faça perguntas como:

- De onde costumam vir as mensagens falsas?
- Porque é que os burlões querem que as pessoas cliquem?
- Que emoções tentam despertar?

Explique brevemente que o phishing é uma técnica de burla usada para enganar pessoas e obter palavras-passe, dinheiro, dados pessoais ou acesso a contas. Mencione táticas comuns como urgência, medo, recompensas, falsa autoridade e imitação de marcas ou pessoas de confiança.

Etapas 3: Formação da equipa e configuração do jogo

Divida os participantes em equipas de 3 a 5 pessoas. Cada equipa escolhe um nome, como por exemplo:

- Caçadores de Burlas
- Detetives de Links
- Guardiões Cibernéticos
- Esquadrão Anti-Phish

Explique as regras:

- As equipas ganham pontos por respostas corretas.
- São concedidos pontos extra a quem explicar porque é que algo é suspeito.
- Algumas rondas incluem armadilhas, nas quais respostas rápidas podem resultar em perda de pontos se forem mal justificadas.
- O objetivo não é apenas vencer, mas aprender a manter-se seguro online.

Sugestão de pontuação:

- Resposta correta: 1 ponto
- Explicação correta: +1 ponto extra
- Excelente recomendação de segurança: +1 ponto extra

Etapas 4: Quiz principal gamificado – “Identifique a burla”

Realize a atividade principal em 3 rondas.

Primeira ronda: Real ou burla?

Mostre ou distribua exemplos de emails, mensagens de texto ou mensagens diretas em redes sociais.

As equipas devem decidir:

Seguro / Suspeito / Definitivamente burla

Exemplos:

- Um email falso de um banco a pedir para "verificar a sua identidade com urgência".
- Uma mensagem de sorteio a solicitar os dados do cartão para o envio.
- Uma mensagem direta falsa no Instagram de um "amigo" a pedir um código.
- Uma mensagem de entrega com um link encurtado estranho.

Após cada exemplo, peça às equipas que expliquem que sinais de alerta notaram.

Ronda 2: Desafio da bandeira vermelha

Cada equipa recebe um cenário impresso ou uma captura de ecrã projetada e deve identificar o maior número possível de sinais de alerta em 2 minutos.

Possíveis sinais de alerta:

- Erros ortográficos.
- Endereço de remetente estranho.
- Link suspeito.
- Urgência ou ameaças.
- Pedido de palavras-passe.
- Ofertas que parecem demasiado boas para serem verdade.
- Identidade visual má ou logótipos falsos.
- Manipulação emocional.

As equipas apresentam as suas respostas. Os pontos são atribuídos com base na quantidade de detalhes relevantes que identificaram.

Ronda 3: O que faria?

Apresente às equipas breves cenários da vida real e peça-lhes que escolham a resposta mais segura.

Exemplos:

- Recebe uma mensagem do seu "banco" a pedir que inicie sessão imediatamente.
- Um colega de turma envia-lhe um link e diz: "vota em mim agora".
- Recebe uma oferta de emprego através de uma rede social a solicitar dados pessoais.
- A sua conta recebeu um "alerta de segurança" falso.

As equipas discutem e apresentam o seu plano de ação.

Boas respostas podem incluir:

- Não clicar.
- Verificar através do site/aplicação oficial.
- Contactar a pessoa ou empresa através de canais de confiança.
- Denunciar/bloquear o remetente.
- Verificar o remetente e o URL com atenção.
- Em caso de dúvida, pedir ajuda a um adulto de confiança, professor ou técnico de juventude.

Etapa 5: Reflexão final e principais pontos de segurança

Conte os pontos e anuncie a equipa vencedora. Mantenha o tom divertido e encorajador.

Em seguida, mude o foco da competição para a aprendizagem. Peça a cada equipa que partilhe:

- Uma coisa que aprendeu.
- Um sinal de phishing que agora irá notar com mais facilidade.
- Um hábito de segurança que quer adotar.

O facilitador conclui com um breve resumo dos hábitos mais importantes para combater o phishing.

PERGUNTAS PARA O DEBRIEFING

- 1 O que fez com que alguns exemplos de phishing parecessem convincentes à primeira vista?
- 2 Quais sinais de alerta foram mais fáceis de identificar e quais foram mais difíceis?
- 3 Por que é que as pessoas às vezes caem em burlas de phishing, mesmo quando conhecem os riscos online?
- 4 De que forma emoções como medo, excitação, urgência ou curiosidade influenciam as decisões online?
- 5 Que medidas práticas pode tomar a partir de agora para se proteger e proteger os outros contra o phishing?

MENSAGENS PRINCIPAIS DE CIBERSEGURANÇA

- ✓ Mensagem principal 1: O phishing muitas vezes parece confiável porque copia marcas, pessoas ou instituições reais.
- ✓ Mensagem principal 2: Urgência, medo e recompensas "demasiado boas para serem verdade" são táticas de manipulação comuns usadas por burlões.
- ✓ Mensagem-chave 3: Antes de clicar, verifique sempre o remetente, o link e o pedido com atenção.
- ✓ Mensagem-chave 4: Se algo parecer suspeito, pare, verifique através dos canais oficiais e peça ajuda, se necessário.

A AGÊNCIA PARA EXPATRIADOS – DESAFIO DE ROUBO DE IDENTIDADE

OBJETIVOS DE APRENDIZAGEM

Objetivo 1	Desenvolver a capacidade de identificar sinais de alerta de "engenharia social" em publicações anónimas nas redes sociais.
Objetivo 2	Compreender o ciclo de vida do roubo de identidade, desde uma simples conversa até à perda total de dados.
Objetivo 3	Reforçar as competências de verificação digital e os hábitos de denúncia no contexto lituano/europeu.

GRUPO-ALVO

Público	Jovens dos 16 aos 30 anos, especialmente aqueles que procuram estágios ou empregos no exterior.
Conhecimento prévio	Uso básico de grupos do Facebook e aplicações de mensagens (WhatsApp/Telegram).

DURAÇÃO

Tempo total	90 minutos
Discriminação	Introdução: 15 min Atividade principal (Investigação): 50 min Debriefing: 25 min

TAMANHO DO GRUPO

Mín. / Máx.	10–24 (divididos em "Unidades de Investigação" de 3 a 4 pessoas)
-------------	--

MATERIAIS NECESSÁRIOS

Físico	Pacotes de evidências impressos (capturas de ecrã de publicações falsas de expatriados, mensagens diretas anónimas).
Digital	Smartphones/portáteis, acesso à internet de alta velocidade ou ao site E-police.lt para a fase de registo da ocorrência.
Preparação	• Imprima 4 conjuntos de "Pacotes de evidências". • Crie um exemplo de perfil de "Empregador falso". • Elabore um "Mapa de perda de dados", que mostre como um número de telefone pode levar ao roubo de identidade.

GUIA DE FACILITAÇÃO PASSO A PASSO

Passo 1: Introduza o conceito de "Recolha de confiança".

Explique que, em 2026, os burlões não usam vírus; eles usam **conversas**.

Destaque a tendência específica na Lituânia: utilizadores anónimos que visam expatriados e estudantes.

Passo 2: Distribua os "Pacotes de evidências".

As equipas devem analisar três "Anúncios de emprego" diferentes encontrados num grupo fictício de expatriados.

A tarefa: devem encontrar 4 anomalias (por exemplo, conta criada no dia anterior, foto genérica de banco de imagens, linguagem "urgente" ou pedido de documento de identidade antes da entrevista).

Etapa 3: O facilitador mostra uma captura de ecrã de um "Chat por mensagem direta" onde o burlão pede um número de telefone e morada.

As equipas devem prever o que o burlão pode fazer apenas com essas três informações (telefone, morada e nome completo).

Atividade: as equipas utilizam uma "Matriz de privacidade" para verificar como essas informações são vendidas na *dark web* ou usadas para troca de cartões SIM.

Passo 4: Os participantes devem encontrar o portal oficial de denúncias da Lituânia.

Tarefa: Redigir uma publicação de "Aviso à comunidade" que seja clara, não agressiva e informativa para alertar outros expatriados no grupo.

Passo 5: Resuma que "anónimo" não significa apenas "oculto" — significa "não verificado".

Reforce a regra: **sem entrevista, sem documento de identidade.**

PERGUNTAS PARA O DEBRIEFING

- 1 Por que é que a publicação "Anónima" pareceu mais útil do que um email aleatório?
- 2 Qual foi o sinal de alerta mais sutil que encontrou no perfil do "Empregador"?
- 3 Por que é que os burlões bloqueiam as vítimas imediatamente após obterem o seu email ou número de telefone?
- 4 Como podemos ajudar amigos que estão "desesperados" por um emprego a se protegerem dessas armadilhas?
- 5 Qual é a primeira coisa que deve fazer se enviar acidentalmente uma foto do seu documento de identidade para um desconhecido?

MENSAGENS PRINCIPAIS DE CIBERSEGURANÇA

- ✓ Mensagem principal 1: A verificação é um sinal de inteligência, não de má educação.
- ✓ Mensagem principal 2: As suas informações de identificação pessoal são a moeda de 2026.
- ✓ Mensagem principal 3: Se um "empregador" o bloquear depois de obter os seus dados, isso não significa que perdeu o interesse - significa que encontrou o que procurava.
- ✓ Mensagem principal 4: Utilize canais oficiais, como o LinkedIn e portais universitários, em vez de grupos anónimos de redes sociais para procurar emprego.

O IMPOSTOR DE RH – DESAFIO DE FRAUDE NO RECRUTAMENTO

OBJETIVOS DE APRENDIZAGEM

Objetivo 1	Identificar os fatores psicológicos utilizados em burlas de recrutamento (urgência, autoridade e exclusividade).
Objetivo 2	Distinguir um processo legítimo de integração de funcionários numa empresa de uma burla para recolha de dados.
Objetivo 3	Desenvolver resiliência contra burlas de "taxas de integração" e falsificação de identidade nas redes sociais.

GRUPO-ALVO

Público	Jovens à procura de emprego dos 18 aos 30 anos, estudantes universitários e pessoas que trabalham pela primeira vez.
Conhecimento prévio	Familiaridade com o Instagram e conhecimento geral sobre candidaturas a empregos online.

DURAÇÃO

Tempo total	90 minutos
Discriminação	Introdução: 15 min Atividade de análise de perfil: 30 min Simulação de entrevista: 25 min Debriefing: 20 min

TAMANHO DO GRUPO

Mín. / Máx.	12–24 participantes (equipas de 3 a 4 pessoas)
-------------	--

MATERIAIS NECESSÁRIOS

Físico	Pacotes impressos para candidatos (uma carta de oferta de emprego falsa, uma lista de verificação de integração e uma fatura de equipamento de amostra).
Digital	Para comparar as informações, consulte os sites oficiais das empresas.
Preparação	Crie uma captura de ecrã falsa de um perfil do Instagram de uma empresa conhecida (por exemplo, "Microsoft_Careers_Official_2026").

GUIA DE FACILITAÇÃO PASSO A PASSO

Etapa 1: Introdução (15 min) - A Ascensão do RH Falso:

Explique que os burlões agora se fazem passar por profissionais de Recursos Humanos (RH) de marcas famosas.

Discuta porque é que os jovens são o alvo: estão ansiosos por iniciar uma carreira e podem não saber como funciona um processo corporativo padrão.

Etapa 2: Análise de Perfil (30 min):

Mostre o Instagram da marca "oficial" ao lado do Instagram de "recrutamento".

A tarefa: as equipas devem encontrar 5 inconsistências (por exemplo, o perfil falso não possui o selo "verificado", o link na biografia usa um encurtador de URL, como o bit.ly, ou a proporção entre envolvimento e seguidores parece suspeita).

Etapa 3: A Armadilha da Integração (25 min):

Distribua a "Lista de verificação de integração", que solicita: nome completo, morada, número de identificação fiscal e uma "taxa de formação" de 50 €.

Atividade: as equipas devem atuar como "auditores legais". Devem marcar cada item da lista como "padrão" ou "aviso". Revelação: explique que nenhum empregador legítimo solicita dinheiro ou dados altamente confidenciais (como uma foto do passaporte) por mensagem direta antes de uma entrevista presencial ou por vídeo.

Etapa 4: A resposta à crise (20 min):

Cenário: "Já enviou a sua foto de identidade para a pessoa falsa do RH. O que faz agora?"

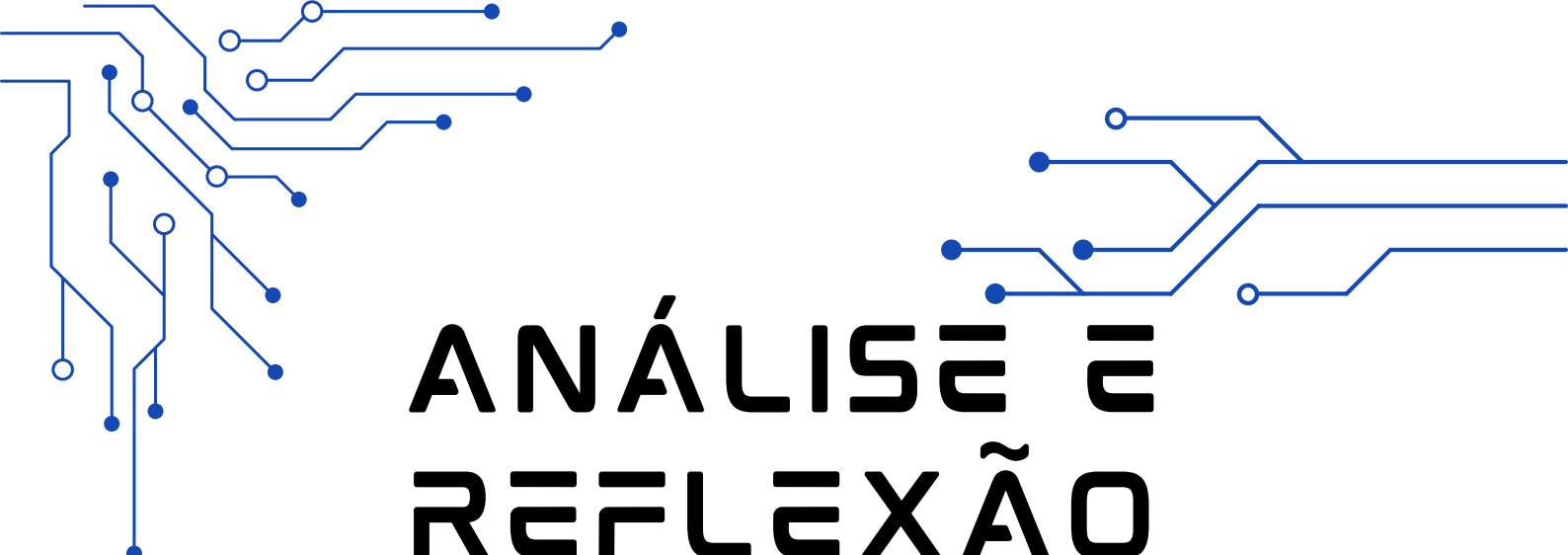
Tarefa: as equipas devem pesquisar e anotar os três passos imediatos para a Lituânia/Espanha/etc. (por exemplo, entrar em contato com o banco, notificar o RH da empresa verdadeira e registar uma denúncia no E-police.lt).

PERGUNTAS PARA O DEBRIEFING

- 1 **Porque é que é mais fácil acreditar numa mensagem de alguém que afirma ser de uma "empresa famosa"?**
- 2 **Qual é a principal diferença entre uma "Candidatura" e uma "Entrevista"?**
- 3 **Porque é que os burlões pedem "taxas de integração" ou "depósitos de equipamentos"?**
- 4 **Como posso verificar se uma pessoa de RH que entrou em contacto comigo pelas redes sociais é real?**
- 5 **Qual foi a parte mais convincente da oferta de emprego falsa que analisou hoje?**

MENSAGENS PRINCIPAIS DE CIBERSEGURANÇA

- ✓ **Mensagem principal 1: Empregadores de verdade pagam-lhe; nunca é o candidato que paga para começar um trabalho.**
- ✓ **Mensagem principal 2: O recrutamento oficial geralmente ocorre através de email corporativo (@empresa.com), e não por mensagens diretas no Instagram.**
- ✓ **Mensagem-chave 3: Táticas de alta pressão como "Assine em 1 hora ou perca o emprego!", são um sinal de alerta muito forte.**
- ✓ **Mensagem-chave 4: Se não encontrar a vaga de emprego no site oficial de "Carreiras" da empresa, provavelmente ela não existe.**



ANÁLISE E REFLEXÃO

TÉCNICAS DE DISCUSSÃO EM GRUPO

Para manter as discussões sobre cibersegurança interessantes e acessíveis, utilize estes métodos de aprendizagem ativa:

- **O "Carrossel de Cenários":** Coloque cartazes pela sala, cada um com uma descrição de uma das ameaças regionais identificadas (por exemplo, uma burla de "arrendamento estudantil" ou um "sorteio no Instagram"). Pequenos grupos alternam entre estações, dedicando 3 minutos para discutir: "Qual é o sinal de alerta aqui?"
- **O "Espectro de Risco":** Crie uma linha imaginária na sala, de "Totalmente Seguro" a "Altamente Perigoso". Leia em voz alta comportamentos online (por exemplo, "Ler um código QR para ganhar uma pizza grátis" ou "partilhar uma foto com localização identificada"). Os participantes devem mover-se para o ponto da linha que representa a sua opinião. Isto gera um debate imediato entre aqueles com diferentes perceções de risco.
- **Discussão em círculo:** Quatro participantes sentam-se num círculo central (o aquário) e discutem um tópico controverso — como, por exemplo, se as plataformas de redes sociais devem ser responsabilizadas pela prevenção da extorsão sexual. O restante do grupo observa. Se alguém do círculo externo quiser falar, deve "tocar" no ecrã e trocar de lugar.
- **Simulação de "Consultor de Segurança":** Divida o grupo em "Burlões" e "Consultores Cibernéticos". Os burlões tentarão criar a mensagem falsa mais convincente; os consultores deverão apontar exatamente como identificar a burla.

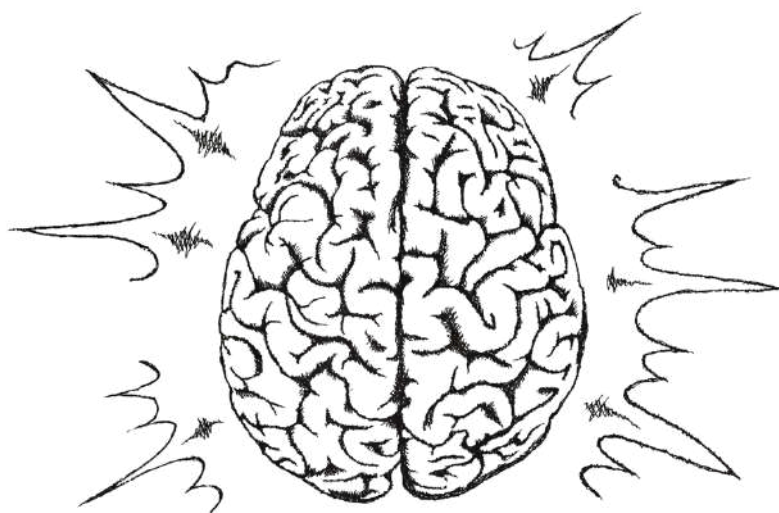
QUESTÕES PARA REFLEXÃO

O debriefing e a reflexão são componentes importantes do ciclo de aprendizagem, pois permitem que os participantes passem da simples experiência de uma ameaça cibernética para a análise crítica das táticas psicológicas e técnicas utilizadas pelos burlões.

Estas perguntas visam preencher a lacuna entre o conteúdo do kit de ferramentas e a vida digital pessoal dos participantes:



- **Hábitos pessoais:** "Pense nas três últimas aplicações que instalou. Lembra-se das permissões (câmera, contactos, localização) que lhes concedeu? Porque é que precisavam dessas permissões?"
- **Estímulos emocionais:** "Os burlões tentam frequentemente fazê-lo sentir urgência ou medo (como numa falsa suspensão de conta). Lembra-se de alguma situação em que uma publicação ou mensagem o fez sentir que precisava de agir imediatamente? O que aconteceu?"
- **Responsabilidade digital:** "Se visse um amigo a participar num 'desafio' viral que parecesse arriscado ou recolhesse muitos dados pessoais, diria algo? Como abordaria essa conversa?"
- **Resiliência futura:** "Depois de ver as burlas direccionadas ao seu país em específico (por exemplo, as ofertas de estágio falsas), qual é a 'regra de ouro' que irá seguir antes de clicar num link num email?"





AVALIAÇÃO DA APRENDIZAGEM

Para garantir uma avaliação holística da jornada de aprendizagem, os facilitadores devem integrar a reflexão diretamente no processo de avaliação, pois isso permite avaliar tanto o conhecimento técnico adquirido como a mudança nas atitudes digitais pessoais.

O teste do "semáforo": no final da sessão, os participantes levantam um cartão:

- **Verde:** sinto-me confiante para identificar este risco.
- **Amarelo:** compreendo, mas ainda estou um pouco inseguro sobre como me proteger.
- **Vermelho:** ainda acho este assunto muito técnico ou confuso.

O desafio de 60 segundos: desafie os participantes a explicar um conceito de cibersegurança (como "2FA" ou "phishing por código QR") a um irmão mais novo ou a um avô/avó em menos de um minuto. Se conseguirem simplificar o conceito, terão dominado o assunto.

Teste "Identifique a burla": mostre 5 exemplos reais de mensagens (algumas verdadeiras, outras falsas). Uma avaliação bem-sucedida ocorre quando o grupo consegue identificar pelo menos 4 das 5 mensagens e, mais importante ainda, explicar o motivo da escolha.

Escala de confiança digital: peça aos participantes que avaliem a sua confiança em "Resiliência Digital" de 1 a 10 antes e depois do workshop. O aumento dessa pontuação é a principal métrica de avaliação.





DICAS PARA TÉCNICOS DE JUVENTUDE

INTEGRAR A CIBERSEGURANÇA NO TRABALHO COM JOVENS.

A cibersegurança deve ser integrada no trabalho com jovens como uma extensão natural das suas experiências digitais diárias, em vez de ser tratada como um tópico separado ou altamente técnico. Os jovens estão constantemente a interagir com redes sociais, plataformas de mensagens e conteúdo online, tomando decisões relacionadas com privacidade, confiança e segurança, muitas vezes sem estarem totalmente cientes dos riscos envolvidos.

Para os técnicos de juventude, a chave é ligar temas de cibersegurança, como privacidade de dados, phishing, desinformação, burlas online, perfis falsos e segurança de palavras-passe, a situações reais que os jovens já vivem. Ao partir de experiências familiares, a cibersegurança torna-se mais relevante e fácil de compreender. Esta abordagem permite que as discussões surjam organicamente dentro de temas mais amplos, como bem-estar digital, participação e pensamento crítico.

Os métodos de educação não formal desempenham um papel central neste processo. Formatos interativos, como desafios de resolução de problemas, simulações, dramatizações ou quizzes gamificados, permitem que os jovens explorem a cibersegurança de forma prática e envolvente. Estas abordagens criam um ambiente seguro onde os participantes podem experienciar cenários como tentativas de phishing ou manipulação nas redes sociais, testar as suas reações e aprender através da experiência.

É importante privilegiar a capacitação em vez do medo. Embora sensibilizar para os riscos seja necessário, o objetivo é ajudar os jovens a sentirem-se confiantes na sua capacidade de reconhecer ameaças e tomar decisões informadas. Ao incorporar a cibersegurança nas atividades regulares com jovens, esta torna-se parte de um processo contínuo de aprendizagem que apoia o desenvolvimento de um comportamento digital responsável e resiliente.

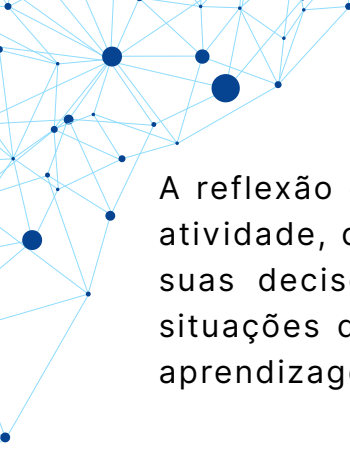
REALIZAÇÃO DE WORKSHOPS OU LABORATÓRIOS PARA JOVENS

Workshops e laboratórios para jovens são formatos eficazes para facilitar a educação em cibersegurança, pois incentivam a participação ativa e a aprendizagem experiencial. Uma sessão bem planeada deve guiar os participantes por um processo claro que os conduza do envolvimento à reflexão.

Um ponto de partida eficaz é introduzir o tema através de uma situação com a qual os participantes se identifiquem, como uma mensagem suspeita, um perfil falso online ou conteúdo enganoso. Isto liga imediatamente a sessão às experiências quotidianas dos participantes e aumenta o seu envolvimento.

O foco principal da sessão deve centrar-se em atividades interativas retiradas dos formatos incluídos neste guia. Diferentes tópicos podem ser explorados através de diferentes métodos. Por exemplo, phishing e burlas online podem ser abordados através de simulações ou cenários de ataques cibernéticos, enquanto desinformação e manipulação nas redes sociais podem ser exploradas através de estudos de caso ou quizzes gamificados. Atividades de dramatização são particularmente úteis para compreender perfis falsos ou interações fraudulentas, enquanto mini-salas de fuga permitem que os participantes apliquem múltiplos conceitos de forma dinâmica e imersiva.

Estes métodos incentivam os jovens a participar ativamente, tomar decisões e colaborar com os outros. A aprendizagem torna-se mais eficaz porque os participantes estão diretamente envolvidos no processo, em vez de receberem informações passivamente. O papel do técnico de juventude é facilitar esse processo, orientando a atividade, apoiando os participantes quando necessário e incentivando a exploração sem fornecer respostas imediatas.



A reflexão é uma parte crucial do processo de aprendizagem. Após cada atividade, deve reservar-se tempo para que os participantes discutam as suas decisões, identifiquem sinais de alerta e liguem a experiência a situações da vida real. Esta etapa ajuda a transformar a atividade numa aprendizagem significativa e apoia a mudança de comportamento.

Criar um ambiente seguro e inclusivo também é essencial. Os participantes devem sentir-se à vontade para expressar as suas ideias e partilhar experiências, principalmente ao discutir temas sensíveis, como riscos online ou experiências digitais negativas. Uma atmosfera respeitosa incentiva o diálogo aberto e um envolvimento mais profundo.

FACILITAR DISCUSSÕES SOBRE SEGURANÇA ONLINE.

As discussões desempenham um papel fundamental no reforço da aprendizagem e ajudam os jovens a refletir sobre o seu comportamento digital. Discussões eficazes devem basear-se nas experiências dos participantes e estar ligadas às atividades realizadas durante a sessão. Os técnicos de juventude devem criar um espaço sem julgamentos, onde os participantes se sintam seguros para partilhar as suas perspetivas. Os jovens podem ter diferentes níveis de consciência ou podem ter tomado decisões arriscadas online, pelo que é importante incentivar a abertura em vez da crítica. Ouvir ativamente e validar as contribuições ajuda a construir confiança e apoia um diálogo significativo.

Os facilitadores devem conduzir as discussões fazendo perguntas abertas que incentivem a reflexão e o pensamento crítico. Questões como a forma de reconhecer informações fiáveis, por que razão as pessoas caem em burlas ou como os dados pessoais podem ser usados indevidamente ajudam os participantes a analisar situações e a considerar diferentes perspetivas. Esta abordagem apoia o desenvolvimento do pensamento crítico, que é essencial para navegar em ambientes digitais. As discussões também devem ajudar os participantes a ligar tópicos específicos, como phishing ou perfis falsos, a conceitos mais amplos, como confiança, identidade e responsabilidade online. Isto permite que os jovens compreendam melhor o impacto das suas ações e a importância de um comportamento digital seguro.

Ao mesmo tempo, é importante garantir que as discussões conduzam a resultados práticos. Os participantes devem sair com ideias claras sobre como se proteger, como reconhecer links suspeitos, usar palavras-passe seguras ou verificar as fontes de informação. Resumir os pontos principais no final da sessão ajuda a reforçar a aprendizagem e proporciona clareza.

Ao combinar atividades interativas com discussões guiadas, os técnicos de juventude podem criar experiências de aprendizagem envolventes e significativas. Esta abordagem ajuda os jovens a tornarem-se mais conscientes, confiantes e responsáveis no uso das tecnologias digitais.





RECURSOS E FERRAMENTAS

PLATAFORMAS DE CIBERSEGURANÇA RECOMENDADAS

UE

enisa.europa.eu

- [Plataforma de Educação em Cibersegurança](#)
- [Kit de Sensibilização](#)
- [Consciencialização e Higiene em Cibersegurança](#)
- [Cibersegurança para PME](#)
- [Desafio Europeu e Internacional de Cibersegurança](#)
- [Plataforma CIRAS](#)

estrategia-digital.ec.europa.eu

- [Estratégia para uma internet melhor para as crianças](#)

melhorinternetparacrianças.eu

cert.europa.eu — CERT-EU

- **Estónia**

itvaatlik.ee — Fiscal de TI ria.ee — Autoridade de Sistemas de Informação

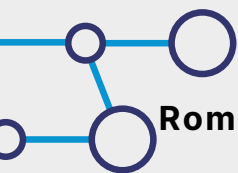
- [Tratamento de Incidentes de Cibersegurança CERT-EE](#)

- **Lituânia**

nksc.lt — Centro Nacional de Cibersegurança draugiskasinternetas.lt

- **Portugal**

- internetsegura.pt
- seguranet.pt



Roménia

sigurantaonline.ro

dnsc.ro — [Directoratul Național de Securitate Cibernetică](http://dnsc.ro)

Espanha

is4k.es

hacksplaining.com

phishingquiz.withgoogle.com

Turquia

usom.gov.tr — [USOM \(National CERT\)](http://usom.gov.tr)

bilgem.tubitak.gov.tr

- [Cyber Security Division](http://bilgem.tubitak.gov.tr)

RECURSOS EDUCACIONAIS

UE

education.ec.europa.eu

- [Digital Education Focus](http://education.ec.europa.eu)

enisa.europa.eu

- [CyberHEAD Tool](http://enisa.europa.eu)
- [Cybereducation Platform](http://enisa.europa.eu)
- [European Cybersecurity Skills Framework](http://enisa.europa.eu)

digital-skills-jobs.europa.eu

- [Cybersecurity Skills Academy](http://digital-skills-jobs.europa.eu)

academy.europa.eu

- [Build Your Own Cyber Awareness Program](http://academy.europa.eu)

edpb.europa.eu — [European Data Protection Board](http://edpb.europa.eu)

childnet.com

thinkuknow.co.uk

better-internet-for-kids.europa.eu

- [Resource Directory](http://better-internet-for-kids.europa.eu)



europol.europa.eu

- [Cybercrime area](#)

arqus-alliance.eu

- [Cybersecurity MOOC – Citizen & Professional Guide](#)

esdc.europa.eu — [European Security & Defence College](#)

digital-strategy.ec.europa.eu

- [Comunicação: Cybersecurity Skills Academy](#)

Estónia

ria.ee — [Information System Authority](#)

- [CERT-EE – Handling Cyber Incidents](#)
- [National Coordination Centre \(NCC-EE\)](#)

Lituânia

better-internet-for-kids.europa.eu

- [Safer Internet Day – Lithuania](#)

cyberwiser.eu

- [Página da Lituânia](#)

Portugal

internetsegura.pt

- [Recursos](#)

seguranet.pt

- [Training / Formação](#)

Roménia

sigurantaonline.ro

- [The Websters S3 – Întâmplări din Viața Digitală \(PDF\)](#)
- [The Websters S4 – Întâmplări din Viața Digitală \(PDF, 2025\)](#)

dnsc.ro — [Directoratul Național de Securitate Cibernetică](#)

- [Ghid Securitate Cibernetică 2021](#)
- [Ghid Control Parental – Protecția Minorilor în Mediul Digital](#)

Espanha

incibe.es — [Instituto Nacional de cibersegurança](#)

Turquia

btkakademi.gov.tr — [Academia BTK](#)

SITES ÚTEIS

UE

enisa.europa.eu — ENISA

saferinternet.org

euvsdisinfo.eu

ecs-org.eu — Organização Europeia de Cibersegurança

estrategia-digital.ec.europa.eu

- [Diretiva NIS2](#)
- [Conteúdo relacionado – tópico 153](#)
- [Conteúdo relacionado – tópico 49](#)
- [Conteúdo relacionado – tópico 99](#)

eucpn.org — Rede Europeia de Prevenção ao Crime

- [EU Kids Online – Final Report](#)

seguranca.google

Estónia

ria.ee — Autoridade de Sistemas de Informação

- [Centro Nacional de cibersegurança \(NCSC-EE\)](#)
- [Como reportar um incidente cibernético](#)

raport.cert.ee — Relatório Anual do CERT-EE

Lituânia

vaikulinijs.lt — Linha de Apoio a Crianças

epolicija.lt — E-Police

Portugal

cncs.gov.pt — Centro Nacional de Cibersegurança

- [Cibersegurança \(PT\)](#)

Roménia

salvaticopiii.ro — Salve as Crianças

- [Segurança na Internet](#)

cybersecurity.certsign.ro

- [Cyber4Kids](#)

unbreakable.ro — Competição nacional de cibersegurança

cyberskill.ro

Espanha

incibe.es — Instituto Nacional de cibersegurança

osi.es — Escritório de Segurança da Internet

Turquia

guvenlinet.org.tr — Internet Segura

kvkk.gov.tr — Autoridade de Proteção de Dados Pessoais

REFERÊNCIAS

Capítulo 1

Eurostat (2024). Jovens – estatísticas do mundo digital
<https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20250715-1>

Comissão Europeia (2021). Plano de Ação para a Educação Digital (2021-2027).
<https://education.ec.europa.eu/focus-topics/digital-education/actions>

Comissão Europeia. Programa Erasmus+
https://commission.europa.eu/education/set-projects-education-and-training/erasmus-funding-programme_en

ENISA (2023). Recursos de educação e consciencialização em cibersegurança
<https://www.enisa.europa.eu/tools/enisa-cybereducation-platform>

Capítulo 3

Cedefop (2024) - Terminologia da política europeia de educação e formação
<https://www.cedefop.europa.eu/en/publications/3095>
David Kolb (1984): “Aprendizagem experiencial: a experiência como fonte de aprendizagem e desenvolvimento”
https://www.fullerton.edu/cice/_resources/pdfs/sl_documents/Experientia%20Learning%20-%20Experience%20As%20The%20Source%20Of%20Learning%20and%20Development.pdf

Comissão Europeia (2020) – Agenda Europeia de Competências
https://employment-social-affairs.ec.europa.eu/policies-and-activities/skills-and-qualifications/european-skills-agenda_en
Garamkhand Surendeleg et al., “O papel da gamificação na educação – uma revisão da literatura”, Ciências da Engenharia Contemporânea, Vol. 7
<https://www.m-hikari.com/ces/ces2014/ces29-32-2014/02surendelegCES29-32-2014.pdf>
SALTO – Juventude, “Métodos não formais. Guia para capacitar a juventude.” (2023).
https://www.salto-youth.net/downloads/toolbox_tool_download-file-3759/Guide-of-Non-formal%20methods.pdf

Pesquisa científica, Hamari, J., Koivisto, J., & Sarsa, H. (2014). "A gamificação funciona? Uma revisão da literatura de estudos empíricos sobre gamificação." 2014 47ª Conferência Internacional do Havaí sobre Ciências de Sistemas, Waikoloa, HI, 6-9 de janeiro de 2014, 3025-3034.

<https://www.scirp.org/reference/referencespapers?referenceid=2757206>

Biblioteca Digital da UNESCO, Juventude e competências: colocar a educação em prática, Relatório de monitorização global da EPT, 2012

<https://unesdoc.unesco.org/ark:/48223/pf0000218003>

Universidade de Cambridge, Bibliotecas e Arquivos, Apollo, Johnson, M., & Majewska, D. (2022). "Aprendizagem formal, não formal e informal: o que são e como podemos investigá-las?" Cambridge University Press & Assessment.

<https://www.repository.cam.ac.uk/items/b4200743-6f60-4d46-a668-c382f5400041>