INFO PSC

4 | 2016

Tema
Cybercriminalità

Gentili lettrici, stimati lettori,


PSC

L'energia dedicata a derubare le persone in Internet, a mentire loro, a fare credere loro di essere corrisposte in amore oppure a esprimere nei loro confronti discorsi intrisi d'odio sembra essere infinita.

Dopo aver intervistato Stéphane Koch, ho acquisito per la prima volta la consapevolezza che la formazione è la chiave per prevenire con successo la criminalità in Internet. Possedere competenze mediali può aiutare a proteggersi adeguatamente, a non credere a tutto quello che si vede o si legge e a capire come funzionano sistemi quali Internet o i media sociali. Il livello di conoscenza degli/delle internauti/e in quest'ambito dovrebbe quindi essere nettamente migliorato.

La polizia della città di Zurigo ha invece consolidato il dialogo istaurato con la popolazione. La polizia utilizza sistematicamente i canali dei media sociali per rendere pubblico il lavoro svolto nell'interesse dei cittadini. Da un po' di tempo, la popolazione, può seguire sulle media sociali i due iCoPs Jean Patrick e Eleni Moschos durante il loro lavoro di poliziotto. Tutti e due sono attivamente in contatto con gli adolescenti e i giovani adulti. In tal modo contribuiscono a soddisfare la richiesta della popolazione di maggior trasparenza, rafforzando nel contempo la fiducia nelle istituzioni.

Cogliamo l'occasione per augurarvi un felice Anno Nuovo!

Martin Boess
Direttore PSC

Situazione attuale e tendenze della cybercriminalità

Intervista a Stéphane Koch

Signor Koch,
Sul suo sito www.intelligentzia.ch, lei riassume così i servizi che offre: «Consulenza e formazione in intelligenza economica e gestione strategica dell'informazione; strategie digitali e reti sociali; sicurezza dell'informazione». Anche la sua formazione è impressionante e, sotto gli aspetti più diversi, interamente dedicata ai media digitali. Per noi, lei è quindi l'interlocutore ideale per un'intervista sul tema «Criminalità su e via Internet» da presentare ai nostri lettori, che pone naturalmente l'accento sulle misure per prevenire la criminalità e sul perseguimento penale.
Ma iniziamo con una domanda generale per introdurre l'argomento:

Qual è la differenza fra la criminalità cosiddetta «normale» e la cybercriminalità? E in che modo il Web ha modificato la criminalità?
La differenza si situa principalmente al livello della dematerializzazione della nostra società. Globalmente, la cybercriminalità rappresenta pertanto una continuità o un adattamento delle forme di criminalità già presenti nel mondo reale. Molti atti criminali compiuti ricorrendo alle TIC (tecnologie dell'informazione e della comunicazione), rispettivamente a Internet, hanno una base ancorata nel mondo reale (che sia a livello d'impiego di un server, di un computer o di una periferica mobile), e sono quindi correlati ad un potenziale «foro» (tribunale al quale è assoggettata l'ubicazione di un server / di un computer nel mondo reale).

Le principali differenze risiedono quindi nell'asimmetria fra i pochi mezzi necessari a compiere un'azione cybercriminale e l'importante impatto che essa può avere a livello sia finanziario, sia del numero di persone o aziende che possono essere colpite da un'azione unica. Un'altra forma di asimmetria si situa a livello della lotta contro le azioni cybercriminali, anche se l'organizzazione e la propagazione di tali azioni (come truffe online, cyberattacchi, cyberestorsioni, ecc.) richiedono pochi mezzi ai cybercriminali. Il lavoro che invece le autorità coinvolte dovranno intraprendere per combattere queste forme di cybercriminalità esigerà notevoli risorse sia a livello umano e tecnico, sia in termini di tempo. Inoltre, il tutto è anche estremamente impegnativo per la giustizia. I luoghi reali in cui si organizza e si compie un'azione cybercriminale e i luoghi in cui si trovano le vittime di quest'azione non sono per forza gli stessi e possono essere suddivisi in varie zone geografiche del mondo con cui non si saranno necessariamente conclusi accordi di assistenza giudiziaria. Un altro importante cambiamento è il seguente: oggi i cybercriminali possono colpire le loro potenziali vittime in casa loro, senza però dover scassinare la serratura della loro abitazione. E lo


m.a.d.

Stéphane Koch, consulente e formatore in comunicazione e strategia digitale, specialista della sicurezza dell'informazione, specialista di reputazione digitale e di reti sociali.

ascyther5/123RF

«La cybercriminalità rappresenta una continuità o un adattamento delle forme di criminalità già presenti nel mondo reale.»

stesso vale per le aziende. Il cybercriminale dista solo un «clic di mouse» dalla sua vittima.

E nel caso delle truffe online, i danni causati possono facilmente superare il valore dei beni che si trovavano fisicamente presso un determinato domicilio. Nel caso di sextorsion, per esempio, la vittima potrebbe subire un trauma psicologico identico a quello di un'aggressione fisica, senza tuttavia essere stata aggredita fisicamente. Paradossalmente e in contrasto con le scienze forensi classiche – ambito in cui l'evoluzione delle tecnologie ha semplificato l'investigazione (ricerca di impronte, utilizzo del DNA, ricostruzione 3 D delle scene del crimine, per esempio) – l'evoluzione del settore delle TIC ha inoltre reso ancora più complessa l'investigazione digitale.

I cybercriminali esperti sono perfettamente in grado di modificare, alterare e addirittura cancellare indizi digitali. Se poi si tiene conto del fatto che ogni computer coinvolto in un'attività cybercriminale può rappresentare una scena del crimine in quanto tale, e che un certo numero di computer «colpiti da questi attacchi» appartengono a persone private innocenti (dato che i loro computer mal protetti o infettati sono stati utilizzati a loro insaputa), ci si rende allora conto dell'estrema complessità dell'investigazione digitale. Per rispondere alla sua domanda posso quindi affermare che sì, il Web ha fondamentalmente modificato la criminalità, anche perché le persone non sono state formate per individuare l'equivalente «informatico» delle forme di criminalità classica, mentre «l'intervento» della polizia è invece diventato molto più complicato.

Secondo lei, quali sono i principali settori in cui si compiono reati in Internet? O detto altrimenti, quali sono i reati basati su Internet che causano i maggiori danni nel nostro Paese?

Non è facile rispondere poiché non tutti i reati sono segnalati né da parte delle persone private, né da parte delle aziende. Talvolta si esita a segnalare che si è stati vittima di una truffa online, di un ricatto o di un furto di dati. Attualmente, però, i tentativi di *phishing,* che mirano ad immettere un *ransomware* (virus informatico che blocca i documenti contenuti nel PC infettato e chiede un riscatto) nei computer di persone private e aziende, sembrano occupare il primo posto sul podio (il 90% degli attacchi tramite *phishing* contiene un *ransomware).* Europol ha d'altronde annunciato che questi software ricattatori sono considerati una minaccia prioritaria a livello europeo. Le «truffe del direttore aziendale» occupano anch'esse un posto importante per l'ammontare dei fondi sottratti. Altri generi di truffe, anch'esse

wk1003mike/Shutterstock.com

«Il 90% degli attacchi tramite phishing contiene un ransomware.»

basate sull'usurpazione d'identità e sull'ingegneria sociale, sono presenti in grandi quantità sulle reti sociali. A proposito di usurpazione di identità: dato che questo delitto non è considerato un reato penale, l'attuale situazione legislativa facilita il lavoro dei cybercriminali.

Vi sono reati che colpiscono in particolar modo la Svizzera? E se sì, per quale motivo?

La Svizzera è considerata un paese ricco, con cittadini che hanno un buon tenore di vita. Globalmente, quindi, la Svizzera è più presa di mira rispetto ad altri paesi: attacchi alle infrastrutture critiche, attacchi DDOS (distributed denial of service, ossia letteralmente negazione del servizio) che, anche quando sono compiuti dall'estero, colpiscono le aziende e gli utenti in Svizzera, data la ripartizione mondiale delle infrastrutture Internet e la loro interdipendenza a livello di connettività.

A seconda della sua importanza, questo tipo di attacco (DDOS) è in grado di rallentare e addirittura di bloccare l'accesso a innumerevoli servizi che dipendono dall'accesso a Internet, a livello sia locale, sia globale. In marzo 2016, dei siti svizzeri di banche e società di commercio online sono stati vittima di un gruppo di cybercriminali denominatio *Armada* che è riuscito a bloccare l'accesso ai servizi delle aziende attaccate in seguito al loro rifiuto di pagare il riscatto chiesto dai cybercriminali. In settembre 2016, «Internet» è stato vittima del più importante attacco DDOS osservato a tutt'oggi (Mirai botnet). La sua particolarità risiedeva nel fatto che, per condurre a buon fine la loro offensiva, i cybercriminali hanno sfruttato circa 400 000 telecamere collegate in tutto il mondo, i cui «accessi amministratori» per difetto non erano stati modificati dai loro proprietari. Un simile attacco, i cui effetti si sono avvertiti pure in Svizzera, ha avuto luogo il mese seguente.

Ma si tratta solo di un esempio, al quale si possono aggiungere gli attacchi per tentativo di *phishing,* il blocco dell'accesso a file digitali – di persone private e di aziende – tramite *ransomware* che bloccano l'accesso ai file fino a quando non viene pagato il riscatto, i furti di dati aziendali (bancari o altri), ecc. Ciò che differenzia un paese dall'altro, sono i mezzi che il paese metterà in atto per combattere la cybercriminalità o altre forme di attacchi lanciati tramite reti connesse, così come il livello di «consapevolezza» dei suoi cittadini e delle aziende. E in questo ambito, la Svizzera è rimasta indietro!

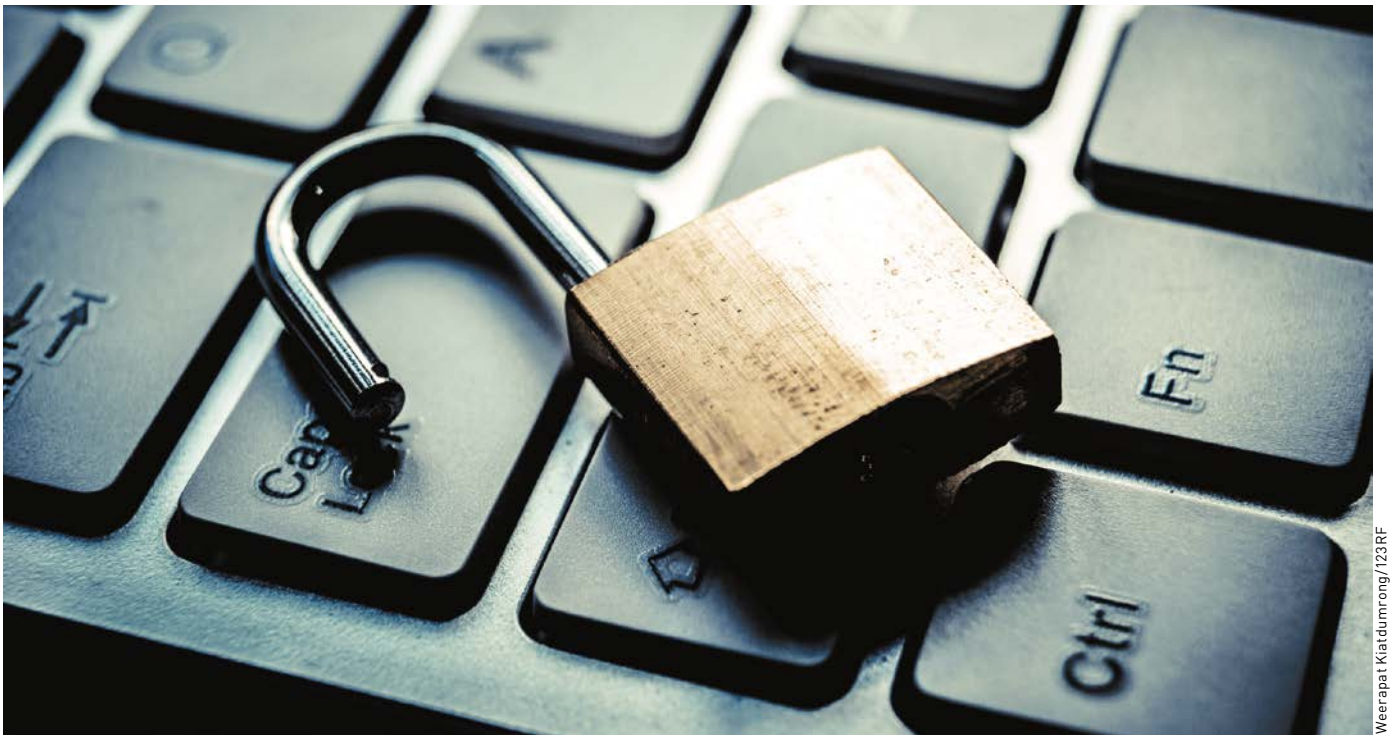
Vi sono notevoli mancanze in relazione con i mezzi di lotta alla cybercriminalità, e il livello di conoscenza e di reattività di aziende e persone private è nettamente insufficiente. Per quanto riguarda i mezzi, si tratta di un problema politico. Oggi che tutti sono interconnessi e che si dà poco peso alle frontiere fisiche culturali e linguistiche, la Svizzera è vittima del proprio federalismo. Solo la Zurigo ha una propria cybersquadra contro il cybercrimine (gli altri cantoni hanno, nella maggior parte dei casi, un'unità anticrimine informatico che fornisce il proprio supporto agli altri servizi di polizia), mentre la maggioranza dei magistrati non ha una formazione specifica nelle TIC, e così gli incarti si ammassano. Per quanto riguarda le aziende e le persone private, la mancanza di consapevolezza e di conoscenze fa sì che la Svizzera rappresenti – logicamente – un terreno privilegiato per i cybercriminali.

Il 22° rapporto semestrale di MELANI (Centrale d'annuncio e d'analisi per la sicurezza dell'informazione) incentrato principalmente sul tema *«La gestione delle lacune di sicurezza»,* ha ben illustrato questa situazione. Guillaume Poupard, direttore generale dell'Agenzia nazionale francese della sicurezza dei sistemi informatici (Anssi), ha recentemente affermato: *«Nelle aziende c'è ovviamente un responsabile della sicurezza dei sistemi informatici. Questa persona è indispensabile, ma da sola non basta. L'idea è veramente di dirsi che ognuno è responsabile della cybersicurezza: il direttore generale, il direttore del servizio giuridico, il direttore del dipartimento delle finanze. Ognuno ha un ruolo da svolgere, e questo vale anche per le persone che assolvono un lavoro interinale, generalmente dimenticate nelle procedure, perché in realtà hanno spesso accesso ai sistemi.».* Questa situazione, che indebolisce l'economia del paese, la sua competitività e quindi la sua crescita, non cambierà finché le mentalità non evolveranno. Oggi, i programmi d'insegnamento nelle scuole elementari, nelle scuole medie inferiori e superiori o nelle scuole universitarie non prevedono quasi nulla che possa permettere ad ognuno di integrare le conoscenze necessarie a capire, assimilare e controllare la trasformazione digitale della nostra società (l'insieme di queste conoscenze è riunita sotto la denominazione «alfabetizzazione digitale» e l'Europa ha messo in piedi un programma di formazione in cultura digitale chiamato «DLit2.0 Curriculum»).

www.digital-literacy2020.eu/content/sections/index.cfm/secid.59

Approfondiamo ulteriormente la questione. In Svizzera esistono categorie specifiche di vittime? Vi sono persone, gruppi o istituzioni particolarmente minacciate dalla cybercriminalità?

Il comportamento dei cybercriminali è assai logico: cercano di ottimizzare il rendimento delle loro azioni criminali e quindi attaccheranno l'elemento più debole. In termini di cybercriminalità, questo significa che gli attacchi colpiranno in primo luogo i computer o altri strumenti informatici o periferiche meno protetti. Per riformulare la domanda, si potrebbe affermare che è il potenziale di profitto a definire il bersaglio. Le aziende saranno dunque un bersaglio importante, ma l'accumulo di piccoli guadagni, grazie alla moltiplicazione degli attacchi contro le persone private, genera molti ricavi e rappresentano nel contempo un rischio minimo per i cybercriminali, in quanto ogni singolo computer colpito costituisce un nuovo caso per la polizia e la giustizia. È tuttavia importante capire che la maggioranza delle truffe richiede, volenti o nolenti, un intervento o una «collaborazione» della vittima. Perciò il fattore di successo di molte di queste truffe online poggia proprio sulla mancanza di conoscenze o sull'incoscienza dell'utente. Occorre inoltre tener presente che alcuni governi (o gruppi sostenuti dai governi) hanno talvolta comportamenti cybercriminali e che pertanto le istituzioni o certi poli strategici possono rappresentare dei bersagli particolarmente interessanti. Il recente attacco alla società RUAG è un esempio emblematico: gli hacker hanno utilizzato un *malware* (software spia) per infiltrarsi nei server di RUAG e saccheggiare il suo



Weerapat Kiatdumrong/123RF

«I cybercriminali cercano di ottimizzare il rendimento delle loro azioni criminali e quindi attaccheranno l'elemento più debole.»

neydt/123RF

«Gli Hacktivist sono una specie di Black Bloc digitali, come il movimento Anonymous, con rivendicazioni di carattere sociale o politico.»

patrimonio intellettuale e industriale. Gli istigatori di questo cyberattacco – che a tutt'oggi non sono stati formalmente identificati – hanno potuto agire diversi mesi prima che si riuscisse ad individuare la loro presenza.

Sa chi sono i criminali? In materia di «criminalità offline», esistono gruppi di criminali specializzati e moventi ben definiti. Si può osservare la stessa cosa a livello di cybercriminalità? E se sì, sotto che forme?

Non è evidente fare un «quadro esaustivo della cybercriminalità», poiché si tratta di un settore polimorfo, caratterizzato da tante sfumature di grigio. Per esempio non vi sono gli «hacker» da una parte e il resto del mondo dall'altra. È invece presente un insieme di «correnti» che è importante definire e categorizzare: vi sono i **«Black Hat»** (comportamento criminale); i **«White Hat»** (comportamento etico, hacker etici, utili alla società che mettono in evidenza le falle di sicurezza); i **«Grey Hat»** (svolgono un po' i due ruoli); gli **«State sponsored hacker»** (comportamenti criminali. Ufficiosamente sono sostenuti da uno stato oppure si tratta di nazionalisti, di fatto sostenuti dal loro paese, che compiono azioni offensive); gli **«Hacktivist»** (specie di Black Bloc digitali, come il movimento **Anonymous,** con rivendicazioni di carattere sociale o politico. In origine non si tratta di criminali, ma la natura del loro comportamento può esserlo), i **«Cybercriminali»** (estensione e sviluppo delle attività criminali classiche nel mondo digitale); gli **«Script kiddie»** (in generale, adolescenti o persone che utilizzano programmi informatici creati da altri con un potenziale d'attacco, poiché essi non possiedono il know-how necessario per svilupparli); i **«Cybermercenari»** (persone che vendono le loro conoscenze informatiche. Il caso «Giroud» è un esempio emblematico. Nel 2014, questo produttore di vini vallesano è stato accusato di aver assunto un cybermercenario che andasse a rubare nei computer di due giornalisti dei documenti che lo incriminavano).

In sintesi, tutta questa bella gente rappresenta allo stesso tempo la diversità e la complessità degli attori che popolano la scena digitale. Questa complessità è ancor più accentuata dal fatto che oggi i cybercriminali si comportano come imprenditori, e certi imprenditori (o governi) si comportano talvolta come cybercriminali. Si osserva pure la presenza di «cybercriminali a tempo parziale», che agiscono sporadicamente di nascosto, mentre alla luce del sole risultano essere impiegati da aziende, poiché considerano che la presa di rischio è minima rispetto ai potenziali guadagni (teoria delle opportunità criminali, Walsh, 1986). Vi sono anche quelli che cercano le falle di sicurezza per rivenderle – fra l'altro – sul *Darknet* (la rete scura della cybercriminalità). Non saranno loro in prima persona a commettere i reati, ma forniranno a cybercriminali (e altri) «le armi e le munizioni», rispettivamente le risorse necessarie a compiere questi crimini. Si tratta di un mercato molto lucrativo e poco rischioso. Certe falle di sicurezza possono essere rivendute per diverse centinaia di migliaia di franchi. A tale titolo, il mercato grigio

delle falle di sicurezza rifornisce non solo i cybercriminali, ma anche aziende, governi e i loro servizi segreti. Alcuni governi hanno stanziato un budget specificatamente dedicato all'acquisto di questo genere di risorse (falle di sicurezza, oppure vulnerabilità sconosciute dei creatori di software per i quali non esistono rimedi o correttivi, e che per loro natura permettono quindi di accedere a programmi o computer, aggirando le misure di sicurezza presenti. Questo genere di falla è anche chiamata vulnerabilità 0-Day.

Nel 2012, il Dr. Michael McGuire, del *John Grieve Centre,* ha tentato di fare un quadro della potenziale relazione fra il crimine organizzato e la cybercriminalità in uno studio intitolato: «Organised Crime in the Digital Age» (Il crimine organizzato nell'era digitale). Secondo questo studio, l'80% dei gruppi di cybercriminali si baserebbe su una forma di struttura organizzata, senza necessariamente appartenere tutti ad un'organizzazione criminale classica. Il 43% dei membri di queste organizzazioni cybercriminali ha più di 35 anni e il 29% meno di 25 anni. La metà dei gruppi è costituita da una struttura di 6 o più persone, e un quarto di essi si compone di 11 o più persone. Il 25% dei gruppi attivi ha agito per meno di sei mesi.

www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf

Lei ha pure una formazione in lotta alla criminalità economica. Può parlarci della lotta alla criminalità economica in Internet? Quali sono i suoi punti forti o quali dovrebbero esserlo? Di quali mezzi si dispone per i perseguimenti penali? E quali mezzi mancano?

Con l'impennata dell'uso delle TIC, la crescente dematerializzazione dei servizi e l'emergere dell'Internet degli oggetti (sempre più connessioni e scambi di dati fra le periferiche collegate ad elementi della nostra vita quotidiana, dove il frigo collegato non pone troppi problemi, ma una pompa ad insulina, un pacemaker, un'auto, o ancora la serratura di un appartamento possono invece risultare problematici), si assiste ad un importante aumento dei casi di criminalità economica in relazione con il settore digitale. Il problema è che – come spiegato nella risposta alla 3ª domanda – la polizia e la giustizia non riescono ad ottenere le risorse che servirebbero loro per essere in grado di trattare la moltitudine di casi che si presentano. E i casi che avvengono in Svizzera non si limitano alle frontiere nazionali, ma necessitano nella maggior parte dei casi di una collaborazione a livello europeo e mondiale. Questa collaborazione è spesso soggetta a domande di assistenza giudiziaria che richiederanno tempo, latenza che torna molto utile ai cybercriminali. Anche se esiste la Convenzione del Consiglio d'Europa sulla criminalità informatica, entrata in vigore in Svizzera nel 2012, non tutti i paesi l'hanno sottoscritta, ed i cybercriminali sfruttano logicamente questo genere di falla. Incaricano inoltre degli specialisti del settore legale per valutare quali saranno – legalmente – le migliori retrovie per sferrare i loro attacchi.

Ad un avvocato specializzato nella protezione dei dati delle strategie nel settore della cybercriminalità, che raccomandazioni farebbe in materia di azioni di perseguimento penale in Svizzera?

È necessario che vi sia una vera e propria riflessione a livello penale, e non deve essere unicamente opera di giuristi e di «esponenti politici». Nel settore delle TIC, il sistema di milizia ha raggiunto i propri limiti. Occorre che i professionisti – del settore pubblico e privato – combattono la cybercriminalità nell'ambito del loro lavoro e possano esporre i problemi ai quali sono confrontati. Le conoscenze lacunose degli esponenti politici in materia di società dell'informazione (anche nelle commissioni specializzate) hanno un impatto estremamente negativo sulla loro capacità di capire i problemi legati alla lotta alla cybercriminalità. Per esempio, all'inizio del 2013, François Charlet, avvocato ginevrino specializzato nella protezione dei dati, ed io siamo stati invitati da un partito politico per condividere alcune riflessioni sulle problematiche legate alle TIC. In seguito a questo incontro è emerso che la penalizzazione dell'usurpazione d'identità risultava essere un tema prioritario. Nel 2016, l'unica cosa ad essere aumentata è il numero delle vittime! Lo stesso succede con le fughe di dati: il Parlamento europeo ha adottato la direttiva NIS «Directive on security of

rangizzz/123RF

«Polizia e giustizia hanno per lo più bisogno di poter contare su una collaborazione a livello europeo e mondiale. Questa collaborazione è però spesso soggetta a domande di assistenza giudiziaria che richiederanno tempo, latenza che torna molto utile ai cybercriminali.»

network and information systems» (Direttiva sulla sicurezza delle reti e dell'informazione) che entrerà in vigore nel 2018.

www.riskinsight-wavestone.com/2016/03/8822/

Questa direttiva contiene un obbligo di dichiarazione alle autorità competenti in caso di pirataggio di infrastrutture considerate critiche, di intrusione nei sistemi informatici, come pure l'obbligo, per le aziende vittime di fughe di dati, di segnalare il loro caso alle competenti autorità nazionali e alle persone colpite entro tre giorni. Questa direttiva impone anche agli attori coinvolti di adottare le misure necessarie per garantire una sicurezza efficace delle loro infrastrutture. La Svizzera – che alcuni presentano come la futura cassaforte digitale del mondo – ha il dovere di applicare il più rapidamente possibile direttive analoghe.

Per quanto riguarda le persone private, anche in questo caso la giustizia è rimasta indietro e numerosi magistrati sembrano essere disconnessi dalle realtà della nostra società... connessa. Ho trattato casi di «sextorsion» e di «Revenge Porn» (pratica che consiste nel diffondere foto intime, a sfondo sessuale, del/della proprio/a coniuge senza il suo consenso) e, nel caso del *Revenge Porn,* la vittima – a seconda dell'età – potrebbe essere potenzialmente considerata, ai sensi del codice penale svizzero, colpevole di creazione e diffusione di contenuti a carattere pornografico. Oltre a non riconoscere alla vittima lo statuto di vittima, neppure l'aggressore rischia un gran ché. Nel Canton Vaud, nel 2013, un uomo riconosciuto colpevole della diffusione di video intimi della sua ex-compagna su un sito pornografico è stato solamente condannato a pagare 50 aliquote giornaliere con sospensione della pena (le donne rappresentano oltre l'80% delle vittime). Lo stesso succede quando una donna è vittima di una violenza carnale: se gli aggressori filmano la scena e la condividono in un gruppo WhatsApp o su Internet – com'è già successo – essi saranno eventualmente condannati per violenza carnale, ma il giudice non terrà conto del fatto che il reato commesso è stato anche filmato e condiviso. Invece, il fatto di filmare una violenza carnale con l'intenzione di condividere il video girato dovrebbe essere considerato, a livello penale, come un atto di crudeltà! La sentenza dovrebbe pure contemplare la possibilità di obbligare per legge a togliere da Internet i contenuti incriminati, sotto pena di un'ulteriore sanzione se ciò non dovesse essere fatto. Riassumendo, per far evolvere la legge, devono evolvere anche le mentalità. È necessario che le autorità toccate da queste problematiche sviluppino un senso di consapevolezza per il vissuto della vittima e i suoi potenziali traumi a seguito di un'aggressione online e per lo stress post-traumatico dovuto al rischio di ricomparsa dei contenuti umilianti per la vittima. Questa evoluzione di mentalità è pure necessaria affinché i magistrati capiscano meglio gli obblighi legati al lavoro d'inchiesta della polizia in relazione con Internet. Per esempio, «l'indagine sotto copertura» che autorizza l'uso di un'identità fittizia, la cui regolamentazione è stata armonizzata a livello federale ed è entrata in vigore nel 2005, dev'essere più facile da realizzare.

In che modo evolverà la criminalità in Internet? Possiamo aspettarci nuovi generi di reati?

Per Michael McGuire, dottore in criminologia, la cybercriminalità corrisponde alla 4ª era della criminalità. Per quanto mi riguarda, potrei riassumere la questione così: più crimini e meno mezzi per combatterli. Non bisogna tuttavia accettare l'aumento della cybercriminalità come una fatalità. Occorre invece dotarsi dei mezzi per combatterla. E ancor più dei mezzi finanziari, legali e polizieschi, la «conoscenza» è e sarà sempre lo strumento più importate per contrastare queste forme di criminalità. In fin dei conti, i cybercriminali utilizzano le stesse nostre tecnologie. La maggioranza dei cyberattacchi e delle truffe online riesce proprio a causa dell'ignoranza degli internauti. Prendiamo per esempio il *phishing:* è quasi un quarto di secolo che il Web esiste e non è ancora stato insegnato agli utenti a leggere correttamente un link in Internet (URL), la cui manipolazione è l'elemento di base sui cui poggia la truffa.

Quale ruolo svolge il Darknet nella cybercriminalità? La polizia ha una possibilità di individuare i crimini nel Darknet oppure occorrerebbe modificare la legislazione?

La problematica rappresentata dal cosiddetto *Darknet* non è unicamente una questione di legislazione. Gli strumenti che permettono di mantenere l'anonimato e che sono generalmente associati al *Darknet* sono gli stessi strumenti che utilizzano i difensori dei diritti umani o i giornalisti in paesi non democratici per riferire di casi di violazione delle libertà individuali o per denunciare comportamenti scorretti di certi governi o casi di corruzione. Riassumendo, questi strumenti salvano anche delle vite.

Motivo per cui la soluzione non è indebolire le tecnologie (per esempio con la cifratura), bensì è migliorare il livello di know-how, la collaborazione e lo scambio di informazioni fra i vari servizi di polizia e giustizia, a livello sia nazionale che internazionale. Inoltre, i fatti ci hanno dimostrato che il *Darknet* non è un universo impenetrabile: nel 2013, l'FBI è riuscita a chiudere «Silk Road», una delle più grandi piazze di commercio illegale del *Darknet.* Poi è riuscito ad infiltrarsi – sin dall'inizio del suo lancio – nel Silk Road 2.0 per poi chiuderlo nel 2014. Oggi esiste ancora una nuova versione del sito che registra un fiorente sviluppo soprattutto nel settore della vendita di droghe. Mi chiederete: qual è la differenza con il mondo reale, dato che neppure qui si è riusciti a sradicare la vendita di droga? Ciò che in realtà voglio dire è che con i mezzi e il livello di know-how adeguati, la polizia è in grado di lottare su tutti i «fronti tecnologici».

scanrail/123RF

«Con i mezzi e il livello di know-how adeguati, la polizia è in grado di lottare su tutti i fronti tecnologici.»

Quali sono i principali consigli per proteggersi dalla cybercriminalità?

A costo di ripetermi: l'utente – che si tratti di una persona privata o di una persona giuridica – deve fondamentalmente migliorare il proprio livello di conoscenza. Nulla si potrà fare, se ciò non avviene. Ed è lo Stato a dover mettere a disposizione di cittadini e aziende i mezzi per poter migliorare queste conoscenze, per esempio attraverso l'istruzione pubblica, nelle aziende e, perché no, in seno all'esercito (si potrebbe immaginare di impartire una formazione in tal senso durante la scuola reclute). In Francia, per esempio, l'Institut national des hautes études de la sécurité et de la justice (INHESJ), ossia il Centro di alti studi per la sicurezza e la giustizia, e la Délégation interministérielle à l'intelligence économique (D2IE), ossia la Delegazione interministeriale all'intelligence economica, si sono impegnate in tal senso costituendo un partenariato il cui scopo è di formare dei «relatori in sicurezza economica» provenienti dal settore economico: aziende, poli, gruppi di società, consulenti, ecc. L'obiettivo è di lanciare un messaggio generale, standardizzato e coerente sulla sicurezza economica e di promuovere gli strumenti esistenti o che saranno creati. Rientra pure nella responsabilità dello Stato individuare le minacce che le aziende e i cittadini non sono in grado di identificare. Occorre mettere in piedi strutture governative che utilizzano le risorse disponibili nel settore privato per ricercare in modo proattivo le future minacce (falle o vulnerabilità 0-day) e valutare il materiale utilizzato nelle infrastrutture strategiche del paese *(hardware, software, firmware).* Il futuro della sicurezza economica della Svizzera, la sua capacità d'innovarsi e crescere, è a questo prezzo. A livello legale, le aziende che non proteggono sufficientemente i loro dati devono essere penalizzate.

Per quanto riguarda l'utente, quest'ultimo ha la responsabilità di capire gli strumenti che utilizza. Il rifiuto di assumersi le proprie responsabilità per le tecnologiche che si utilizzano quotidianamente non è più accettabile. Nella nostra società reale, generalmente le persone accettano la responsabilità di informarsi sui medicinali che vengono loro prescritti, sulla composizione dei cibi che consumano, così come sulle modalità di utilizzazione e sul funzionamento del veicolo che si apprestano a guidare. Anche se sono recalcitranti, accettano tuttavia di adattarsi al principio della separazione dei rifiuti e alle «nuove regole» legate all'evoluzione e ai cambiamenti che si verificano nel nostro mondo reale.

Lo stesso deve succedere con le TIC! Esse sono alla base della trasformazione digitale della nostra società, e il mondo numerico rappresenta solo la «realtà» smaterializzata. Invece la società, rimane pur sempre la nostra società, quella in cui viviamo, e non è uno «spazio virtuale» separato da essa, come affermato da Edgard Morin: «In una società complessa, occorre adottare un pensiero complesso.». Mi permetto di riformulare quanto da lui espresso dichiarando: «Prendersi il tempo di imparare a vivere al passo coi tempi per non esistere al di fuori del tempo.».

Chi combatte la criminalità su Internet e chi protegge le strutture digitali in Svizzera?

La strategia del Consiglio federale per una Svizzera digitale e il suo impatto sulla sicurezza della popolazione

Con l'approvazione, in aprile 2016, della strategia «Svizzera digitale», il Consiglio federale intende adoperarsi affinché il nostro Paese sfrutti maggiormente la progressiva digitalizzazione. Per avere una società democratica ed informata, è inoltre fondamentale che i cittadini e le cittadine della Svizzera possano utilizzare le moderne tecnologie dell'informazione e della comunicazione in tutta sicurezza e con la dovuta competenza.

Nell'ambito della strategia, si devono fra l'altro attuare le seguenti misure importanti per la sicurezza:

- avviare la procedura di consultazione per la revisione della legge sulle telecomunicazioni (LTC) che lascia alla Confederazione la possibilità di proteggere i giovani dai pericoli dei servizi di telecomunicazione. In tal modo i fornitori di accessi ad Internet possono essere obbligati a consigliare la loro clientela sulle misure di protezione dei minori e a bloccare i contenuti a carattere pedopornografico (attuazione entro fine 2016);
- chiarire le possibilità di proteggere la sfera privata degli utenti di media digitali, in particolare di bambini e giovani, nell'ambito della revisione della legge sulla protezione dei dati (attuazione entro fine 2016);
- rafforzare la protezione dei giovani dai rischi dei media, in particolare nel caso di contenuti inadatti, con indicazione del limite d'età minimo per videofilm e videogiochi, varando una nuova legge (attuazione entro fine 2017);
- valutare l'evoluzione della sicurezza dei dati e dell'elaborazione dei dati (Big Data), valutare le conseguenze per la società e verificare il quadro legislativo esistente (attuazione entro metà 2018).

Più informazioni al riguardo:
www.bakom.admin.ch → Svizzera digitale e internet → Strategia «Svizzera digitale»

Il Servizio di coordinazione per la lotta contro la criminalità su Internet (SCOCI)

SCOCI è incorporato nella Polizia giudiziaria federale (PGF), una divisione principale dell'Ufficio federale di polizia (fedpol).

SCOCI effettua ricerche in Internet in assenza di sospetti. Dopo l'analisi degli incarti e dei casi aperti, questi sono poi trasmessi – in funzione dell'importanza penale – alle competenti autorità di perseguimento penale in Svizzera e all'estero. Per contenuti in Internet penalmente rilevanti s'intendono in particolare (elenco non esaustivo):

- la pornografia dura (atti sessuali con fanciulli, animali o atti violenti);
- la pornografia legale, quando è liberamente accessibile anche ai minorenni, senza che ne venga verificata l'età;
- la rappresentazione di atti di cruda violenza;
- la discriminazione razziale e l'estremismo;
- i reati contro l'onore e le minacce;
- le truffe e la criminalità economica;
- l'accesso illecito a sistemi informatici;
- la diffusione di virus informatici e il danneggiamento di dati.

Le persone che desiderano segnalare contenuti sospetti in Internet, possono scaricare l'apposito formulario nel sito www.cybercrime.ch.

SCOCI è il centro di competenza a cui possono rivolgersi i/le cittadini/e privati/e, le amministrazioni e i provider di servizi Internet per qualsiasi questione di natura giuridica, tecnica o criminale riguardante la criminalità su Internet. In veste di servizio nazionale di coordinazione per la lotta contro la criminalità su Internet, SCOCI funge anche da interlocutore privilegiato per i servizi omologhi all'estero che svolgono compiti analoghi.

Più informazioni al riguardo:
www.cybercrime.admin.ch

La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI)

MELANI è un modello di cooperazione fra il Dipartimento federale delle finanze (DFF), rappresentato dall'organo di direzione informatica della Confederazione (ODIC), e il Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS), rappresentato dal Servizio delle attività informative della Confederazione (SIC).

MELANI offre i suoi servizi a due cerchie di clienti. La *cerchia aperta di clienti* comprende gli utenti privati di computer e Internet come pure le piccole e medie imprese (PMI) in Svizzera. Per la loro protezione MELANI offre:

- informazioni su pericoli e misure correlati all'impiego delle moderne tecnologie dell'informazione e della comunicazione (per es. Internet, e-banking);

- rapporti che illustrano le principali tendenze ed evoluzioni riguardanti incidenti ed eventi in relazione con le tecnologie dell'informazione e della comunicazione (TIC);
- un modulo di notifica per segnalare incidenti che hanno colpito personalmente gli/le utenti.

La *cerchia chiusa* di clienti comprende gestori selezionati di infrastrutture critiche (per es. fornitori di energia, società di telecomunicazione, banche, ecc.) su tutto il territorio nazionale. In quest'ambito, MELANI ha il compito di proteggere queste infrastrutture, specialmente quando dipendono dal funzionamento delle infrastrutture di informazione e di comunicazione.

Più informazioni al riguardo:
www.melani.admin.ch

Il **Rapporto semestrale 2016/I** (gennaio – giugno) sulla **«Sicurezza delle informazioni»** che presenta la **situazione in Svizzera e a livello internazionale,** pubblicato a fine ottobre, illustra i più importanti incidenti informatici verificatisi a livello nazionale e internazionale nel primo semestre del 2016. Il rapporto si focalizza in particolare sui cyber-attacchi a scopo di estorsione sempre più frequenti.

www.melani.admin.ch → Documentazione → Rapporti → Rapporti di situazione → Rapporto semestrale 2016/1

Delitti frequenti in Internet

Forte della sua pluriennale esperienza in materia di delitti commessi in Internet, la PSC è molto spesso il primo interlocutore a cui si rivolgono i cittadini e le cittadine. La PSC fornisce una prima consulenza e si occupa di selezionare i delitti nel settore dei media digitali. Alle vittime indica per esempio se nel caso specifico è opportuno sporgere denuncia o chi è l'interlocutore più adatto da contattare presso la polizia. Mentre parla con loro, la PSC può inoltre raccogliere preziose informazioni sulle strategie messe in atto dai delinquenti, informazioni che le permettono poi di aggiornare i diversi articoli che scrive sulla prevenzione delle varie forme di reato.

In questo contributo, la PSC descrive quei delitti di cui la popolazione parla maggiormente, vuoi perché le persone che contattano la PSC sono state loro stesse vittime di uno di questi delitti, vuoi perché hanno il sospetto che un/a loro parente o amico/a potrebbe diventare una vittima.

Quando desiderio e amore fanno la fortuna del truffatore

È ormai risaputo che i truffatori in rete imbroglino ricorrendo a tutti i trucchi possibili e utilizzano Internet come specchietto per le allodole. Per far cadere in trappola una vittima, è sufficiente raccontarle tutta una serie di bugie. E se la persona è disposta a crederci, il gioco è fatto. Questa disponibilità a farsi fregare nasce da un bisogno soggettivo: una mancanza di denaro, di prestigio oppure, per l'appunto, anche una carenza affettiva, a livello sia fisico che emotivo.

Le due forme di truffa o ricatto descritte qui di seguito si focalizzano proprio su questi bisogni e prendono quindi di mira le persone alla ricerca di calore umano o desiderio fisico, anche se prese singolarmente, esse presentano profili molto diversi fra loro.

Romance Scam

La bugia dell'amore o la truffa del finto matrimonio

I termini inglesi *«Romance Scam»* o *«Love Scam»* designano una forma di truffa in Internet che prende di mira le persone alla ricerca di un partner. Questa forma di truffa è particolarmente subdola perché non svuota solo i conti, bensì spezza anche i cuori delle vittime. Come funziona esattamente?

Modus operandi

I truffatori e le truffatrici si spacciano, sotto falsa identità, per corteggiatori innamorati e corteggiatrici innamorate in siti di incontri e sui media sociali. Corteggiano la loro vittima facendole complimenti e promesse d'amore, e poi tentano di sottrarre loro denaro con storie commoventi. Ecco un esempio: su una piattaforma di ricerca partner, un certo Bob Tyler[1], che si presenta come un ingegnere canadese di bell'aspetto

1 Nome fittizio

stokkete/123RF

Romance Scam: questa forma di truffa è particolarmente subdola perché non svuota solo i conti, bensì spezza anche i cuori.

e con una buona posizione, entra in contatto con la Signora Daniela Bernasconi[2] residente a L. Dopo breve tempo e vari scambi, il Signor Tyler diventa molto insistente e dichiara alla Signora Bernasconi di aver trovato in lei la donna dei suoi sogni. La Signora Bernasconi non diffida molto di Internet e forse non sa quanto sia facile creare profili completamente falsi. Non immagina neppure che gli indirizzi e-mail e i numeri telefonici indicati non forniscono informazioni sicure sul paese di provenienza del suo interlocutore. La Signora Bernasconi desidera inoltre avere una relazione anche perché è da tanto tempo che non le hanno più detto parole romantiche. Finalmente anche lei ha la fortuna di incontrare il grande amore! I *Love Scammer* sono maestri nell'arte della seduzione, dell'adulazione e del raggiro. Così, più la Signora Bernasconi chatta o telefona con il Signor Tyler, più si convince della sincerità del corteggiamento. Perché altrimenti qualcuno dovrebbe darsi tanta pena? Si dice che l'amore renda ciechi. Tutti noi per certi versi lo sappiamo per averlo vissuto noi stessi. Ma nel caso del *Love Scam* non solo! Qui si aggiunge il fatto che spesso non si conoscano gli specifici meccanismi di inganno e falsificazione in rete, motivo per cui le bugie sono è ancora più difficili da identificare in quanto tali.

Quando il truffatore è sicuro di aver creato una dipendenza emotiva sufficientemente forte nella sua vittima e l'illusione di fissare un vero e proprio appuntamento per incontro personale, inizia a raccontarle i suoi problemi: infortuni, malattie, difficoltà con le autorità o urgenze familiari o di lavoro. Quando per esempio il Signor Tyler annuncia alla Signora Bernasconi il suo arrivo in Svizzera, all'improvviso le fa sapere che ha dovuto deviare su Dubai per motivi di lavoro. Lì potrà concludere con successo un affare solo se gli viene anticipata una certa somma di denaro. Per svariati motivi, il Signor Tyler racconta che purtroppo non può disporre immediatamente di questo importo e chiede alla Signora Bernasconi di essere così gentile da versargli la somma richiesta il più presto possibile, per permettergli finalmente di intraprendere il viaggio in Svizzera per venire a trovarla. Con queste storie, i *Romance Scammer* ottengono con l'inganno centinaia di migliaia di franchi fino a quando la vittima innamorata realizza che l'obiettivo del corteggiamento non era il suo cuore bensì era il suo borsello. Dato che le e-mail, i numeri di telefono ed i profili sono tutti quanti falsi o anonimizzati e che i pagamenti sono stati effettuati tramite servizi di trasferimento di denaro come «Western Union» o «MoneyGram», le operazioni finanziarie non possono essere tracciate e quindi il denaro versato non è più recuperabile. La fiducia delle vittime è stata inoltre completamente tradita e queste persone provano grande vergogna.

Modus operandi «per avanzati»

E come se ciò non bastasse, l'illusione e l'inganno vanno ancora oltre! La vittima che non paga o non vuole più pagare è inondata da false lettere di presunte autorità di polizia e giustizia in cui si asserisce che il truffatore verrà arrestato. Poi la si persuade di nuovo a fare dei versamenti anticipati, facendole credere che un inquirente di Interpol specializzato avrebbe identificato il Signor Tyler e che è per questo motivo che sarebbe a conoscenza del fatto che la Signora Bernasconi è stata una sua vittima. Per poter recuperare il suo denaro, la Signora Bernasconi dovrebbe effettuare questo e altri pagamenti alla dogana o al ministero di giustizia a Dubai. Può così capitare che la vittima sia doppiamente truffata e che invece di ricevere aiuto, si indebiti ancora di più. I truffatori sono creativi, innovativi, perseveranti, pazienti, la sanno lunga sui trucchi da attuare e sono esperti nell'uso dei media digitali. E, come riferito, questa attività criminale può essere molto redditizia.

Misure per prevenire la Romance Scam

Fidarsi è bene ma non fidarsi è meglio! Dato che, nel caso di questa truffa in Internet, non vi è praticamente alcuna possibilità di individuare il truffatore, la prevenzione diventa quindi un fattore importantissimo. Le persone ben informate alla ricerca di un partner riconoscono relativamente bene questo genere di raggiro perché il suo modus operandi è molto standardizzato. Perciò è determinate far conoscere questa forma di truffa. E in ogni caso, il seguente consiglio torna sicuramente utile: non si deve mai versare del denaro a persone che non si conoscono personalmente,

2 Nome fittizio

ossia che non si sono mai incontrate nella vita reale, anche se la storia che viene raccontata è commovente!

Sextortion o ricatto con materiale video e fotografico compromettente

Momenti eccitanti prima del brusco risveglio!

Forse è un cliché, ma si dice che, nel gioco della seduzione, è più facile stuzzicare gli uomini con i piaceri della carne che con parole romantiche. Se in realtà sono spesso le donne (ma non solo!) a diventare vittime di *Love Scam,* nel caso del *Sextortion* sono piuttosto gli uomini ad essere presi di mira. Il significato di «Sextortion», parola composta da «Sex» e «Extortion» che in italiano significa letteralmente estorsione o ricatto sessuale, è ovvio perché è proprio di questo che si tratta! Persone, per lo più uomini, sono abbordati con molta insistenza nei social network (Facebook, WhatsApp, ecc.) da «signore sexy». Dopo un breve scambio in chat, segue ben presto un invito a fare una video-chiacchierata, per esempio su Skype. Lì le cose diventano rapidamente eccitanti e si lasciano cadere le inibizioni. Le signore propongono spettacoli erotici ed invitano il loro interlocutore a partecipare al cybersex. A due, infatti, è molto più divertente! Il passaggio dal divertimento alle cose serie è però molto rapido! Non appena queste signore dispongono di materiale video compromettente, appare ben presto chiaro il vero motivo di questo flirt. Le truffatrici esigono del denaro e minacciano le loro vittime di pubblicare le riprese su Youtube o di inviarle direttamente alla loro lista di amici in Facebook in caso di mancato pagamento.

loganban/123RF

Sextortion: sono piuttosto gli uomini ad essere presi di mira.

Pagare non protegge!

Naturalmente la vergogna è enorme, e le vittime non osano parlare del ricatto con altri. Per paura che famiglia, amici o colleghi di lavoro possano ricevere e vedere del materiale video compromettente, alcuni pagano le somme di denaro richieste che di regola ammontano ad alcune centinaia di euro, dollari o franchi svizzeri.

Anche in questo caso è importante essere bene informati, cosa che non è difficile! Non si deve mai fare sesso virtuale in una videochat con sconosciuti! Tutto ciò che si può scaricate in Internet sulle persone può essere usato in modo indebito. E i video con dettagli intimi rientrano proprio nel materiale che si presta molto bene ad un uso illecito.

Purtroppo, quando si è eccitati, la massima «think before you post» (pensa prima di postare) finisce nel dimenticatoio. Se si ha quindi avuto un momento di debolezza e ci si è illusi che «la signora sexy dal paese della webcam» fosse veramente impazzita per la vittima e non per il suo denaro, è raccomandabile tener ben presente le regole seguenti.

- Mantenere la calma! Interrompere immediatamente qualsiasi contatto. Bloccare l'indirizzo e/o segnalare i falsi profili delle ricattatrici al gestore del sito.
- Non dar seguito in alcun caso alle richieste e non versare denaro! Pagare non protegge da una pubblicazione del materiale raccolto. Al contrario, spesso le ricattatrici diventano ancora più sfacciate ed esigono sempre più denaro, se sanno che la vittima è ricattabile.
- Mettere in atto un cosiddetto «Google Alert» per il proprio nome. In questo modo le vittime saranno informate su nuovi video, foto e altri contenuti visibili che contengono il loro nome.
- Se compaiono in Internet foto/video (e questo non è certo sempre il caso!) informare i gestori dei siti: di regola, i social network come Facebook eliminano rapidamente i contenuti a sfondo sessuale.

E anche se nel caso di questo delitto è quasi impossibile per la polizia rintracciare gli uomini e le donne che agiscono dietro le quinte, in quanto si nascondono dietro l'anonimato, si dovrebbe comunque sporgere denuncia. Solo in questo modo la polizia riceve informazioni sulle dimensioni di questa forma di delitto, può creare interrelazioni ed eventualmente trovare possibilità di indagare.

A tale fine occorre disporre di prove importanti che dimostrano l'estorsione rispettivamente la truffa: lo «screenshot» (foto della schermata) dei falsi profili, il verbale della chat e/o l'intero scambio di e-mail. Si può sporgere denuncia presso ogni posto della polizia cantonale. Il ricatto, l'estorsione e la truffa sono reati perseguibile d'ufficio, perciò la polizia svolge automaticamente un'indagine.

E per concludere un'osservazione importante: non ci si deve vergognare! La polizia punisce i criminali e non le persone che hanno avuto un momento di debolezza!

Truffa dell'anticipo

Cosa s'intende per «truffa dell'anticipo»?

Il reato chiamato «truffa dell'anticipo» è noto da oltre 30 anni. Un truffatore tenta di ottenere anticipatamente del denaro per un prodotto o una prestazione di servizio da una (potenziale) persona

da truffare, senza fornire né il prodotto né la prestazione di servizio. La truffa dell'anticipo ha raggiunto la notorietà con le presunte vincite alla lotteria («Ha vinto 2 milioni di euro alla lotteria spagnola. Venga a ritirare la sua vincita!») oppure con le false eredità («Uno zio con importante patrimonio che lei non conosce personalmente è morto in Namibia. Le invieremo la sua eredità.»), comunicate per lettera, fax o e-mail alla vittima presa di mira. Oggi, la truffa dell'anticipo è ancora praticata quasi esclusivamente via e-mail o sui siti web.

Quali sono le forme più frequenti di «truffa dell'anticipo»?

La PSC dispone di un ampio quadro d'insieme delle forme più frequenti di «truffa dell'anticipo». La PSC riceve delle segnalazioni da media, organizzazioni dei consumatori, come pure da privati cittadini che sono direttamente vittime di un caso di truffa oppure che si informano per conto di qualcun altro. Particolarmente toccate da queste truffe sono le persone non molto pratiche dei media digitali e che credono ancora che un giorno o l'altro il denaro investito nella truffa sarà loro restituito. Spesso i familiari si rivolgono alla PSC per sapere come convincere una persona anziana che è stata vittima di una truffa.

Per quanto riguarda la truffa dell'anticipo, la PSC fornisce informazioni soprattutto nei quattro casi seguenti:

1. Finte lotterie

zentilia/123RF

I truffatori informano le vittime, principalmente via e-mail, della vincita del primo premio a una lotteria all'estero. Attualmente quella più in voga è la cosiddetta «Loteria primitiva», una lotteria spagnola di grande successo che esiste veramente. La vincita è pronta per essere pagata e rimangono solo ancora le ultime formalità (imposta d'acconto, onorari dell'avvocato, spese bancarie, di versamento e di ricerca, ecc.) da sbrigare. A tale fine, si richiede alla vittima un cospicuo anticipo. I pagamenti devono essere fatti tramite un servizio di trasferimento di denaro, come per esempio Western Union, MoneyGram o altri. Naturalmente, la vincita alla lotteria non viene mai pagata, e neppure gli anticipi versati saranno mai rimborsati. Adducendo scuse sempre nuove, la vittima è invitata ad effettuare altri pagamenti. A questo scopo sono pure impiegati lettere e documenti falsi di società rispettabili (spesso istituti bancari) e importanti autorità (Europol, Interpol). L'importo in gioco arriva rapidamente ad essere di migliaia di franchi. La PSC è a conoscenza di casi in cui sono stati versati anticipi all'estero fino a 250 000 franchi.

Forme simili di «truffa dell'anticipo»: la finta eredità dall'estero, il finto trasferimento del patrimonio di noti capi di stato su conti insospettabili in Svizzera.

2. Finto appartamento in affitto

Vitaly Krivosheev/123RF

I truffatori mettono su noti portali immobiliari inserzioni credibili per bellissimi appartamenti in affitto in posizioni fantastiche ad un prezzo molto vantaggioso. In realtà, si offrono oggetti che in quel momento non sono per nulla da affittare. Le inserzioni sono state prese da un portale immobiliare su cui l'oggetto in questione era stato precedentemente offerto in affitto, copiate e conservate per poter essere utilizzate in un secondo tempo per una truffa dell'anticipo. È anche possibile che l'oggetto in locazione non esista affatto.

Alla richiesta del locatario interessato (e futura vittima della truffa), il truffatore risponde di trovarsi in quel momento all'estero, di non aver bisogno dell'appartamento e che perciò desidera affittarlo a persone di fiducia. L'appartamento può essere visitato autonomamente dall'interessato, che però dovrebbe per sicurezza pagare in anticipo almeno un mese d'affitto come cauzione. Il truffatore può anche richiedere una cauzione per la chiave. Né l'affitto mensile pagato in anticipo, né la cauzione per la chiave saranno mai più rimborsati, né risulta possibile affittare l'appartamento offerto.

Forme simili di «truffa dell'anticipo»: finte case unifamiliari o finti spazi per ufficio in affitto.

3. Finto appartamento di vacanza in affitto

Martin Valigursky/123RF

I truffatori annunciano su noti portali Internet appartamenti o case di vacanza che in realtà non esistono. I truffatori cercano di attirare le loro vittime fuori dal portale Internet, affinché la locazione non possa essere sorvegliata dal portale Internet. I truffatori allettano le loro vittime con affitti bassi e le invitano a pagare il dovuto non tramite il portale Internet, bensì effettuando direttamente un versamento bancario o un trasferimento di denaro. I truffatori possono anche richiedere una cauzione per la chiave. Né l'affitto pagato in anticipo, né la cauzione per la chiave saranno mai più rimborsati. E oltre al danno anche la beffa: una volta giunta nella località di villeggiatura, la vittima si ritrova senza alloggio, situazione che in periodo di alta stagione si trasforma in un incubo.

4. Finto veicolo

m.a.d.

I truffatori mettono su noti portali Internet un'inserzione per vendere un veicolo. La vittima interessata all'acquisto contatta il truffatore, il quale la informa che incaricherà una ditta di trasporti per consegnare il veicolo. La ditta di trasporti, che fa anch'essa parte della rete del truffatore, contatta l'acquirente poco prima della consegna del veicolo e gli chiede il suo indirizzo e altre informazioni che lo riguardano. Poi viene anche chiesto un anticipo sul trasporto e, talvolta addirittura il versamento del prezzo di vendita, prima di consegnare il veicolo. Ovviamente, il veicolo non viene consegnato, e neppure i costi di trasporto e il prezzo di vendita saranno rimborsati.

Forme simili di «truffa dell'anticipo»: finti articoli messi in vendita su portali Internet.

Con che frequenza si verificano casi di truffa dell'anticipo?

Non esistono dati statistici sulla frequenza dei casi di truffa dell'anticipo. In una statistica si inseriscono solo i casi di cui la polizia è venuta a conoscenza perché è stata sporta denuncia. In numerosi casi di truffa dell'anticipo, la vittima rinuncia a sporgere denuncia perché fin dal principio sembra impossibile risalire agli autori del reato, spesso perché i truffatori sono entrati in contatto con la vittima dall'estero. Le vittime rinunciano anche a sporgere denuncia in polizia per la vergogna, in quanto a posteriori anche le vittime stesse non capiscono perché sono cadute nella trappola della truffa. Neppure i tentativi di truffa sono quasi mai segnalati alla polizia.

Per questi motivi non è possibile determinare la frequenza con cui si verificano casi di truffa dell'anticipo. In seguito alle frequenti richieste poste dai cittadini sulle possibilità di indagare su casi di truffa dell'anticipo, la PSC suppone che esista un'enorme zona grigia in quest'ambito. Inoltre, se si fa una proiezione dei guadagni realizzati con le truffe citate, questa forma di delitto frutta somme molto alte.

Particolare problematica che riguarda la truffa dell'anticipo

I trucchi dei truffatori cambiano molto rapidamente. È quasi impossibile mantenere un quadro d'insieme di tutte le possibili forme di truffa dell'anticipo. Inoltre, i truffatori dell'anticipo utilizzano spesso il nome di ditte serie e note e tentano, nascondendosi dietro questi nomi, di confondere le persone da truffare e di ottenere da loro altre informazioni personali.

Alla base di ogni truffa dell'anticipo vi è il problema seguente: una volta pagato il denaro, è praticamente impossibile esigere la sua restituzione. Nella maggior parte dei casi, le persone truffate perdono per sempre i loro soldi. Di regola, perseguire i truffatori dell'anticipo non ha senso per i motivi seguenti.

- I truffatori dell'anticipo agiscono per lo più dall'estero, utilizzando falsi nominativi e numeri di telefono e indirizzi e-mail non registrati. Gli autori sono pertanto sconosciuti.
- Se i truffatori dell'anticipo sono noti all'estero e potrebbero essere resi responsabili dei loro atti, un sistema giudiziario che funziona male in un determinato paese può eventualmente rendere impossibile il perseguimento penale (corruzione).
- Se le persone truffate avevano la possibilità di proteggersi dalla truffa, prestando un minimo d'attenzione, o di evitare l'errore con un minimo ragionevole di cautela, non sussiste alcuna truffa ai sensi del codice penale. Al truffatore non può essere rimproverata nessun'astuzia! Vedere al riguardo DTF 126 IV 165.

È tuttavia indispensabile che la polizia chiarisca in ogni caso se il comportamento del truffatore dell'anticipo è effettivamente punibile. A seconda dei casi sussiste una truffa ai sensi dell'articolo 146 CP.

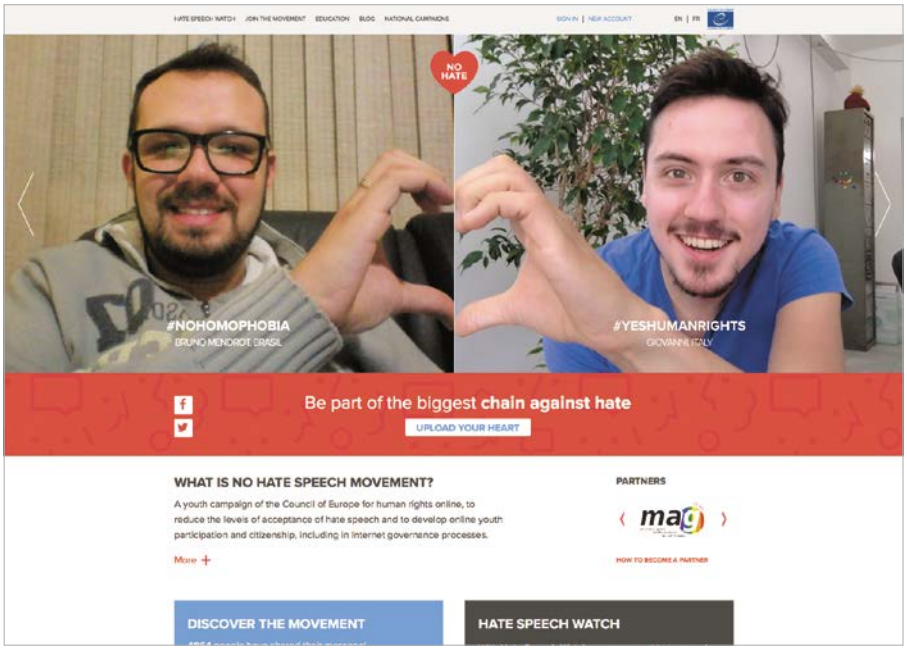
Misure per prevenire la truffa dell'anticipo

- Non pagare nessun anticipo per merci o prestazioni di servizio.
- Insistere nel chiedere di consegnare la merce nello stesso momento in cui si paga, in particolare se si tratta di elevate somme di denaro. La miglior cosa da fare è di incontrare il venditore per prendere in consegna la merce e nel contempo pagare.
- Utilizzare un servizio Escrow (p. es. possibile su eBay).
- Diffidare di un'offerta se appare estremamente allettante (molto economica, subito disponibile, un'occasione da cogliere al volo).
- Diffidare pure di un venditore se incita a concludere un acquisto il più rapidamente possibile, perché altrimenti l'oggetto sarà subito venduto a qualcun altro. Lo stress può spingere ad abbassare la guardia e a non prestare più la dovuta attenzione.

Discorsi d'incitamento all'odio (hate speech)

Cosa s'intende per «discorsi d'incitamento all'odio»?

Il concetto di «discorsi d'incitamento all'odio» contempla qualsiasi dichiarazione o immagine che mira ad offendere o emarginare altre persone, oppure che incita alla violenza nei confronti di una determinata persona o un gruppo di persone. Le dichiarazioni o immagini offensive riguardano spesso il sesso, la religione, l'origine, certi attributi fisici o l'orientamento sessuale di una persona o di un gruppo, oppure la combinazione di queste caratteristiche. Non vi sono limiti ai discorsi d'incitamento all'odio. Essi possono colpire una singola persona, come per esempio una ragazzina in sovrappeso o una persona in sedia



Sito «No Hate Speech», una campagna del Consiglio d'Europa, https://www.nohatespeechmovement.org

a rotelle, oppure dei gruppi come i musulmani o le persone di colore. Parallelamente, si constata che i discorsi d'incitamento all'odio si rivolgono ad un numero crescente di persone e gruppi. In realtà, qualsiasi persona che si espone nella società, sia in ambito professionale che come persona privata, oppure che fa una dichiarazione pubblica che polarizza l'attenzione, può essere vittima di discorsi d'incitamento all'odio.

Le conseguenze dei discorsi d'incitamento all'odio possono essere molteplici. Per le persone singole, come la ragazzina in sovrappeso, questi attacchi possono essere molto difficili da sopportare emotivamente. Quando invece il discorso d'incitamento all'odio colpisce un gruppo di persone, esso sfocia soprattutto in una sua stigmatizzazione e nell'evidenziazione di possibili stereotipi negativi.

Con che frequenza si verificano discorsi d'incitamento all'odio?

Internet è il luogo in cui i discorsi d'incitamento all'odio si diffondono il più rapidamente. Le reti sociali, i blog e i campi riservati ai commenti permettono agli internauti di esprimersi e di discutere liberamente sui temi più diversi. Questa libertà d'opinione virtuale è però anche spesso sfruttata per diffondere, da parte di singole persone o gruppi, dichiarazioni estreme e discriminanti sui media sociali. Inoltre, l'assenza di contatto fisico e il parziale anonimato in rete fanno abbassare le inibizioni in numerose comunità online (che non hanno regole stabilite per le discussioni). Improvvisamente, le persone osano scrivere cose che non avrebbero mai detto ad un loro prossimo. L'anonimato degli autori combinato ai meccanismi di diffusione di Internet rendono difficile risalire alle fonti dei discorsi d'incitamento all'odio, raccogliere le prove dei delitti e determinare la frequenza delle denunce. Diverse indagini hanno però permesso di dimostrare che i discorsi d'incitamento all'odio sono un fenomeno diffuso e di individuare le persone che ne sono vittima. Nel 2015, per esempio, il Consiglio d'Europa ha condotto un'inchiesta online sui discorsi d'incitamento all'odio. I risultati dell'inchiesta hanno evidenziato che l'83% delle persone interrogate era già stato confrontato con discorsi d'incitamento all'odio in Internet. È pure emerso che i principali gruppi presi di mira erano i giovani LGBTI[3], i musulmani e le donne.

Misure per prevenire i «discorsi d'incitamento all'odio»

I discorsi d'incitamento all'odio sono prima di tutto un problema perché contribuiscono a diffondere l'odio. Con l'avvento dei media sociali questa diffusione si è notevolmente semplificata. Ogni persona in grado di scrivere può esprimere la propria opinione in Internet e favorire, che lo voglia o no, la diffusione dell'odio. Per questo motivo, ci si dovrebbe sempre chiedere se i propri commenti o le proprie dichiarazioni non offendono o non mettono al bando nessuno, oppure non inducono altre persone a fare dichiarazioni negative. Inoltre, non si dovrebbero condividere opinioni o contenuti avventati o estremi, o addirittura vietati, come l'incitamento alla violenza (Legge federale sulle misure per la salvaguardia della sicurezza interna) oppure il sostegno a organizzazioni vietate come Al-Qaïda o lo Stato islamico (Legge federale che vieta i gruppi «Al-Qaïda» e «Stato islamico» nonché le organizzazioni associate).

Esistono tuttavia anche varie possibilità per agire a posteriori contro i «discorsi d'incitamento all'odio». Non spetta solo alle vittime difendersi, bensì è responsabilità anche dei testimoni di mostrare coraggio civile e di opporsi con determinazione alle diffamazioni e alle discriminazioni.

- Durante o dopo un incidente, è importante rivolgersi alla propria famiglia, a conoscenti o ad un centro di consulenza per parlare delle dichiarazioni offensive che sono state rivolte o diffuse da terzi.
- Bloccare gli/le utenti che diffondono in Internet dichiarazioni diffamanti e/o discriminatorie, affinché queste persone non abbiano più la possibilità di diffonderle.

3 LGBTI è un acronimo inglese che significa: lesbiche, gay, bisessuali, transgender e intersessuali.

- Segnalare la diffusione di dichiarazioni diffamanti e/o discriminatorie ai rispettivi provider di piattaforme come Facebook o Instagram.
- Se si vuole avviare un procedimento penale contro una persona o un gruppo, sporgere denuncia presso la polizia cantonale. Si raccomanda però di rivolgersi dapprima ad un centro di consulenza per valutare se questo passo è veramente sensato.
- Si deve assolutamente conservare le prove come per esempio foto delle schermate con data e ora e URL, i verbali delle chat o le fotografie che documentano il caso.

Più informazioni su questo tema:

Giovani e media – il portale informativo per la promozione delle competenze mediali: www.giovaniemedia.ch/it/opportunita-e-rischi/rischi/estremismo.html

Campagna «No Hate Speech» del Consiglio d'Europa in Italia: www.nohatespeech.it

Furto e usurpazione d'identità

Oggi, in Svizzera, più nessuno vuole fare a meno di Internet. La maggior parte di noi ha almeno un indirizzo e-mail privato che utilizza per condividere notizie con parenti e amici. Sempre più cittadini pagano le loro fatture tramite eBanking risparmiandosi di andare una volta al mese in banca o in posta. Sono inoltre sempre di più le persone che apprezzano gli acquisti online in Svizzera e all'estero e che si connettono per svolgere le proprie attività professionali. In altre parole: la nostra vita quotidiana si sta digitalizzando e questo comporta che vi siano in Internet numerosi dati che ci riguardano.

everythingpossible/123RF

Oggi, con carte di credito rubate, si può facilmente pagare online camere d'albergo, acquistare vestiti, vino o altri prodotti.

È prevalentemente una questione di denaro, ma talvolta è anche per rovinare la reputazione

Se i nostri dati finiscono nelle mani di sconosciuti e sono utilizzati in modo indebito, si parla allora di furto d'identità o usurpazione d'identità. Nulla di strano che un'enorme quantità di dati venga rubata ed utilizzata indebitamente allo scopo di arricchirsi in modo illegale. Basti pensare per esempio ai dati delle carte di credito con cui online si può molto semplicemente pagare camere d'albergo, acquistare vestiti, vino o altri prodotti da farsi recapitare a qualsiasi indirizzo. Capita però anche che si rubino o utilizzino in modo indebito dei dati per rovinare la reputazione della persona derubata. L'autore o l'autrice si manifesta poi in Internet come la vittima, crea per esempio dei falsi *account* nelle reti sociali o offre prestazioni sessuali a nome della vittima su siti erotici.

Raccogliere o saccheggiare dati

Rubare o usurpare l'identità è talvolta proprio un gioco da ragazzi per gli autori o le autrici di questi reati. Alcuni dati in Internet non hanno bisogno di essere né rubati, né saccheggiati. Basta «raccoglierli»! Alcuni utenti sono incuranti e fiduciosi al punto tale da rendere accessibili a tutti il loro indirizzo e numero di telefono, la loro data di nascita, i nomi dei loro famigliari, le loro foto private e persino il loro datore di lavoro nel loro account sui media sociali. Altri consentono di vedere questi dati sono ai loro amici, ma accettano di diventare amici di persone che non hanno mai incontrato della vita reale. Accedere ai dati bancari e delle carte di credito è senz'altro molto più difficile, però spesso i criminali riescono, per esempio con e-mail di *phishing*, a indurre cittadini e cittadine ingenui ed inconsapevoli a comunicare dati sensibili.

La prudenza individuale protegge solo limitatamente

Purtroppo non basta credere che sia sufficiente rinunciare ad utilizzare Internet per proteggersi dal furto e dall'usurpazione di identità. Oggi, innumerevoli dati sensibili riguardanti ogni singolo circolano già in Internet o nelle sue immediate vicinanze. Naturalmente, i nostri dati bancari, i dati sulla nostra salute e informazioni analoghe sono ben protetti. Tuttavia, un errore umano (per esempio archiviare un pacchetto dati su un server sbagliato) o un pirataggio possono dar luogo ad un uso indebito dei nostri dati, senza che avessimo potuto impedirlo con provvedimenti individuali.

Misure di prevenzione

Anche se l'uso di Internet comporta un certo rischio di diventare vittima di un furto d'identità, ognuno di noi può minimizzare questo rischio adottando determinati comportamenti e certe misure tecniche.

- Sul sito della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI, si trovano numerosi consigli utili e raccomandazioni per proteggere i dati dal furto e gli apparecchi (PC, portatile, ecc.) da attacchi informatici. www.melani.admin.ch
- Sul sito del Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet (SCOCI), ci si può informare sui modi operandi più frequenti utilizzati in Internet e aggiornarsi sulle false e-mail e sui falsi siti diffusi. www.cybercrime.admin.ch

Il furto o l'usurpazione d'identità non sono citati esplicitamente nel codice penale svizzero (CP). Questi reati sono tuttavia sempre assimilati ad azioni penalmente punibili. Fra questi rientrano fra l'altro (a seconda del tipo di furto o di usurpazione) l'acquisizione illecita di dati (art. 143 CP), l'accesso indebito ad un sistema per l'elaborazione di dati (art. 143bis e 126 CP), i delitti contro l'onore e contro la sfera segreta e privata (art. 173 ss. CP).

La Polizia comunale di Zurigo e la sua strategia per i media sociali: da ICoP a Instagram

Intervista a Michael Wirz, Capo della sezione Comunicazione della polizia comunale di Zurigo

Signor Wirz, sono molti anni che la Polizia comunale di Zurigo sfrutta i media digitali per tenere costantemente informata la popolazione cittadina. Perché la polizia comunale di Zurigo ha deciso di lavorare attivamente con i media sociali?
Nel 2008, molte persone si erano date appuntamento via *Facebook* a Zurigo per un *botellón.* Oltre un migliaio di adolescenti e giovani adulti avevano poi partecipato a questa «sbevazzata collettiva», causando costi per diverse centinaia di migliaia di franchi a carico dell'amministrazione comunale. In quell'occasione abbiamo capito per la prima volta che dovevamo occuparci di *Facebook.* Dal 2009 al 2011 ho allora elaborato, su mandato del comandante, una strategia per i media sociali e condotto a tale fine un'inchiesta fra gli utenti della comunità online. Sono rimasto sorpreso dal grande consenso che ho incontrato: le persone interrogate erano molto interessate a poter comunicare con la polizia attraverso i media sociali. Oggi siamo attivi su *Facebook, Twitter, YouTube* e *Instagram.*

Quale strategia e quali obiettivi perseguite utilizzando i media sociali come canali di comunicazione?
Ci preme innanzitutto avviare un vero e proprio dialogo con la popolazione e desideriamo puntualizzare che non vogliamo utilizzare i media sociali semplicemente come canali supplementari di diffusione dei nostri comunicati stampa e di altre informazioni. Dato che molti cittadini utilizzano oggi i media sociali, anche noi come polizia dobbiamo essere presenti su questi media. Questo significa che dobbiamo mettere sistematicamente online la filosofia e la cultura che viviamo fuori dall'universo di Internet. In fondo, il lavoro della polizia, in Internet o nella vita di tutti i giorni, è identico. Portiamo avanti la nostra strategia di comunicazione che abbiamo semplicemente completato. Così restiamo autentici, agiamo in modo mirato e creiamo un clima di fiducia. Inizialmente pianificavamo in anticipo i contenuti (content plan), ma questo ci limitava troppo. Oggi «postiamo» messaggi quando succede qualcosa, ed abbiamo constatato che se non pubblichiamo nulla per due settimane, non è un problema per i nostri amici di *Facebook* e i nostri abbonati.

Che canale è più adatto a quale uso?
Utilizziamo *Twitter* per un'informazione diretta e immediata. In questo modo raggiungiamo particolarmente bene gli *opinion maker,* gli esponenti politici, ma anche diverse organizzazioni. *Twitter* ci permette, in alcuni casi, di influenzare in una certa misura *l'agenda setting.* Dato che la modalità di comunicazione è più *«colloquiale»,* si può talvolta trattare un tema che altrimenti sarebbe più difficile da affrontare.

Facebook funziona molto bene per le storie più lunghe e approfondite, spesso corredate da foto. Qui raccogliamo anche il parere e lo stato d'animo della popolazione, e permettiamo inoltre di dare un'occhiata dietro le quinte del lavoro della polizia. A livello tematico, utilizziamo i nostri canali di comunicazione e la loro ampia portata anche per diffondere i nostri messaggi di prevenzione.

Si può conquistare la fiducia della popolazione attraverso i media sociali?
Naturalmente, ma non solo, perché il comportamento a diretto contatto con le persone è altrettanto importante. Se considero le reazioni e le numerose domande che riceviamo su questi canali, sono però convinto che questo impegno contribuisca a rafforzare la fiducia! Ci teniamo moltissimo alla fiducia che ci viene accordata e rispondiamo alle domande sottoposteci in modo molto serio e dettagliato. Ci adoperiamo inoltre affinché vengano diffusi solo contenuti sicuri al 100%.


m.a.d.

Michael Wirz, 40 anni, poliziotto di formazione, è capo della sezione Comunicazione della polizia comunale di Zurigo. In questi ultimi anni si è dedicato intensamente al tema «Digitalizzazione e lavoro della polizia». Per il suo lavoro di master, Michael Wirz ha studiato in particolare le opportunità e i rischi legati all'uso dei media sociali da parte delle organizzazioni di soccorso. Per la Polizia comunale di Zurigo, invece, ha pianificato la strategia per i media sociali e introdotto la loro utilizzazione. Nel frattempo, questo corpo di polizia ha assunto un ruolo di leader in quest'ambito nei paesi europei germanofoni. Michael Wirz è inoltre docente di comunicazione amministrativa presso varie scuole universitarie professionali.

Patrick Jean è il primo ICoP della Svizzera. Come è nata l'idea di un poliziotto di prossimità in Internet?

Quando c'è un problema, di regola si preferisce parlare con persone e non con organizzazioni anonime. La stessa considerazione vale anche quando si è online. In occasione di un simposio dell'Accademia europea di polizia (cepol), abbiamo incontrato Marko Forrs, un collega di Helsinki che lavora online da anni come «nettipoliisi» *(ICoP)* per la polizia finlandese. Questa idea di polizia

L'ICoP Patrick Jean su Facebook.

di prossimità online mi ha affascinato e volevo scoprire se poteva funzionare anche per la città di Zurigo. Ci siamo quindi messi in cerca di un collega adatto. All'epoca, Patrick Jean stava svolgendo uno stage nel nostro reparto e sembrava essere la persona ideale per questo lavoro. È comunicativo, aperto, scrive bene, ha una grande sensibilità e il tatto necessario. Lo abbiamo perciò formato appositamente per svolgere questa mansione e quindi abbiamo lanciato un progetto pilota di sei mesi. L'interesse e la fiducia dimostratagli nei panni di *ICoP* erano enormi e Patrick si è rapidamente fatto numerosi «amici» e *follower!* Oggi, molti adolescenti e giovani adulti spesso lo riconoscono e lo fermano per strada. Patrick lavora al 50% come poliziotto di quartiere a Zurigo-Hottingen e al 50% come *ICoP.*

Quali sono i prossimi progetti previsti o già in atto?

Da luglio di quest'anno, Eleni Moschos è il pendant femminile di Patrick Jean. Da un lato, il suo arrivo ha permesso di sgravare parzialmente il lavoro di Patrick e, dall'altro, vi sono temi e ambiti ai quali, per una donna, è più facile accedere. Non bisogna dimenticare che Patrick e Eleni lavorano soprattutto dietro le quinte: trattano i messaggi diretti che giungono loro via *Facebook,* li elaborano per poi fornire una consulenza o fungere da mediatore, il tutto senza complicazioni burocratiche. Svolgono spesso un ruolo di «apriporta» per gli adolescenti e i giovani adulti che si rivolgono a loro via *Facebook* o *Instagram.* Capita ripetutamente che organizzino per esempio degli appuntamenti presso l'ufficio giovani o che indichino loro un servizio di consulenza adatto. Le donne e le ragazze, se possono scegliere, preferiscono rivolgersi ad una donna per trattare determinate tematiche.

Per quanto riguarda l'utilizzo di nuovi canali e piattaforme di comunicazione, ci teniamo costantemente aggiornati. Attualmente stiamo esaminando piattaforme come *Snapchat* e *Periscope,* e ci occupiamo molto di video online.

Quali problemi avete già dovuto affrontare? Vi sono già stati «shitstorm» (valanghe d'insulti), minacce contro la polizia comunale, lesioni della personalità e atti simili?

Non siamo mai stati colpiti da un «shitstorm». Ma ci è già successo di ricevere 50 commenti negativi in relazione con un «post» su un concetto di sicurezza per una partita di calcio. Finora, però, siamo sempre stati in grado di gestire la situazione e ci siamo presi il tempo necessario per rispondere ad ogni commento.

Di quando in quando siamo invece confrontati alle lesioni della personalità. Per esempio, vi sono utenti che caricano in Internet la foto di un'auto mal parcheggiata davanti alla loro casa. In quei casi chiariamo loro la situazione e chiediamo di eliminare la foto.

Il corpo della polizia comunale di Zurigo lavora sui e con i media sociali da diversi anni. Secondo lei, i media sociali contribuiscono a facilitare il lavoro della polizia oppure l'impegno sui media sociali rappresenta in primo luogo un compito supplementare? Quali sono le sue conclusioni al riguardo?

Globalmente, il mio bilancio è positivo e sono convinto che questa attività faciliti il nostro lavoro. Ciò che facciamo sui media sociali va ben oltre il servizio di relazioni pubbliche: noi fungiamo da polizia di prossimità in Internet. Il nostro lavoro lo svolgiamo sempre con lo stesso pragmatismo, non importa se siamo online o offline. Mi ricordo per esempio di un caso in cui abbiamo ritrovato più o meno per caso su Facebook una persona che era stata segnalata come scomparsa. Le abbiamo allora inviato un messaggio e ci ha risposto che andava bene tutto, che si trovava all'estero e che avrebbe contattato immediatamente i propri familiari. In questi casi, la nostra presenza sui media sociali può facilitare, se non addirittura sgravare l'insieme del nostro lavoro.

Naturalmente, tutto il lavoro sui media sociali rappresenta anche una promessa di trasparenza e quindi una misura che rafforza la fiducia, aspetto che costatiamo in seguito alle numerose richieste che ci giungono. Per esempio capita spesso che la gente ci dica sui media sociali di non avere una particolare considerazione per la polizia, ma di trovare positivo il lavoro che svolgiamo.

A mio avviso, sarebbe interessante se in futuro venissero impiegati poliziotti online di altri corpi, poiché i nostri *ICoP* hanno amici anche al di fuori della città e del cantone di Zurigo. Talvolta sarebbe utile poter indirizzare queste persone ad altri colleghi. Già oggi notiamo un interesse per la nostra attività da parte di altri corpi di polizia. Seguendo il principio fondamentale dei media sociali, siamo più che volentieri disposti a condividere le nostre esperienze. Poiché il sapere, quando è condiviso, è l'unico bene che aumenta anziché diminuire!

Facebook www.fb.com/StadtpolizeiZH
Twitter @StadtpolizeiZH

ICoPs

Patrick Jean
Facebook www.fb.com/stapojean
Instagram @stapojean

Eleni Moschos
Facebook www.fb.com/eli.stapo
Instagram @eli.stapow

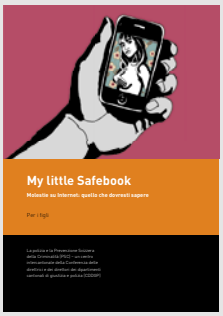
Materiale informativo della PSC

La prevenzione, con focalizzazione sui media digitali, è importante e utile per varie ragioni. Oggigiorno, i bambini e i giovani crescono offline e online, e devono quindi acquisire competenze sia nel mondo reale che digitale. Molti tipi di truffa in Internet sono relativamente facili da intuire e individuare, sempreché si conoscano. Perciò l'informazione in sé costituisce spesso già una misura di prevenzione sufficiente. E se le cittadine e i cittadini imparano il funzionamento di Internet e capiscono quanto questo strumento può essere insidioso e ingannevole, la probabilità di riconoscere le attività criminali aumenta nettamente.

La PSC ha perciò elaborato alcuni opuscoli e pieghevoli che tengono conto di queste circostanze e dei gruppi target.

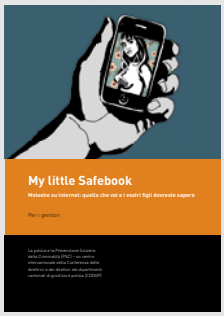
Le varie pubblicazioni possono essere scaricate dal sito www.skppsc.ch e sono pure disponibili presso i posti di polizia comunali e cantonali.

Opuscolo «My little Safebook»
per adolescenti

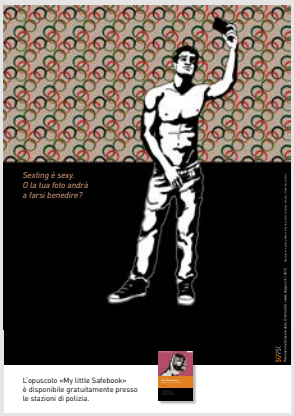


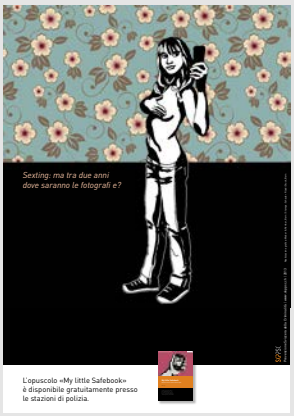
«My little Safebook» si rivolge ai ragazzi a partire da 12 anni di età e spiega loro ciò che devono sapere sulle molestie in Internet. L'opuscolo illustra come i ragazzi possano proteggersi dal cybermobbing, dalle aggressioni sessuali e dalle trappole degli abbonamenti in Internet e li indirizza su come riflettere in modo critico sulla propria fruizione dei media e sulla differenza fra mondo reale e virtuale. L'opuscolo è integrato da una breve sintesi dei riferimenti giuridici e da link con maggiori informazioni.

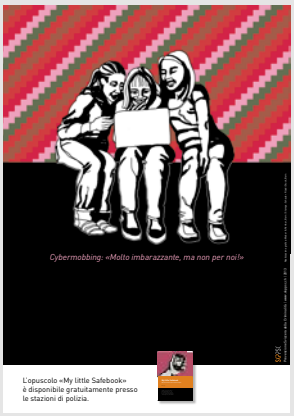
Opuscolo «My little Safebook»
per genitori



«My little Safebook» si rivolge ai genitori e agli educatori di ragazzi a partire dai 12 anni di età. L'opuscolo li aiuta a comprendere perché Internet affascina i giovani e come accompagnarli in modo competente nel loro rapporto con i social network. L'opuscolo fornisce informazioni dettagliate sul cybermobbing, sulle aggressioni sessuali e sulle trappole degli abbonamenti in Internet e su come i giovani possano proteggersi da questi pericoli. L'opuscolo tratta i temi della fruizione dei media e della competenza sui media e spiega come un adulto esemplare debba comportarsi in Internet. L'opuscolo è integrato da una breve sintesi dei riferimenti giuridici e da link con maggiori informazioni.







Poster A3
«Sexting» e «Cybermobbing»

«Sexting è sexy. O la tua foto andrà a farsi benedire?»

«Sexting: ma tra due anni dove saranno le fotografi e?»

«Cybermobbing: «Molto imbarazzante, ma non per noi!»»

Opuscolo «C'era una volta... Internet»

In un mondo in cui i bambini entrano in contatto con Internet sempre più piccoli, l'opuscolo «C'era una volta... Internet» si rivolge proprio ai genitori di bambini di età inferiore ai dodici anni.
La cinque favole rivisitate e illustrate, pensate per essere lette dai genitori oppure autonomamente dai bambini in età scolare, trattano in modo spiritoso e divertente i cinque principali pericoli che Internet può presentare (la dipendenza da Internet, la pedocriminalità, il cybermobbing, gli acquisti online e gli abbonamenti trappola e la protezione dei dati). Nei brevi capitoli intitolati «E la morale di questa fiaba?», inoltre, i genitori troveranno informazioni e consigli su ciascuna problematica affrontata.

«Cybermobbing: tutto ciò prevede la legge»

Il pieghevole «Cybermobbing: tutto ciò prevede la legge» fornisce informazioni sui più importanti articoli di legge che affrontano il tema del cybermobbing. Due casi esemplificativi spiegano come si metta in atto il mobbing sui nuovi media e sette consigli spiegano come si possa agire contro il cybermobbing. Il pieghevole si propone inoltre di fare in modo che i giovani riconoscano il limite fra bisticci e cybermobbing. Il pieghevole dovrebbe inoltre fornire a genitori ed educatori una certa sicurezza nella discussione di questo tema.

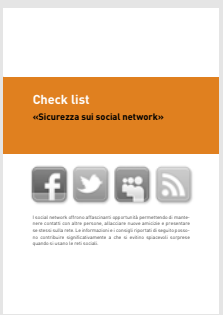
«Pornografia: tutto ciò che prevede la legge»

Il pieghevole «Pornografia: tutto ciò che prevede la legge» fornisce informazioni sui principali articoli di legge che affrontano il tema della pornografia e intende contribuire a fare in modo che i giovani possano sperimentare la loro curiosità sessuale in un campo esclusivamente legale. Il pieghevole spiega la situazione giuridica e fornisce a genitori ed educatori importanti informazioni sul tema dell'età minima, del sexting e della pornografia illegale. Il suo scopo è inoltre quello di dare sicurezza a genitori ed educatori nella discussione su questo delicato tema.

«La propria immagine: tutto ciò che prevede la legge»

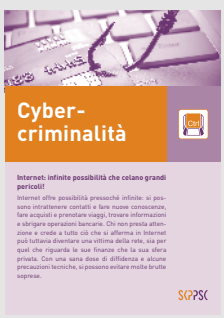
Il pieghevole «La propria immagine: tutto ciò che prevede la legge», con l'aiuto di casi esemplificativi, mostra in quali condizioni si violi il diritto alla propria immagine e come si possa procedere in questo genere di situazione. Il pieghevole spiega le basi giuridiche e descrive in quali casi i tribunali presuppongano una situazione di tacito consenso. Il pieghevole fornisce informazioni su ciò a cui prestare particolare attenzione quando si fotografano bambini e ragazzi, per non violare i diritti dei minorenni alla propria immagine.

«Check list – Sicurezza sui social network»



Su una pagina doppia, questa check list fornisce cinque avvertenze generali sul funzionamento dei social network e quattro raccomandazioni comportamentali, affinché sia possibile evitare brutte sorprese e godersi i vantaggi dei social network.

Cartolina «Cybercriminalità» e «Truffa»



Cambiamento in seno alla commissione di direzione della PSC

La commissione di direzione approva la pianificazione annuale delle attività, il conto annuale della PSC e le campagne di prevenzione che la PSC elabora e attua.

Maya Büchi-Kaiser, Consigliera di Stato del Canton Obvaldo, ha cambiato dipartimento e si è quindi dimessa dalla commissione di direzione al 30 giugno 2016. Le succede **Christoph Amstad,** Consigliere di Stato del Canton Obvaldo e Direttore del dipartimento di giustizia e sicurezza. L'onorevole Amstad assume inoltre la rappresentanza del Concordato della polizia della Svizzera centrale in seno alla commissione di direzione.

Adrian Lobsiger, vicedirettore di fedpol, è stato nominato nuovo incaricato federale della protezione dei dati e della trasparenza. In primavera 2016 ha quindi lasciato la commissione di direzione. La rappresentanza di fedpol in seno alla commissione di direzione è ora assunta da **René Bühler,** vicedirettore dell'ufficio federale di polizia.

Cambiamento in seno alla commissione di progetto della PSC

La commissione di progetto analizza la situazione della criminalità in Svizzera e propone dei temi per le campagne alla commissione di direzione. Prende inoltre posizione sui concetti portati avanti dalle campagne che poi sottopone alla commissione di direzione, prima che quest'ultima li trasmetta alla CDDGP.

Robert Steiner è stato il membro della commissione di progetto con il maggior numero di anni di servizio. In veste di delegato della commissione di progetto, ha partecipato alle riunioni della commissione di direzione della PSC. Fungeva quindi da importante anello di collegamento fra la commissione di direzione e la commissione di progetto.

Robert Steiner è stato capo della polizia giudiziaria del Canton Vallese fino al 2016, anno del suo pensionamento. Per questo motivo si è congedato dalla commissione di progetto in occasione della sua seduta primaverile 2016. Gli succede **Florian Walser,** capo della polizia giudiziaria del Canton Friburgo, che ha già partecipato alla seduta autunnale 2016 della commissione di progetto. Egli assume inoltre la rappresentanza dei capi della polizia giudiziaria del Concordato di polizia della Svizzera romanda.

fedpol/Gaëtan Bally

Christoph Amstad

m.a.d.

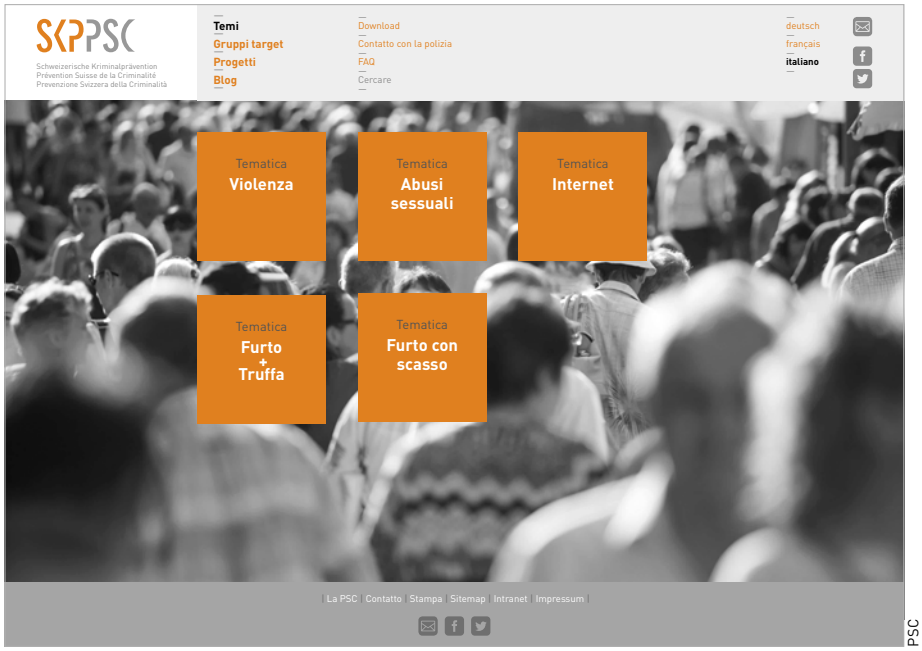
René Bühler

m.a.d.

Florian Walser

Totale rielaborazione del sito della PSC (www.skppsc.ch)

Il nuovo sito della PSC sarà online e consultabile a partire dal 1° gennaio 2017. L'attuale struttura dei temi era sorpassata e ha perciò dovuto essere totalmente rielaborata. Questo significa quindi che i link diretti ai contenuti del sito PSC, che i partner che cooperano con la PSC hanno inserito nei loro siti, non funzioneranno più e dovranno quindi essere sostituiti dai link delle nuove pagine tematiche. La PSC si adopera affinché i partner con cui coopera siano già informati sui nuovi link importanti prima dell'attivazione del nuovo sito.



PSC

Piano nazionale d'azione per prevenire e combattere la radicalizzazione e l'estremismo violento

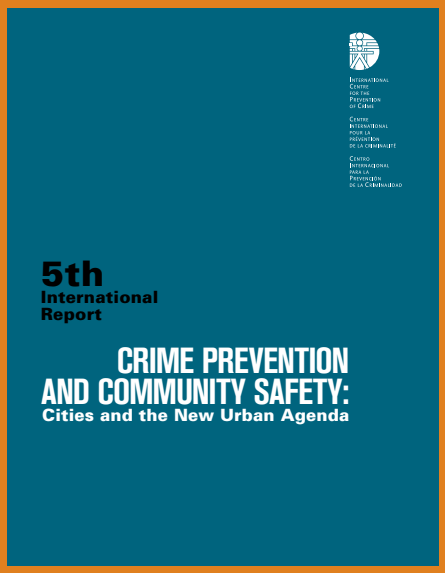
La «Rete integrata svizzera per la sicurezza» (RSS) ha iniziato ad elaborare un piano nazionale d'azione (PNA) su mandato di Confederazione, Cantoni, Città e Comuni. Questo PNA, che contempla quattro diverse aree d'intervento – prevenzione, repressione, protezione e prevenzione delle crisi – si prefigge di prevenire qualsiasi tipo di radicalizzazione e di estremismo violento. Le priorità tematiche, designate come aree tematiche nel PNA, saranno attribuite a queste aree d'intervento. Si tratteranno nove diverse aree tematiche – istruzione, integrazione, riconoscimento/formazione, socialità, sicurezza, collaborazione interdisciplinare, sensibilizzazione, deradicalizzazione/riabilitazione e collaborazione internazionale – la cui elaborazione sarà di volta in volta di competenza di un'organizzazione con un ruolo guida in quest'area tematica. L'elaborazione del PNA dovrà essere ultimata al più tardi entro inizio settembre 2017, mentre in giugno 2017, il PNA sarà oggetto di una consultazione da parte delle competenti autorità e istanze.

Maggiori informazioni su: www.svs.admin.ch

5° rapporto internazionale sulla prevenzione della criminalità e la pubblica sicurezza

A inizio novembre 2016, il Centro internazionale per la prevenzione della criminalità (CIPC) ha pubblicato il suo 5° rapporto internazionale intitolato «Cities and the New Urban Agenda» (città e agenda urbana) in cui si sono affrontati i temi seguenti: «Trends in crime and its prevention» (tendenze criminali e loro prevenzione), «Urban safety», (sicurezza urbana), «Cities, territory and public safety policies: A latin american perspective» (Città, territori e le loro strategie nell'ambito della pubblica sicurezza: un esempio latinoamericano), «Crime prevention on urban public transport» (Prevenzione della criminalità nei trasporti pubblici), «Crime prevention in relation to drug use in the urban environment» (Prevenzione della criminalità in relazione con il consumo di droghe nel contesto urbano) e «Cities and preventing violent radicalization» (Le città e la prevenzione della radicalizzazione violenta).

Il rapporto si rivolge principalmente a tre diversi gruppi target: gli organi decisionali, con i parlamentari e i membri del governo responsabili del settore della sicurezza, gli esperti nel settore della sicurezza urbana e le organizzazione di ricerca che studiano il modo di trovare ed elaborare buone pratiche e che effettuano e commentano valutazioni. Il rapporto in lingua inglese è scaricabile gratuitamente dal sito del CIPC.



Maggiori informazioni su:
www.crime-prevention-intl.org

22. Deutscher Präventionstag 2017 (22ª giornata tedesca di prevenzione), Hannover, Germania

La manifestazione «22. Deutscher Präventionstag» (DPT) si svolgerà il 19 e 20 giugno 2017 ad Hannover. Il tema principale della giornata di quest'anno sarà «Prävention & Integration» (prevenzione ed integrazione). I partner della manifestazione ospitanti sono il Land della Bassa Sassonia, la città di Hannover, capoluogo del Land, e il Landespräventionsrat (LPR) della Bassa Sassonia (Consiglio di prevenzione del Land). Iscrizioni alla manifestazione DPT sul seguente sito: www.praeventionstag.de → DPT 2017 in Hannover → Anmeldung

Nuovo corso all'Istituto svizzero di polizia (ISP) Sicurezza urbana (6.40.00.d)

Gruppo target

- Collaboratori e collaboratrici dei corpi di polizia che rilasciano, verificano e preparano autorizzazioni o che in futuro saranno incaricati di effettuare questi compiti.
- Membri dei corpi di polizia cantonale (p. es. capiposto), autorità comunali che forniscono la consulenza su varie questioni tecniche in materia di autorizzazioni e manifestazioni.
- Collaboratori di amministrazioni che si occupano di questioni di sicurezza in relazione con manifestazioni e autorizzazioni.

Obiettivi

I partecipanti:

- preparano una procedura d'autorizzazione per manifestazioni su suolo pubblico, semipubblico e privato, e sanno spiegare e elaborare formulari di autorizzazione e formulari di domanda;
- avvalendosi di liste di controllo e di altri strumenti ausiliari, sono in grado di preparare in modo corretto ed efficiente varie domande di autorizzazione, di svolgere compiti di collegamento e di definire interfacce;
- grazie ad un caso che fa testo, e che elaborano in gruppo, sono sensibilizzati sulle sfide e sui problemi specifici che si presentano durante le manifestazioni, ciò che consente loro di elaborare autonomamente le relative soluzioni ai vari problemi;
- acquisiscono maggiori conoscenze nei settori domande e autorizzazioni, diritto amministrativo, sorveglianza tecnica degli spazi pubblici e sicurezza urbana, conoscenze che possono poi mettere in pratica.

Contenuti
Sicurezza urbana; procedure d'autorizzazione per manifestazioni; formulari d'autorizzazione e di domanda; diritto amministrativo, questioni di responsabilità in veste di istanza che rilascia le autorizzazioni, autorizzazioni per la mescita e il commercio al minuto di bevande alcoliche, alcol e protezione dei giovani; Crowd Management; prescrizioni della polizia del fuoco, responsabili del comitato organizzativo e i loro doveri; sorveglianza tecnica degli spazi pubblici, concetti di eventi.
Il corso è tenuto solo in tedesco.

Informazioni disponibili solo in tedesco:
www.edupolice.ch → kurse → kursangebot → 6.40.00.d Urban Sicherheit

Reto Habermacher nominato nuovo direttore dell'ISP

Il 1° ottobre 2016, **Reto Habermacher** ha assunto la funzione di direttore dell'ISP, succedendo a Pius Valier. L'Istituto svizzero di polizia dirige, su mandato della CDDGP, il progetto CGF 2020, e parallelamente adegua di conseguenza la propria organizzazione. Questo progetto di riorganizzazione, unitamente al CGF 2020 e alla direzione dell'ISP stesso, rappresentano un carico di lavoro che va ben oltre un tempo pieno. Accanto alla direzione dell'ISP, Reto Habermacher dirigerà il progetto di riorganizzazione interna. Pius Valier, a cui è stata chiesta la disponibilità, si è dichiarato disposto a lavorare a tempo parziale e ad assumere la direzione operativa del progetto CGF 2020 nell'ambito di un mandato esterno su incarico della direzione di progetto strategica.


m.a.d.

Maggiori informazioni su:
www.institut-police.ch

Giovani e media: il portale informativo per la promozione delle competenze mediali

Proteggere i bambini e i giovani significa accompagnarli anche nel mondo digitale! Questo portale informativo spiega a genitori, insegnanti e altre persone con compiti educativi come fare per garantire un uso quotidiano dei media digitali sicuro e adeguato all'età.
www.giovaniemedia.ch

«eBanking, ma sicuro!»

Sul sito www.ebankingabersicher.ch/it, le persone interessate trovano informazioni pratiche sulle misure necessarie e sulle regole comportamentali da adottare per utilizzare le applicazioni eBanking in tutta sicurezza. Primari istituti finanziari svizzeri hanno incaricato il dipartimento di informatica dell'Università di Lucerna di creare questo portale, attualmente sostenuto da oltre 70 istituti finanziari con sede in tutta la Svizzera e nel Principato del Liechtenstein.

Maggiori informazioni su:
www.ebankingabersicher.ch/it

Informazioni sulla manifestazione del 2017

La **3ª Conferenza della Rete integrata svizzera per la sicurezza** permette di prendere visione dei risultati della valutazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi e stimola il dialogo sugli ulteriori passi da intraprendere nel settore della cybersicurezza e della cybercriminalità.

Maggiori informazioni su: www.svs.admin.ch

SKPPSC
Prevenzione Svizzera della Criminalità
Casa dei Cantoni
Speichergasse 6
Casella postale
CH-3000 Berna 7

www.skppsc.ch

Editore e fonte di informazioni
Prevenzione Svizzera della Criminalità PSC
e-mail: info@skppsc.ch, tel. +41 31 320 29 50

Responsabile	Martin Boess, direttore PSC
Redattore	Wolfgang Wettstein, Zurigo
Versione francese	ADC, Martigny
Versione italiana	Annie Schirrmeister, Massagno
Grafica	Weber & Partner, Berna
Stampa	Vetter Druck AG, Thun
Tiratura	i: 100 | f: 300 | t: 1350

Data di pubblicazione dell'edizione 4 | 2016: dicembre 2016

L'Info PSC 4 | 2016 è disponibile come file PDF nel sito: www.skppsc.ch/skpinfo.
L'Info PSC 4 | 2016 esce anche in tedesco e francese.


vectomart/123RF