



ESCAP(E+)

**Educar os Jovens em Segurança através
de um Programa de Sensibilização e
Envolvimento em Cibersegurança**

INVESTIGAÇÃO DOCUMENTAL



Co-funded by
the European Union

Projeto e Colaboradores

Este relatório de Investigação documental foi desenvolvido como parte do programa “ESCAP(E+) Educar Jovens em Segurança através da Sensibilização e do Envolvimento em Cibersegurança”.

Número do Projeto: 2025-1-ES02-KA220-YOU-000358192

Data de publicação: 1 de abril de 2026

Parceiros e Colaboradores:

Suatas Project Academy SPA - Lituânia
info@suatasprojectacademy.lt

EducAI - Portugal
educai.ngo@gmail.com

EducPro - Spain
projects@educpro.eu

EuroReach - Estónia
info@euroreach.org

Universidade de Istambul-Cerrahpasa - Turquia
irfan@iuc.edu.tr

Scout Society - Roménia
contact@scoutsociety.ro

Este projeto foi financiado com o apoio da Comissão Europeia. Este documento reflete apenas as opiniões do(s) autor(es), e a Comissão Europeia não pode ser responsabilizada por qualquer uso que possa ser feito das informações nele contidas. Número do Acordo: 2025-1-ES02-KA220-YOU-000358192

Reconhecimento

Este Relatório de Investigação Documental foi desenvolvido como parte da Parceria de Cooperação ERASMUS+ no projeto juvenil "ESCAP(E+) Educar Jovens em Segurança através de Programas de Sensibilização e Envolvimento em Cibersegurança", financiado pela Comissão Europeia ao abrigo do Acordo de Subvenção 2025-1-ES02-KA220-YOU-000358192. O projeto tem a duração de 24 meses, decorrendo entre 1 de dezembro de 2025 e 30 de novembro de 2027, tendo esta publicação sido lançada a 1 de abril de 2026.

Este projeto foi possível graças aos esforços colaborativos dos nossos parceiros:

EducPro(SP)

- EuroReach (EE)
- Universidade de Istambul-Cerrahpasa (TR)
- Scout Society (RO)
- Suatas Project Academy SPA (LT)
- EducAi (PT)

Um agradecimento especial aos parceiros, investigadores, animadores juvenis e colaboradores que apoiaram o processo de investigação documental.

Aviso

O apoio da Comissão Europeia à produção desta publicação não constitui uma aprovação do seu conteúdo, o qual reflete apenas as opiniões dos autores, não podendo a Comissão Europeia ser responsabilizada por qualquer utilização que possa ser feita das informações nela contidas.

Aviso de direitos de autor

Esta licença permite que os utilizadores distribuam, adaptem e criem obras derivadas a partir deste material em qualquer meio ou formato, exclusivamente para fins não comerciais, desde que seja feita a devida atribuição à fonte original. Quaisquer adaptações devem ser partilhadas nos mesmos termos da licença.

Caso utilize ou adapte conteúdo desta publicação, inclua a seguinte declaração:

"Este conteúdo foi desenvolvido com recurso a materiais do projeto ESCAP(E+) (Número do Projeto: 2025-1-ES02-KA220-YOU-000358192). Todos os elementos visuais utilizados nesta publicação são livres de direitos de autor e foram obtidos através Canva."

Índice

5	Introdução
7	Investigação Documental Lituânia
15	Investigação Documental Roménia
32	Investigação Documental IUC
46	Investigação Documental Estónia
66	Investigação Documental Espanha
79	Investigação Documental Portugal
92	Conclusão

INTRODUÇÃO

Esta investigação documental foi desenvolvida no âmbito do Pacote de Trabalho 2 do projeto ESCAP(E+): Estrutura - Explorando Ameaças à cibersegurança, liderado pela Suatas Project Academy. O seu objetivo é identificar e analisar as ameaças à cibersegurança mais relevantes que afetam os jovens, especialmente aquelas que aparecem em plataformas digitais amplamente utilizadas, como Facebook, Instagram, TikTok e e-mail. Dentro da lógica mais ampla do projeto, esta investigação fornece a base de evidências para o desenvolvimento da estrutura de cibersegurança do ESCAP(E+) e apoia a criação de produtos futuros do projeto, incluindo conteúdo de formação para técnicos de juventude, cenários de jogos de fuga em realidade virtual, materiais de sensibilização e outros recursos educacionais.

O relatório foi elaborado através de um processo coordenado de investigação documental em parceria. Seguindo uma metodologia partilhada e acordada no âmbito do WP2, cada parceiro realizou pesquisas nacionais utilizando um modelo comum, a fim de garantir consistência e comparabilidade entre os países. Os parceiros foram solicitados a concentrarem-se nos hábitos digitais dos jovens, nos principais fatores de risco, nas ameaças online mais comuns e nos mecanismos de prevenção e denúncia disponíveis nos seus respectivos contextos nacionais. Para tornar as conclusões práticas e úteis, cada parceiro descreveu as principais ameaças através de uma estrutura padrão que incluía a plataforma em questão, uma breve descrição da ameaça, um cenário realista envolvendo jovens, o funcionamento da ameaça, sinais de alerta, Medidas de prevenção, etapas de resposta, gravidade e principais fontes.

Este relatório, portanto, reúne as contribuições nacionais de todos os parceiros num único documento consolidado. Inclui uma visão geral do contexto digital da juventude em cada país parceiro, uma apresentação das ameaças cibernéticas mais relevantes que visam os jovens e orientações práticas sobre prevenção e resposta. Desta forma, o relatório ajuda a garantir que o projeto ESCAP(E+) esteja fundamentado em experiências reais da juventude, reflita os riscos específicos de cada país e responda às reais necessidades educacionais dos jovens e daqueles que trabalham com eles.

METODOLOGIA

Cada parceiro foi solicitado a realizar uma investigação documental a nível nacional, no contexto do respetivo país, e a submeter as suas conclusões num formato partilhado, para que os resultados pudessem ser consolidados num único relatório comparativo do projeto. Esta abordagem comum possibilitou combinar evidências específicas de cada país, mantendo a consistência em todo o documento.

Para os relatórios nacionais, os parceiros seguiram uma estrutura comum composta por quatro secções principais: **Visão Geral, Principais Ameaças, Conclusões e Recursos**. A secção de visão geral apresentou o contexto nacional, incluindo os hábitos digitais dos jovens, as principais vulnerabilidades, estatísticas selecionadas e os canais de denúncia. A investigação concentrou-se nos ambientes digitais e nas ameaças cibernéticas mais relevantes para os jovens no seu dia a dia. Em consonância com a estrutura do projeto, os parceiros foram solicitados a examinar os riscos associados a plataformas e canais de comunicação amplamente utilizados, especialmente **Facebook, Instagram, TikTok e E-mail**, incluindo ameaças como phishing, burlas, roubo de identificação, desinformação, falsificação de identificação e outras formas de engenharia social. Além de mapear as próprias ameaças, os parceiros também examinaram o contexto digital mais amplo dos jovens nos seus países, incluindo hábitos online, utilização de plataformas, vulnerabilidades comuns e mecanismos de apoio ou denúncia disponíveis.

Outro ponto forte da metodologia é a combinação da relevância específica de cada país com a coerência a nível do projeto. Cada parceiro conseguiu identificar as burlas, as táticas de manipulação e os riscos digitais mais visíveis no seu contexto nacional, enquanto a utilização de um modelo comum garantiu que todas as contribuições pudessem ser comparadas, integradas e traduzidas em recomendações comuns para o projeto. Como resultado, o relatório final não só descreve as ameaças em termos abstratos, como também as relaciona com a realidade digital quotidiana dos jovens nos países parceiros.



ESCAP(E+)

Lituânia

INVESTIGAÇÃO DOCUMENTAL



Co-funded by
the European Union

European Union
Digital Education Programme
Grant Agreement No. 101017744

Visão geral

Contexto Digital da Juventude na Lituânia

Na Lituânia, a integração digital está entre as mais altas da União Europeia. Em 2026, as estatísticas nacionais indicavam que 99,2% dos jovens entre os 16 e os 24 anos utilizavam a internet diariamente (Estatísticas da Lituânia, 2026). As ferramentas digitais são essenciais para o estilo de vida "e-residente" comum nos países bálticos, com os jovens a utilizarem redes 5G de alta velocidade para redes sociais (TikTok, Instagram), investigação académica e serviços governamentais. Para a maioria dos jovens lituanos, o smartphone é o principal dispositivo para verificação de identificação através do Smart-ID ou Mobile-ID, que estão integrados em praticamente todos os aspetos da vida (Centro Nacional de cibersegurança [NCSC], 2025).

Principais Fatores de Risco

Apesar da elevada proficiência técnica, existe uma "lacuna de confiança" em relação à engenharia social. Muitos utilizadores jovens, particularmente estudantes internacionais e pessoas à procura de emprego, demonstram um elevado nível de confiança em ambientes "comunitários" como os Grupos do Facebook (NCSC, 2025). A utilização intensiva de ferramentas de autenticação automatizadas (Smart-ID) pode, por vezes, levar à "fadiga de autenticação", em que os utilizadores aprovam notificações push numa avaliação crítica, facilitando o acesso não autorizado às contas (Communications Regulatory Authority [RRT], 2026).

Canais de Apoio e Denúncia

A Lituânia oferece diversos canais robustos de assistência cibernética. O Centro Nacional de cibersegurança (NCSC) atua como a principal autoridade técnica. Para casos de fraude e roubo de identificação, a Polícia Lituana opera o portal epolicija.lt para denúncias formais. Além disso, a iniciativa Saugus Internetas disponibiliza recursos educacionais e uma linha de apoio direcionada especificamente para jovens e educadores (Saugus Internetas, 2026).

Ameaça do Facebook

Recrutamento anónimo e recolha de dados



Plataforma principal

Grupos do Facebook (por exemplo, "Estrangeiros em Vilnius", "Empregos para Estudantes")



Descrição resumida

Burlões exploram o recurso "Membro Anónimo" para publicar vagas de emprego fraudulentas. Estes visam os jovens, oferecendo trabalho remoto "fácil" para recolher fotografias de documentos de identificação e autorizações de residência para roubo de identidade (NCSC, 2025).



Cenário típico da juventude

Um estudante vê uma publicação anónima para um "Assistente de Redes Sociais". Após uma breve conversa pelo Messenger, o "empregador" pede uma fotografia do seu documento de identificação para "verificar o direito ao trabalho na UE". Assim que a fotografia é enviada, o utilizador é bloqueado e o seu documento de identificação é usado para abrir uma conta num neobanco (Lietuvos Policija, 2026).



Como funciona?

- O burlão publica anonimamente uma vaga de emprego bem remunerada.
- Transfere a conversa para aplicações privadas e encriptadas.
- Solicita documentos confidenciais (Cartão de Cidadão/Passaporte) imediatamente.
- A vítima é bloqueada e os seus dados são vendidos na dark web.



Sinais de alerta

- Utilização do estatuto de "Membro Anónimo" para anúncios de vagas de emprego.
- Solicitações de documentos pessoais antes da formalização de um contrato ou entrevista.
- Ofertas salariais que ultrapassam largamente o salário médio de um estudante lituano.



Sugestões de prevenção

- Nunca partilhe fotografias de documentos de identificação em chats de redes sociais.
- Verifique a existência da empresa através do site Rekvizitai.lt.
- Solicite uma entrevista por vídeo ou uma reunião presencial num escritório registado.



O que fazer se isto acontecer?

- Denuncie imediatamente o roubo de dados em epolicija.lt.
- Contacte o seu banco para alertar sobre uma possível tentativa de falsificação de identidade.
- Avise os moderadores do grupo para removerem a publicação.



Gravidade

Probabilidade 5/5 - Esta é a ameaça de engenharia social mais prevalente nos círculos de expatriados e jovens lituanos em 2026 (NCSC, 2025).



Fontes principais

NCSC (2025); Polícia Lituana (2026)

Ameaça do Instagram

Burlas de Emprego / Fraudes de Recrutamento



Plataforma principal

Instagram



Descrição resumida

A fraude de recrutamento no Instagram tornou-se uma ameaça relevante para os jovens na Lituânia. Os burlões fazem-se passar por funcionários de RH, recrutadores ou representantes de empresas conhecidas e usam mensagens diretas ou publicações com aparência patrocinada para oferecer falsas oportunidades de emprego. O objetivo geralmente é recolher dados pessoais, cópias de documentos de identificação, informações bancárias ou pequenas taxas de "registo" ou "processamento".



Cenário típico da juventude

Um estudante universitário ou recém-licenciado na Lituânia vê uma publicação no Instagram que anuncia um trabalho remoto flexível com um salário atraente. Após gostar ou seguir a página, recebe uma mensagem direta de uma conta que alega representar uma empresa conhecida. O "recrutador" pede que a vítima avance rapidamente com a candidatura, enviando currículo, dados do documento de identificação e informações bancárias, ou pagando uma pequena taxa para materiais de formação ou processamento de contrato. Após o envio dos dados ou o pagamento, a conta desaparece ou continua a burla, usando as informações da vítima.



Como funciona?

- Um burlão cria um perfil falso de empresa ou recrutador usando um logótipo copiado, imagens de vagas de emprego e publicações com aparência profissional.
- Estes têm como alvo os jovens através de publicações no Instagram, stories, anúncios ou mensagens diretas, oferecendo empregos a tempo parcial, remotos ou adequados para estudantes.
- O burlão cria uma sensação de urgência, dizendo que a vaga é limitada ou que a inscrição deve ser feita imediatamente.
- A vítima é solicitada a fornecer documentos pessoais, dados de contacto, informações bancárias ou um pequeno pagamento para "registo", "formação" ou "integração".
- Após receber os dados ou o dinheiro, o burlão bloqueia a vítima ou usa as informações para roubo de identidade ou outros tipos de fraude.

Ameaça do Instagram

Burlas de emprego / Fraudes de recrutamento



Sinais de alerta

O recrutador entra em contacto com o utilizador inesperadamente através de mensagens diretas no Instagram.

A conta tem poucos seguidores, pouca interação real ou foi criada recentemente.

A oferta de emprego promete um rendimento muito alto para um trabalho simples.

O recrutador solicita cópias de documentos de identificação, dados bancários ou pagamento logo no início do processo.



Medidas de prevenção

Verifique a empresa através do seu site oficial e canais de contacto oficiais.

Nunca envie documentos de identificação, dados bancários ou códigos pessoais pelo chat do Instagram.

Não pague nenhuma taxa para ter acesso a uma oferta de emprego, formação ou processo de recrutamento.

Solicite um e-mail formal do domínio da empresa e peça uma entrevista presencial.



O que fazer se isto acontecer?

- Interrompa imediatamente a comunicação e não envie mais informações nem dinheiro.
- Guarde capturas de ecrã da conta, mensagens, oferta de emprego e qualquer solicitação de pagamento.
- Caso dados pessoais ou documentos de identificação tenham sido partilhados, denuncie o incidente à Polícia da Lituânia através do site epolicija.lt.
- Caso dados bancários tenham sido partilhados ou algum pagamento tenha sido efetuado, entre em contacto com o banco imediatamente.
- Denuncie a burla ao Centro Nacional de cibersegurança e procure orientação através dos canais nacionais de segurança online.



Gravidade

Probabilidade 4/5 - Esta ameaça é altamente relevante para estudantes, recém-licenciados e jovens à procura de emprego, pois o Instagram é amplamente utilizado para networking, trabalhos extra e oportunidades digitais, e os burlões exploram a confiança em marcas conhecidas.



Fontes principais

Centro Nacional de cibersegurança (NCSC)

Polícia Lituana

Internet Segura

Autoridade Reguladora das Comunicações (RRT)

Ameaça do TikTok

Fraude em transmissões em direto e passatempos com figuras públicas



Plataforma principal

TikTok



Descrição resumida

Burlões usam videoclipes em loop de alta qualidade de influenciadores ou figuras públicas populares para apresentar eventos "em direto". Estes enganam os jovens para que paguem "taxas de verificação" ou insiram dados bancários para ganhar prémios (Saugus Internetas, 2026).



Cenário típico da juventude

Um adolescente entra numa transmissão em direto de um gamer famoso. Um chat automatizado afirma que ele ganhou um iPhone, mas precisa pagar uma "taxa aduaneira" de 10€ através de um link na bio. O adolescente paga, mas o link leva a um site de phishing que permite aos burlões aceder aos dados do cartão e realizar pagamentos fraudulentos.



Como funciona?

- Um burlão transmite em direto um vídeo roubado de uma figura pública.
- Falsifica os números de espectadores "em direto" para aumentar a credibilidade.
- Direciona os utilizadores para um link de phishing para "reclamar" recompensas.
- Recolhe informações de cartão de crédito ou início de sessões Smart-ID.



Sinais de alerta

- O vídeo "Em direto" tem baixa resolução ou está claramente em loop.
- O nome de utilizador da conta é uma variação de um nome real (por exemplo, @FamousStar_LT_Official).
- Exigência de pagamento para obter um prémio "gratuito".



Medidas de prevenção

- Verifique se há o selo de verificação azul oficial.
- Consulte a secção "Sobre esta conta" para ver o histórico da conta.
- Nunca forneça os dados do seu cartão para "reclamar" um prémio.



O que fazer se isto acontecer?

- Bloqueie o seu cartão bancário imediatamente através da aplicação para telemóvel.
- Denuncie a transmissão como fraudulenta à plataforma.
- Informe o NCSC sobre o URL malicioso.



Gravidade

Probabilidade 4/5 – Altamente eficaz entre adolescentes mais jovens que seguem influenciadores populares (RRT, 2026).



Fontes principais

Internet Segura (2026); Alertas de Segurança Meta (2025).

Ameaça por e-mail

Phishing através de códigos QR (Quishing)



Plataforma principal

E-mail



Descrição resumida

E-mails maliciosos fazem-se passar por instituições lituanas (por exemplo, VMI ou Sodra) usando códigos QR para contornar os filtros de e-mail. Estes códigos levam a portais de início de sessão falsos concebidos para roubar credenciais do Smart-ID (NCSC, 2025).



Cenário típico da juventude

Um estudante universitário recebe um e-mail sobre um "Reembolso de Impostos VMI". Em vez de um link, o e-mail mostra um código QR para "Digitalizar para iniciar sessão com Smart-ID". O estudante digitaliza o código, insere o seu PIN num site falso e a sua conta bancária é acedida (VMI, 2026).



Como funciona?

- O burlão envia um e-mail de alta urgência com um código QR.
- O código contorna o software de segurança que apenas analisa links de texto.
- O utilizador digitaliza o código QR com o telemóvel, abrindo um site de phishing.
- O utilizador fornece credenciais Smart-ID/bancárias.



Sinais de alerta

- Utilização de um código QR como única forma de início de sessão.
- O endereço de e-mail do remetente não pertence a um domínio .gov.lt ou .vmi.lt.
- Linguagem que pressiona o utilizador a agir em questão de minutos.



Medidas de prevenção

- Aceda sempre diretamente aos portais estatais (vmi.lt, sodra.lt).
- Use um leitor de QR Code que mostre uma pré-visualização do URL de destino.
- Desconfie de qualquer e-mail que solicite autenticação por Smart-ID.



O que fazer se isto acontecer?

- Revogue imediatamente os seus certificados Smart-ID.
- Contacte a linha de emergência do seu banco.
- Denuncie o e-mail para cert@nksc.lt.



Gravidade

Probabilidade 4/5 – Uma ameaça que cresce rapidamente em 2026, à medida que os scanners se tornam mais hábeis em contornar os filtros tradicionais (NCSC, 2025).



Fontes principais

VMI (2026); NCSC (2025).



Co-funded by
the European Union

Conclusões

Os resultados indicam que os jovens lituanos são cada vez mais visados por burlas "específicas da plataforma" que exploram a infraestrutura digital local (Smart-ID e confiança da comunidade do Facebook). Estas ameaças são relevantes porque refletem os hábitos diários dos jovens: procura de emprego, interação com influenciadores e utilização de serviços públicos online.

Candidatura ao Projeto ESCAP(E+):

Orientações de formação: Foque-se em "Alfabetização Visual" - reconhecendo transmissões "em direto" falsas e publicações fraudulentas do "Anonymous".

Cenários de Realidade Virtual: Crie um "Escritório VMI Digital" imersivo onde os jogadores devem distinguir entre um início de sessão QR legítimo e uma tentativa de phishing.

Conteúdo informativo: Distribua infográficos que destaquem a exigência legal de que os empregadores lituanos se registem no Rekvizitai.lt.

Recursos

- Autoridade Reguladora das Comunicações [RRT]. (2026). Relatório sobre os hábitos digitais e a segurança dos jovens lituanos. <https://www.rrt.lt>
- Polícia da Lituânia. (2026). Diretrizes de prevenção de crimes cibernéticos e fraudes para 2026. <https://policija.lrv.lt>
- Centro Nacional de cibersegurança [NCSC]. (2025). Relatório sobre o estado da cibersegurança na Lituânia: Tendências da engenharia social. <https://www.nksc.lt>
- Saugus Internetas. (2026). Segurança online dos jovens e protocolos de denúncia. <https://www.saugusinternetas.lt>
- Estatísticas da Lituânia. (2026). Sociedade da informação na Lituânia: Utilização das TIC por faixa etária. <https://osp.stat.gov.lt>
- Inspeção Tributária Estatal [VMI]. (2026). Aviso de segurança sobre phishing e códigos QR fraudulentos. <https://www.vmi.lt>



ESCAP(E+)

Roménia

INVESTIGAÇÃO DOCUMENTAL

Visão geral

Hábitos digitais dos jovens (principais plataformas e utilização típica)

Na Roménia, a utilização da internet entre adolescentes é quase universal e fortemente baseada em hábitos diários: um estudo nacional recente revela que 95,7% dos alunos do ensino secundário utilizam a internet todos os dias, principalmente para comunicar nas redes sociais e consumir conteúdo em plataformas sociais, muitas vezes consumindo mais do que criando. Isto torna o TikTok, Instagram, YouTube e as aplicações de mensagens (Messenger/WhatsApp) essenciais para a forma como os jovens socializam, acompanham tendências, descobrem oportunidades (eventos, empregos, bolsas de estudo) e constroem a sua identidade. Este mesmo padrão de elevado consumo também cria um ambiente propício à rápida disseminação de desinformação viral, desafios arriscados e esquemas de fraude (links na bio, redirecionamentos no Telegram/WhatsApp, "sorteios", formulários falsos).

Principais fatores de risco/vulnerabilidades na Roménia

Os desafios de segurança online enfrentados pelos jovens romenos são moldados pela entrada precoce nas redes sociais, pelo tempo excessivo passado em frente aos ecrãs e pela dinâmica de pressão social que se estende da escola para os espaços online:

Elevado tempo de exposição e acesso precoce

Um estudo da Save the Children Roménia de 2025 (conforme relatado pela Agerpres) indica que 48,3% das crianças passam mais de 6 horas por dia no ambiente digital, sendo que grande parte desse tempo é gasto em redes sociais. A exposição prolongada aumenta o contacto com estranhos, a visibilidade de conteúdo prejudicial e a probabilidade de partilha ou cliques impulsivos.

Cyberbullying, assédio e ataques motivados por humilhação (frequentemente ligados ao ambiente escolar)

O perfil da Roménia elaborado pela EU Kids Online observa que as experiências negativas online das crianças aumentaram (por exemplo, 33% em 2018 contra 21% em 2010) e descreve padrões de cyberbullying (presenciar bullying aumenta com a idade; as raparigas geralmente relatam sentir-se mais incomodadas com isso).

Visão geral

Na prática, isto geralmente manifesta-se através de páginas de "confissões/exposições", partilha de capturas de ecrã, disseminação de boatos e assédio coordenado entre colegas da mesma turma.

Fraude, falsificação de identificação e exploração de "pagamentos instantâneos".

Jovens romenos estão expostos a burlas que exploram a confiança e a rapidez: pedidos de "dinheiro urgente" em contas hackeadas, sorteios falsos, links de pagamento de marketplaces/serviços de entrega ou phishing disfarçado de bilhetes/empregos/bolsas de estudo. Normalmente, estas burlas levam os utilizadores do TikTok/Instagram para o Telegram/WhatsApp e, em seguida, para links encurtados ou formulários clonados, onde dados pessoais ou informações de pagamento são recolhidos.

Operações de desinformação e influência em ecossistemas de vídeos curtos.

A elevada dependência das redes sociais para notícias/atualizações aumenta a vulnerabilidade a conteúdo enganoso, especialmente quando a plataforma valoriza vídeos emocionais ou sensacionalistas e quando a verificação é rara.

Principais canais de apoio/denúncia na Roménia

DNSC (Diretoria Nacional Romena de cibersegurança): autoridade nacional com a PNRISC (Plataforma Nacional de Notificação de Incidentes de cibersegurança) para notificação de incidentes; a DNSC também disponibiliza o telefone 1911 (acessível a partir da Roménia) e o link da PNRISC na sua página de contacto oficial.

Telefone para Crianças - 116 111: linha de apoio gratuita para crianças/adolescentes (incluindo bullying/abuso, problemas de saúde mental e danos online); também desenvolve iniciativas de prevenção do cyberbullying.

Denúncia à polícia: em casos de crimes cibernéticos (fraude/chantagem/roubo de identidade/extorsão sexual), as vítimas podem apresentar queixa através dos canais da Polícia Romena (unidades locais/estruturas de combate ao crime cibernético).

Ameaça do Facebook

Anúncios falsos de "Alojamento para Estudantes" e pagamentos antecipados.



Plataforma principal

Facebook



Descrição resumida

Falsos senhorios publicam anúncios de arrendamento atrativos em grupos de cidades universitárias ou do ensino secundário, pedem um pagamento antecipado para “garantir o quarto” e enviam contratos ou documentos de identificação convincentes, mas falsificados. Após o pagamento, o anúncio desaparece e o perfil bloqueia a vítima.



Cenário típico da juventude

Um estudante do primeiro ano, ou um recém-diplomado do ensino secundário que se muda para uma cidade universitária como Bucareste, Cluj, Iași ou Timișoara, entra em grupos de arrendamento no Facebook para encontrar alojamento rapidamente antes do início do ano letivo. Encontra um apartamento que parece perfeito – boas fotografias, localização central, “perto do campus” e um preço abaixo do mercado. O “senhorio” diz que há muitas pessoas interessadas e pede um pequeno pagamento antecipado, como depósito, para reservar o quarto, enviando uma fotografia de um documento de identificação aparentemente credível e um “contrato” simples para criar confiança. Depois de a transferência ser feita, muitas vezes por transferência bancária imediata ou Revolut, o anúncio desaparece, o perfil bloqueia o estudante e o número de telefone deixa de responder.

Ameaça do Facebook

Anúncios falsos de "Alojamento para Estudantes" e pagamentos antecipados.



Como funciona?

- Um burlão publica um anúncio atrativo de "arrendamento para estudantes" em grupos romenos de alojamento no Facebook, frequentemente em grandes cidades universitárias.
- O preço é geralmente abaixo do valor de mercado e as fotografias/descrição parecem profissionais, por vezes copiadas de anúncios reais.
- O burlão transfere rapidamente a conversa para mensagens privadas ou WhatsApp e cria urgência, usando frases como "há muitas pessoas interessadas" ou "o primeiro a pagar reserva".
- Envia "provas" para parecer legítimo: uma fotografia de um documento de identificação falsificada/editada, um contrato falso ou um pequeno vídeo do apartamento, roubado de outro local.
- Recusa uma visita presencial e apresenta desculpas, como estar fora da cidade, a chave estar com um vizinho ou o atual inquilino ainda estar no apartamento.
- Pede um pagamento antecipado, como taxa de reserva, depósito ou primeira renda, através de transferência imediata ou Revolut para "garantir o quarto".
- Assim que o dinheiro é enviado, o anúncio é apagado, a vítima é bloqueada e toda a comunicação termina.

Ameaça do Facebook

Anúncios falsos de "Alojamento para Estudantes" e pagamentos antecipados.



Sinais de alerta

- O preço está visivelmente abaixo do valor de mercado para uma área popular ("demasiado bom para ser verdade").
- O "proprietário" pressiona para que a situação pareça urgente: "muitas pessoas interessadas", "pague hoje ou o imóvel será arrendado".
- Recusa uma visita (presencial ou por vídeo em tempo real) ou dá desculpas constantes (está fora da cidade, as chaves não estão disponíveis).
- Exige pagamento antecipado antes de qualquer visita (taxa de reserva/depósito/primeiro mês).
- Prefere pagamento apenas por transferência instantânea/Revolut e evita contratos rastreáveis ou canais oficiais.
- Envia fotografias de identificação/contrato que parecem editadas (texto desfocado, nomes diferentes, fontes inconsistentes, detalhes em falta).
- O perfil parece suspeito: conta nova, poucos amigos, fotografias genéricas, atividade inconsistente ou publicações copiadas.
- O estilo de comunicação é inconsistente (respostas copiadas e coladas, evita perguntas específicas sobre serviços públicos, termos do contrato de aluguer ou vizinhança).



Medidas de prevenção

- Insista sempre numa visita presencial ou, no mínimo, numa chamada de vídeo em direto onde o proprietário mostre o apartamento em tempo real (incluindo a vista da rua, a entrada e detalhes importantes do interior).
- Nunca envie um pagamento antecipado para "reservar" um imóvel antes de verificar a propriedade e a identificação do proprietário.
- Solicite comprovativos claros e consistentes de propriedade ou do direito de arrendar (por exemplo, documentos de propriedade) e verifique os nomes em todos os documentos; desconfie se os documentos parecerem editados ou ilegíveis.
- Utilize um contrato por escrito com todos os detalhes (morada completa, dados de identificação do inquilino/proprietário, aluguer, depósito, contas de serviços públicos, forma de pagamento) e não confie em capturas de ecrã ou "modelos" enviados por chat.
- Pague apenas por métodos rastreáveis após a assinatura e verificação; evite a pressão para usar transferências instantâneas.
- Analise cuidadosamente o perfil do proprietário (idade da conta, histórico de atividades, amigos em comum, consistência das publicações) e tenha cautela com perfis recém-criados ou "vazios".
- Use plataformas ou agências de aluguer fiáveis sempre que possível e denuncie anúncios suspeitos aos administradores do grupo do Facebook e à própria plataforma.

Ameaça do Facebook

Anúncios falsos de "Alojamento para Estudantes" e pagamentos antecipados.



O que fazer se isto acontecer?

- Interrompa toda a comunicação e não envie mais dinheiro, mesmo que o burlão prometa um reembolso.
- Reúna e guarde imediatamente as provas: capturas de ecrã do anúncio, detalhes do perfil, mensagens de chat, números de telefone, dados bancários/Revolut, recibos e quaisquer documentos que tenham sido enviados.
- Denuncie o perfil e a publicação ao Facebook e informe os administradores do grupo para que possam removê-los e alertar outros utilizadores.
- Contacte o seu banco/provedor de pagamento o mais rápido possível para solicitar uma reversão da transferência e sinalizar a conta do destinatário como fraudulenta (o sucesso depende da rapidez, portanto, aja rapidamente).
- Se partilhou os dados do seu cartão, bloqueie-o e solicite um novo; monitorize as suas contas à procura de transações não autorizadas.
- Apresente uma participação à polícia na Roménia e forneça todas as provas e detalhes do pagamento, especialmente a conta/IBAN do beneficiário e a referência da transferência.
- Se partilhou documentos pessoais (Cartão de Cidadão/NIF), fique atento a possíveis usos indevidos da sua identificação, considere informar o seu banco e a sua operadora de telemóvel e tenha cautela redobrada com futuras solicitações de verificação ou empréstimos/assinaturas inesperados.
- Avise os seus amigos/colegas de turma que vivem no mesmo alojamento para que a burla não se espalhe, mas evite divulgar informações confidenciais publicamente (partilhe-as apenas com administradores, polícia ou banco).



Gravidade

Alta gravidade, pois as vítimas podem perder quantias significativas de dinheiro rapidamente (depósito/aluguer adiantado) e, se partilharem dados de identificação ou informações pessoais, a burla pode agravar-se, resultando em uso indevido de identificação e fraudes mais direcionadas.



Fontes principais

Diretoria Nacional de cibersegurança (DNSC). (s.d.). Contacto / apoio e denúncias. <https://www.dnsc.ro/contact>
DNSC. (s.d.). Plataforma Nacional de Denúncia de Incidentes de cibersegurança (PNRISC). <https://pnrisc.dnsc.ro/>
SigurantaOnline.ro. (s.d.). O que fazer em caso de fraude online. <https://sigurantaonline.ro/ce-fac-in-caz-de-frauda/>
Polícia Romena. (s.d.). Métodos de fraude online e ataques de spoofing (orientações). <https://politiaromana.ro/ro/comunicate/metode-de-inselaciune-in-mediul-online-si-atacurile-de-tip-spoofing>

Ameaça do Instagram

Burla do "Embaixador da Marca" direcionada a pequenos criadores de conteúdo.



Plataforma principal

Instagram



Descrição resumida

Mensagens diretas oferecem promoções exclusivas para embaixadores da marca (roupa, cosméticos, tecnologia) e pedem aos utilizadores que paguem "taxas alfandegárias/de envio" ou iniciem sessão no "portal da marca". As vítimas perdem dinheiro ou têm as suas contas comprometidas e usadas para outras burlas.



Cenário típico da juventude

Um adolescente ou jovem adulto com uma conta pequena, mas ativa, no Instagram (geralmente a publicar conteúdo de moda, ginásio, estilo de vida ou maquilhagem) recebe uma mensagem direta de uma "marca" oferecendo um contrato de embaixador(a) e produtos gratuitos. A mensagem parece profissional e inclui um link para um "portal da marca" ou um pedido para pagar uma pequena taxa de envio/alfândega. Entusiasmado(a) com a colaboração, o(a) criador(a) paga a taxa ou acede ao site através do link, após o que perde o dinheiro e/ou a conta do Instagram é invadida e usada para enviar mensagens a amigos com burlas.



Como funciona?

- Um burlão cria um perfil de marca falso (logótipo, destaques, seguidores falsos e publicações copiadas).
- Estes enviam mensagens diretas para pequenos criadores na Roménia com uma oferta de "embaixador/colaboração" e prometem produtos gratuitos + códigos de desconto.
- Enfatizam a urgência e a exclusividade ("vagas limitadas", "responda hoje").
- Solicitam uma "pequena taxa" (envio/alfândega/manuseamento) paga através de um link, Revolut ou transferência bancária, ou enviam um link para um "portal da marca".
- O link de pagamento recolhe dados do cartão ou desencadeia fraude de subscrição; o link do portal é uma página de phishing que rouba credenciais do Instagram (por vezes também códigos de autenticação de dois fatores).
- Uma vez comprometida, a conta da vítima é usada para aplicar burlas aos seguidores (pedidos de dinheiro, sorteios falsos, links de phishing).

Ameaça do Instagram

Burla do "Embaixador da Marca" direcionada a pequenos criadores de conteúdo.



Sinais de alerta

- A marca entra em contacto consigo do nada, com uma mensagem genérica e sem detalhes reais da campanha.
- Insistem que deve pagar o envio/taxas alfandegárias para receber produtos "gratuitos".
- Enviam um link suspeito (URL encurtada, domínio estranho, erros ortográficos, páginas não oficiais).
- Solicitam os seus dados de início de sessão, código de autenticação de dois fatores (2FA) ou querem que "verifique" a sua identidade através de uma página de início de sessão.
- O perfil da marca parece artificial: conta recente, publicações repetitivas, fotografias roubadas, baixo envolvimento, padrões estranhos de seguidores.
- Recusam-se a enviar um contrato/fatura por e-mail e evitam fornecer um endereço comercial verificável, detalhes do IVA ou um site oficial.
- Pressionam-no com urgência ou culpa ("escolheremos outra pessoa em 1 hora").



Medidas de prevenção

- Verifique a marca fora do Instagram: site oficial, detalhes da empresa, avaliações independentes e informações de contacto consistentes.
- Nunca pague taxas alfandegárias/de envio/manuseamento por uma colaboração que alega ser gratuita.
- Não faça "início de sessão" através de links enviados por mensagens diretas; aceda ao Instagram apenas pela aplicação ou site oficial.
- Analise cuidadosamente o perfil do remetente (idade da conta, envolvimento, qualidade dos comentários, parceiros marcados, colaborações reais com influenciadores).
- Solicite detalhes que os burlões geralmente não podem fornecer: contrato por escrito, resumo da campanha, domínio de e-mail oficial e método legítimo de faturação/envio.
- Ative uma segurança robusta: palavra-passe exclusiva, autenticação de dois fatores, alertas de início de sessão e revisão regular das sessões ativas.
- Se quiser testar a legitimidade, sugira que lhe enviem e-mails de um domínio oficial da empresa; recuse e-mails pessoais do Gmail/Yahoo que se referem à sua empresa.

Ameaça do Instagram

Burla do "Embaixador da Marca" direcionada a pequenos criadores de conteúdo.



O que fazer se isto acontecer?

- Pare de comunicar e não pague mais nada.
- Faça capturas de ecrã de tudo: mensagens diretas, perfil, links, solicitações de pagamento, recibos, endereços de e-mail e nomes de utilizador.
- Se iniciou sessão através de um link, altere imediatamente a palavra-passe do Instagram e a do seu e-mail, revogue as sessões desconhecidas e ative/atualize a autenticação de dois fatores.
- Denuncie o perfil e as mensagens ao Instagram e avise os seus seguidores através de stories/publicações caso a sua conta tenha sido comprometida.
- Se pagou com cartão, entre em contacto com o seu banco imediatamente para bloquear o cartão e solicitar uma reversão da transferência, se possível; monitorize as transações.
- Se o dinheiro foi enviado através do Revolut ou transferência bancária, denuncie ao provedor e apresente uma queixa à polícia com todas as provas.



Gravidade

- Gravidade média a alta, pois a burla pode causar prejuízo financeiro direto e também pode escalar para apropriação de contas, vitimização de seguidores e danos à reputação.



Fontes principais

- Meta. (s.d.). Evite burlas e phishing no Instagram. <https://help.instagram.com/>
- Meta. (s.d.). Proteja a sua conta do Instagram (dicas de segurança). <https://help.instagram.com/>
- Meta. (s.d.). Denuncie conteúdo abusivo ou suspeito no Instagram. <https://help.instagram.com/>
- SigurantaOnline.ro. (s.d.). O que fazer em caso de fraude online. <https://sigurantaonline.ro/ce-fac-in-caz-de-frauda/>
- Direção Nacional de cibersegurança (DNSC). (s.d.). Contacto / suporte e denúncias. <https://www.dnsc.ro/contact>
- DNSC. (s.d.). Plataforma Nacional de Relato de Incidentes de cibersegurança (PNRISC). <https://pnrisc.dnsc.ro/>

Ameaça do TikTok

Falsa "Seleção de Talentos/Concurso" com recolha de dados e reconhecimento facial.



Plataforma principal

TikTok



Descrição resumida

Os anúncios prometem oportunidades de seleção para anúncios/concursos musicais e solicitam o envio de vídeos curtos, além de dados de identificação "para comprovar a idade". Os vídeos e dados recolhidos podem ser reutilizados para tentativas de deepfake, falsificação de identificação ou burlas direcionadas.



Cenário típico da juventude

Um adolescente que publica vídeos no TikTok (dança, canto, comédia) vê um vídeo viral anunciando um "casting" para um comercial, videoclipe ou "concurso de talentos", com prémios e "seleção rápida". É solicitado que envie um vídeo curto e informações pessoais para "comprovar a idade" (foto do documento de identificação, nome completo, data de nascimento). Acreditando ser uma oportunidade real, envia o material através de um formulário, e-mail ou WhatsApp/Telegram, e os dados são reutilizados para falsificação de identificação, assédio ou futuras burlas, e o vídeo pode aparecer posteriormente em conteúdo deepfake ou contas falsas.



Como funciona?

- Os burlões publicam vídeos convincentes de castings/concursos usando logótipos, referências a figuras públicas ou linguagem que remete a "agências".
- Prometem seleção rápida, trabalhos remunerados ou prémios e têm como público-alvo adolescentes/jovens criadores na Roménia.
- Orientam os utilizadores a enviar as suas inscrições através de links na bio, Formulários Google, e-mail ou WhatsApp/Telegram.
- Solicitam um vídeo curto mostrando o rosto e a voz, além de dados para "verificação de idade" (foto do documento de identificação, data de nascimento, morada e telefone).
- Os dados recolhidos são usados para criar perfis falsos, tentar recuperar contas ou aplicar burlas personalizadas contra a vítima/família.
- As gravações de rostos e vozes são reutilizadas para conteúdo no estilo deepfake, para fins de personificação ou para pressionar a vítima através de chantagem.

Ameaça do TikTok

Falsa "Seleção de Talentos/Concurso" com recolha de dados e reconhecimento facial.



Sinais de alerta

- A "agência" não possui um site verificável, domínio de e-mail oficial ou dados da empresa (NIF/IVA/morada).
- Pedem fotografias de identificação ou dados sensíveis logo no primeiro passo "para comprovar a idade".
- O método de envio é informal ou arriscado (Telegram/WhatsApp, links de formulários aleatórios, e-mail pessoal).
- Promessas irreais: "seleção garantida", "pagamento instantâneo", "vagas limitadas - inscreva-se em 1 hora".
- A conta é nova, tem baixo envolvimento, conteúdo copiado ou os comentários parecem artificiais.
- Desencorajam os pais/responsáveis ou recusam-se a fornecer um processo de consentimento por escrito para menores.
- Pedem vídeos adicionais com ângulos/frases específicas que parecem mais uma "recolha de dados" do que uma seleção de casting.



Medidas de prevenção

- Considere qualquer solicitação de dados de identificação como de alto risco - castings profissionais raramente exigem identificação completa no primeiro contacto; para menores de idade, deve ser solicitado o envolvimento dos pais/responsáveis e procedimentos de consentimento claros.
- Verifique o organizador fora do TikTok: site oficial, registo da empresa, portefólio real, menções independentes e domínio de e-mail oficial.
- Utilize uma abordagem de envio segura: coloque marca de água nos vídeos (nome/data), evite enviar digitalizações completas de documentos de identificação e partilhe apenas informações mínimas até que a legitimidade seja confirmada.
- Solicite um briefing de casting formal: descrição do papel, datas, local, condições de pagamento, política de privacidade, retenção de dados e quem processa os dados.
- Caso seja necessária a verificação de idade, ofereça alternativas mais seguras (declaração de idade, ocultação parcial do documento de identificação ou verificação presencial posterior).
- Mantenha as contas seguras (palavras-passe fortes, autenticação de dois fatores) e limite os dados pessoais visíveis publicamente nos perfis.

Ameaça do TikTok

Falsa "Seleção de Talentos/Concurso" com recolha de dados e reconhecimento facial.



O que fazer se isto acontecer?

- Interrompa a comunicação e não forneça vídeos ou documentos adicionais.
- Guarde as evidências: capturas de ecrã do TikTok, do seu perfil, das mensagens, dos links dos formulários e do que enviou.
- Se enviou dados de identificação, monitorize possíveis usos indevidos de identificação (tentativas inesperadas de empréstimo/assinatura, chamadas/mensagens suspeitas) e reforce a segurança das suas contas de e-mail e redes sociais.
- Denuncie a conta e o conteúdo no TikTok e avise os seus colegas se a burla estiver a circular na sua comunidade.
- Se a burla evoluir para ameaças/chantagem, envolva imediatamente um adulto de confiança e denuncie o caso às autoridades romenas; guarde todas as provas.
- Em caso de incidentes cibernéticos ou suspeita de uso indevido de dados, denuncie ou comunique o caso ao DNSC/PNRISC e procure orientação.



Gravidade

- Alta gravidade, pois pode combinar a exposição de dados pessoais com a recolha de imagem e voz, possibilitando a falsificação de identificação, o uso indevido de deepfakes, burlas direcionadas e, potencialmente, coerção ou danos à reputação.



Fontes principais

- TikTok. (s.d.). Como denunciar um problema / uma conta. <https://support.tiktok.com/>
- TikTok. (s.d.). Privacidade e segurança de adolescentes. <https://support.tiktok.com/>
- DNSC. (s.d.). Contacto / apoio e denúncias. <https://www.dnsc.ro/contact>
- DNSC. (s.d.). Plataforma Nacional de Relato de Incidentes de cibersegurança (PNRISC). <https://pnrisc.dnsc.ro/>
- SigurantaOnline.ro. (s.d.). O que fazer em caso de fraude online. <https://sigurantaonline.ro/ce-fac-in-caz-de-frauda/>

Ameaça por e-mail

Falsa entrega - e-mails de "taxas alfandegárias" com links de pagamento por QR Code.



Plataforma principal

E-mail



Descrição resumida

E-mails falsos imitam notificações de entrega e cobram uma pequena taxa pendente, geralmente com um código QR ou link curto. As vítimas são direcionadas para uma página de pagamento falsa que captura os dados do cartão ou leva a burlas de subscrição.



Cenário típico da juventude

Um estudante ou jovem trabalhador faz regularmente compras online (roupa, eletrónica, cosméticos) e recebe um e-mail que parece ser uma notificação de entrega. A mensagem informa sobre uma pequena taxa de "alfândega/manuseamento/redirecionamento" e inclui um código QR ou um link curto para pagamento rápido. Como o valor é baixo e o e-mail parece urgente ("a entrega será devolvida"), a vítima digitaliza o código QR com o telemóvel, insere os dados do cartão numa página de pagamento convincente e, posteriormente, descobre transações não autorizadas ou uma subscrição recorrente.



Como funciona?

Os burlões enviam e-mails em massa que imitam notificações comuns de entregas/serviços de entregas em romeno.

O e-mail alega o pagamento de uma pequena taxa pendente (alfândega/manuseamento/confirmação de morada) e ameaça atrasar ou devolver a encomenda.

Um código QR ou link encurtado direciona a vítima para uma página de pagamento falsa, adaptada a dispositivos móveis. A página captura os dados do cartão e por vezes solicita confirmação por OTP/3D Secure.

As vítimas sofrem utilização fraudulenta do cartão (transações não autorizadas) ou são inscritas em esquemas de subscrições fraudulentas ocultas.

Os atacantes podem reutilizar os dados da vítima para futuros ataques de phishing e burlas direcionadas.

Ameaça por e-mail

Falsa entrega - e-mails de "taxas alfandegárias" com links de pagamento por QR Code.



Sinais de alerta

- O endereço/domínio do remetente não corresponde ao domínio oficial da transportadora/empresa (verifique atentamente se há erros de ortografia).
- Mensagem com saudação genérica e detalhes vagos sobre a encomenda (sem número de seguimento real, sem referência de pedido precisa).
- Pressão urgente: "pague hoje", "último aviso", "pacote devolvido", "entrega falhou".
- O pagamento é solicitado via QR Code/link curto, em vez de ser feito através da página/aplicação oficial de seguimento da transportadora.
- O link leva a um domínio suspeito que não parece ser de uma empresa de entregas ou de um sistema de pagamento bancário.
- A mensagem contém erros de linguagem, inconsistências na identidade visual da marca ou logótipos de baixa qualidade.
- O valor da taxa é excecionalmente baixo e foi concebido para transmitir uma sensação de "segurança ao pagar rapidamente".



Medidas de prevenção

- Nunca pague taxas de entrega/alfandegárias através de códigos QR ou links recebidos por e-mail - aceda diretamente ao site/aplicação da transportadora e verifique o estado da sua encomenda por lá.
- Verifique o domínio do remetente e compare-o com o site oficial da transportadora; considere pequenos erros ortográficos como um forte sinal de alerta.
- Verifique se o número de seguimento é válido e confirme os detalhes da encomenda através da plataforma onde fez a sua compra ou na página oficial de seguimento.
- Evite digitalizar códigos QR em e-mails; se for imprescindível, verifique o URL antes de abrir e não prossiga se o domínio parecer desconhecido.
- Use cartões virtuais ou cartões de utilização única, quando disponíveis, para pagamentos online e ative os alertas bancários para cada transferência.
- Mantenha o seu navegador e telemóvel atualizados e use filtros de spam/phishing; denuncie e-mails suspeitos como phishing no seu cliente de e-mail.

Ameaça por e-mail

Falsa entrega - e-mails de "taxas alfandegárias" com links de pagamento por QR Code.



O que fazer se isto acontecer?

- Pare imediatamente e não realize etapas ou pagamentos adicionais.
- Guarde as evidências: o e-mail (incluindo os cabeçalhos, se possível), capturas de ecrã do código QR/link, da página de pagamento e quaisquer confirmações de transferência.
- Contacte o seu banco com urgência para bloquear o cartão, contestar as cobranças e solicitar a reversão da transferência, se aplicável; monitorize a sua conta para pagamentos recorrentes.
- Se inseriu as suas credenciais de início de sessão em algum lugar, altere as suas palavras-passe imediatamente e ative a autenticação de dois fatores (2FA).
- Denuncie o e-mail de phishing no seu cliente de e-mail e informe a empresa de entregas caso a marca dela esteja a ser falsificada.
- Comunique ou denuncie o incidente ao DNSC/PNRISC e apresente uma queixa à polícia caso haja prejuízo financeiro, utilizando todos os detalhes do pagamento e do destinatário.



Gravidade

- Alta gravidade, pois a isca de uma "pequena taxa" pode rapidamente levar ao roubo de dados do cartão, cobranças repetidas de subscrições e comprometimento mais amplo da identificação/conta.



Fontes principais

- Google. (s.d.). Evite e denuncie e-mails de phishing. <https://support.google.com/mail/answer/8253>
- Microsoft. (s.d.). Proteja-se contra phishing. <https://support.microsoft.com/>
- DNSC. (s.d.). Contacto / apoio e denúncias. <https://www.dnsc.ro/contact>
- DNSC. (s.d.). Plataforma Nacional de Relato de Incidentes de cibersegurança (PNRISC). <https://pnrisc.dnsc.ro/>
- SigurantaOnline.ro. (s.d.). O que fazer em caso de fraude online. <https://sigurantaonline.ro/ce-fac-in-caz-de-frauda/>

Conclusões

O contexto da segurança online dos jovens na Roménia é moldado pelo uso quase universal e diário da internet entre adolescentes, o que torna o TikTok, Instagram, YouTube e aplicações de mensagens (Messenger/WhatsApp) essenciais para a forma como os jovens socializam, acompanham tendências e acedem a oportunidades. Este ecossistema de alto alcance e consumo intenso cria caminhos rápidos para o risco: conteúdo prejudicial, desinformação viral, desafios arriscados e esquemas de burlas podem espalhar-se rapidamente através de feeds, mensagens diretas, links em biografias e redirecionamentos para Telegram/WhatsApp.

Uma conclusão fundamental é que as principais vulnerabilidades não são apenas técnicas, mas também fortemente comportamentais e sociais. O acesso precoce às redes sociais, o tempo excessivo gasto em frente aos ecrãs e a pressão dos pares aumentam a probabilidade de cliques e partilhas impulsivas, da partilha excessiva de dados pessoais e de reações impulsivas - condições que os burlões e manipuladores exploram ativamente. Paralelamente, o cyberbullying e o assédio moral são amplificados pela dinâmica dos grupos escolares, pela cultura de capturas de ecrã e por páginas de "confissões/exposição", que podem escalar rapidamente e causar danos emocionais significativos.

Os riscos de fraude e falsificação de identificação são particularmente relevantes porque exploram a rapidez e a confiança: pedidos de dinheiro provenientes de contas invadidas, sorteios falsos, links de pagamento de marketplaces/serviços de entrega e phishing disfarçado de bilhetes/empregos/bolsas de estudo frequentemente levam os jovens do TikTok/Instagram para o Telegram/WhatsApp e, em seguida, para formulários clonados ou páginas de pagamento falsas. Em ambientes de vídeos curtos, onde o conteúdo com forte apelo emocional é recompensado e a verificação é rara, a desinformação e as táticas de influência também podem ter um impacto desproporcional.

Por fim, embora a Roménia possua canais claros de apoio e denúncia (DNSC/PNRISC, SOS Criança 116 111, denúncia à polícia), a sua eficácia depende da sensibilização e da usabilidade prática para jovens e famílias.

Conclusões

A resposta mais relevante neste contexto nacional é, portanto, uma abordagem combinada: alfabetização digital prática (reconhecer padrões de burlas e indícios de desinformação), hábitos de proteção de contas (autenticação de dois fatores, palavras-passe fortes, verificação de sessão), orientações de resposta rápida (o que fazer nos primeiros minutos/horas) e uma cultura mais forte de denúncia e apoio que reduza o estigma - especialmente em casos de assédio, extorsão sexual e fraude.

Recursos

- Direção Nacional de cibersegurança. <https://www.dnsc.ro/contact>
- Direção Nacional de cibersegurança. Plataforma Nacional de Notificação de Incidentes de cibersegurança (PNRISC). <https://pnrisc.dnsc.ro/>
- Save the Children Roménia. (28 de março de 2025). Estudo: Quase metade das crianças passa mais de 6 horas por dia em ambientes digitais. Agerpres. <https://agerpres.ro/english/2025/03/28/save-the-children-study-almost-half-of-children-spend-over-6-hours-day-in-the-digital-environment--1435334>
- Pont Group. (24 de fevereiro de 2025). Resultados do estudo “A relação entre os hábitos de consumo de informação e media de crianças e jovens na Roménia”. <https://en.pontgroup.org/2025/02/24/findings-of-the-study-the-relationship-with-information-and-media-consumption-habits-of-children-and-young-people-in-romania/>
- EU Kids Online. (s.d.). Roménia: Perfil do país. London School of Economics and Political Science. <https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online/participating-countries/romania>
- Associação de Telefones Infantis. (s.d.). Telefone Infantil – 116111 (Casa). <https://telefonulcopilului.ro/>
- Associação de Telefones Infantis. (s.d.). #BeCyberSafe (Campanha de prevenção ao cyberbullying). <https://telefonulcopilului.ro/proiecte/becybersafe/>



ESCAP(E+)

**Universidade de Istambul-
Cerrahpasa IUC**

**INVESTIGAÇÃO
DOCUMENTAL**



Co-funded by
the European Union

Visão geral

Na Turquia, o uso da internet entre crianças e adolescentes já está profundamente enraizado no quotidiano. De acordo com as estatísticas infantis de 2024 do TurkStat, 91,3% das crianças entre os 6 e os 15 anos utilizam a internet e 66,1% usam redes sociais; entre os jovens dos 11 aos 15 anos, o uso da internet atinge os 94,7%. As redes sociais também representam uma das utilizações mais comuns da internet entre as crianças que a utilizam regularmente (72,6%). Estes padrões fazem das redes sociais e do e-mail pontos de entrada centrais para riscos online, e não espaços periféricos.

Para os jovens turcos, os riscos cibernéticos mais relevantes não se limitam a ataques altamente técnicos. Em vez disso, as ameaças mais comuns baseiam-se na confiança e no comportamento: links de phishing, sorteios falsos, pedidos fraudulentos de compras ou pagamentos, falsificação de identificação, apropriação indevida de contas, roubo de identidade e conteúdo enganoso criado para manipular a atenção, as crenças ou as ações. Estes riscos propagam-se com especial facilidade em plataformas que combinam conteúdo visual, mensagens diretas, comentários, publicações patrocinadas e partilha rápida.

O contexto nacional também sugere diversos fatores de vulnerabilidade. Os jovens utilizadores acedem frequentemente à internet principalmente através de smartphones, interagem com conteúdo de influenciadores ou dos seus pares e transitam rapidamente entre o conteúdo da plataforma e links externos. Ao mesmo tempo, a partilha excessiva de informações pessoais, o uso de palavras-passe fracas, a reutilização de credenciais, a baixa frequência de verificação e o design persuasivo dos algoritmos de pesquisa podem aumentar a exposição a burlas e conteúdo enganoso.

A Turquia dispõe de diversos canais de apoio e denúncia relevantes para jovens e técnicos de juventude. Incidentes técnicos e ameaças cibernéticas prejudiciais podem ser comunicados à USOM (autoridade nacional de resposta a incidentes cibernéticos). Casos de crimes, fraudes e uso indevido de contas também podem ser encaminhados para o Departamento de Crimes Cibernéticos/unidades locais de combate ao cibercrime da Polícia Nacional Turca. Para orientação, prevenção e sensibilização, o ecossistema Internet Segura, ligado à BTK/GüvenliWeb e à Central de Ajuda da Internet, disponibiliza materiais de apoio práticos.

Visão geral

Comportamento digital dos jovens

Na Turquia, a conectividade digital está profundamente enraizada no quotidiano dos jovens. De acordo com os dados de TIC para crianças do TurkStat de 2024, 91,3% das crianças entre os 6 e os 15 anos utilizam a internet regularmente e 66,1% utilizam as redes sociais. Entre os utilizadores regulares de internet entre as crianças, as atividades mais comuns são assistir a vídeos (83,9%), fazer tarefas de casa ou aprendizagem online (75,0%), jogar ou baixar jogos (72,7%), usar redes sociais (72,6%) e enviar mensagens (65,2%). O envio e receção de e-mails é muito menos comum entre as crianças (13,2%), o que sugere que as plataformas sociais e as aplicações de mensagens dominam a interação diária, enquanto o e-mail é usado de forma mais seletiva para comunicação relacionada com a escola, matrículas e recuperação de contas.

Entre os jovens de 16 a 24 anos, o padrão torna-se ainda mais centrado na comunicação. Os dados da TurkStat sobre a juventude em 2024 mostram que os usos mais comuns da internet nessa faixa etária são mensagens de texto (98,5%), chamadas de voz ou vídeo (95,7%) e uso de redes sociais (95,3%). A exposição aos ecrãs também é substancial: entre os jovens de 11 a 15 anos que usam smartphones regularmente, 15,1% passam seis horas ou mais online aos fins de semana. Por essa razão, o Facebook, o Instagram e o TikTok devem ser compreendidos não como ferramentas ocasionais, mas como ambientes quotidianos onde a comunicação, o entretenimento, a influência dos pares e a exposição a riscos online ocorrem continuamente.

Principais fatores de risco

Um dos principais fatores de risco na Turquia é a normalização de comportamentos rápidos e frequentes de cliques, partilhas e reações em plataformas de redes sociais. As diretrizes oficiais turcas de segurança digital identificam o phishing e a engenharia social como ameaças centrais e alertam os utilizadores para não confiarem em links suspeitos, mensagens sobre prémios ou sorteios, ofertas de dinheiro fácil, ameaças, conteúdo que incite o medo ou comentários e mensagens diretas manipuladoras. Isto é especialmente relevante no Instagram, TikTok e Facebook, onde agentes maliciosos podem disseminar burlas através de stories, anúncios, perfis falsos, secções de comentários e mensagens privadas. A mesma lógica de manipulação também aparece em e-mails, através de avisos bancários falsos, mensagens de envio, alertas governamentais falsos e solicitações de verificação de conta.

Visão geral

Um segundo fator de risco importante é o roubo de identidade e o uso indevido de contas. As diretrizes turcas sobre roubo de identidade digital enfatizam que dados pessoais, como números de identificação nacional, palavras-passe, endereços, nomes de solteira da mãe e dados bancários ou de cartão, podem ser roubados através de phishing e engenharia social e, em seguida, usados para ações financeiras ou administrativas fraudulentas. Um terceiro fator é a desinformação e a desordem informacional. A SİBERAY observa que os mecanismos de controlo frágeis das redes sociais facilitam a rápida disseminação de informações falsas, capturas de ecrã falsas, publicações que induzem ao pânico e narrativas enganosas, antes que os utilizadores verifiquem a fonte original.

Canais de Apoio e Denúncia

Na Turquia, o apoio e a denúncia devem seguir uma abordagem em camadas. Primeiramente, publicações prejudiciais, contas falsas, tentativas de falsificação de identificação e mensagens fraudulentas visualizadas no Facebook, Instagram ou TikTok devem ser denunciadas por meio das ferramentas de denúncia integradas nas suas próprias plataformas, para que a remoção do conteúdo ou a ação contra a conta possam ser iniciadas rapidamente. Em âmbito nacional, o İhbarWeb da BTK e o serviço “İnternet İhbar Başvurusu” do e-Devlet são canais oficiais para denúncia de conteúdo ilegal online. Além disso, o İnternet Yardım Merkezi oferece orientação e apoio prático para utilizadores que enfrentam problemas de segurança online.

Quando o problema envolve links de phishing, sites maliciosos, tentativas de roubo de identificação ou ameaças mais amplas à segurança da informação, as denúncias podem ser enviadas à USOM, que opera 24 horas por dia, 7 dias por semana, e disponibiliza um formulário oficial de notificação. Em casos de fraude, coerção, extorsão, apropriação indevida de contas ou outros crimes, jovens e famílias podem utilizar os canais de denúncia do Departamento de Crimes Cibernéticos da Polícia Nacional Turca ou entrar em contacto com a polícia/112 em casos urgentes. Quando dados pessoais forem processados ou expostos ilegalmente, o titular dos dados deve primeiro entrar em contacto com o controlador de dados relevante e, em seguida, pode apresentar uma reclamação à Autoridade de Proteção de Dados Pessoais (KVKK), inclusive através do seu módulo de reclamações. Para apoio preventivo e sensibilização, a GüvenliWeb e a SİBERAY também oferecem orientações públicas sobre phishing, engenharia social, desinformação, privacidade e comportamento digital mais seguro.

Ameaça do Facebook

Páginas Falsas, Burlas no Marketplace e Links Fraudulentos no Facebook



Plataforma principal

Facebook



Descrição resumida

As ameaças geralmente surgem através de páginas falsas, publicações fraudulentas em grupos, ofertas fraudulentas em marketplaces e links maliciosos partilhados em comentários ou mensagens privadas. O objetivo costuma ser roubar dinheiro, credenciais ou informações pessoais.



Cenário típico da juventude

Um jovem na Turquia vê um telemóvel, bilhete ou produto de jogos muito barato num grupo do Facebook ou numa publicação de um marketplace. Após o envio de um depósito ou a inserção de dados através de uma página de pagamento falsa, o item nunca chega e dados pessoais ou financeiros podem ser expostos.



Como funciona?

1. O atacante cria um perfil, página ou anúncio falso.
2. É publicado um produto atraente ou uma mensagem urgente.
3. A vítima é direcionada para um chat privado ou para um link externo.
4. A vítima paga ou partilha dados pessoais/de pagamento.
5. O atacante desaparece ou reutiliza os dados.



Sinais de alerta

Preços irrealisticamente baixos;
Perfis de vendedor novos ou vazios;
Pedidos para sair da plataforma;
Pressão para enviar um depósito rapidamente;
Links de pagamento ou início de sessão suspeitos.



Medidas de prevenção

Verificar a identificação do vendedor e o histórico da conta;
Evitar pagamentos antecipados a pessoas desconhecidas;
Nunca partilhar dados de cartão de crédito ou de identificação através de chats;
Verificar ofertas suspeitas através dos canais oficiais;
Usar palavras-passe fortes e autenticação de dois fatores.

Ameaça do Facebook

Páginas Falsas, Burlas no Marketplace e Links Fraudulentos no Facebook



O que fazer se isto acontecer?

Interrompa imediatamente a comunicação.

Se o dinheiro foi enviado, entre em contacto com o banco ou provedor de pagamento.

Altere as palavras-passe caso os dados de início de sessão tenham sido partilhados.

Denuncie o perfil, a página ou o anúncio no Facebook.

Guarde capturas de ecrã e denuncie o incidente através dos canais nacionais de combate ao cibercrime.



Gravidade

4/5 - Alto, pois pode levar tanto a perdas financeiras quanto ao uso indevido de dados pessoais.



Fontes principais

GüvenliWeb - orientações sobre fraudes online GüvenliWeb - orientações sobre roubo de identidade

Canal oficial de denúncias da USOM

Canais de reclamação da EGM sobre crimes cibernéticos e da BTK

Ameaça do Instagram

Falsificação de Identidade, Phishing por Mensagem Direta e Sequestro de Contas no Instagram



Plataforma principal

Instagram



Descrição resumida

As ameaças cibernéticas frequentemente manifestam-se através de perfis falsos, contas comprometidas, burlas de sorteios e mensagens diretas criadas para roubar credenciais ou informações pessoais. Estes ataques baseiam-se na confiança, na curiosidade ou na pressão social.



Cenário típico da juventude

Um adolescente na Turquia recebe uma mensagem direta perguntando "É a pessoa presente nesta fotografia?" ou "Ganhou uma caixa de presentes". Depois de inserir os dados de início de sessão através do link partilhado, o utilizador perde o acesso à conta e o invasor começa a enviar mensagens aos seguidores a partir do perfil roubado.



Como funciona?

1. O atacante usa uma conta falsa ou roubada.
2. Uma mensagem direta, um comentário ou uma resposta nos stories cria curiosidade ou um sentido de urgência.
3. A vítima clica num link malicioso.
4. A vítima insere as suas credenciais numa página falsa.
5. O atacante sequestra a conta e utiliza-a para atacar outras pessoas.



Sinais de alerta

Mensagens do tipo "Ganhou"; pedidos de credenciais de início de sessão ou códigos de verificação; mensagens incomuns de um amigo; links encurtados ou não oficiais; perfis falsos a imitar marcas ou influenciadores.



Medidas de prevenção

Verificar mensagens incomuns por outro canal.
Ativar a autenticação de dois fatores.
Evitar aceder à conta através de links enviados por mensagens diretas.
Rever regularmente as definições de privacidade.
Denunciar imediatamente contas falsas ou suspeitas.

Ameaça do Instagram

Falsificação de Identidade, Phishing por Mensagem Direta e Sequestro de Contas no Instagram



O que fazer se isto acontecer?

Altere a palavra-passe do Instagram imediatamente.
Proteja a conta de e-mail vinculada.
Avisar os seguidores para não confiarem em mensagens recentes.
Denuncie casos de falsificação de identidade ou sequestro de conta ao Instagram.
Guarde capturas de ecrã e utilize os canais de denúncia nacionais quando necessário.



Gravidade

4/5 - Alto, pois pode expor mensagens pessoais, imagens, redes de contactos e informações relacionadas com a identificação.



Fontes principais

TÜİK - Estatísticas sobre Crianças 2024
TÜİK - Estatísticas sobre a Juventude 2024
GüvenliWeb - orientações sobre roubo de identificação e burlas online
Canais de denúncia de crimes cibernéticos da USOM e EGM

Ameaça do TikTok

Desinformação Viral, Redirecionamentos Fraudulentos e Conteúdo Manipulador no TikTok



Plataforma principal

TikTok



Descrição resumida

Os riscos cibernéticos propagam-se frequentemente através de vídeos virais, alegações enganosas, oportunidades falsas e redirecionamentos maliciosos inseridos em biografias, comentários ou mensagens privadas. A rápida circulação de conteúdo aumenta o risco de desinformação e de comportamentos de clique inseguros.



Cenário típico da juventude

Um jovem utilizador na Turquia assiste a um vídeo viral que afirma que uma bolsa de estudos, apoio governamental ou recompensa pode ser obtida através de um link na bio. O utilizador clica no link e envia os seus dados pessoais numa página falsa.



Como funciona?

1. O agressor partilha conteúdo emocional ou sensacionalista.
2. O vídeo incentiva os utilizadores a agir imediatamente.
3. A vítima clica num link na biografia, nos comentários ou nas mensagens.
4. A vítima insere credenciais, dados pessoais ou detalhes de pagamento.
5. O atacante recolhe dados ou continua a disseminar a burla.



Sinais de alerta

Alegações virais sem fonte oficial; mensagens do tipo "Aja agora" ou que incitam o medo; instruções para usar um link na bio para ações sensíveis; capturas de ecrã ou vídeos editados de origem duvidosa; solicitações de palavras-passe, dados de identificação ou informações de pagamento.



Medidas de prevenção

Verificar informações importantes através de instituições oficiais. Não confie em informações apenas porque estão em alta. Ter cuidado com links em biografias, comentários e mensagens diretas. Ajustar as definições de privacidade para reduzir contactos indesejados. Fazer uma pausa antes de reagir a conteúdos emocionais ou urgentes.

Ameaça do TikTok

Desinformação Viral, Redirecionamentos Fraudulentos e Conteúdo Manipulador no TikTok



O que fazer se isto acontecer?

Pare imediatamente de partilhar o conteúdo.
Apague qualquer publicação repetida se o conteúdo for falso.
Faça capturas de ecrã como prova.
Denuncie o vídeo ou a conta no TikTok.
Altere as palavras-passe caso alguma credencial tenha sido enviada e denuncie casos graves.



Gravidade

4/5 - Alto, porque a desinformação pode levar a comportamentos inseguros e os redirecionamentos fraudulentos podem resultar em roubo de dados.



Fontes principais

TÜİK - Estatísticas sobre Crianças 2024
TÜİK - Estatísticas sobre a Juventude 2024
SİBERAY - orientações sobre desordem informacional
Recursos da USOM, EGM Cybercrime, BTK e KVKK

Ameaça por e-mail

Roubo de Credenciais e Apropriação de Contas via E-mail



Plataforma principal

E-mail



Descrição resumida

E-mails fraudulentos imitam instituições confiáveis, como bancos, universidades, empresas de transporte, provedores de bolsas de estudo ou organismos públicos. O objetivo é induzir jovens a clicar em links falsos, inserir credenciais, partilhar dados pessoais ou descarregar anexos maliciosos.



Cenário típico da juventude

Um estudante na Turquia recebe um e-mail alegando que uma conta escolar, uma candidatura a bolsa de estudo ou a entrega de uma encomenda necessita de verificação urgente. A mensagem parece legítima, por isso o estudante insere os dados de início de sessão numa página falsa e, posteriormente, perde o acesso à caixa de correio eletrónico ou às contas associadas.



Como funciona?

1. Um e-mail falso é enviado.
2. Cria urgência, medo ou curiosidade.
3. A vítima clica num link malicioso ou abre um anexo.
4. A vítima acede a uma página de início de sessão falsa ou instala um malware.
5. Credenciais ou dados são roubados e reutilizados.



Sinais de alerta

Solicitações urgentes de verificação; endereços ou domínios de remetentes suspeitos; saudações genéricas; avisos inesperados de prémios, reembolsos ou entregas; solicitações de palavras-passe, códigos OTP ou dados bancários.



Medidas de prevenção

Não clicar em links ou anexos suspeitos.
Verificar atentamente o endereço do remetente.
Usar sites oficiais em vez de links de mensagens.
Ativar palavras-passe fortes e autenticação de dois fatores.
Nunca partilhar palavras-passe, códigos OTP ou informações de cartão por e-mail.

Ameaça por e-mail

Roubo de Credenciais e Apropriação de Contas via E-mail



O que fazer se isto acontecer?

Pare de interagir com o e-mail.
Altere a palavra-passe afetada.
Redefina a autenticação de dois fatores, se necessário.
Analise o dispositivo à procura de malware.
Denuncie o incidente ao provedor e aos canais de combate ao cibercrime na Turquia.



Gravidade

5/5 - Muito alto, pois a violação de segurança pode levar ao roubo de identidade, fraude financeira e acesso a múltiplos serviços interligados.



Fontes principais

TÜİK - Estatísticas sobre Crianças 2024;
Estatísticas da Juventude 2024;
GüvenliWeb - orientações sobre phishing e burlas online;
Recursos de denúncia da USOM, BTK, EGM Cybercrime e KVKK.

Conclusões

Estas ameaças são as mais relevantes na Turquia porque se alinham estreitamente com a forma como os jovens realmente usam os ambientes digitais: com frequência, visualmente, socialmente e, principalmente, através de dispositivos móveis. Os riscos mais graves, portanto, não são ataques cibernéticos abstratos, mas manipulações quotidianas que se aproveitam da confiança, da urgência, da identidade e da familiaridade com as plataformas.

Para os técnicos de juventude, a principal implicação é que a educação em cibersegurança deve ser prática, baseada em cenários e específica para cada plataforma. Os jovens precisam reconhecer o phishing para além do e-mail, compreender como os dados pessoais alimentam a falsificação de identidade e desenvolver o hábito de verificar as fontes antes de partilhar ou agir.

Os resultados apoiam as diretrizes do ESCAP(E+) de diversas formas concretas. No âmbito do projeto e nas orientações de formação, deve ser dada ênfase às rotinas de verificação, às definições de privacidade, à autenticação de dois fatores, à recuperação de contas, às reações seguras a mensagens suspeitas e à utilização de canais de denúncia locais. Para o *escape room* em realidade virtual, cenários relevantes incluiriam um sorteio falso, um perfil clonado do Instagram, uma mensagem direta a solicitar um código ou pagamento, um alerta “oficial” falso ou uma corrente viral de desinformação ao estilo do TikTok. Para infográficos e materiais de sensibilização animados, o conteúdo deve ser conciso, visual, adequado ao público jovem e baseado em comportamentos reais das plataformas, em vez de terminologia cibernética genérica.

Recursos

- TurkStat (2025). Estatísticas sobre a Infância 2024.
https://www.tuik.gov.tr/media/announcements/Turkiye_Cocuk_2024TR.pdf
- Direção-Geral de Segurança (EGM). Departamento de Combate aos Crimes Cibernéticos.
<https://www.egm.gov.tr/siber>
- Direção-Geral de Segurança (EGM). Fraude nas Redes Sociais.
<https://www.egm.gov.tr/sosyal-medya-dolandiriciligi>
- Direção-Geral de Segurança (EGM). Combate aos crimes cibernéticos – Perguntas frequentes. <https://www.egm.gov.tr/siber/sikca-sorulan-sorular>
- Centro Nacional de Resposta a Incidentes Cibernéticos (USOM). Site oficial e canais de contacto/denúncia. <https://www.usom.gov.tr/>
- SecureWeb. Não dê chance aos burlões da internet!
<https://www.guvenliweb.org.tr/haber-detay/internet-dolandiricilarina-gecit-vermeyin>
- SecureWeb. Riscos de Engenharia Social. <https://www.guvenliweb.org.tr/index-orj.php/blog-detay/sosyal-muhendislik-riskleri>
- SafeWeb. Sensibilização sobre privacidade digital em crianças.
<https://www.guvenliweb.org.tr/blog-detay/cocuklarda-digital-privacy-awareness>
- SecureWeb. Segurança na Internet e da Informação.
<https://www.guvenliweb.org.tr/blog/internet-ve-bilgi-guvenligi>
- SafeWeb. Formas de disseminação e prevenção da desinformação.
<https://www.guvenliweb.org.tr/blog-detay/dezenformasyonun-yayilma-yollari-ve-onlenmesi>
- SecureWeb. 7 maneiras de prevenir a desinformação.
<https://www.guvenliweb.org.tr/blog-detay/7-adimda-dezenformasyonu-onlemenin-yollari>
- SafeWeb. Algoritmos de redes sociais sociais e seu impacto sobre as crianças.
<https://www.guvenliweb.org.tr/blog-detay/sosyal-medya-algoritmaları-ve-cocuklar-uzerindeki-etkisi>
- EU Kids Online Turquia (Relatório resumido de 2015). As mudanças no uso mais seguro da internet por crianças na Turquia.
https://eukidsonline.metu.edu.tr/tr/system/files/raporlar/euko_turkey2015_summaryreport.pdf



ESCAP(E+)

Estónia

INVESTIGAÇÃO DOCUMENTAL



Co-funded by
the European Union

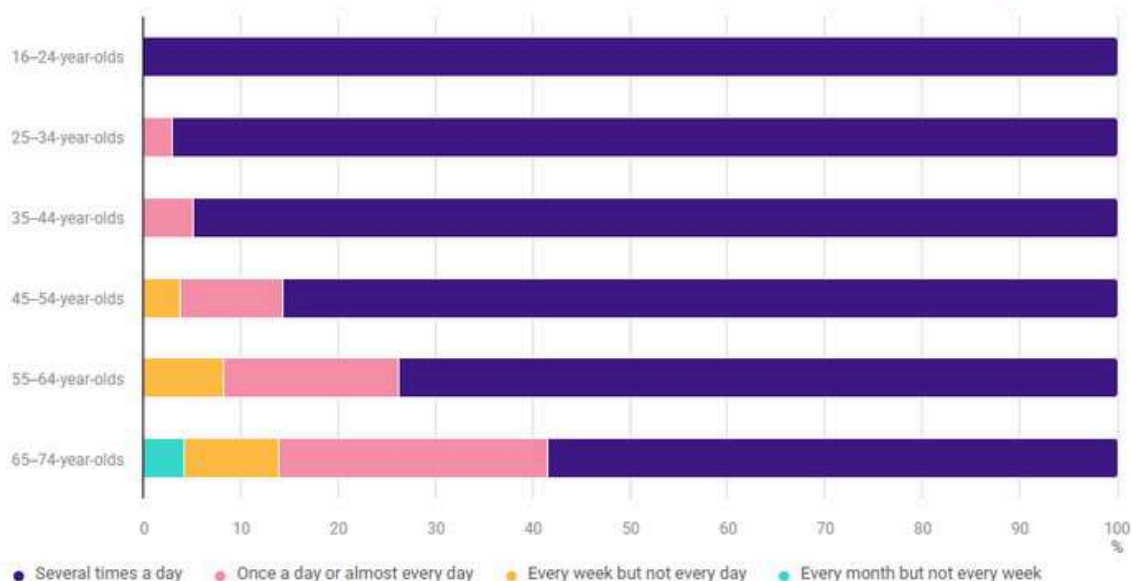
Visão geral

A Estónia é amplamente reconhecida como uma das sociedades mais avançadas digitalmente na Europa. Nas últimas duas décadas, o amplo investimento nacional em infraestrutura digital, serviços de governo Eletrónico e iniciativas de educação digital moldou um ambiente altamente conectado no qual os jovens crescem. Como resultado, as tecnologias digitais estão profundamente integradas no quotidiano, às práticas de aprendizagem e às interações sociais da juventude estoniana.

O acesso à tecnologia digital entre os jovens na Estónia é quase universal. De acordo com o Instituto de Estatística da Estónia, 93,2% dos domicílios no país possuem conexão à internet em casa, e o uso é particularmente elevado entre os grupos etários mais jovens, como mostra o diagrama abaixo:

Frequency of internet use by age group, 2023

Source: Statistics Estonia

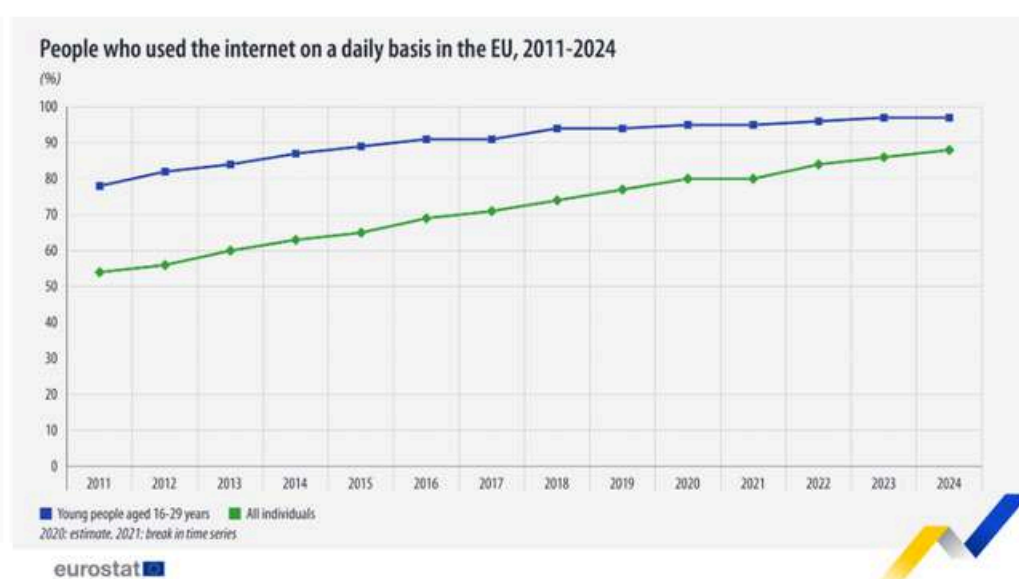


Visão geral

Sigrid Saagpakk, analista do Instituto Nacional de Estatística da Estónia, explicou que a internet e os serviços online desempenham um papel cada vez maior na vida das pessoas: “Por faixa etária, a maior proporção de utilizadores de internet é entre os jovens, com quase 100% deles utilizando a internet. O uso da internet é mais frequente entre os jovens de 16 a 24 anos, com 96% deles a aceder à internet várias vezes ao dia”.

A tecnologia digital está fortemente integrada no sistema educativo e nas políticas de desenvolvimento juvenil da Estónia. As escolas frequentemente incentivam o uso de ferramentas digitais em ambientes de aprendizagem, em vez de as restringirem. Iniciativas nacionais continuam a promover a alfabetização digital, competências de programação e tecnologias emergentes, como a inteligência artificial, para preparar os alunos para a participação na economia digital e na sociedade do conhecimento.

Estas tendências estão alinhadas com padrões europeus mais amplos. De acordo com dados do Eurostat, o uso da internet entre jovens em toda a União Europeia é extremamente alto: 97% dos cidadãos da UE com idades entre os 16 e os 29 anos relataram utilizá-la diariamente em 2024, em comparação com 88% da população em geral, conforme ilustrado no diagrama abaixo:



Visão geral

Em todos os países da UE, os jovens demonstraram uma participação muito maior em atividades nas redes sociais do que a população em geral. Criar um perfil de utilizador e publicar mensagens ou realizar atividades relacionadas era uma prática comum para 88% dos jovens entre os 16 e os 29 anos, em comparação com 65% da população total. No entanto, a Estónia frequentemente apresenta um desempenho acima da média da UE em indicadores de competência digital. De acordo com o Relatório da Década Digital 2024 da Comissão Europeia, 62,6% da população da Estónia possui pelo menos competências digitais básicas, superando a média da UE de 55,6%. A Estónia também possui uma proporção maior de especialistas em TIC na força de trabalho do que a média da UE, o que reflete o foco político de longa data do país na inovação e educação digital.

Principais Fatores de Risco

Apesar das inúmeras oportunidades oferecidas pelas tecnologias digitais, os jovens na Estónia enfrentam diversos riscos à segurança online. Pesquisas do projeto EU Kids Online indicam que as crianças estonianas estão expostas a uma série de experiências online potencialmente prejudiciais, incluindo cyberbullying, contacto com estranhos e exposição a conteúdo nocivo ou inadequado. De acordo com os resultados do projeto mencionado, 97% das crianças estonianas dos 9 aos 17 anos acedem à internet diariamente, utilizando pelo menos um dispositivo. A comunicação online é um aspeto fundamental da vida social dos jovens: 46% das crianças relataram ter tido contacto online com alguém que não haviam conhecido pessoalmente antes, e aproximadamente um terço dessas crianças encontrou posteriormente essa pessoa offline.

Estudos mostram que uma parcela significativa dos jovens estonianos já se deparou com discursos de ódio, conteúdo violento ou informações enganosas online, refletindo tendências mais amplas observadas em toda a Europa. O elevado nível de utilização da internet, principalmente através de smartphones e plataformas de redes sociais, aumenta a probabilidade de exposição a esses riscos. Além disso, os jovens podem enfrentar desafios relacionados com a privacidade, como a partilha de informações pessoais online ou o risco de serem alvo de burlas ou manipulação.

Visão geral

Principais Indicadores Nacionais

Outras análises a nível da UE também destacam desafios relacionados com a segurança online e o bem-estar digital. Os dados do Eurostat mostram que 49% dos jovens europeus entre os 16 e os 29 anos relataram ter encontrado mensagens online hostis ou abusivas em 2023. A Estónia registou uma das taxas de exposição mais elevadas, com 69%, o que reflete tanto o elevado nível de envolvimento online como a crescente prevalência de conteúdos digitais nocivos.

Canais de Apoio e Denúncia

A Estónia possui diversos canais oficiais de apoio e denúncia que jovens, pais e educadores podem utilizar ao enfrentar riscos online, como cyberbullying, aliciamento ou exposição a conteúdo prejudicial. Um dos serviços mais importantes é a Linha de Apoio à Criança da Estónia (Lasteabi), que opera uma linha gratuita 24 horas (116 111) oferecendo aconselhamento e orientação a crianças, pais e profissionais sobre questões como cyberbullying, assédio online e conteúdo prejudicial na internet. O serviço também pode ser contactado via chat online ou e-mail e permite que os utilizadores permaneçam anónimos, se necessário.

A linha direta estoniana Vihjeliin permite que os utilizadores denunciem material ilegal online, especialmente conteúdo relacionado com abuso sexual infantil, para que possa ser avaliado e encaminhado às autoridades policiais para remoção. Estes serviços operam como parte da iniciativa mais ampla do Centro de Internet Segura da Estónia, que promove sensibilização, educação e mecanismos de apoio para melhorar a segurança digital entre crianças e jovens.

Ameaça do Facebook

Campanhas de Desinformação e Informações Falsas



Plataforma principal

Facebook



Descrição resumida

Os jovens deparam-se com conteúdo falso ou enganoso e amplificam-no, desde rumores sobre saúde até narrativas com motivação política. O algoritmo do Facebook prioriza o envolvimento em detrimento da precisão, e a proximidade da Estónia com a Rússia torna-a um alvo prioritário para operações coordenadas de informação direcionadas à sua minoria de língua russa e à população em geral.



Cenário típico da juventude

Um estudante de 17 anos em Tallinn vê uma publicação no Facebook partilhada por um colega de turma, alegando que uma nova regulamentação da UE irá proibir aplicações de mensagens encriptadas. A publicação inclui um gráfico com aparência profissional e links para um site de notícias falsas. Sem verificar a fonte, o estudante partilha a publicação no seu próprio feed e num grupo de conversa da escola, espalhando a informação falsa por dezenas de colegas. Vários amigos ficam alarmados e começam a partilhá-la, gerando ansiedade e desconfiança em relação às instituições da UE - exatamente a reação que a campanha de desinformação original pretendia provocar.



Como funciona?

1. Um agente ou grupo organizado patrocinado pelo Estado cria uma notícia falsa ou uma imagem manipulada com o objetivo de provocar uma reação emocional, indignação, medo ou desconfiança, em torno de um tema politicamente ou socialmente sensível.
2. O conteúdo é disseminado pelo Facebook através de contas falsas, redes de bots ou páginas comprometidas que aparentam ser meios de comunicação locais legítimos ou grupos comunitários.
3. O algoritmo do Facebook, focado no envolvimento, deteta um elevado nível de interação (reações de raiva, comentários, partilhas) e amplifica o conteúdo nos feeds de mais utilizadores, incluindo jovens que seguem tópicos ou grupos relacionados.
4. Os utilizadores mais jovens, que tendem a consumir notícias principalmente através das redes sociais e podem não ter o hábito de verificar as fontes, partilham o conteúdo com as suas próprias redes, muitas vezes acrescentando comentários pessoais que lhe conferem maior credibilidade entre os seus pares.
5. Quando os verificadores de factos sinalizam o conteúdo, este já alcançou milhares de utilizadores. O impacto emocional persiste mesmo após a publicação das correções, pois estudos mostram que as retratações raramente atingem o mesmo público que a alegação falsa original.

Ameaça do Facebook

Campanhas de Desinformação e Informações Falsas



Sinais de alerta

A fonte é um site desconhecido, sem equipa editorial clara, informações de contacto ou histórico de publicação. A manchete usa linguagem extrema ou emocionalmente carregada, criada para provocar indignação ou pânico imediato. O conteúdo não tem autor identificado ou cita "especialistas" e "autoridades" não identificados, sem especificar quem são. A publicação incentiva a partilha antes que seja apagada ou sugere censura para criar urgência. Imagens ou estatísticas são apresentadas sem contexto, datas ou fontes verificáveis. A notícia não pode ser encontrada em nenhum meio de comunicação reconhecido, apenas em páginas obscuras ou grupos extremamente partidários. A página do Facebook que partilha a notícia foi criada recentemente e tem um histórico de publicações inconsistente ou publica exclusivamente sobre um tópico polémico.



Medidas de prevenção

Verifique sempre se a notícia foi confirmada por pelo menos duas fontes de notícias independentes e fiáveis antes de a partilhar. Use ferramentas de verificação de factos como EUvsDisinfo.eu, Propastop.org (o rastreador de desinformação da Estónia) ou AFP Fact Check. Examine a fonte, aceda ao site, verifique a página "Sobre" e observe se há irregularidades no nome do domínio. Pense bem antes de partilhar conteúdo que provoque emoções fortes; a desinformação é criada para contornar o pensamento crítico, despertando sentimentos intensos. Ajuste as preferências do seu feed do Facebook para priorizar fontes de notícias fiáveis e reduzir as recomendações algorítmicas de páginas desconhecidas. Converse com os seus amigos sobre literacia mediática, pois os jovens tendem a dar mais atenção aos amigos do que aos alertas das instituições. Denuncie suspeitas de desinformação diretamente ao Facebook através da opção "Encontrar apoio ou denunciar publicação".

Ameaça do Facebook

Campanhas de Desinformação e Informações Falsas



O que fazer se isto acontecer?

Pare imediatamente de partilhar o conteúdo e apague a publicação, caso já a tenha partilhado. Informe os amigos ou membros do grupo que possam tê-la visto de que o conteúdo não foi verificado ou é falso e partilhe um link para uma verificação de factos fiável, se houver. Denuncie a publicação e a página ao Facebook como desinformação, utilizando as ferramentas de denúncia integradas da plataforma. Se a desinformação for dirigida a uma comunidade específica ou estiver relacionada com eleições, denuncie ao CERT-EE da Estónia (cert@cert.ee) ou à Polícia e Guarda de Fronteiras. Reflita sobre o que tornou o conteúdo convincente - isso fortalece a sua resiliência contra futuras tentativas de desinformação. Se o conteúdo fizer parte de uma campanha coordenada contra interesses da Estónia ou da UE, denuncie-o ao Propastop.org ou ao EUvsDisinfo.eu para documentação e sensibilização pública.



Gravidade

Probabilidade 4/5 – Este tipo de ameaça é generalizado e persistente em toda a UE. A Estónia é um país particularmente exposto devido à sua fronteira com a Rússia, à grande população de língua russa e à sociedade altamente digitalizada. O Facebook continua a ser um dos principais meios de campanhas de desinformação transfronteiriças, e os jovens dependem desproporcionalmente das redes sociais como fonte de notícias, tornando-os simultaneamente alvos e amplificadores involuntários. O relatório de 2024 da Comissão Europeia sobre a Lei dos Serviços Digitais destacou os riscos sistémicos de desinformação nas grandes plataformas como uma preocupação constante.



Fontes principais

- EUvsDisinfo.eu – Base de dados sobre desinformação da Força-Tarefa East StratCom da UE: <https://euvsdisinfo.eu>
- Propastop.org – Monitorização de desinformação realizada por voluntários na Estónia: <https://www.propastop.org/en/>
- Relatório da RIA sobre Cibersegurança na Estónia em 2026: <https://www.ria.ee/en/cyber-security-estonia-2026>
- Atualizações sobre a aplicação da Lei dos Serviços Digitais da Comissão Europeia: <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>
- Investigação da Fundação Molly Rose sobre a amplificação algorítmica de conteúdo prejudicial: <https://mollyrosefoundation.org>
- Relatório de Inteligência e Impactos de burlas da F-Secure para 2025: <https://www.f-secure.com/us-en/partners/insights/scam-intelligence-and-impacts-report-2025>

Ameaça do Instagram

Sextorsão e Chantagem Sexual



Plataforma principal

Instagram



Descrição resumida

Criminosos que se fazem passar por interesses amorosos contactam adolescentes por mensagens diretas, solicitam fotografias íntimas e ameaçam partilhá-las, a menos que a vítima pague ou forneça mais conteúdo. O FBI relatou um aumento de 1.000% nos casos de extorsão sexual, com o Instagram identificado como a principal plataforma. Duas famílias processaram o Meta, alegando que a plataforma ignorou estes perigos; um dos rapazes contactados através do Instagram cometeu suicídio dois dias depois.



Cenário típico da juventude

Um rapaz de 16 anos em Tartu recebe um pedido para o seguir no Instagram de uma rapariga atraente que parece ter a mesma idade que ele. O perfil dela parece genuíno, selfies, amigos identificados, menções, stories casuais. Depois de alguns dias de mensagens amigáveis, a conversa torna-se mais íntima e ela sugere que troquem fotografias privadas. Ele envia uma imagem íntima. Em poucos minutos, o tom muda completamente. A conta envia uma captura de ecrã da fotografia dele, juntamente com a lista de seguidores, e exige 200 euros em criptomoeda no prazo de uma hora, ameaçando enviar a imagem aos colegas de turma, pais e professores. Em pânico e envergonhado, ele paga, mas uma segunda exigência surge imediatamente. Sentindo-se incapaz de contar a alguém, isola-se da escola e da vida social nas semanas seguintes.



Como funciona?

Redes criminosas organizadas, frequentemente a operar na África Ocidental ou no Sudeste Asiático, criam perfis falsos convincentes no Instagram, utilizando fotografias roubadas de jovens atraentes. Estas redes preenchem as contas com publicações, stories e seguidores para parecerem autênticas.

O burlão envia pedidos para seguir ou mensagens diretas para um grande número de adolescentes, geralmente identificados através de contas de escolas públicas, hashtags, marcações de localização ou listas de seguidores de páginas dirigidas a jovens. As mensagens iniciais são casuais e amigáveis para estabelecer uma relação de confiança.

Ao longo de horas ou dias, a conversa é direcionada para tópicos românticos ou sexuais. O burlão pode enviar primeiro imagens íntimas falsas para criar uma sensação de reciprocidade e diminuir a cautela da vítima, incentivando-a em seguida a partilhar as suas próprias fotografias ou vídeos.

Ameaça do Instagram

Sextorsão e Chantagem Sexual

- Assim que recebe o material íntimo, o burlão revela imediatamente as suas verdadeiras intenções. Ele faz uma captura de ecrã da lista de seguidores ou dos amigos da vítima e ameaça distribuir as imagens a familiares, amigos e colegas de escola, a menos que a vítima envie dinheiro – geralmente através de cartões-presente, criptomoedas ou aplicações de pagamento móvel.
- O pagamento raramente põe fim à extorsão. Os burlões aumentam as exigências, solicitam conteúdo adicional ou vendem o material a outras redes criminosas. As vítimas – dominadas pela vergonha, medo e isolamento – muitas vezes sofrem graves danos psicológicos. Nos casos mais trágicos, isso levou à automutilação e ao suicídio, especialmente entre adolescentes do sexo masculino.



Sinais de alerta

Um desconhecido com um perfil atraente envia um pedido para seguir ou uma mensagem direta do nada, especialmente se vocês não têm contactos em comum. A conversa evolui muito rapidamente, de uma conversa casual para tópicos de flerte ou sexuais em questão de horas ou dias. Essa pessoa insiste em levar a conversa para outra plataforma – como Snapchat, WhatsApp ou um serviço de videochamada – onde alega que será "mais privada". Ela envia fotografias íntimas logo no início da conversa, sem que lhe sejam solicitadas, criando pressão para que haja reciprocidade. O perfil dela é relativamente novo, tem poucas publicações em comparação com o número de seguidores, ou apresenta fotografias que parecem excessivamente produzidas ou inconsistentes. Ela evita videochamadas ou dá desculpas quando lhe é solicitado que converse em direto – porque a sua aparência não corresponde ao perfil. Ela demonstra um apego emocional incomumente intenso muito rapidamente, usando frases como "Nunca me senti assim por ninguém" para criar uma falsa intimidade. Qualquer pedido de fotografias ou vídeos íntimos, independentemente de quão confortável a conversa pareça, deve ser considerado um sinal de alerta sério.



Medidas de prevenção

Nunca partilhe imagens ou vídeos íntimos com ninguém online, independentemente de quanto acha que conhece a pessoa – uma vez enviado, perde-se todo o controlo sobre o conteúdo. Configure a sua conta do Instagram como privada e não aceite pedidos para seguir pessoas que não conhece pessoalmente. Desconfie de novos contactos que rapidamente direcionam conversas para assuntos românticos ou sexuais.

Ameaça do Instagram

Sextorsão e Chantagem Sexual

Desative a possibilidade de estranhos enviarem mensagens diretamente para si ajustando as definições de solicitação de mensagens do Instagram nas Definições de privacidade. Se for menor de 18 anos, ative os recursos da Conta Adolescente do Instagram, que restringem o contacto com estranhos e limitam a exposição a conteúdo sensível. Converse abertamente com amigos de confiança ou adultos sobre relacionamentos online – a extorsão sexual prospera no silêncio e no isolamento. Lembre-se de que partilhar imagens íntimas de outra pessoa é ilegal na Estónia e em toda a UE, portanto, quem está a cometer um crime é a pessoa que o está a ameaçar, não a vítima. Use a pesquisa reversa de imagens (como o Google Imagens ou o TinEye) para verificar se as fotografias de perfil de um novo contacto aparecem noutros locais online com um nome diferente.



O que fazer se isto acontecer?

Não pague ao extorsionista – o pagamento quase nunca interrompe as ameaças e geralmente leva a exigências cada vez maiores. Não apague as mensagens, imagens ou interações da conta – guarde as capturas de ecrã de tudo como prova, incluindo o nome de utilizador, o perfil e todas as mensagens do burlão. Interrompa imediatamente toda a comunicação com o burlão – não responda a novas ameaças nem negocie. Denuncie a conta diretamente ao Instagram usando a função de denúncia na aplicação, selecionando "burla ou fraude" e "exploração sexual" como categorias. Entre em contacto com a Polícia e Guarda de Fronteiras da Estónia (denuncie online em politsei.ee ou ligue para o 112 em caso de emergência) – a extorsão sexual é um crime e as autoridades podem agir com base nas denúncias. Procure um adulto de confiança – um dos pais, um professor, um orientador escolar ou um assistente social. Se não se sentir à vontade para falar com alguém que conhece, entre em contacto com a Linha de Apoio à Criança da Estónia através do número 116 111 (gratuita, confidencial e disponível 24 horas por dia, 7 dias por semana). Denuncie o incidente à linha direta de denúncias cibernéticas do Centro Nacional para Crianças Desaparecidas e Exploradas (report.cybertip.org) ou à linha direta da UE para uma Internet mais Segura na Estónia, através do serviço Lasteabi. Lembre-se de que você é a vítima – a vergonha pertence inteiramente ao criminoso. Milhares de jovens em toda a Europa foram alvo destas redes organizadas, e procurar ajuda é a ação mais eficaz que pode tomar. Se estiver em sofrimento emocional ou tiver pensamentos suicidas, entre em contacto com a linha de apoio em crise da Estónia através do número 116 123 ou com a linha de apoio emocional pan-europeia através do número 116 006.

Ameaça do Instagram

Sextorsão e Chantagem Sexual



Gravidade

Probabilidade 5/5 – Esta é uma das ameaças cibernéticas mais perigosas e de crescimento mais rápido dirigidas aos jovens em toda a UE. Os ataques de sextorsão são realizados por redes criminosas organizadas à escala industrial, com o FBI, a Europol e a própria Polícia e Guarda de Fronteiras da Estónia a sinalizarem um aumento acentuado nos casos. O Instagram foi especificamente identificado em vários processos judiciais e relatórios policiais como um dos principais meios utilizados para este tipo de crime. Rapazes entre os 14 e os 17 anos são desproporcionalmente visados, e as consequências psicológicas – incluindo ansiedade grave, isolamento social e suicídio – fazem desta uma das ameaças de maior gravidade no panorama da cibersegurança juvenil. A população jovem da Estónia, altamente conectada digitalmente, e as elevadas taxas de utilização das redes sociais colocam os jovens estonianos perante uma exposição significativa.



Fontes principais

Relatório do Network Contagion Research Institute sobre os Yahoo Boys e a extorsão sexual financeira: <https://networkcontagion.us>
Reportagem da NBC News sobre processos por extorsão sexual envolvendo a Meta (dezembro de 2025): <https://www.nbcnews.com/tech/social-media/two-families-sue-meta-teens-deaths-suicide-citing-sex-tortion-scams-rcna248136>
Denúncias online da Polícia e Guarda de Fronteiras da Estónia: <https://www.politsei.ee/en> Linha de Apoio à Criança da Estónia (Lasteabi): <https://www.lasteabi.ee/en> Better Internet for Kids – Centro de Internet Segura da Estónia: <https://better-internet-for-kids.europa.eu/en> Avaliação de Ameaças do Crime Organizado na Internet da Europol (IOCTA): <https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment>

Ameaça do TikTok

Desinformação Através de Tendências Virais



Plataforma principal

TikTok

A cultura dos vídeos curtos incentiva a partilha rápida de informações não verificadas – desde desafios perigosos relacionados com a saúde, até falsidades políticas. O algoritmo da página "Para Ti" do TikTok pode amplificar rapidamente conteúdo enganoso para milhões de jovens utilizadores antes que os verificadores de factos possam responder, tornando-se um importante meio de disseminação de desinformação nos Estados-Membros da UE.



Descrição resumida



Cenário típico da juventude

Um estudante de 15 anos em Pärnu abre o TikTok depois das aulas e vê um vídeo com 800 mil visualizações alegando que um ingrediente comum em bebidas energéticas causa insuficiência cardíaca em adolescentes. O vídeo apresenta música dramática, uma captura de ecrã do que parece ser um artigo científico e um criador de conteúdo a falar com convicção. O estudante imediatamente partilha o vídeo num grupo de WhatsApp da turma, alertando os amigos para pararem de consumir a bebida. Em poucas horas, a alegação espalha-se pela escola. Um dos pais entra em contacto com a escola alarmado. Quando um professor investiga, descobre que a captura de ecrã do "artigo científico" é uma imagem falsa – o estudo nunca existiu. Mas o pânico já tinha perturbado o dia letivo e, semanas depois, alguns alunos ainda acreditam na alegação porque nunca viram uma correção.



Como funciona?

Um criador publica conteúdo emocional ou alarmante para ganhar visualizações, influenciar opiniões ou apoiar uma campanha de desinformação mais ampla. O vídeo recebe partilhas e comentários, levando o TikTok a exibi-lo para mais utilizadores. Os jovens podem então espalhá-lo pelo WhatsApp, Instagram ou grupos de conversa da escola.

Os espectadores partilham o conteúdo em diversas plataformas – em grupos do WhatsApp, stories do Instagram, Snapchat e fóruns escolares – ampliando o seu alcance muito além do próprio TikTok. Cada partilha adiciona uma camada de prova social, já que os jovens tendem a confiar mais em conteúdo encaminhado por amigos do que em conteúdo de fontes desconhecidas.

Quando os verificadores de factos, moderadores da plataforma ou adultos de confiança sinalizam o conteúdo, ele já foi visualizado milhões de vezes e internalizado por uma parcela significativa do público.

Ameaça do TikTok

Desinformação através de tendências virais



Sinais de alerta

O vídeo faz uma afirmação dramática ou alarmante, mas não fornece nenhuma fonte verificável – nenhum estudo citado, nenhum artigo com link, nenhum especialista identificado. O criador usa linguagem altamente emotiva, música urgente ou táticas de choque concebidas para provocar uma reação imediata em vez de uma reflexão ponderada. Capturas de ecrã de "evidências", como manchetes de notícias, artigos científicos ou declarações oficiais, aparecem no vídeo, mas estão muito desfocadas para serem lidas, estranhamente recortadas ou não podem ser encontradas através de uma simples pesquisa na internet. A afirmação está a circular apenas no TikTok ou noutras plataformas de redes sociais e não é relatada por nenhum meio de comunicação reconhecido ou organização de verificação de factos. O vídeo incentiva os espectadores a "partilharem antes que seja removido" – uma tática de manipulação comum que enquadra a possível moderação de conteúdo como censura para criar urgência.



Medidas de prevenção

Antes de partilhar qualquer conteúdo que provoque uma forte reação emocional, faça uma pausa. A desinformação é criada para contornar o pensamento crítico, explorando o medo, a raiva ou o choque. Verifique se a alegação foi confirmada por pelo menos duas fontes de notícias independentes e fiáveis antes de acreditar nela ou partilhá-la. Use ferramentas de verificação de factos apoiadas pela UE, como EUvsDisinfo.eu, AFP Fact Check ou Full Fact, para verificar alegações suspeitas. Procure a fonte original citada no vídeo. Se nenhuma fonte for fornecida ou se o estudo ou artigo citado não existir, considere a alegação como não verificada. Siga contas fiáveis no TikTok especializadas em desmentir informações falsas, como organizações de literacia mediática ou jornalistas verificados. Seja especialmente cético em relação a alegações sobre saúde, declarações políticas e conteúdo relacionado com crises no TikTok – estes são os tópicos mais frequentemente visados por campanhas de desinformação. Discuta o que vê online com amigos, professores ou familiares. Conversar sobre conteúdo suspeito com outras pessoas é uma das defesas mais eficazes contra a desinformação. Ajuste as suas definições do TikTok para reduzir as recomendações algorítmicas, limpando o histórico de visualização periodicamente e usando o recurso "Não tenho interesse" em conteúdo sensacionalista. Aprenda a distinguir entre opinião, sátira e reportagem factual – a literacia mediática é uma competência que melhora com a prática e faz parte do currículo nacional de educação digital da Estónia.

Ameaça do TikTok

Desinformação através de tendências virais



O que fazer se isto acontecer?

Se já partilhou informações falsas, apague a sua publicação ou mensagem e informe as pessoas com quem a partilhou de que o conteúdo era falso. Denuncie o vídeo enganoso ao TikTok usando a função de denúncia na aplicação, selecionando "desinformação" como categoria. Se a desinformação parecer fazer parte de uma campanha coordenada, denuncie-a ao EUvsDisinfo.eu ou à Autoridade de Sistemas de Informação da Estónia (RIA) para fins de documentação. Converse com um professor, bibliotecário escolar ou profissional da área da juventude se não tiver certeza se algo que viu é verdade. Não há vergonha em verificar informações, e criar o hábito de verificar fortalece a sua resiliência a longo prazo contra a desinformação. Se a desinformação lhe causou sofrimento real, fale com um adulto de confiança ou entre em contacto com a Linha de Apoio à Criança da Estónia através do número 116 111.



Gravidade

Probabilidade 4/5 – Esta ameaça é generalizada e afeta praticamente todos os jovens utilizadores do TikTok na UE. O TikTok é a principal fonte de notícias para uma parcela crescente de adolescentes europeus, e o seu algoritmo é estruturalmente concebido para priorizar o envolvimento em detrimento da precisão. A Estónia enfrenta um risco elevado devido à sua posição como alvo de operações de desinformação em língua russa, à sua população jovem altamente digitalizada e à velocidade com que conteúdo falso pode espalhar-se numa sociedade pequena e fortemente conectada.



Fontes principais

EUvsDisinfo.eu – Base de dados de desinformação da Força-Tarefa East StratCom da UE: <https://euvsdisinfo.eu>

Propastop.org – Monitorização de desinformação administrada por voluntários na Estónia: <https://www.propastop.org/en>

Comissão Europeia – Aplicação da Lei dos Serviços Digitais e o TikTok como um VLOP (Very Large Online Platform - Plataforma de Oportunidades de Desinformação Voluntárias): <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>

Fundação Molly Rose – Investigação sobre a amplificação algorítmica de conteúdo prejudicial para adolescentes: <https://mollyrosefoundation.org>

Relatório da RIA sobre Cibersegurança na Estónia 2026: <https://www.ria.ee/en/cyber-security-estonia-2026>

Relatório de Notícias Digitais do Instituto Reuters – Tendências de consumo de notícias entre jovens: <https://reutersinstitute.politics.ox.ac.uk/digital-news-report>

Better Internet for Kids – Centro de Internet Segura da Estónia e atividades do SID 2025: <https://better-internet-for-kids.europa.eu>

Ameaça por E-mail

Ofertas falsas de emprego e estágio



Plataforma principal

E-mail



Descrição resumida

Burlões visam estudantes com e-mails em massa oferecendo dinheiro fácil através de trabalhos como "cliente oculto", vagas de assistente remoto ou estágios remunerados. As vítimas são enganadas e induzidas a depositar cheques fraudulentos, comprar cartões-presente ou partilhar informações pessoais. Endereços de e-mail de universidades e escolas são alvos específicos porque os estudantes estão sob pressão financeira e têm menos experiência em segurança.



Cenário típico da juventude

Uma estudante universitária de 19 anos em Tallinn recebe um e-mail no seu endereço institucional de alguém que se diz professor de uma universidade parceira, oferecendo uma vaga de assistente de investigação remota em tempo parcial com pagamento de €400 por semana. O e-mail é bem escrito, menciona a sua área de estudo e inclui o logótipo da universidade. Ela responde demonstrando interesse. O remetente pede que ela preencha um formulário de registo com o seu nome completo, endereço, data de nascimento, número de telefone e dados bancários "para configuração da folha de pagamento". Em seguida, ela recebe um cheque de €1.500 por correio expresso e é instruída a depositá-lo imediatamente, ficar com €400 como primeiro pagamento e usar o restante para comprar cartões-presente digitais para "incentivos de participação na investigação", enviando os códigos de volta por e-mail. Inicialmente, o seu banco mostra os fundos como disponíveis, então ela compra os cartões-presente e envia os códigos. Três dias depois, o cheque é devolvido, os €1.100 que ela gastou em cartões-presente desaparecem, o seu banco cobra uma taxa de descoberto e o endereço de e-mail do burlão deixa de existir. Ela fica com prejuízo financeiro, dados pessoais comprometidos e o stress de ter de relatar o incidente durante a época de exames.



Como funciona?

Burlões recolhem endereços de e-mail de estudantes em sites de universidades, diretórios, LinkedIn ou outras plataformas online. Eles enviam mensagens com aparência profissional, usando logótipos de universidades, nomes copiados ou contas comprometidas para parecerem confiáveis. Os estudantes que respondem são solicitados a fornecer dados pessoais, informações bancárias ou ajuda com "pagamentos". Em alguns casos, são instruídos a depositar um cheque, transferir dinheiro ou comprar cartões-presente. Assim que o burlão recebe o dinheiro ou os códigos, ele desaparece.

Ameaça por e-mail

Ofertas falsas de emprego e estágio



Sinais de alerta

- A oferta surgiu inesperadamente e não foi anunciada através de um portal de carreiras oficial.
- A remuneração é excecionalmente alta para um trabalho simples ou flexível.
- O remetente utiliza um endereço de e-mail pessoal em vez de um domínio institucional oficial.
- O empregador solicita dados de identificação, informações bancárias ou endereço residencial antes de uma entrevista ou contrato.
- A função envolve depositar cheques, transferir dinheiro ou comprar cartões-presente.
- A mensagem cria um sentido de urgência e pressiona o aluno a agir rapidamente.



Medidas de prevenção

Antes de responder a qualquer oferta de emprego não solicitada, verifique-a de forma independente – pesquise a empresa ou organização em registos oficiais (na Estónia, use o Registo Eletrónico de Empresas em ariregister.rik.ee), consulte o site e ligue para o número de telefone listado para confirmar a existência da vaga. Nunca forneça informações pessoais sensíveis – número do documento de identificação, dados bancários, data de nascimento ou endereço residencial – a um empregador que não conheça pessoalmente nem tenha verificado através dos serviços de carreira da sua universidade. Se a oferta alegar vir de um professor ou membro da equipa da sua instituição, entre em contacto diretamente com essa pessoa pelos canais oficiais da universidade para confirmar – não responda ao e-mail. Use o portal de carreiras oficial da sua universidade ou plataformas fiáveis da UE, como EURES (eures.europa.eu) ou Erasmus+ Intern, para encontrar oportunidades legítimas. Desconfie imediatamente de qualquer vaga que envolva depósito de cheques, transferência de dinheiro ou compra de cartões-presente – esses são sinais de fraude, não de emprego. Discuta ofertas de emprego inesperadas com um adulto de confiança, um orientador de carreira da universidade ou um representante da associação estudantil antes de tomar qualquer providência. Ative a autenticação de dois fatores na sua conta de e-mail da universidade para reduzir o risco do seu endereço ser comprometido e usado para atacar outros estudantes. Lembre-se de que empregadores legítimos na UE são obrigados a fornecer um contrato de trabalho por escrito antes do início das atividades – se nenhum contrato for oferecido, a oportunidade não é genuína.

Ameaça por E-mail

Ofertas falsas de emprego e estágio



O que fazer se isto acontecer?

- Interrompa imediatamente a comunicação.
- Salve capturas de ecrã de e-mails, solicitações de pagamento, endereços de remetentes e registos de transações.
- Entre em contacto com o seu banco se partilhou informações financeiras ou fez um pagamento.
- Denuncie o incidente à Polícia e à Guarda de Fronteiras da Estónia.
- Informe a equipa de TI/segurança da sua universidade para que possa alertar outros alunos.
- Caso dados de identificação pessoal tenham sido partilhados, entre em contacto com a Autoridade de Sistemas de Informação da Estónia para obter orientações.



Gravidade

Probabilidade 4/5 – Burlas de emprego e estágio falsos são extremamente relevantes para estudantes, pois exploram a pressão financeira, a confiança nas instituições académicas e o uso frequente do e-mail universitário. Essa ameaça pode levar a perdas financeiras, roubo de identidade e stress emocional.



Fontes principais

Polícia e Guarda de Fronteiras da Estónia – denúncia de fraudes online: <https://www.politsei.ee> RIA – Autoridade de Sistemas de Informação da Estónia e CERT-EE: <https://www.ria.ee/en> Registo de Empresas Eletrónico da Estónia (verificação de empresas): <https://ariregister.rik.ee/eng> EURES – portal de empregos legítimos em toda a UE: <https://eures.europa.eu> Escritório de Segurança da Informação da UC Berkeley – arquivo de exemplos de phishing (burlas direcionadas a universidades): <https://security.berkeley.edu/education-awareness/phishing/phishing-examples-archive> Tecnologia da Informação da NYU – principais burlas de cibersegurança direcionadas a estudantes: <https://www.nyu.edu/life/information-technology/safe-computing/checklists-guides/cyberthreats/scams-targeting-students.html> Relatório de Inteligência e Impactos de Burlas da F-Secure 2025: <https://www.f-secure.com/us-en/partners/insights/scam-intelligence-and-impacts-report-2025> Better Internet for Kids – Recursos do Dia da Internet Segura 2025 sobre burlas que afetam jovens: <https://better-internet-for-kids.europa.eu>

Conclusões

De modo geral, pode-se afirmar que o ambiente digital da juventude na Estónia é caracterizado pelo amplo acesso à tecnologia, altos níveis de competência digital e forte apoio institucional à aprendizagem digital. Pesquisas da União Europeia posicionam consistentemente a Estónia entre as principais sociedades digitais da Europa. Contudo, o uso extensivo de redes sociais digitais entre os jovens também destaca a importância de abordar questões relacionadas com a segurança online, o cyberbullying, o bem-estar digital e a alfabetização digital crítica. Portanto, formuladores de políticas e educadores enfatizam cada vez mais o comportamento online responsável, a alfabetização mediática e a resiliência digital como competências essenciais para os jovens que crescem na sociedade altamente digitalizada da Estónia.

Os relatórios da Comissão Europeia e do Eurostat também destacam as crescentes preocupações com o cyberbullying, o assédio online e a disseminação de conteúdo digital prejudicial entre adolescentes na União Europeia. É por isso que pesquisadores e formuladores de políticas enfatizam a importância de fortalecer a alfabetização digital, o pensamento crítico em relação aos media e a educação para a segurança online, a fim de ajudar os jovens a navegar em ambientes digitais de forma segura e responsável.

Os resultados desta investigação documental mostraram que existem muitas ameaças às quais os jovens estão expostos ao usar as redes sociais ou mesmo os seus e-mails. O projeto ESCAP(E+) visa desenvolver recursos abrangentes para jovens, como ferramentas digitais interativas, incluindo uma aplicação de jogo de fuga em realidade virtual, infográficos e vídeos animados, a fim de promover a sua inclusão digital e aumentar a sua sensibilização em termos de cibersegurança e práticas de segurança online.

Recursos

- “Estónia: um panorama das competências digitais”, criado por Lidija Kralj, atualizado em 2 de agosto de 2024 e acessado em 11 de março de 2026 <https://digital-skills-jobs.europa.eu/en/latest/briefs/estonia-snapshot-digital-skills>
- Euronews, artigo: “Quase metade dos jovens da UE expostos a abusos online, revela novo relatório”, por Alessio Dell’Anna, publicado em 07/11/2024 e consultado em 11 de março de 2026 <https://www.euronews.com/my-europe/2024/11/07/nearly-half-of-eu-youngsters-exposed-to-online-abuse-new-report-finds>
- União Europeia, Melhor Internet para Crianças, Centro Estoniano de Internet Segura, consultado em 12 de março de 2026 <https://better-internet-for-kids.europa.eu/en/sic/estonia>
- Eurostat, artigo: “97% dos jovens na UE usam a internet diariamente”, publicado em 15 de julho de 2025 e acessado em 11 de março de 2026 <https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20250715-1>
- London School of Economics and Political Science. (2020). “EU Kids Online: Resultados do projeto na Estónia”, acessado em 11 de março de 2026. <https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online/participating-countries/estonia>
- República da Estónia, Conselho de Seguridade Social, “Linha de Ajuda para Crianças 116111”, acessado em 12 de março de 2026 <https://sotsiaalkindlustusamet.ee/en/child-and-adult-need-help/child-protection-and-family-support/child-helpline-116111>
- Instituto de Estatística da Estónia: “O uso da internet está aumentando na Estónia”, publicado em 14 de setembro de 2023 e acessado em 11 de março de 2026 <https://stat.ee/en/news/information-technology-households-2023>



Espanha

INVESTIGAÇÃO DOCUMENTAL



Co-funded by
the European Union

Visão geral

Estatísticas nacionais demonstram que o uso da internet entre jovens em Espanha é extremamente difundido. Dados do Instituto Nacional de Estatística da Espanha (INE) indicam que 99,6% dos indivíduos entre 16 e 24 anos são utilizadores regulares da internet. As ferramentas digitais são comumente utilizadas para comunicação, entretenimento, fins académicos e acesso à informação. Plataformas de redes sociais como o Instagram e o TikTok, bem como aplicações de mensagens como o WhatsApp, desempenham um papel central nas interações diárias de adolescentes e jovens adultos.

Para a maioria dos jovens espanhóis, os smartphones constituem a principal porta de entrada para os ambientes online. A conectividade contínua permite o uso frequente de mensagens privadas, a partilha de conteúdo e a participação em comunidades online. No entanto, este alto nível de exposição também aumenta a interação com contactos desconhecidos, links suspeitos e espaços digitais potencialmente inseguros.

Principais fatores de risco

Em Espanha, altos níveis de envolvimento digital juvenil coexistem com lacunas persistentes na sensibilização sobre cibersegurança e na competência em segurança digital. Relatórios e iniciativas de sensibilização promovidas pelo Instituto Nacional de cibersegurança da Espanha (INCIBE) indicam que muitos jovens utilizadores subestimam os riscos online e demonstram conhecimento limitado sobre princípios de proteção de dados, privacidade e estratégias de prevenção de riscos online.

O uso intensivo de plataformas de redes sociais e serviços de mensagens privadas aumenta a exposição a contactos desconhecidos, links externos e conteúdo digital partilhado rapidamente. Quando combinado com respostas rápidas via smartphone e menor capacidade de avaliação crítica das informações online, estes padrões podem enfraquecer a resiliência cibernética e facilitar a vulnerabilidade a técnicas de engenharia social, tentativas de phishing, desinformação, roubo de identidade e outras formas de fraude online.

Visão geral

Portanto, fortalecer as competências digitais, o pensamento crítico e a consciência mediática entre os jovens é essencial para promover o uso seguro da internet e a cidadania digital responsável. Esses elementos são fundamentais para fomentar a resiliência digital europeia e apoiar a educação digital inclusiva em contextos de aprendizagem formais e não formais.

Canais de suporte e denúncia

Em Espanha, diversos órgãos públicos contribuem para a prevenção de riscos online e para a gestão de incidentes cibernéticos envolvendo jovens. O Instituto Nacional de Cibersegurança da Espanha (INCIBE) oferece orientação específica para menores e famílias através de iniciativas especializadas em segurança online, com o objetivo de fortalecer a sensibilização sobre cibersegurança, a proteção da privacidade e o uso responsável da internet. Além disso, a linha direta nacional de cibersegurança 017 oferece assistência confidencial a pessoas que enfrentam problemas de segurança digital ou ameaças online. Casos graves de crimes cibernéticos também podem ser formalmente comunicados às autoridades policiais nacionais, incluindo a Polícia Nacional e a Guarda Civil.

Ameaça do Facebook

Burlas de phishing com falsas alegações de violação de direitos de autor ou suspensão de conta



Plataforma principal

Facebook



Descrição resumida

Utilizadores recebem mensagens fraudulentas alegando que as suas contas ou páginas do Facebook violaram direitos de autor ou padrões da comunidade. A mensagem redireciona-os para uma página de início de sessão falsa, onde as credenciais são recolhidas. Esta burla de phishing frequentemente visa pequenas empresas, associações e jovens criadores de conteúdo em Espanha.



Cenário típico da juventude

Um jovem criador de conteúdo recebe uma mensagem alegando que a sua página do Facebook violou as regras de direitos de autor e será suspensa. A mensagem exige ação imediata e inclui um link para uma página de verificação falsa. O utilizador insere as suas credenciais de início de sessão, após o que a conta é comprometida e usada indevidamente para atividades fraudulentas.

A vítima recebe uma mensagem ou publicação que finge ser do suporte do Facebook.



Como funciona?

A mensagem alega violação de direitos de autor ou de políticas da empresa. Um link redireciona o utilizador para uma página falsa de início de sessão ou de apelação.

O utilizador insere as credenciais de início de sessão e, possivelmente, códigos de verificação.

O invasor obtém acesso à conta e utiliza-a indevidamente.



Sinais de alerta

Mensagens que criam urgência sobre a suspensão da conta.

Links que não pertencem aos domínios oficiais do Facebook ou da Meta.

Solicitações de palavras-passe ou códigos de verificação através de mensagens privadas.

Mensagens de contas criadas recentemente ou não verificadas.

Erros ortográficos ou formatação incomum.



Medidas de prevenção

Verifique as notificações da conta diretamente na plataforma oficial do Facebook.

Evite clicar em links suspeitos recebidos por mensagens privadas.

Ative a autenticação de dois fatores (2FA).

Use palavras-passe fortes e exclusivas.

Participe em iniciativas de sensibilização sobre segurança digital e cibersegurança promovidas pelo INCIBE ou outros programas nacionais.

Ameaça do Facebook

Burlas de phishing com falsas alegações de violação de direitos de autor ou suspensão de conta



**O que fazer
se isto
acontecer?**

Altere imediatamente a palavra-passe da conta.
Encerre todas as sessões ativas.
Utilize as ferramentas oficiais de recuperação de conta do Facebook.
Denuncie a mensagem fraudulenta através do sistema de denúncias do Facebook. Se necessário, entre em contacto com a linha de ajuda 017 da INCIBE para obter orientações.



Gravidade

Probabilidade 4/5 - Este tipo de phishing é comum em plataformas de redes sociais em Espanha e frequentemente tem como alvo páginas geridas por utilizadores jovens, associações e pequenas organizações.



**Fontes
principais**

Meta. (s.d.). Central de Ajuda do Facebook – Alertas de segurança e início de sessão. <https://www.facebook.com/help/>

Instituto Nacional de Cibersegurança (INCIBE). (s.d.). Phishing e fraude online. <https://www.incibe.es/menores>

Ameaça do Instagram

Burlas de falsificação de identidade de influenciadores e marcas



Plataforma principal

Instagram



Descrição resumida

Contas fraudulentas do Instagram fazem-se passar por marcas, instituições públicas ou influenciadores e contactam utilizadores através de mensagens diretas com ofertas de colaboração, sorteios falsos ou solicitações de verificação de conta. Essas interações geralmente redirecionam os utilizadores para links de phishing ou resultam na invasão da conta.



Cenário típico da juventude

Uma jovem utilizadora do Instagram recebe uma mensagem direta de uma conta que alega representar uma marca ou influenciador conhecido, oferecendo uma colaboração ou prémio num sorteio. A mensagem inclui um link solicitando a verificação da conta. Confiando na oferta, a utilizadora insere os seus dados de início de sessão ou códigos de verificação num site falso. Pouco tempo depois, a conta é invadida e usada indevidamente.



Como funciona?

A vítima recebe uma mensagem direta de uma marca falsa ou de uma conta de influenciador.

A mensagem oferece colaboração, prémios ou verificação.

O link redireciona o utilizador para um site de phishing.

O utilizador insere as credenciais de início de sessão ou os códigos de verificação.

O invasor obtém acesso à conta.



Sinais de alerta

Mensagens a oferecer colaborações ou prémios de contas não verificadas. Contas com nomes de utilizador ligeiramente alterados de marcas conhecidas.

Solicitações de credenciais de início de sessão ou códigos de verificação via mensagem direta.

Links que direcionam para domínios não oficiais do Instagram ou de marcas.

Linguagem urgente que pressiona por ação imediata.



Medidas de prevenção

Verifique as contas através de perfis oficiais da marca ou do influenciador.

Evite partilhar dados de início de sessão ou códigos de verificação por mensagens diretas.

Ative a autenticação de dois fatores (2FA).

Verifique atentamente os nomes de utilizador e os selos de verificação de conta.

Denuncie contas suspeitas através das ferramentas de denúncia do Instagram.

Ameaça do Instagram

Burlas de falsificação de identidade de influenciadores e marcas



O que fazer se isto acontecer?

Altere imediatamente a palavra-passe do Instagram.
Encerre todas as sessões ativas.
Ative ou redefina a autenticação de dois fatores.
Denuncie a conta falsa ao Instagram.
Contacte a INCIBE (linha de apoio 017) se precisar de mais ajuda.



Gravidade

Probabilidade 4/5 - Burlas de falsificação de identidade são comuns no Instagram em Espanha, afetando principalmente utilizadores jovens e criadores de conteúdo emergentes.



Fontes principais

Meta. (s.d.). Central de Ajuda do Instagram.
<https://help.instagram.com/>

Instituto Nacional de Cibersegurança (INCIBE). (s.d.). Roubo de identidade e fraude em redes sociais.
<https://www.incibe.es/menores>

Ameaça do TikTok

Sorteios falsos e burlas associadas a desafios populares



Plataforma principal

TikTok



Descrição resumida

Burlões exploram tendências e desafios virais do TikTok partilhando links que prometem prémios, dispositivos gratuitos ou aumento de seguidores. Esses links redirecionam os utilizadores para sites de phishing ou aplicações maliciosas fora da plataforma TikTok.



Cenário típico da juventude

Um jovem utilizador do TikTok vê um vídeo viral promovendo um sorteio relacionado com uma tendência popular. A publicação promete um smartphone grátis ou mais seguidores em troca de um registo rápido. O utilizador clica no link na bio ou nos comentários e é redirecionado para um site externo que solicita informações pessoais ou dados de início de sessão. Pouco tempo depois, a conta é comprometida ou os dados pessoais são usados indevidamente.



Como funciona?

1. A vítima depara-se com uma publicação ou desafio viral que promove um prémio.
2. O conteúdo inclui um link na biografia, nos comentários ou no perfil.
3. O link redireciona para um site ou aplicação externo de phishing.
4. O utilizador insere informações pessoais ou da conta.
5. O atacante recolhe os dados ou obtém acesso à conta.



Sinais de alerta

Ofertas de prémios caros ou rápido crescimento de seguidores.
Links que direcionam os utilizadores para fora da plataforma oficial do TikTok.
Solicitações de credenciais de início de sessão ou dados pessoais.
Contas criadas recentemente com poucas interações reais.
Instruções urgentes para "agir rapidamente" e reivindicar as recompensas.



Medidas de prevenção

Verifique os sorteios através das contas oficiais da marca ou do criador.
Evite clicar em links suspeitos em comentários ou biografias.
Ative a autenticação de dois fatores (2FA).
Não descarregue aplicações de fontes desconhecidas.
Denuncie conteúdo suspeito através das ferramentas de denúncia do TikTok.

Ameaça do TikTok

Sorteios falsos e burlas associadas a desafios populares



O que fazer se isto acontecer?

Mude imediatamente a palavra-passe do TikTok.
Ative ou redefina a autenticação de dois fatores.
Remova quaisquer aplicações desconhecidas vinculadas.
Denuncie o conteúdo fraudulento ao TikTok.
Contacte a INCIBE (linha de apoio 017) para obter orientações adicionais.



Gravidade

Probabilidade 4/5 - Burlas de sorteios baseados em tendências aparecem com frequência no TikTok em Espanha e afetam desproporcionalmente os utilizadores jovens que interagem ativamente com conteúdo viral e desafios online.



Fontes principais

TikTok. (s.d.). Central de Segurança do TikTok.
<https://www.tiktok.com/safety/pt-pt/>

Instituto Nacional de Cibersegurança (INCIBE). (s.d.). Fraudes e burlas nas redes sociais. <https://www.incibe.es/menores>

Ameaça por e-mail

E-mails de phishing que se fazem passar por bancos e serviços públicos



Plataforma principal

E-mail



Descrição resumida

E-mails fraudulentos fazem-se passar por bancos espanhóis, autoridades fiscais ou serviços públicos e solicitam aos utilizadores que confirmem informações pessoais ou financeiras com urgência. Essas mensagens geralmente contêm links ou anexos maliciosos que levam ao roubo de credenciais ou à instalação de malware.



Cenário típico da juventude

Um jovem universitário recebe um e-mail supostamente de um banco espanhol ou da Autoridade Tributária, referente a um reembolso ou multa não paga. A mensagem solicita a confirmação imediata dos dados bancários através de um link fornecido. Acreditando ser legítimo, o estudante insere informações pessoais ou bancárias num site falso. Pouco tempo depois, dados sensíveis são roubados ou a conta bancária é comprometida.



Como funciona?

1. A vítima recebe um e-mail que finge ser de uma instituição confiável.
2. A mensagem cria urgência (reembolso, multa, conta bloqueada).
3. Um link ou anexo redireciona para um site falso ou instala malware.
4. O utilizador insere dados pessoais ou financeiros.
5. O atacante obtém acesso às informações ou contas da vítima.



Sinais de alerta

Solicitações urgentes para confirmação de dados ou para evitar penalidades.
Endereços de remetentes suspeitos que não correspondem a domínios oficiais.
Solicitações de dados bancários ou códigos de verificação.
Anexos inesperados ou solicitações de download.
Saudações genéricas como "Caro cliente".



Medidas de prevenção

Verifique as informações diretamente nos sites oficiais do banco ou do governo.
Não clique em links suspeitos nem abra anexos inesperados.
Ative a autenticação de dois fatores (2FA) em contas financeiras.
Mantenha o antivírus e o software de segurança atualizados.
Nunca forneça dados bancários por e-mail.

Ameaça por e-mail

E-mails de phishing que se fazem passar por bancos e serviços públicos



O que fazer se isto acontecer?

Caso dados financeiros tenham sido partilhados, entre em contacto com o banco imediatamente.
Altere palavras-passe e ative a autenticação de dois fatores (2FA).
Desligue o dispositivo se houver suspeita de malware.
Reporte o incidente à INCIBE (linha de apoio 017).
Apresente uma reclamação à Policía Nacional ou à Guardia Civil, se necessário.



Gravidade

Probabilidade 5/5 - E-mails de phishing que se fazem passar por instituições financeiras e públicas estão entre as ameaças cibernéticas mais disseminadas na Espanha e frequentemente levam a perdas financeiras e roubo de identidade.



Fontes principais

Instituto Nacional de Cibersegurança (INCIBE). (s.d.). Fraudes e burlas nas redes sociais. <https://www.incibe.es/menores>

Polícia Nacional. (s.d.). https://www.policia.es/_es/index.php

Conclusões

Os resultados desta investigação documental indicam que o phishing, as burlas de falsificação de identidade e várias formas de fraude online representam algumas das ameaças de cibersegurança mais relevantes enfrentadas pelos jovens em Espanha. Estas ameaças são especialmente significativas porque ocorrem nas plataformas mais utilizadas pelos jovens, como o Instagram, o TikTok, o Facebook e o e-mail, e dependem fortemente de técnicas de engenharia social que exploram a urgência, a credibilidade e a resposta emocional. Dado o elevado nível de envolvimento dos jovens na comunicação online, na criação de conteúdos e nas atividades académicas, a sua exposição a links enganosos, contas falsas e mensagens fraudulentas é considerável.

Para os técnicos de juventude, estes riscos criam uma necessidade crescente de aumentar a sensibilização sobre cibersegurança, promover práticas de segurança digital e fortalecer a resiliência cibernética entre os jovens utilizadores. Os riscos identificados revelam lacunas persistentes nas práticas de proteção da privacidade, na compreensão da segurança de dados e na capacidade de avaliar criticamente o conteúdo digital. Para lidar com estas vulnerabilidades, é necessário um programa estruturado de educação em cibersegurança voltado para jovens, que incentive a cidadania digital responsável e o uso seguro da internet em contextos de aprendizagem formais e não formais.

Estas descobertas apoiam diretamente os objetivos do projeto ESCAP(E+). Dentro da estrutura do projeto e dos materiais de formação, deve-se enfatizar a prevenção de phishing, a sensibilização sobre engenharia social, as medidas de proteção de identidade e as estratégias práticas de resposta a incidentes cibernéticos. O desenvolvimento de cenários de jogos de fuga em realidade virtual pode simular situações realistas de risco online, permitindo que os jovens participantes desenvolvam competências práticas de tomada de decisão em ambientes de aprendizagem imersivos. Além disso, os materiais de sensibilização, como infográficos e vídeos animados, devem comunicar mensagens-chave de segurança de forma clara, envolvente e acessível, reforçando as competências digitais e promovendo a educação digital inclusiva entre diversos grupos de jovens.

Conclusões

Através da integração de abordagens de aprendizagem experiencial, métodos de ensino inovadores e campanhas de sensibilização digital direcionadas, a ESCAP(E+) tem o potencial de aumentar a resiliência digital europeia e promover melhorias a longo prazo na sensibilização sobre cibersegurança entre os jovens em Espanha.

Recursos

- Instituto Nacional de Estatística (INE). (s.d.). Inquérito sobre equipamentos e uso de tecnologias de informação e comunicação em domicílios. https://www.ine.es/ss/Satellite?L=es_ES&c=INESeccion_C&cid=1259925528559&p=%5C&pagename=ProductosYServicios%2FPYSLayout
- Instituto Nacional de Cibersegurança (INCIBE). (s.d.). Cidadania. <https://www.incibe.es/ciudadania>
- Instituto Nacional de Cibersegurança (INCIBE). (s.d.). Menores – segurança na internet. <https://www.incibe.es/menores>
- Instituto Nacional de Cibersegurança (INCIBE). (s.d.). A linha de apoio 017 oferece assistência em cibersegurança. <https://www.incibe.es/el-017-se-ocupa>
- Polícia Nacional. (s.d.). <https://www.policia.es/es/index.php>
- Guarda Civil. (s.d.). <https://web.guardiacivil.es/es>



ESCAP(E+)

Portugal

INVESTIGAÇÃO DOCUMENTAL



Co-funded by
the European Union

Visão geral

De acordo com as estatísticas nacionais de educação e digitais publicadas pela Direção-Geral de Estatísticas da Educação e da Ciência (DGEEC) (1), os jovens em Portugal utilizam frequentemente as tecnologias digitais tanto em contextos académicos como pessoais. O acesso à Internet e aos dispositivos digitais é amplamente utilizado para a comunicação, a obtenção de informação, as atividades de aprendizagem e a interação social.

As plataformas digitais desempenham um papel importante na rotina diária dos estudantes, incluindo o acesso a materiais educacionais, a participação em ambientes virtuais de aprendizagem e a manutenção de conexões sociais. As redes sociais e as aplicações de mensagens são comumente utilizadas em conjunto com sistemas formais de aprendizagem digital, contribuindo para um estilo de vida digital altamente conectado e interativo.

Os dispositivos móveis permitem que os jovens permaneçam constantemente conectados a conteúdo e serviços online. Como resultado, os utilizadores frequentemente envolvem-se em mensagens privadas, partilha de conteúdo e colaboração online em diversas plataformas. No entanto, a verificação limitada de informações online aumenta a exposição à desinformação, mensagens fraudulentas e interações digitais inseguras. De modo geral, as tecnologias digitais criam tanto oportunidades como riscos potenciais, tornando a sensibilização sobre cibersegurança essencial em iniciativas de educação e empoderamento juvenil.

Principais fatores de risco

De acordo com a Agência da União Europeia para a Cibersegurança (ENISA), os jovens enfrentam vários fatores de risco que aumentam a sua vulnerabilidade às ameaças digitais (2), incluindo competências limitadas em cibersegurança, elevada exposição a estratégias de engenharia social, utilização extensiva de serviços de mensagens privadas e compreensão limitada da proteção de dados e da privacidade. Estes fatores contribuem para uma maior exposição a fraudes, tentativas de falsificação de identidade e outras formas de cibercrime.

Visão geral

Principais indicadores nacionais

Os dados estatísticos da PORDATA (3) e do Eurostat (4) indicam que a utilização da Internet é generalizada entre os jovens em Portugal. A maioria dos utilizadores tem acesso regular às tecnologias digitais, embora persistam diferenças nas competências digitais e na consciencialização sobre as práticas de segurança online.

Canais de suporte e denúncia

Em Portugal, várias instituições nacionais disponibilizam apoio e mecanismos de denúncia para riscos online, incluindo CERT.PT, o Centro Nacional de Cibersegurança (CNCS), a Linha Internet Segura, o Portal de Cibercrime do Ministério Público e a Polícia Judiciária. Estes serviços contribuem para ambientes digitais seguros e garantem acesso a apoio fiável para jovens (5).

Notas de rodapé:

Direção-Geral de Estatísticas da Educação e Ciência. (n.d.). DGEEC – Direção-Geral de Estatísticas da Educação e Ciência.

1. Agência da União Europeia para a Cibersegurança. (s.d.). Sensibilização e higiene cibernética.
2. PORDATA. (n.d.). Base de Dados Portugal Contemporâneo.
3. Eurostat. (s.d.). Eurostat – Serviço de Estatística da União Europeia.
4. CERT.PT (n.d.); Centro Nacional de cibersegurança (n.d.); CISLab (n.d.); Ministério Público (n.d.); Polícia Judiciária (n.d.).

Ameaça do Facebook

Mensagens de suporte falsas e burlas de recuperação de página



Plataforma principal

Facebook



Descrição resumida

Utilizadores recebem mensagens falsas que alegam representar os serviços de suporte do Facebook e alertam que as suas contas ou páginas podem ser suspensas. As mensagens incluem links para sites de phishing que solicitam dados de início de sessão e informações de segurança.



Cenário típico da juventude

Um jovem que administra a página de uma associação estudantil ou comunidade no Facebook recebe uma mensagem alegando que a página violou as regras da plataforma. A mensagem alerta para a desativação permanente da conta em breve. Preocupado com a possibilidade de perder o acesso, o utilizador clica no link e insere os dados de início de sessão num site falso de recuperação. Pouco tempo depois, a conta é invadida e utilizada indevidamente.



Como funciona?

1. A vítima recebe uma mensagem que finge ser do Suporte do Facebook.
2. A mensagem alega que a conta violou as políticas da plataforma.
3. Um link redireciona o utilizador para uma página falsa de recuperação ou verificação.
4. O utilizador insere as suas credenciais de início de sessão e códigos de segurança.
5. O invasor obtém acesso à conta e utiliza-a indevidamente.



Sinais de alerta

Mensagens que criam urgência sobre a suspensão imediata da conta. Links que direcionam para sites que não são domínios oficiais do Facebook ou da Meta.

Solicitações de palavras-passe, códigos de verificação ou informações pessoais através de mensagens privadas.

Mensagens enviadas por contas desconhecidas ou criadas recentemente.

Erros ortográficos ou formatação incomum na mensagem.



Medidas de prevenção

Verifique as notificações de segurança diretamente na plataforma oficial do Facebook.

Evite clicar em links recebidos por mensagens privadas.

Ative a autenticação de dois fatores e use palavras-passe fortes e exclusivas.

Revise regularmente as definições de segurança da sua conta.

Participe em formações de sensibilização sobre segurança digital e

Ameaça do Facebook

Mensagens de suporte falsas e burlas de recuperação de página



O que fazer se isto acontecer?

Altere imediatamente a palavra-passe da conta e encerre todas as sessões.
Use as ferramentas oficiais de recuperação do Facebook para recuperar o acesso.
Denuncie a mensagem fraudulenta através do sistema de denúncias do Facebook.
Informe os seus seguidores ou membros da página sobre o incidente.
Se necessário, contacte os serviços de apoio nacionais, como o CERT.PT.



Gravidade

Probabilidade 4/5 - Este tipo de burla é comum em plataformas de redes sociais e frequentemente visa utilizadores que administram páginas ou contas de comunidades. Tentativas de phishing semelhantes são relatadas regularmente em toda a Europa e em Portugal, tornando os utilizadores jovens particularmente vulneráveis.



Fontes principais

Meta. (s.d.). Proteja a sua conta contra phishing e burlas.
<https://www.facebook.com/help/181495968648557>

Meta. (s.d.). Proteja a sua conta do Facebook.
<https://www.facebook.com/help/203305893040179>

Ameaça do Instagram

Burlas de verificação de conta e avisos de direitos de autor



Plataforma principal

Instagram



Descrição resumida

Utilizadores recebem mensagens fraudulentas alegando que as suas contas do Instagram serão removidas devido a violação de direitos de autor ou falsificação de identidade. As mensagens incluem links para sites de phishing que solicitam palavras-passe e códigos de verificação. Esta burla explora o medo dos utilizadores de terem as suas contas suspensas.



Cenário típico da juventude

Um jovem criador de conteúdo recebe uma mensagem informando que a sua conta do Instagram violou as regras de direitos de autor. A mensagem avisa que a conta será removida em breve. Temendo perder o acesso, o utilizador clica no link e insere os seus dados de início de sessão numa página de verificação falsa. Pouco tempo depois, a conta é invadida e usada indevidamente.



Como funciona?

A vítima recebe uma mensagem que finge ser do suporte do Instagram.

A mensagem alega violação de direitos de autor ou falsificação de identidade.

Um link redireciona o utilizador para um site de verificação falso.

O utilizador insere as credenciais de início de sessão e os códigos de segurança.

O invasor obtém acesso à conta.



Sinais de alerta

Mensagens alertando para a remoção urgente da conta.

Links que não pertencem aos domínios oficiais do Instagram ou da Meta.

Solicitações de palavras-passe ou códigos de verificação.

Mensagens de contas desconhecidas ou criadas recentemente.

Erros de ortografia ou formatação.



Medidas de prevenção

Verifique as notificações de segurança dentro da aplicação Instagram.

Ative a autenticação de dois fatores.

Evite clicar em links em mensagens privadas.

Use palavras-passe fortes e exclusivas.

Revise regularmente as definições de segurança da sua conta.

Ameaça do Instagram

Burlas de verificação de conta e avisos de direitos de autor



O que fazer se isto acontecer?

Altere a palavra-passe da conta imediatamente.
Encerre todas as sessões ativas.
Use as ferramentas oficiais de recuperação do Instagram.
Denuncie a burla pelo Instagram.
Procure o apoio da Linha Internet Segura, se necessário.



Gravidade

Probabilidade 4/5 - Este burla é comum no Instagram, especialmente entre utilizadores jovens e criadores de conteúdo. Ataques de phishing semelhantes são frequentemente relatados em Portugal, tornando esta ameaça altamente relevante.



Fontes principais

Meta. (s.d.). Central de Ajuda do Instagram.
<https://help.instagram.com/>

Centro de Segurança na Internet Portugal. (s.d.). Internet Segura.
<https://internetsegura.pt/>

Ameaça do TikTok

Links falsos para monetização e programas de criadores



Plataforma principal

TikTok



Descrição resumida

Utilizadores recebem mensagens convidando-os a participar em programas falsos de monetização do TikTok ou fundos para criadores. Essas mensagens incluem links para sites externos criados para recolher credenciais de início de sessão ou dados pessoais. Esta burla explora o interesse de jovens utilizadores em obter visibilidade e recompensas financeiras.



Cenário típico da juventude

Um jovem utilizador do TikTok recebe uma mensagem oferecendo acesso a um programa de monetização ou recompensas para criadores. A mensagem promete benefícios financeiros e maior visibilidade. Interessado em expandir a sua presença online, o utilizador clica no link e insere informações pessoais e da conta numa página de registo falsa. Pouco tempo depois, a conta é invadida e usada indevidamente.



Como funciona?

A vítima recebe uma mensagem oferecendo acesso a um programa de monetização ou para criadores de conteúdo.

A mensagem promete benefícios exclusivos ou recompensas financeiras.

Um link redireciona o utilizador para um site de registo falso. O utilizador insere as suas credenciais de início de sessão e informações pessoais.

O invasor obtém acesso à conta.



Sinais de alerta

Mensagens que prometem dinheiro fácil ou programas exclusivos para criadores de conteúdo.

Links que levam a sites fora dos domínios oficiais do TikTok.

Solicitações de palavras-passe ou informações pessoais.

Pressão para se inscrever rapidamente.

Mensagens de contas desconhecidas ou não verificadas.



Medidas de prevenção

Verifique as informações de monetização através da aplicação oficial do TikTok.

Evite clicar em links suspeitos.

Ative a autenticação de dois fatores.

Use palavras-passe fortes e exclusivas.

Não compartilhe dados pessoais em sites externos.

Ameaça do TikTok

Links falsos para monetização e programas de criadores



O que fazer se isto acontecer?

- Proteja a conta alterando a palavra-passe e ativando a autenticação de dois fatores.
- Remova quaisquer e-mails, números de telefone ou dispositivos suspeitos associados.
- Analise a atividade recente e elimine publicações ou mensagens não autorizadas.
- Denuncie o link ou mensagem fraudulenta através das ferramentas de segurança do TikTok.
- Envie um pedido de recuperação de conta se o acesso estiver restrito.



Gravidade

Probabilidade 3/5 - Esta burla afeta principalmente criadores de conteúdo jovens e principiantes e aparece com frequência no TikTok. Embora menos disseminada do que o phishing por e-mail ou redes sociais, continua a ser um risco relevante em Portugal.



Fontes principais

TikTok. (s.d.). Centro de Segurança do TikTok (Portugal). <https://www.tiktok.com/safety/en-br/>

TikTok. (s.d.). Segurança da conta e do utilizador. https://support.tiktok.com/pt_BR/safety-hc/account-and-user-safety/account-safety

Ameaça por e-mail

Burlas com faturas falsas e notificações de entrega falsas



Plataforma principal

E-mail



Descrição resumida

Utilizadores recebem e-mails fraudulentos que se fazem passar por empresas de entrega, fornecedores de telecomunicações ou prestadores de serviços. Estas mensagens solicitam pagamento, dados pessoais ou downloads de anexos. Esta burla visa roubar informações confidenciais ou instalar malware no dispositivo do utilizador.



Cenário típico da juventude

Um jovem recebe um e-mail supostamente de uma empresa de entregas sobre uma encomenda não entregue ou uma fatura em aberto. A mensagem inclui um link ou anexo que solicita ação imediata. Acreditando que a mensagem é legítima, o utilizador clica no link ou abre o ficheiro e insere informações pessoais ou bancárias. Pouco tempo depois, dados sensíveis são roubados ou um malware é instalado.



Como funciona?

A vítima recebe um e-mail que finge ser de uma empresa legítima. A mensagem solicita pagamento urgente, download de documento ou verificação. Um link ou anexo redireciona o utilizador para um site falso ou instala malware. O utilizador insere informações pessoais ou financeiras. O atacante obtém acesso a dados sensíveis ou ao dispositivo.



Sinais de alerta

E-mails que criam sentido de urgência em relação a pagamentos ou entregas.
Anexos ou solicitações de download inesperados.
Endereços de remetente que não correspondem aos domínios oficiais da empresa.
Solicitações de informações bancárias ou pessoais.
Saudações genéricas como "Caro cliente".



Medidas de prevenção

Verifique os e-mails diretamente nos sites oficiais das empresas.
Não abra anexos suspeitos.
Evite clicar em links desconhecidos.
Utilize um software antivírus atualizado.
Nunca partilhe informações bancárias por e-mail.

Ameaça por e-mail

Burlas com faturas falsas e notificações de entrega falsas



O que fazer se isto acontecer?

Desligue o dispositivo da internet se houver suspeita de malware.
Altere as suas palavras-passe imediatamente.
Entre em contacto com o banco caso dados financeiros tenham sido partilhados.
Denuncie o e-mail como phishing.
Execute uma verificação completa de antivírus.
Procure apoio junto do CERT.PT ou da Linha Internet Segura.



Gravidade

Probabilidade 5/5 - A fraude por e-mail é uma das ciberameaças mais disseminadas em Portugal e tem como alvo frequente os utilizadores mais jovens. Burlas semelhantes são relatadas regularmente, tornando este um risco bastante relevante.



Fontes principais

Safer Internet Centre Portugal. (s.d.). Internet Segura - Phishing e burlas online. <https://cislab.cncs.gov.br/>
Polícia Judiciária. (s.d.). Cibercrime e burlas informáticas. <https://www.policiajudiciaria.pt/>

Conclusões

Os resultados desta investigação documental indicam que o phishing, a falsificação de identidade e a fraude online continuam a ser as ameaças mais significativas à cibersegurança que afetam os jovens em Portugal. Estas ameaças são especialmente comuns nas plataformas de redes sociais e através da comunicação por e-mail, onde os utilizadores são frequentemente expostos a mensagens fraudulentas, pedidos de verificação falsos e links enganosos. Dada a forte presença dos jovens em ambientes digitais para aprendizagem, comunicação e interação social, estes são particularmente vulneráveis a estas ameaças. Consequentemente, os técnicos de juventude são cada vez mais solicitados a apoiar os jovens utilizadores no desenvolvimento de comportamentos online mais seguros e na resposta eficaz aos riscos digitais.

A análise também demonstra a importância de reforçar a literacia digital, o pensamento crítico e a sensibilização sobre cibersegurança entre os jovens. Muitas das ameaças identificadas exploram a pressão emocional, a falta de conhecimento técnico e a limitada sensibilização sobre práticas de segurança online. Estas descobertas destacam a necessidade de iniciativas educacionais estruturadas com foco na prevenção de phishing, proteção de dados, sensibilização sobre privacidade e cidadania digital responsável. Ao fortalecer estas competências, os técnicos de juventude podem contribuir para a construção de maior resiliência cibernética em contextos de aprendizagem formais e não formais.

Em resposta a estes desafios, o projeto ESCAP(E+) deve dar prioridade a abordagens educacionais práticas e envolventes. A estrutura do projeto e as diretrizes de formação devem enfatizar exemplos realistas, deteção precoce de riscos e estratégias de resposta eficazes. O desenvolvimento de cenários de jogos de fuga em realidade virtual pode proporcionar experiências de aprendizagem imersivas que permitem aos jovens praticar a tomada de decisões em incidentes cibernéticos simulados.

Conclusões

Além disso, materiais de sensibilização, como infográficos e vídeos animados, devem comunicar mensagens-chave de segurança de forma clara, acessível e visualmente atrativa. Estes recursos podem promover a inclusão digital e contribuir para melhorias a longo prazo na sensibilização sobre cibersegurança e nas práticas de segurança online entre os jovens.

Recursos

- Direção-Geral de Estatísticas da Educação e Ciência. (s.d.). DGEEC - Direção-Geral de Estatísticas da Educação e Ciência. <https://dgeec.medu.pt/>
- Agência da União Europeia para a Cibersegurança. (s.d.). Sensibilização e higiene cibernética. <https://enisa.europa.eu/topics/awareness-and-cyber-hygiene>
- PORDATA. (s.d.). Base de Dados Portugal Contemporâneo.
- Eurostat. (s.d.). Eurostat - Serviço de Estatística da União Europeia. <https://ec.europa.eu/eurostat>
- CERT.PT. (s.d.). Equipa de Resposta a Incidentes de Cibersegurança de Portugal. <https://cert.pt/>
- Centro Nacional de Cibersegurança. (s.d.). Centro Nacional de Cibersegurança. <https://cncs.gov.pt/>
- Centro Nacional de Cibersegurança. (s.d.). CISLab - Centro de Investigação em Segurança Digital. <https://cislab.cncs.gov.pt/>
- Ministério Público. (s.d.). Portal de Cibercrime. <https://cibercrime.ministeriopublico.pt/>
- Polícia Judiciária. (s.d.). Polícia Judiciária. <https://policiajudiciaria.pt/>



ESCAP(E+)

CONCLUSÃO

Conclusões

Esta investigação documental demonstra que as ameaças de cibersegurança mais relevantes que afetam os jovens nos países parceiros da ESCAP(E+) já não são principalmente ataques técnicos, mas sim ameaças de engenharia social incorporadas no comportamento digital quotidiano. Na Lituânia, Roménia, Turquia, Estónia, Espanha e Portugal, os riscos mais elevados estão associados às plataformas e canais de comunicação mais utilizados pelos jovens, especialmente o Instagram, o TikTok, o Facebook, aplicações de mensagens e o e-mail. Estas ameaças incluem phishing, falsificação de identidade, fraude, uso indevido de identidade, desinformação, apropriação indevida de contas e, nos casos mais graves, extorsão sexual e chantagem sexual.

Ao mesmo tempo, a investigação confirma que estes riscos assumem formas diferentes dependendo do contexto nacional. Na Lituânia, os jovens estão cada vez mais expostos a burlas específicas de plataformas que exploram a infraestrutura digital local, como o Smart-ID, phishing baseado em código QR e a confiança em comunidades do Facebook. Na Roménia, as principais vulnerabilidades são fortemente comportamentais e sociais, moldadas pelo elevado tempo passado em frente aos ecrãs, pressão dos pares, esquemas de fraude, cyberbullying e rápida migração de plataformas sociais para canais de mensagens privadas. Na Turquia, os riscos estão intimamente ligados ao comportamento online, altamente visual e frequente, com foco em dispositivos móveis, onde phishing, sorteios falsos, falsificação de identidade e conteúdo enganoso são particularmente eficazes. Na Estónia, a integração digital avançada não reduz o risco; pelo contrário, a elevada conectividade aumenta a exposição à desinformação, ao contacto com estranhos, à manipulação e a danos graves, como extorsão sexual. Em Espanha e Portugal, a investigação destaca o phishing, a falsificação de identidade e a fraude online como as ameaças mais persistentes e significativas, principalmente através de redes sociais e e-mail.

Uma constatação comum em todos os países parceiros é que a vulnerabilidade dos jovens é menos determinada pela falta de acesso à tecnologia e mais pelos padrões de uso.

Conclusões

Isto significa que a educação em cibersegurança para jovens não se pode basear apenas em terminologia técnica ou avisos abstratos. Esta educação precisa de ser prática, acessível, adequada ao grupo etário e diretamente relacionada com situações reais que os jovens encontram online no seu dia a dia digital.

Para os técnicos de juventude, estas descobertas reforçam a necessidade de educação em cibersegurança específica para cada plataforma e baseada em cenários. Estes profissionais precisam de ferramentas que os ajudem a explicar como as burlas funcionam na prática, como reconhecer sinais de alerta e o que fazer imediatamente quando ocorre um incidente. Nos relatórios dos parceiros, várias prioridades emergem repetidamente: literacia visual, pensamento crítico, reconhecimento de phishing, proteção de contas, uso seguro das definições de privacidade, autenticação de dois fatores, proteção de identidade, verificação da origem e conhecimento dos canais locais de denúncia e apoio. A investigação também mostra que as dimensões emocionais e sociais devem ser incluídas, especialmente em relação a assédio, ataques baseados em vergonha, extorsão sexual e manipulação, onde o silêncio e o estigma podem impedir que os jovens procurem ajuda.

Estas descobertas apoiam diretamente os objetivos do projeto ESCAP(E+) e fornecem uma base sólida para os próximos resultados. Em primeiro lugar, a estrutura do projeto e as orientações de formação devem enfatizar a resiliência digital prática, em vez de apenas o conhecimento técnico. Isto inclui reconhecer padrões de burlas, verificar a credibilidade da plataforma, confirmar identidades e ligações, proteger contas, compreender como os dados pessoais são explorados e responder de forma rápida e segura quando surgirem riscos. A estrutura também deve ajudar os técnicos de juventude a traduzir a cibersegurança para contextos de aprendizagem não formal, usando exemplos realistas e linguagem simples.

Conclusões

Em segundo lugar, a investigação documental fornece material robusto para o desenvolvimento de cenários de jogos de fuga em realidade virtual. As conclusões dos parceiros sugerem que os cenários mais eficazes serão aqueles baseados em experiências realistas dos jovens, como falsos recrutamentos de emprego, burlas de aluguer, mensagens de contas hackeadas, sorteios fraudulentos, phishing por código QR, pedidos falsos de taxas alfandegárias ou de entrega, perfis clonados, disseminação de desinformação e tentativas de extorsão sexual ou chantagem. Estes cenários podem ajudar os jovens a praticar o reconhecimento, a tomada de decisões e a resposta segura em ambientes imersivos, porém controlados, o que está totalmente alinhado com o objetivo do projeto de utilizar métodos de aprendizagem gamificados e experienciais.

Em terceiro lugar, as descobertas também orientam o conteúdo de sensibilização, incluindo infográficos, vídeos animados e materiais de campanha. Em todos os países, as evidências sugerem que os materiais de sensibilização devem ser curtos, visuais, claros, acessíveis e baseados em comportamentos reais nas plataformas, em vez de linguagem cibernética genérica. Devem destacar sinais de alerta, hábitos seguros, medidas de resposta imediata e opções de denúncia locais, além de promover a cidadania digital, a inclusão e a confiança para procurar ajuda. Isto é especialmente importante para alcançar jovens com diferentes níveis de competências digitais e para garantir que os resultados do projeto permaneçam relevantes e úteis mesmo após o fim do projeto.

Em conclusão, as descobertas conjuntas dos parceiros confirmam que a cibersegurança juvenil na Europa deve ser abordada através de uma abordagem localizada, prática e educativa. Embora as ameaças específicas variem entre os países, o padrão subjacente é comum: os jovens estão expostos a riscos de cibersegurança manipulativos, baseados na confiança e emocionalmente persuasivos, através das plataformas que utilizam diariamente. Ao transformar estas descobertas num quadro estruturado, em ferramentas de aprendizagem imersivas e em recursos de sensibilização direcionados, a ESCAP(E+) pode dar um importante contributo para a resiliência digital, para um comportamento online mais seguro e para o fortalecimento a longo prazo do trabalho juvenil na área da educação em cibersegurança.



ESCAP(E+)

Fique atento!

Acompanhe o nosso site para aceder a mais recursos e atualizações.

<https://escapeerasmus.com/>



Co-funded by
the European Union