Digital Kidnapping: foto di bambini rubate



Il **furto di foto di bambini dai social media** per creare **truffe solidali false** rappresenta una delle forme di criminalità digitale più insidiose e in crescita esponenziale. Nel 2024, la Polizia Postale italiana ha registrato **181 milioni di euro sottratti** attraverso truffe online, con un aumento del 32% rispetto all'anno precedente. Questo fenomeno, noto come **digital kidnapping** o **rapimento digitale**, combina furto di identità, frode finanziaria e sfruttamento dell'immagine dei minori, causando danni economici devastanti e gravi violazioni dei diritti dei bambini.

Le statistiche globali rivelano che **l'84% dei casi di rapimenti di bambini** sono facilitati attraverso i social media, mentre il **90% dei bambini** ha una presenza online entro i 2 anni di età. Questa massiccia esposizione digitale, combinata con l'inconsapevolezza dei genitori sui rischi del **sharenting** (condivisione compulsiva di foto dei figli), crea un ambiente fertile per i criminali informatici.

Come funziona il digital kidnapping

I truffatori utilizzano **tecniche sofisticate** per appropriarsi illegalmente delle foto dei bambini. Il processo inizia con lo **scraping automatico** attraverso bot programmati per raccogliere massivamente immagini da profili pubblici, seguito dall'**hacking diretto** di account social per accedere a contenuti privati. Nel dark web, gli account hackerati vengono venduti a partire da 35 dollari, facilitando l'accesso a migliaia di foto personali.

Una volta ottenute le immagini, i criminali creano **false campagne solidali** utilizzando modelli standardizzati. Copiano

fundraiser autentici, si appropriano di loghi di ONG riconosciute come Save the Children e UNICEF, e costruiscono narrazioni emotive false su malattie terminali, povertà estrema o disastri naturali. **Facebook, Instagram e TikTok** risultano le piattaforme più vulnerabili, con TikTok che registra il 68,2% di bambini sotto i 13 anni attivi sulla piattaforma.

La diffusione avviene attraverso **reti coordinate** di account falsi che condividono simultaneamente le stesse campagne, sfruttando hashtag trending come #SaveTheChildren per amplificare la visibilità. I truffatori creano falsi sensi di urgenza con messaggi come “ultimi giorni per donare” e sfruttano strategicamente eventi di attualità come pandemie e disastri naturali per massimizzare l’impatto emotivo.

Casi reali di digital kidnapping e impatto economico devastante

Durante l’emergenza COVID-19, la Polizia Postale di Roma ha denunciato due persone per aver organizzato **raccolte fondi fraudolente** per gli ospedali Spallanzani e San Camillo, utilizzando foto di bambini per aumentare l’impatto emotivo delle campagne. Il **Commissariato di P.S. Online** ha ricevuto 82.000 segnalazioni nel 2024, con 23.000 richieste di assistenza specificamente legate a truffe online.

A livello internazionale, dopo il crollo del condominio Surfside in Florida, oltre **20 campagne GoFundMe** sono state identificate come fraudolente, utilizzando foto e storie rubate di vittime reali. Nel Regno Unito, sette persone sono state condannate per una frode organizzata che ha rubato centinaia di migliaia di sterline a enti di beneficenza per bambini, inclusi Children in Need e Great Ormond Street Hospital.

Le **piccole donazioni** vanno dai 10 ai 50 euro per singola

transazione, ma le campagne di successo possono raccogliere tra 5.000 e 50.000 euro. Le organizzazioni criminali più sofisticate arrivano a sottrarre fino a 16 milioni di euro attraverso reti complesse di false campagne coordinate.

Riconoscere le truffe solidali false

Esistono **segnali di allarme** chiari che permettono di identificare queste truffe. Le storie sono spesso **troppo emotive** con foto e video scioccanti, accompagnate da richieste di denaro urgenti con frasi come “serve aiuto subito”. I dettagli medici risultano spesso falsi o copiati da altre fonti, mentre le informazioni sull’uso effettivo del denaro raccolto rimangono vaghe.

Altri indicatori includono **gruppi Facebook** creati di recente specificamente per la campagna, dati bancari non verificabili, e l’assenza di codice fiscale o partita IVA dell’ente benefico. Le campagne legitimate hanno sempre trasparenza totale sui fondi raccolti e sulle spese sostenute, oltre a essere verificabili attraverso i media tradizionali.

Per **verificare l’autenticità** di una campagna, è essenziale controllare l’esistenza reale dell’ente benefico, cercare notizie sulla vicenda sui media tradizionali, e consultare i siti ufficiali delle ONG per confermare eventuali partnership. La consultazione del sito della Polizia Postale (commissariatodips.it) può rivelare se una specifica campagna è già stata segnalata come truffa.

Proteggere le foto dei bambini online

La **prevenzione** rappresenta l’arma più efficace contro il digital kidnapping. Le impostazioni privacy sui social media

devono essere **configurate rigorosamente**. Su TikTok, gli account devono essere obbligatoriamente privati per minori tra 13-15 anni, con la funzione “Collegamento familiare” che permette di impostare limiti di tempo e attivare la modalità limitata per filtrare contenuti inappropriati.

Per **Instagram e Facebook**, è essenziale impostare account privati, attivare filtri automatici per commenti, limitare i messaggi diretti ai soli amici e richiedere approvazione manuale per tutti i tag. **Mai pubblicare foto** con bambini nudi o in situazioni intime, e utilizzare sempre emoji o effetti blur per nascondere i volti quando necessario.

I **genitori devono evitare** di condividere informazioni identificative come nome, età, scuola e abitazione. Il **consenso di entrambi i genitori** è obbligatorio per legge per pubblicare foto di minori, mentre l’età del consenso digitale in Italia è fissata a 14 anni secondo il GDPR.

Strumenti tecnologici avanzati per la protezione

Il **watermarking digitale** rappresenta una protezione fondamentale. Le filigrane visibili con nome o logo sovrapposti all’immagine, posizionate strategicamente al centro per massima protezione, rendono le foto inutilizzabili per scopi fraudolenti. Strumenti gratuiti come Canva, GIMP e Photoshop permettono di applicare facilmente questi sistemi di protezione.

Tecnologie più avanzate includono **Glaze** (filigrana invisibile anti-AI sviluppata dall’Università di Chicago), **Nightshade** (che altera pixel contro training AI), e **Kudurru** (blocca scraper automatici). La **ricerca inversa** attraverso Google Images e TinEye permette di monitorare la diffusione delle immagini online e identificare usi non autorizzati.

Il **controllo parentale** deve essere implementato attraverso software specializzati come Kids Place, Family Link di Google e Screen Time di Apple. Filtri a livello di router possono bloccare siti inappropriati per tutta la rete domestica, mentre antivirus famiglia offrono protezione integrata per tutti i dispositivi.

Aspetti legali e conseguenze penali per il digital kidnapping

Il **quadro normativo italiano** prevede severe sanzioni per chi commette questi reati. L'**articolo 494 del Codice Penale** punisce la sostituzione di persona, mentre l'**articolo 640** disciplina la truffa con reclusione da 6 mesi a 3 anni. Il **D.Lgs. 196/2003** stabilisce il reato di trattamento illecito di dati personali per la pubblicazione non autorizzata di foto di bambini.

Le **sanzioni** prevedono reclusione da 6 mesi a 3 anni per il furto di foto di minori, con obbligo di risarcimento danni e multa da 51 a 1.032 euro. Per le truffe solidali false, la pena può arrivare fino a 5 anni di reclusione e multa fino a 1.549 euro, mentre la frode informatica è punita con reclusione da 2 a 6 anni.

Il **Garante Privacy** può comminare sanzioni fino a 20 milioni di euro o il 4% del fatturato annuo secondo il GDPR. La **Cassazione Penale** ha stabilito precedenti importanti, confermando che creare profili social con foto altrui integra il reato di sostituzione di persona.

Segnalazione e denuncia digital kidnapping immediata

La **segnalazione tempestiva** è cruciale per limitare i danni. Il **Commissariato di P.S. Online** (commissariatodips.it) offre un

servizio specifico per segnalazioni di reati informatici, mentre l'**app YouPol** permette segnalazioni immediate con foto e video. La documentazione necessaria include screenshot dei contenuti illeciti, codici identificativi dei profili social e cronistoria dettagliata dei fatti.

Telefono Azzurro (19696) offre supporto per situazioni di emergenza, mentre il **Garante Privacy** interviene per violazioni specifiche della privacy dei minori. Le **Procure specializzate** in criminalità informatica e i **Tribunali per i Minorenni** gestiscono i casi più complessi che coinvolgono minori.

I **diritti delle vittime** includono il risarcimento danni, la rappresentanza legale attraverso genitori o tutori, e l'assistenza legale gratuita per famiglie prive di mezzi economici. I bambini hanno diritto specifico alla riservatezza, alla protezione dell'immagine e al diritto all'oblio per la cancellazione dei contenuti.

Conclusioni: educare per proteggere

Il **digital kidnapping** rappresenta una minaccia crescente che richiede consapevolezza, prevenzione e azione coordinata. La combinazione di educazione digitale, strumenti tecnologici avanzati e applicazione rigorosa delle normative esistenti può proteggere efficacemente i bambini da queste forme di sfruttamento.

I **genitori** devono essere i primi responsabili della protezione digitale dei propri figli, mantenendo equilibrio tra libertà e sicurezza. L'educazione all'uso consapevole della tecnologia, unita a impostazioni privacy appropriate e controllo parentale attivo, rappresenta la migliore difesa contro i criminali informatici.

La **cooperazione internazionale** tra autorità, piattaforme tecnologiche e organizzazioni per la protezione dei minori è essenziale per combattere efficacemente questo fenomeno

globale. Solo attraverso un approccio multidisciplinare che combina prevenzione, educazione e repressione potremo proteggere i nostri bambini nell’era digitale.

Fonti:

Polizia Postale – Commissariato di P.S. Online.

Polizia di Stato – Rapporto C3 Combating Cyber Crime 2024.

Garante Privacy – Sharenting e protezione minori.

Ministero delle Imprese e del Made in Italy – 9 consigli per difendersi dalle truffe.

University of California San Francisco – Studio TikTok e Minori 2025. *Ricerca su utilizzo social media da parte di minori sotto i 13 anni.*

UNICEF Italia – Tutto sullo Sharenting.

UNICEF – Online Privacy Checklist for Parents. *Lista di controllo per la privacy online dei minori.*

ParentMap – Digital Kidnapping: What It Is and How to Keep Your Kids Safe.

Crown Prosecution Service UK – Fraud gang jailed after stealing charity donations.

U.S. Department of Justice – Charity Founders Sentenced to Prison.

Studio Legale Calvello – Garante Privacy: stop alle foto di minori sui social.

Brocardi.it – Art. 640 Codice Penale – Truffa.

Legal for Digital – Creare profili fake sui social: quando è reato.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/digital-kidnapping/