INFO PSC

1 | 2021

LA RIVISTA DELLA PREVENZIONE SVIZZERA DELLA CRIMINALITÀ

Tema
Cybersicurezza

La cybersicurezza è

S-U-P-E-R.ch

Gentili lettrici, stimati lettori,


PSC

Non passa giorno in Svizzera senza che qualcuno finisca nella trappola di un truffatore online. Per esempio, si riceve un'e-mail di phishing nella propria casella di posta elettronica che invita ad effettuare un pagamento per ricevere un pacco. Oppure un'e-mail di ricatto in cui si è dapprima informati che qualcuno è apparentemente in possesso di foto intime e poi minacciati della loro diffusione se non si paga la somma di denaro richiesta. I siti web falsi offrono merci o immobili a prezzi incredibilmente allettanti, utilizzando come esche le ragioni sociali e i loghi di aziende ben note o persino i nomi di celebrità per far sembrare serie le loro offerte e attirare così le potenziali vittime nella loro trappola. Intere aziende e organizzazioni sono vittime di pirataggio informatico e vengono ricattate. La lista dei metodi adottati è infinita e la fantasia dei truffatori non ha limiti. E, nella maggior parte dei casi, le autorità di perseguimento penale non possono far altro che prendere atto di questa situazione. Non perché non vogliano intervenire, bensì perché come autorità nazionali non possono (ancora) contrastare i criminali che operano prevalentemente a livello internazionale. Ecco perché la prevenzione svolge un ruolo particolarmente importante in questi settori della criminalità.

La PSC e tutti i corpi di polizia si sono ora alleati al Centro nazionale per la cibersicurezza (NCSC), alla Swiss Internet Security Alliance (SISA) e a "eBanking – ma sicuro!" (EBAS) per sensibilizzare la popolazione svizzera ai rischi di Internet. Insieme lanceranno una vasta campagna di prevenzione denominata "5 operazioni per la vostra sicurezza digitale" per attirare l'attenzione sui semplici comportamenti che ognuno può adottare per proteggersi efficacemente nello spazio digitale.

Questo numero di INFO PSC vi fornirà informazioni più dettagliate su questo progetto comune e sulle autorità e organizzazioni che si dedicano alla prevenzione dei reati informatici. Il NCSC illustra il suo nuovo orientamento e i suoi principali punti di forza. La SISA, associazione che riunisce rappresentanti dell'economia e delle autorità svizzere, presenta la sua piattaforma digitale dedicata alla sicurezza in Internet chiamata "iBarry.ch". Viene pure presentata la piattaforma indipendente EBAS, messa in piedi dalla Scuola universitaria professionale di Lucerna su mandato degli istituti finanziari svizzeri. E l'agenzia incaricata di realizzare le idee di questa campagna di sensibilizzazione racconta in un'intervista le esperienze fatte e gli insegnamenti tratti dal suo lavoro con i responsabili del progetto. Infine, la PSC, insieme a "La vostra polizia", spiegheranno brevemente perché si sta realizzando questo progetto comune. Inoltre, anche la NEDIK (la rete delle autorità di polizia di supporto digitale alle indagini sulla criminalità informatica) presenta in questo numero il suo nuovo orientamento nel campo della prevenzione della criminalità informatica.

Se vi abbiamo fatto "venire l'acquolina in bocca" e volete ora sapere cosa accadrà esattamente durante questa campagna di sensibilizzazione che si svolgerà dal 3 al 7 maggio 2021, seguiteci sui nostri canali di media sociali. Il 3 maggio si inizia!

Ed ora vi auguro una buona lettura!

Fabian Ilg
Vicedirettore della PSC e capo progetto per la criminalità informatica

IMPRESSUM

Editore e fonte di informazioni
Prevenzione Svizzera della Criminalità
Casa dei Cantoni
Speichergasse 6
3001 Berna

e-mail: info@skppsc.ch
tel. 031 511 00 09

L'INFO PSC 1 | 2021 è disponibile come file PDF nel sito: www.skppsc.ch/skpinfo.
L'INFO PSC 1 | 2021 esce anche in tedesco e francese.

Responsabile	Chantal Billaud, Direttrice PSC
Redazione, interviste	Volker Wienecke, Berna
Versione francese	ADC, Vevey
Versione italiana	Annie Schirrmeister, Massagno
Grafica	Weber & Partner, Berna
Stampa	Länggass Druck AG, Berna
Tiratura	i: 250 | f: 300 | t: 1350
Data di pubblicazione	dell'edizione 1 | 2021: aprile 2021

La cybersicurezza è S-U-P-E-R: settimana di sensibilizzazione alla sicurezza digitale!

Dal 3 al 7 maggio 2021, la Prevenzione Svizzera della Criminalità, insieme ad altre organizzazioni, lancerà una campagna online per sensibilizzare la popolazione alla sicurezza digitale. Quest'azione si prefigge di sorprendere, interessare, informare e di permettere a tutti di trarne un proprio tornaconto grazie ad un'offerta multilivello. Beatrice Kübli, responsabile del progetto alla PSC, spiega perché quest'azione è S-U-P-E-R portandoci dietro le quinte della campagna.

S-U-P-E-R serve da promemoria per le cinque operazioni per la sicurezza digitale e funge anche da URL della landing page.

Autrice

Beatrice Kübli
Responsabile di progetto alla Prevenzione Svizzera della Criminalità


PSC

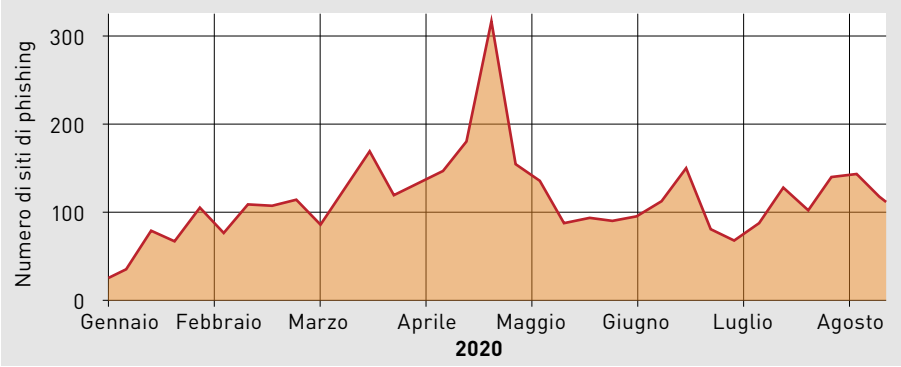
Chi non conosce questa situazione quando si sta per fare una visita dal dentista. Come di consueto quest'ultimo chiederà quante volte si è usato il filo interdentale. E come di consueto ci si dirà che si sarebbe dovuto utilizzarlo, solo che... Lo stesso vale per molte misure di prevenzione, compresa la sicurezza digitale. In altri termini, avete fatto recentemente un backup dei vostri dati privati? Nella maggior parte dei casi basta un piccolo impulso esterno per attivarsi, per esempio la sfortuna di un collega che ha perso tutti i suoi album fotografici perché il suo computer portatile è caduto nel fiume Aare. Siccome non auguriamo a nessuno di perdere i propri album fotografici o altri dati ancora più importanti, ci assumiamo il compito di dare questo "piccolo impulso esterno" organizzando una settimana di sensibilizzazione.

Per "Noi" intendiamo la PSC insieme ai corpi di polizia riuniti sotto il marchio "La vostra polizia", al Centro nazionale per la cibersicurezza NCSC, alla Swiss Internet Security Alliance (SISA) con la sua piattaforma "iBarry" e alla piattaforma "eBanking – ma sicuro!" (EBAS) della Scuola universitaria professionale di Lucerna. La campagna di sensibilizzazione, che si svolgerà dal 3 al 7 maggio 2021, presenterà ai cittadini le famose cinque operazioni che li aiutano a proteggere i loro dati e accessi a Internet. La realizzazione di questa campagna è stata affidata all'agenzia "Partner & Partner" di Winterthur.

Ci si potrebbe chiedere: "Perché trattare proprio il tema della sicurezza digitale?". Dopo tutto, ci sono altri temi importanti nel panorama della prevenzione ai quali si dovrebbe sensibilizzare la popolazione. Ma veniamo al punto: in futuro possiamo immaginare di organizzare regolarmente una settimana di sensibilizzazione anche su altri temi. Abbiamo però buoni motivi per iniziare con la sicurezza digitale.

È più facile prevenire che indagare

Internet offre ai criminali innumerevoli opportunità per truffare ed arricchirsi. I computer possono essere utilizzati per scopi criminali senza che gli stessi utenti se ne accorgano. Vi sono pirati informatici che prendono di mira dati privati come i login dell'e-banking, che rubano intere identità o bloccano l'accesso ai dati della vittima. Indagare, in



Siti di phishing segnalati e confermati settimanalmente su antiphishing.ch nel primo semestre del 2020[1].

questo caso, è difficile e spesso poco fruttuoso, perché gli autori operano dall'estero e usano le risorse offerte da Internet per anonimizzare la loro identità e dissimulare le loro attività. Fare indagini e ricerche richiede una cooperazione internazionale, cosa non facile da organizzare con tutti i paesi, così come solide conoscenze in informatica e un'infrastruttura appropriata. Rispetto all'insieme dei reati penali, i cybercrimini sono in costante aumento, con una preponderanza di truffe online e casi di phishing. Più della metà delle segnalazioni inoltrate a fedpol negli ultimi anni riguardava questi due tipi di reato[2]. E nel primo semestre del 2020, circa 100 siti di phishing sono stati segnalati settimanalmente alla centrale d'annuncio del NCSC.

Ma non tutte le vittime di cyberattacchi si rivolgono alla polizia. Alcune, infatti, si vergognano di essere cascate nella trappola ed essersi fatte truffare. Altre si rassegnano, non credendo che la polizia riuscirà a elucidare questo delitto, e quindi non sporgono denuncia. Il numero di casi non denunciati è alto, e i danni personali ed economici sono considerevoli. Vale quindi la pena di puntare sulla prevenzione, soprattutto in materia di sicurezza digitale. Si possono evitare molte disavventure con pochi e semplici mezzi. Chi usa password sicure, aggiorna regolarmente il proprio software e ha installato un programma antivirus corre meno rischi di essere vittima di un cyberattacco. È inoltre importante che i cittadini diventino consapevoli dei rischi che corrono e mettano in discussione con spirito critico le e-mail o gli SMS di dubbia provenienza. Chi sa come funziona un attacco di phishing o di hacking è meno propenso a cadere nel tranello e a dar subito seguito ad una proposta, anche se molto allettante. Più il singolo è consapevole del pericolo, più le aziende sono protette da attacchi di vasta portata, perché il dipendente informato non cliccherà più sul primo link che capita. Ovviamente, ci sono anche attacchi informatici commessi a un livello puramente tecnico, ma la maggior parte dei delinquenti punta di solito "sull'anello più debole della catena, ossia l'essere umano". Ed è proprio su questo aspetto che fa leva la nostra campagna.

Una settimana? È fattibile!

L'idea originale della campagna era di fare una sorta di pulizia di primavera digitale, per fare finalmente ordine e evadere le pendenze in attesa da tempo. Per finire, però, ci è sembrato che questa idea non fosse poi così adatta al tema, perché in questo caso è più una questione di sicurezza che di pulizia. Ma il concetto alla base della settimana di sensibilizzazione, ossia fare man mano ordine, è rimasto. Il progetto delle "5 operazioni per la sicurezza digitale", che avevamo già elaborato insieme a EBAS nel 2020, si prestava per organizzare una settimana di sensibilizzazione perché prevede un'operazione al giorno. Una settimana è facile da gestire e permette di aumentare la motivazione a partecipare. Inoltre, speriamo in un forte impatto grazie alla possibilità di concentrare tutta la sua forza in questo lasso di tempo.

Questa campagna mira prima di tutto a sensibilizzare la popolazione all'importanza della sicurezza digitale. Si tratta quindi di acquisire la consapevolezza che occorre proteggere anche i propri dispositivi digitali, siano essi computer, tablet o cellulari. Ognuno può e deve anche essere responsabile della propria sicurezza digitale: deve quindi sapere come proteggersi, come riconoscere e prevenire un attacco e come mettere in pratica le conoscenze acquisite. Questi sono i tre elementi al centro della nostra campagna.

Creare consapevolezza

L'elemento più importante di una campagna di prevenzione è la sua visibilità. I migliori manifesti e *post* non servono a niente se nessuno li guarda. In questa campagna puntiamo quindi sull'umorismo e sulla sorpresa. Per noi era inoltre

1 Fonte: Centro nazionale per la cibersicurezza NCSC/MELANI: "Sicurezza delle informazioni. La situazione in Svizzera e a livello internazionale. Rapporto semestrale 2020/I (gennaio – giugno)", 29 ottobre 2020, disponibile online: www.ncsc.admin.ch → Documentazione →Rapporti → Rapporti di situazione → Rapporto semestrale 2020/1

2 National Risk Assessment (NRA): «Betrug und Phishing zwecks betrügerischen Missbrauchs einer Datenverarbeitungsanlage als Vortat zur Geldwäscherei Bericht der interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT)» (Truffa e phishing a scopo di uso fraudolento di un computer come reato preliminare al riciclaggio di denaro – Rapporto del Gruppo di coordinamento interdipartimentale per la lotta contro il riciclaggio di denaro e il finanziamento del terrorismo (KGGT)"), gennaio 2020, disponibile online in tedesco e francese: www.sif.admin.ch → Finanzmarktpolitik und -strategie → Integrität des Finanzplatzes → Berichte

importante stabilire un legame con l'argomento fin dal primo momento, per permettere a tutti di capire immediatamente di cosa si tratta. A tale fine, l'agenzia ha ideato cinque temi: si vede un dispositivo digitale – di volta in volta un computer, un tablet o un cellulare – combinato con un elemento che si associa alla "sicurezza" nella quotidianità. Dato che non esistono nella vita reale, queste combinazioni stupiscono, sorprendono o turbano, e hanno un effetto divertente. Per esempio, si vede un computer portatile in un salvagente o del dentifricio su un tablet. Basta un breve sguardo per cogliere intuitivamente il messaggio trasmesso: "occorre proteggere i dispositivi digitali". Chi guarda con maggiore attenzione, potrà poi approfondire la tematica.

Acquisire conoscenze

I temi sono accompagnati da un breve messaggio che spiega il legame tra l'immagine e la cybersicurezza. Ogni tema illustra una delle cinque operazioni. Il messaggio sull'immagine con il salvagente è: "Mettete al sicuro i vostri dati prima che colino a picco". Così facendo, si comunica in modo semplice e facile da capire che fare il backup dei dati è un'operazione importante per la propria la sicurezza digitale. Per aiutare le persone a memorizzare le cinque operazioni, l'agenzia ha creato una parola promemoria: S-U-P-E-R! La S sta per "Salvare sempre i propri dati", la U per "Usare gli aggiornamenti", la P per "Proteggere il PC con un antivirus", la E per "Elaborare password complesse" e la R per "Ridurre i rischi". S-U-P-E-R funge anche da URL del sito web dove si trovano tutte le informazioni utili e istruzioni pratiche.

Far propria la capacità d'agire

Chi desidera saperne di più su come proteggere se stesso e i propri dispositivi potrà consultare la landing page del progetto dove troverà informazioni dettagliate e spiegazioni su come mettere in pratica le singole operazioni. Ogni operazione è corredata di un breve testo esplicativo. Inoltre, chi desidera approfondire un tema potrà cliccare su vari link che lo reindirizzeranno verso i siti delle organizzazioni partner dove si spiegano i diversi elementi in dettaglio o dove si può partecipare a uno dei webinar proposti dal NCSC.

Questa offerta multilivello rivolta ai cittadini permette di selezionare le informazioni in funzione delle proprie conoscenze. Chi è ben aggiornato potrà accedere a conoscenze specializzate, mentre chi è ancora inesperto potrà avvicinarsi a questo tema in modo semplice e graduale.

Diffondere la campagna tramite le nostre reti

Per diffondere su larga scala la campagna trilingue in tutta la Svizzera, ci affidiamo alle nostre reti. È infatti indispensabile trasmettere i contenuti del maggior numero possibile di partner per fare in modo che la campagna raggiunga i suoi obiettivi. I corpi di polizia e varie banche hanno già confermato la loro partecipazione, e diversi partner economici della SISA sono interessati. Coordinare gli sforzi di tutte le parti coinvolte è una sfida, ma non è niente di nuovo per la PSC. Abbiamo già fatto ottime esperienze con la nostra rete e siamo sicuri che funzionerà bene anche per questa settimana di sensibilizzazione. Ora dobbiamo mostrare la solidità della nostra rete anche alla collettività. Quest'azione, infatti, non riguarda solo la sicurezza digitale. Si tratta pure di fare in modo che la polizia e le organizzazioni partner siano identificati come interlocutori competenti e di mostrare quanto la rete nazionale funzioni a più livelli e sia ben coordinata per garantire la cybersicurezza. E questo sarà sicuramente S-U-P-E-R!

m.a.d.

Salvare i dati è una delle 5 operazioni per la sicurezza digitale. Ogni operazione ha il proprio tema illustrato.

“eBanking – ma sicuro!”

La piattaforma “eBanking – ma sicuro!” (EBAS), messa a disposizione dal Dipartimento di Informatica della Scuola universitaria professionale di Lucerna, ha lo scopo di aiutare le persone private e i dipendenti delle banche a migliorare la loro sicurezza informatica, in particolare quando effettuano operazioni bancarie online.

Nell’aprile 2017, la polizia di Zugo aveva organizzato un evento sul tema della prevenzione a cui il sottoscritto ha partecipato. Durante il rinfresco che è seguito (sì, si usava ancora fare prima del coronavirus), ho iniziato a chiacchierare con un cyberinvestigatore zughese che mi ha parlato della Prevenzione Svizzera della Criminalità (PSC) con cui aveva lavorato. Ho subito capito quali avrebbero potuto essere i vantaggi reciproci di una collaborazione, e alla fine dell’evento mi ha fornito il contatto della PSC.

Nel mese di giugno dello stesso anno, ci siamo ritrovati per un incontro presso il nuovo Dipartimento di Informatica della Scuola universitaria professionale di Lucerna a Rotkreuz. Un’analisi incrociata degli obiettivi della Prevenzione Svizzera della Criminalità e di “eBanking – ma sicuro!” ha rapidamente evidenziato che sarebbe stata possibile una collaborazione in vari ambiti. L’attenzione si è dapprima focalizzata sugli opuscoli e sui pieghevoli in materia di prevenzione, già molto popolari e ben affermati, realizzati dalla PSC. E già nel corso dell’autunno/inverno 2017 abbiamo pubblicato il primo opuscolo prodotto congiuntamente intitolato “5 operazioni per la vostra sicurezza digitale”. Ne sono poi seguiti molti altri, e a tutt’oggi la cooperazione PSC-EBAS ha prodotto sette opuscoli:

- 5 operazioni per la vostra sicurezza digitale
- Lavorare per i criminali come “Money Mule”?
- Phishing
- Telefonate fraudolente dall’assistenza
- Mobile Banking e Mobile Payment
- Navigare in tutta sicurezza nei media sociali
- Rendimenti da sogno? No, perdite da incubo!

Gli opuscoli e i pieghevoli sono distribuiti non solo dalla PSC, ma anche da EBAS, direttamente nell’ambito di formazioni, corsi ed eventi, e anche indirettamente tramite le banche partner della piattaforma “eBanking – ma sicuro!”.

Torniamo all’immediato futuro! Dal 3 al 7 maggio 2021, la Prevenzione Svizzera della Criminalità organizzerà a livello nazionale una settimana di sensibilizzazione alla cybersicurezza. Questa campagna permetterà in qualche modo di completare il cerchio con il primo opuscolo prodotto congiuntamente, poiché la campagna fornirà ogni giorno informazioni dettagliate su una delle “5 operazioni per la vostra sicurezza digitale”. Come una delle quattro organizzazioni promotrici, siamo molto felici di aver partecipato allo sviluppo e al lancio di questa campagna, e naturalmente ci auguriamo di poter continuare ancora a lungo questa fruttuosa collaborazione in materia di prevenzione e sensibilizzazione della popolazione svizzera ai pericoli nel cyberspazio.

A proposito di “eBanking – ma sicuro!”

“eBanking – ma sicuro!” (EBAS) è una campagna di sensibilizzazione nazionale che da oltre dieci anni informa con successo la popolazione svizzera e gli attori del settore finanziario in materia di e-banking sicuro. Lanciata nel 2009 con tre banche partner pilota (Credit Suisse, PostFinance e Zürcher Kantonalbank), la campagna è oggi sostenuta da quasi una cinquantina di banche partner in tutta la Svizzera. La campagna di sensibilizzazione multilingue si basa su quattro pilastri fondamentali:

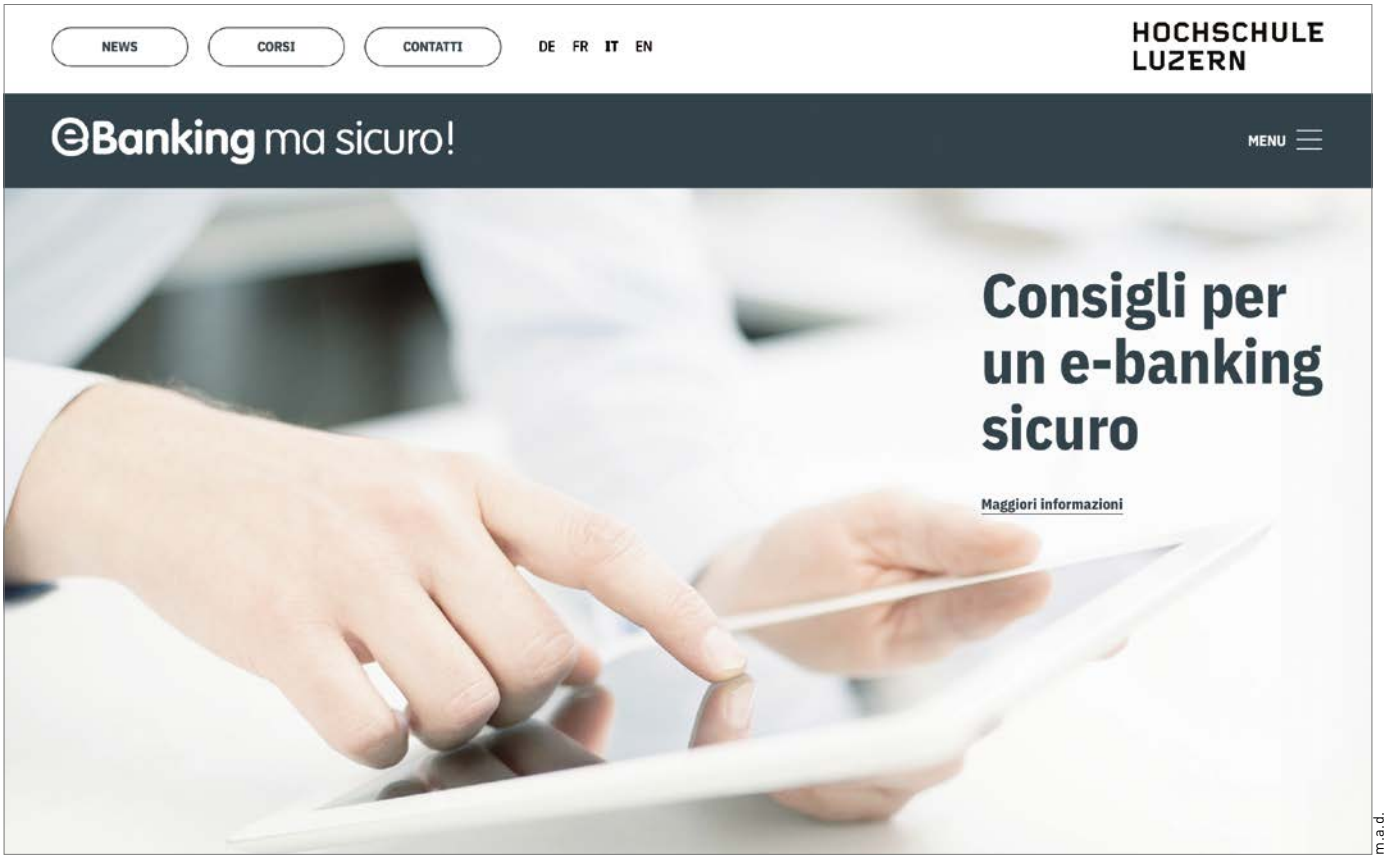
1. Sito web
(servizio pubblico, accessibile a tutti)
Per permettere alla popolazione di aumentare efficacemente e a lungo termine il livello di sicurezza dei propri dispositivi digitali, occorre fornirle consigli utili e assistenza. Questo supporto mira anche ad insegnare agli utenti ad essere più circospetti quando effettuano una sessione di e-banking.

Sul suo sito www.ebas.ch, il Dipartimento di Informatica della Scuola universitaria professionale di Lucerna fornisce informazioni concrete e pratiche sulle misure di sicurezza di base da adottare e sulle regole di comportamento da seguire per utilizzare in tutta sicurezza i dispositivi digitali, in particolare quando si effettuano sessioni di e-banking.

Autore


m.a.d.

Oliver Hirschi
Informatico di formazione, è docente di sicurezza dell’informazione digitale alla Scuola universitaria professionale di Lucerna, dov’è tra l’altro responsabile della gestione della piattaforma «eBanking – ma sicuro!» (www.ebas.ch). È co-autore del manuale «Informationssicherheitshandbuch für die Praxis» (Manuale sulla sicurezza dell’informazione digitale per la pratica) (www.sihb.ch) e membro del gruppo Sicherheitsgruppe Schweiz SGRP (Gruppo di sicurezza Svizzera) (www.sgrp.ch).



m.a.d.

Sul sito Internet www.ebas.ch della Scuola universitaria professionale di Lucerna si trovano informazioni concrete e pratiche sulle misure di sicurezza di base e sulle regole di comportamento da adottare.

2. Corsi per clienti finali
(servizio pubblico, accessibili a tutti)
Il nostro sito propone ogni anno corsi pubblici, di facile comprensione, concepiti per vari gruppi target. L'offerta, disponibile in varie località della Svizzera, comprende un corso di base, un corso pratico con esercizi su dispositivi forniti, uno speciale corso online destinato ai minori di 30 anni e un corso per le PMI. Il corso di base, per esempio, dura due ore e mezza e fornisce informazioni sulla sicurezza digitale in generale e sull'uso dell'e-banking in sicurezza in particolare. Per l'attuale offerta di corsi consultare il sito: www.ebas.ch → corsi.

3. Monitoraggio dei media
(solo per gli istituti partner)
I media influenzano notevolmente il senso di sicurezza e il comportamento degli utenti finali. I vari articoli sul tema e-banking possono disorientare e sollevare molte domande a cui il servizio clienti o i consulenti alla clientela dovranno poi rispondere. Il monitoraggio regolare delle attività nel panorama mediatico svizzero, la preparazione di rispettive prese di posizione destinate all'helpdesk e ai consulenti alla clientela e una banca dati sugli articoli pubblicati e sulle relative prese di posizione fornite migliorano significativamente la qualità del servizio.

In collaborazione con la società Argus Data Insights Schweiz AG, la Scuola universitaria professionale di Lucerna monitora quotidianamente la produzione mediatica svizzera (giornali, media online, radio e TV). Si raccolgono tutti gli articoli incentrati sull'e-banking e sulla sicurezza informatica. Si redigono quindi prese di posizione su ogni articolo importante messe poi a disposizione delle banche partner. Questo permette agli impiegati di banca di rispondere in modo fondato e competente alle domande dei loro clienti in materia di sicurezza.

4. Corsi di formazione per il personale del servizio clienti
(solo per gli istituti partner)
I consulenti alla clientela e il personale dell'helpdesk devono essere in grado di rispondere in modo chiaro, circostanziato e professionale a tutte le domande sulla sicurezza informatica. La Scuola universitaria professionale di Lucerna offre agli istituti finanziari un pacchetto di corsi mirati per formare i consulenti alla clientela e il personale dell'helpdesk.

Da notare infine che il sito dell'EBAS è attualmente visualizzato quasi 40000 volte al mese. A tutt'oggi, oltre 1200 dipendenti degli istituti finanziari partner e più di 4800 persone private hanno seguito formazioni e corsi EBAS sull'e-banking sicuro.

Link e altre informazioni: www.ebas.ch

Sensibilizzare ai ciber-rischi: un compito importante del NCSC

La cibersicurezza svolge un ruolo centrale nella politica di sicurezza nazionale e internazionale e nella politica estera, e rappresenta anche un fattore importante per la piazza economica svizzera. Il Centro nazionale per la cibersicurezza (NCSC) è il primo punto di contatto per l'economia, l'amministrazione, gli istituti di formazione e la popolazione per tutte le questioni relative alla cibersicurezza.

Il Centro nazionale per la cibersicurezza (National Cyber Security Centre, ossia NCSC) è diretto da Florian Schütz, delegato della Confederazione alla cibersicurezza, e responsabile, tra l'altro, dell'attuazione coordinata della Strategia nazionale per la protezione della Svizzera contro i ciber-rischi (SNPC). Questa strategia stabilisce gli obiettivi e le misure sostanzialmente sostenuti dagli attori provenienti dai cantoni, dagli ambienti economici, dalla società e dalle università. L'ordinanza sulla protezione contro i ciber-rischi nell'Amministrazione federale (OCiber) costituisce dal canto suo la base legale per la creazione e lo sviluppo del NCSC. Ne regola inoltre la struttura, i compiti e le competenze delle autorità coinvolte, e prescrive anche le attività di sensibilizzazione e prevenzione nell'ambito dei ciber-rischi[1]. È proprio in quest'ambito che la cooperazione e lo scambio all'interno e all'esterno dell'amministrazione federale sono di centrale importanza per il NCSC.

Autrice

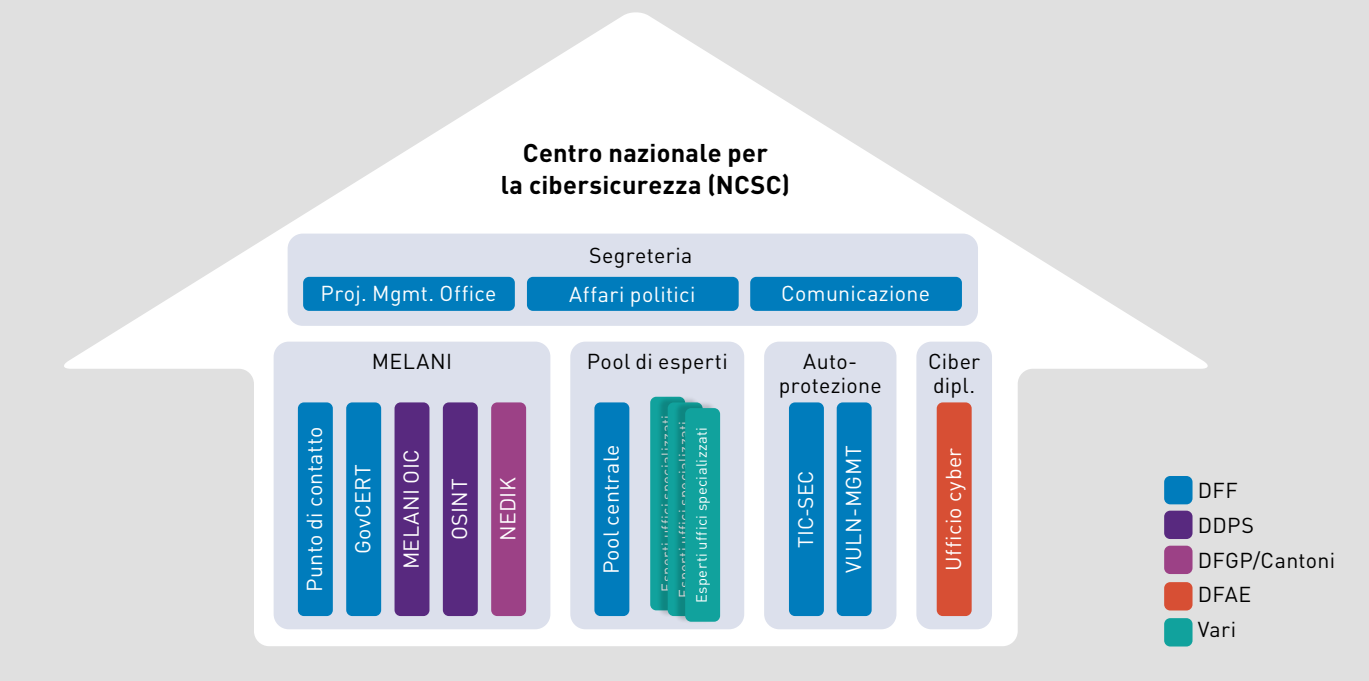
m.a.d.

Dominique Trachsel
lic.phil., MAS, MSc FCCI, responsabile della sensibilizzazione e della prevenzione del NCSC.

Sensibilizzazione e prevenzione in seno al NCSC

Siamo tutti responsabili della cibersicurezza. Uno dei compiti del NCSC è quindi quello di informare in modo mirato la popolazione sui ciber-rischi per sensibilizzarla ai pericoli nel ciberspazio. A tale fine, il NCSC lavora a stretto contatto con servizi interni ed esterni all'amministrazione federale per elaborare indicazioni sulle misure preventive da adottare e fornire a chi è diventato vittima di un crimine informatico raccomandazioni sul modo di reagire. Di conseguenza, il NCSC sostiene la settimana di sensibilizzazione

1 Art. 12, lett. h, Ordinanza contro i ciber-rischi



Fonte: NCSC

nazionale promossa dalla Prevenzione Svizzera della Criminalità (PSC), che mira ad illustrare a un vasto pubblico le misure concrete per muoversi in tutta sicurezza nel mondo virtuale. Questa settimana di sensibilizzazione è finanziata e organizzata in partenariato dalla piattaforma indipendente "eBanking – ma sicuro!" della Scuola universitaria professionale di Lucerna, dalla Swiss Internet Security Alliance (SISA/iBarry), dalla PSC e dal NCSC.

Organizzazione del NCSC

Il NCSC è suddiviso in vari settori e comprende la segreteria, la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), un pool di esperti, l'autoprotezione e la ciberdiplomazia.

La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), creata nel 2004, è stata integrata nel NCSC con il servizio tecnico Computer Emergency Response Team (GovCERT) ed è stata ampliata ulteriormente. Da allora si occupa del coordinamento insieme al servizio informazioni della Confederazione e al servizio di perseguimento penale per garantire il flusso di informazioni sulle minacce attuali. Anche questo servizio specializzato nazionale è integrato in questo settore. Riceve le segnalazioni sui ciberincidenti della popolazione e del settore economico, li analizza e dà a chi li ha segnalati una valutazione dell'incidente e raccomandazioni per il seguito della procedura.

Inoltre, il NCSC mette a disposizione un pool di esperti per fornire un supporto ai vari attori specializzati nello sviluppo e nell'attuazione degli standard di cibersicurezza. Questo pool si occupa anche del settore "Sensibilizzazione e prevenzione".

Nell'ambito dell'autoprotezione dell'amministrazione federale, il NCSC emette direttive sulla cibersicurezza, ne verifica l'osservanza e supporta i fornitori di servizi nell'eliminazione delle vulnerabilità. Sempre a livello federale, il "Vulnerability Management" sviluppa processi e strumenti ausiliari e pubblica anche rapporti sulle vulnerabilità informatiche identificate.

Infine, il cyberufficio del Dipartimento federale degli affari esteri (DFAE) assicura la cooperazione e il coordinamento con la politica estera svizzera.

Altre informazioni: ncsc.admin.ch

Swiss Internet Security Alliance: un'associazione senza scopo di lucro per proteggere dai pericoli di Internet

La Swiss Internet Security Alliance (SISA) riunisce rappresentanti dell'economia e delle autorità. Obiettivo: gestire congiuntamente la cyberprevenzione. Con il sito ibarry.ch, la SISA mette a disposizione uno strumento completo dedicato alla cyberprevenzione che possono raccomandare anche i corpi di polizia nell'ambito delle loro attività di prevenzione.

La Svizzera deve diventare il Paese con la rete internet più sicura del mondo

La Swiss Internet Security Alliance, o SISA in breve, è stata istituita nel 2014 da rinomati rappresentanti dell'economia con il coinvolgimento dei principali provider di Internet in Svizzera. Questi ultimi hanno accettato di non farsi concorrenza quando si tratta di proteggere la popolazione dai pericoli di Internet e della sua utilizzazione. Rendere la Svizzera il Paese con la rete internet più sicura del mondo è sempre stata la missione dichiarata della SISA. Di conseguenza, il suo scopo è di rendere attenta la popolazione ai rischi che rappresentano le vulnerabilità dei loro dispositivi collegati a Internet, di fornirle soluzioni a questi problemi e di sensibilizzarla ai potenziali pericoli. In breve, la SISA fa cyberprevenzione.

Autore

m.a.d.

Daniel Nussbaumer è presidente della Swiss Internet Security Alliance dal 2019. In precedenza, è stato per quattro anni capo della cybercriminalità presso la Polizia cantonale zurighese e ha diretto la rete intercantonale di polizia NEDIK, responsabile a livello nazionale del sostegno alle indagini nella lotta contro la criminalità informatica.

La cyberprevenzione è un lavoro impegnativo: sfruttiamo le sinergie!

La cyberprevenzione è un lavoro impegnativo. Creare e diffondere campagne di prevenzione, sviluppare siti web ed effettuarne la manutenzione, o anche preparare e tenere relazioni su questo tema richiede tante risorse. Molte aziende e autorità ne sono consapevoli, ma hanno regolarmente difficoltà ad ottenerle, tenuto conto del contesto globale dei loro obiettivi aziendali.

Eppure, il volume della cybercriminalità è stimato in circa 600 miliardi di dollari all'anno. Questo significa che i crimini informatici generano più soldi del commercio mondiale di droga. In altre parole: fare cyberprevenzione vuol dire per le autorità e gli ambienti economici lottare contro un'industria da 600 miliardi di dollari.

È quindi sensato sfruttare le sinergie in questo settore, per evitare di fare due o tre volte lo stesso il lavoro, e soprattutto per scambiarsi reciprocamente contenuti e prodotti sviluppati e – idealmente – per concepire congiuntamente strategie, campagne e homepage e attuarle coordinando gli sforzi.

Swiss Internet Security Alliance: un partenariato pubblico-privato

Oggi la SISA riunisce i rappresentanti non solo dell'economia, ma anche delle autorità e delle università. Come associazione senza scopo di lucro, la SISA offre quindi ai suoi membri e partner la possibilità di sviluppare e diffondere congiuntamente prodotti di prevenzione.

E la SISA lo fa essenzialmente in due modi. Da un lato incarica il suo comitato consultivo, in seno al quale vi sono i membri e partner dell'associazione, di stabilire i contenuti in materia di prevenzione. Dall'altro, la SISA stessa gestisce la piattaforma ibarry.ch che fornisce alla popolazione consigli utili su come comportarsi in Internet e suggerimenti concreti su tutti i fenomeni informatici attuali. Il sito contiene inoltre strumenti che i cittadini possono utilizzare gratuitamente per controllare in che misura il loro computer è protetto da attacchi informatici.

Il comitato consultivo

Il comitato consultivo è composto da specialisti in sensibilizzazione provenienti dagli organismi membri e partner della SISA. Si tratta di un gruppo di esperti che sviluppa congiuntamente contenuti in materia di prevenzione per organizzare campagne mirate. I rispettivi messaggi di prevenzione sono coordinati in modo che tutti i partner utilizzino le stesse formulazioni quando diffondono i messaggi di prevenzione.

Attualmente aderiscono al comitato consultivo rappresentanti di provider di servizi internet, istituti finanziari, autorità e università. In questo modo, il comitato consultivo assicura lo sviluppo congiunto di messaggi di prevenzione per il settore privato e il settore pubblico, e quindi anche il coordinamento degli sforzi in materia di prevenzione.

Dal canto suo, la stessa SISA lancia almeno ogni anno quattro campagne di sensibilizzazione elaborate dal comitato consultivo. In questo modo, la SISA contribuisce attivamente – coordinando gli sforzi di tutti i suoi partner – alla sensibilizzazione della popolazione.

ibarry.ch: una piattaforma per il lavoro di prevenzione svolto dai corpi di polizia

I cyberattacchi, che stanno diventando sempre più complessi e diversificati, sono diretti contro le persone e/o le vulnerabilità digitali. Sempre più spesso, però, i cybercriminali ritornano alla carica con metodi sempre nuovi che mirano ad ingannare le persone. Esempi tipici sono le e-mail con link o allegati che, se vengono cliccati o aperti per errore, possono portare all'installazione di malware sul computer, oppure le e-mail fraudolente sotto forma di truffa romantica (love scam) o truffa del CEO. Oltre a questi attacchi contro le persone, questi delinquenti sfruttano anche le vulnerabilità dei dispositivi digitali per introdursi nei vari apparecchi.

Tanto più gli attacchi informatici sono multiformi, quanto più è difficile proteggere la popolazione in modo mirato. Di conseguenza, anche le misure di prevenzione devono essere altrettanto diversificate. La loro elaborazione è quindi molto dispendiosa in termini di tempo e risorse.

Con il marchio ibarry.ch, la SISA ha lanciato nel 2019 un sito web completo dedicato alla cyberprevenzione che tratta tutti i temi informatici attuali e fornisce consigli concreti sul comportamento da adottare quando si usa Internet. Con la gestione di questo sito, che viene aggiornato costantemente e sottoposto a continua manutenzione, i membri della SISA finanziano una piattaforma di sensibilizzazione completa destinata alla popolazione svizzera. Questo permette di sollevare altre istituzioni dal dover investire individualmente risorse nello sviluppo di altri siti dedicati alla cyberprevenzione. Inoltre consente alle aziende private o alle istituzioni, come per esempio i corpi di polizia, di far riferimento a ibarry.ch invece di sviluppare un proprio materiale di prevenzione.

m.a.d.

Cooperazione nazionale: la campagna di maggio sulle “5 operazioni per la sicurezza digitale”

Oltre alle attività sopracitate, la SISA partecipa anche alla prossima campagna sulle “5 operazioni per la sicurezza digitale”, sviluppata congiuntamente da PSC, NCSC, SISA e EBAS e che sarà lanciata congiuntamente in maggio. Anche questa cooperazione è nata dalla considerazione che possiamo avere un maggiore impatto se gli ambienti economici e i poteri pubblici mettono in comune le loro risorse e agiscono insieme. Tutti noi – che si tratti di provider di servizi internet, istituti finanziari, università o autorità – abbiamo un interesse comune a sensibilizzare la popolazione ai pericoli di Internet e a fornirle consigli concreti sul comportamento da adottare quando si usa Internet. Attuando la campagna sulle “5 operazioni per la sicurezza digitale”, teniamo conto proprio di questo.

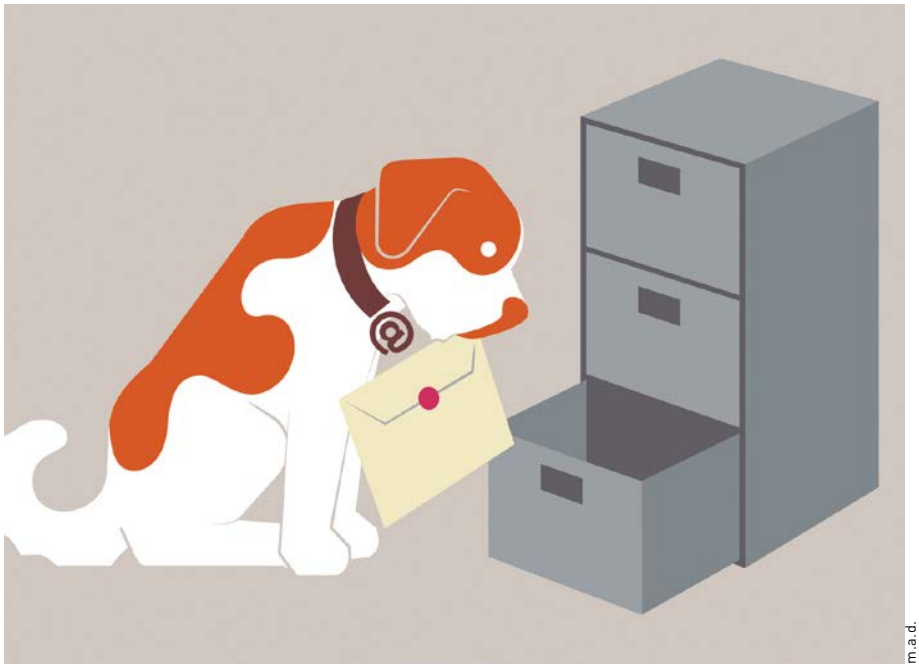
La missione dichiarata della SISA è di continuare a promuovere partenariati pubblico-privato e di portare avanti campagne nazionali congiunte anche in futuro. Lo scopo di queste campagne è di raggiungere e sensibilizzare il maggior numero possibile di cittadini per far sì che la Svizzera diventi un paese con una rete internet più sicura.

Diventate membri della SISA!

La SISA è felice di dare il benvenuto a nuovi membri e partner e offre in particolare ai corpi di polizia della Svizzera la possibilità di diventare gratuitamente partner dell’associazione. L’idea alla base di un tale partenariato è di sostenersi a vicenda e, soprattutto, di utilizzare e diffondere attivamente i prodotti della SISA, come il materiale di prevenzione di ibarry.ch. Diversi corpi di polizia della Svizzera stanno già approfittando di questa opportunità, ciò che permette loro di preservare le proprie risorse. Di conseguenza, non esitate a contattarci, preferibilmente su ibarry.ch (www.ibarry.ch → Chi siamo → Contatto).

iBarry.ch: il San Bernardo dal pelo bianco-arancio vi aiuterà a navigare in tutta sicurezza

È carino, curioso e rischia spesso di cadere nelle trappole dei truffatori online. In questo modo, iBarry – il simpatico cane San Bernardo online – riesce ad attirare l’attenzione su un tema che poche persone amano affrontare: i pericoli in Internet.



m.a.d.

iBarry ha tratti piuttosto umani nelle molte immagini che lo rappresentano, come in questa dove si fa riferimento al tema del backup dei dati. Di tanto in tanto, però, si comporta come un cane vero e proprio e abbaia quando fiuta il pericolo o annusa con curiosità qualcosa che lo attira.

Autrice

m.a.d.

Annette Hirschberg è responsabile della comunicazione e del marketing di iBarry presso la Swiss Internet Security Alliance dall’agosto 2019.

Si dice che Barry, il cane San Bernardo da valanghe, abbia salvato più di 40 vite all’inizio del XIX secolo. Ora, all’inizio del XXI secolo, iBarry, il suo successore virtuale, vuole seguire le sue tracce in Internet. Nel frattempo, il ruolo di questo cane virtuale è cambiato un po’. Dato che non può più rintracciare direttamente le persone e tirarle fuori dalla neve come lo faceva il suo predecessore,


m.a.d.

Riguardo alla sicurezza degli smartphone, iBarry gironzola curiosamente nel telefonino e annusa le icone delle applicazioni. Scaricare malware è uno dei pericoli ai quali ci si espone utilizzando dispositivi mobili.


m.a.d.

Il tema dello shopping online descrive come i truffatori cercano di ingannare le loro vittime. Si ricorre ad un esempio reale per mostrare come riconoscere i falsi shop.

iBarry dà ora il buon esempio ed esplora con entusiasmo le profondità di Internet per scoprirne le insidie. Ingenuo e credulone, si imbatte in ogni sorta di pericoli, senza tuttavia farsi fregare dai truffatori.

Regole semplici per una tecnologia complessa

iBarry incarna in qualche modo l'internauta medio. Un cane, anche un cane da ricerca e soccorso, non è molto ferrato in informatica e non sa un gran ché sui trucchi usati dai truffatori online. Grazie a questa caratterizzazione e al suo aspetto di cagnolone simpaticone, iBarry insegna che chiunque è in grado di riconoscere i pericoli in Internet. Questo cagnolone ha quindi il compito di facilitare l'uso dei dispositivi elettronici e la navigazione in rete in tutta sicurezza.

Questo è importante per sensibilizzare ai rischi di Internet. Oggi, praticamente tutta la popolazione – dai bambini della scuola dell'infanzia ai centenari – usa Internet per scrivere messaggi, fare shopping, cercare informazioni o chiacchierare. Nel contempo, però, in secondo piano si nasconde un mondo virtuale così complesso e difficile da capire che la maggior parte delle persone si sente impotente e in balia della tecnologia. Ecco perché sulla sua piattaforma di sicurezza in Internet, questo cane San Bernardo mostra alla popolazione, usando immagini simpatiche e un linguaggio semplice, che la sicurezza online non è poi così complicata.

iBarry sensibilizza la popolazione fornendo consigli chiari e semplici

All'inizio delle sue pagine informative, iBarry, il più delle volte, dà subito alcuni semplici consigli su vari temi, come la sicurezza dei dispositivi mobili. Rivolgendosi direttamente ai suoi lettori, formula cinque semplici regole per rendere più sicuro il proprio smartphone e quindi la navigazione:

1 **Bloccare il cellulare:** utilizziamo un potente sistema di blocco per proteggere l'accesso al nostro smartphone.
2 **Verificare le app:** installiamo solo app offerte dagli app store autorizzati e diamo il consenso soltanto allo stretto indispensabile.
3 **Installare gli aggiornamenti:** verifichiamo che per il software e le app siano disponibili aggiornamenti recenti e li installiamo il prima possibile.
4 **Chiamate, messaggi, occasioni online:** non ci facciamo ingannare e mettiamo in dubbio le offerte allettanti.
5 **Attenzione al Wi-Fi pubblico:** siamo consapevoli che utilizzando il Wi-Fi pubblico tutte le nostre attività in internet sono visibili a terzi.

Coloro che vogliono saperne di più, possono informarsi in dettaglio leggendo poi i testi con spiegazioni più particolareggiate su come adottare un comportamento sicuro che si trovano sulla piattaforma.

Qui vi sono anche schermate che illustrano esempi reali per spiegare come riconoscere shop falsi online o e-mail di phishing. L'intento è di aiutare gli internauti ad acquisire competenze in materia. Più si è informati, meno si correrà il rischio di diventare una vittima dei truffatori online.

Divertirsi facendo test per aumentare la sicurezza in rete

Il sito è diviso in tre sezioni denominate "Dispositivi sicuri", "Navigare in sicurezza" e "Rischi di Internet". Vi si trovano pagine informative sui temi più importanti relativi alla sicurezza digitale, come la gestione dei dispositivi intelligenti (Internet of Things o Internet delle cose), la protezione dei dati sui media sociali o ancora il phishing e le truffe romantiche (Romance Scam.)

iBarry promuove un comportamento online sicuro non solo con pagine informative facili da capire. Ultimamente,

gli utenti possono verificare in modo ludico le loro competenze in Internet. Facendo un quiz sul tema della sicurezza delle password possono per esempio mettere alla prova le loro conoscenze sulle comuni regole di sicurezza per le password. Altri test seguiranno a breve sui temi della sicurezza degli smartphone, della protezione dei dati, della navigazione sicura e del phishing.

Tuttavia, vi sono test per verificare non solo le proprie conoscenze in materia, ma anche la propria infrastruttura. Su iBarry.ch si trovano diversi strumenti gratuiti per effettuare dei controlli di sicurezza:

- **lo strumento per controllare le e-mail** permette di verificare se il proprio indirizzo e-mail figura in una banca dati piratata;
- **lo strumento per controllare la rete** permette di verificare se negli ultimi giorni il proprio computer ha cercato di connettersi a un server noto per essere infetto;
- **lo strumento per rilevare i malware** scansiona il computer alla ricerca di virus, trojan e worm.
- **lo strumento per controllare il software** verifica se ci sono falle di sicurezza sul computer.

Anche nella sezione dei controlli di sicurezza è inoltre previsto di aggiungere altri test di controllo utili.

La SISA sta attualmente elaborando anche un flyer da distribuire nell'ambito di eventi informativi. A breve, lo si potrà ordinare e, se lo si desidera, potrà anche essere corredato del proprio logo.

L'ambizioso obiettivo della Swiss Internet Security Alliance (SISA), l'associazione che gestisce iBarry.ch, è di fare della Svizzera il Paese con la rete internet più sicura del mondo con l'aiuto del cane San Bernardo dal pelo bianco-arancio. A tal fine, la piattaforma di sicurezza in Internet deve diventare il *sito di prevenzione per la sicurezza in Internet della Svizzera.* Già oggi, numerose autorità e aziende fanno riferimento a iBarry.ch. La SISA accoglie con favore qualsiasi ulteriore impegno che sostenga questo obiettivo.

Altre informazioni: ibarry.ch

La cybercriminalità è un tema che riguarda tutti noi

Oggi, quasi nessun altro settore criminale presenta sfide tanto grandi e complesse quanto la cybercriminalità per le autorità di perseguimento penale. Per questo motivo è ancora più importante coniugare misure preventive e repressive e lavoro in rete. Ci vuole infatti una stretta cooperazione fra i vari partner coinvolti per combattere efficacemente la criminalità informatica.

Nessuno è al riparo dai cyberattacchi: oltre alle persone private, anche le aziende piccole e grandi, le istituzioni o le autorità amministrative ne sono ripetutamente vittime. Vista la crescente complessità dei metodi d'attacco e la professionalizzazione degli aggressori, diventa sempre più difficile agire efficacemente contro i cybercriminali o addirittura identificarli. Data la situazione e a causa del numero crescente di casi, la prevenzione nel settore informatico è oggi di centrale importanza.

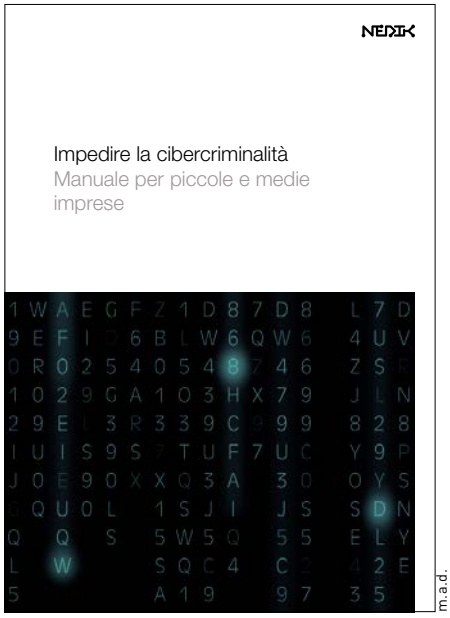
Con il suo lavoro di sensibilizzazione, la Polizia cantonale bernese mira a raggiungere anche chi finora non si è sentito colpito da questa forma di criminalità. Oggi, Internet permea quasi tutti i settori della vita ed è usato dai più diversi attori. E le minacce in quest'ambito possono addirittura nasconderne altre. Per esempio, un presunto consulente per gli investimenti ("truffa sugli investimenti") può allo stesso tempo intrappolare la sua vittima in una relazione amorosa fraudolenta ("truffa romantica"), causandole così diversi danni contemporaneamente. Un altro esempio, a riprova della complessità delle sfide: alcune aziende sensibilizzano certo i propri dipendenti ai pericoli informatici ma nel contempo non si dotano delle necessarie misure tecniche e organizzative per proteggersi. Senza la combinazione di tutti i provvedimenti del caso, tali aziende difficilmente avranno una possibilità di difendersi dai cybercriminali organizzati o dai professionisti del pirataggio informatico.

Per combattere la cybercriminalità e fare un buon lavoro di prevenzione è quindi fondamentale adottare un approccio globale per quanto riguarda sia i temi da affrontare che le misure da mettere in atto. L'obiettivo a lungo termine è di radicare saldamente nelle

Autrice


m.a.d.

Fernanda Gurzeler lavora come collaboratrice scientifica in materia di prevenzione per il centro di competenza "Progetti e Cyber" della Polizia cantonale bernese.



m.a.d.

Le pubblicazioni "Guida per i Comuni" (www4.ti.ch → Polizia cantonale → Prevenzione → Documentazione Crimini informatici → Prevenire la cybercriminalità – Guida per i Comuni) e "Manuale per piccole e medie imprese" (... → 1. NEDIK – Manuale per le piccole e medie imprese) sono state concepite in collaborazione con diversi partner.

coscienze non solo i molti vantaggi offerti dai media digitali, ma anche i rischi e le sfide tecniche che questi comportano. In considerazione della diversità degli attori – persone private, autorità, aziende, associazioni o università – è quindi imperativo cooperare non solo tra autorità giudiziarie ma con altri partner.

Cooperazione a livello nazionale

Un esempio di questa cooperazione è il materiale informativo elaborato per le PMI e per i comuni nell'ambito della rete di polizia NEDIK (vedere riquadro). Dato il numero crescente di casi e i grandi danni finanziari che questi causano, diversi corpi di polizia svizzeri hanno espresso la necessità di sensibilizzare le piccole e medie imprese alla prevenzione dei cyberreati. Anche le amministrazioni comunali hanno chiesto di disporre di maggiori informazioni in materia. Uno degli obiettivi che la polizia auspica raggiungere è anche quello di incoraggiare le vittime a collaborare con le autorità di perseguimento penale. Basandosi su varie ricerche emerge infatti che molte vittime non contattano la polizia in caso di danno, o lo fanno solo molto più avanti nel tempo.

In stretta collaborazione con il Centro nazionale per la cibersicurezza (NCSC), la Polizia cantonale zurighese, la Rete integrata Svizzera per la sicurezza (RSS), l'Ufficio federale per l'approvvigionamento economico del Paese (UFAE), l'Amt für Informatik und Organisation des Kantons Bern (KAIO) (Ufficio per l'informatica e l'organizzazione del Cantone di Berna) e i rappresentanti dei rispettivi gruppi destinatari, la Polizia cantonale bernese ha coordinato la raccolta di informazioni sulle esigenze e l'analisi della situazione reale. Questo lavoro ha permesso di riunire preziosi dati molto utili per preparare i vari documenti informativi. Perché tutti lo sanno: esistono certo molti documenti e consigli in materia, ma l'importante è utilizzarli e metter in pratica le raccomandazioni fornite. Per questo motivo, era chiaro fin dall'inizio che oltre ai documenti era necessario elaborare altri strumenti. Durante i vari scambi fra i diversi corpi di polizia è ben presto nata l'idea di elaborare delle modelli di conferenze su questo tema e di tenere un corso di formazione in materia destinato agli agenti di polizia. Su mandato della NEDIK nell'ambito della cyber-strategia nazionale 2018–2022, la Polizia cantonale bernese partecipa inoltre a eCyAd, un progetto nazionale di eLearning. Lo scopo di questo progetto è di sensibilizzare i circa 400 000 impiegati delle amministrazioni pubbliche in Svizzera.

Le misure sopracitate sono attuate di concerto con quelle della Prevenzione Svizzera della Criminalità (PSC) e sono destinate a completarle. Oltre a produrre materiale di sensibilizzazione, la PSC coordina anche altre misure

NEDIK

Su mandato della Conferenza dei comandanti delle polizie cantonali della Svizzera (CCPCS), i corpi di polizia della Svizzera hanno istituito la **Rete nazionale di sostegno alle indagini nella lotta contro la criminalità informatica** (NEDIK). L'obiettivo della NEDIK è di promuovere la cooperazione tra i corpi di polizia svizzeri nel settore della cybercriminalità. Questa rete permette di riunire per quanto possibile le capacità e le competenze dei corpi di polizia cantonali e di coordinare le azioni e le indagini volte a combattere i crimini informatici in modo più mirato, anche a livello intercantonale. Grazie allo scambio di informazioni nella rete, si coordinano le misure repressive, si scambiano conoscenze specialistiche e si adattano i corsi di formazione di base e continua. Nell'ambito della NEDIK, inoltre, si promuove e si coordina la cooperazione nel settore della pedocriminalità a livello intercantonale non solo tramite il monitoraggio peer-to-peer, bensì anche svolgendo indagini in incognito in assenza di sospetti nel cyberspazio.

a livello nazionale. Nel 2019, per esempio, in collaborazione con i corpi di polizia della Svizzera romanda, la PSC ha lanciato la campagna *"E lei? Avrebbe detto di sì?"* incentrata sui vari aspetti delle cybertruffe. Quest'anno, la campagna si focalizza sul sexting, sulle truffe sugli investimenti, sulle truffe immobiliari e sul phishing. Tra il 3 e il 7 maggio verrà inoltre lanciata una campagna di sensibilizzazione sulla cybersicurezza che nel giro di cinque giorni si prefigge di far conoscere meglio alla popolazione le cinque operazioni importanti per migliorare la propria sicurezza digitale.

Uno sguardo al lavoro di prevenzione cantonale

Oltre a svolgere questo lavoro di coordinamento a livello nazionale, la Polizia cantonale bernese, come molti altri corpi di polizia, è sempre più sollecitata dalle enormi sfide poste dalla cybercriminalità. Nel Canton Berna, la stragrande maggioranza dei crimini informatici rientra nella categoria della criminalità economica come le truffe delle inserzioni pubblicitarie, il phishing, i vari malware o le truffe sugli investimenti. Per poter reagire rapidamente in quest'ambito, è essenziale che la polizia intensifichi le misure preventive quali informazioni sui propri siti web, giochi online, webinar o brevi filmati esplicativi che illustrano alla popolazione i rispettivi modi operandi dei truffatori online. Anche in questo caso, la cooperazione con i vari attori del settore privato, dell'amministrazione e della formazione è di centrale importanza. Appena possibile, si dovrebbe anche curare di nuovo il contatto diretto con la popolazione organizzando, oltre a manifestazioni destinate ad un vasto pubblico, anche conferenze e workshop per gruppi destinatari specifici, come i rappresentanti delle PMI o dei comuni.

Dato che aziende e comuni manifestano un grande interesse per conferenze sulla cybercriminalità e su come proteggersi da questi reati, è importante in quest'ambito integrare esempi reali tratti dal lavoro quotidiano della polizia e fornire consigli concreti su come proteggersi da questi atti criminali. Anche lo scambio reciproco dopo le conferenze costituisce una parte importante di questo lavoro di prevenzione, poiché i partecipanti possono condividere le loro conoscenze ed esperienze reciproche.

La prevenzione in materia di cybersicurezza si rivolge anche a bambini e giovani, così come agli insegnanti. È vero che le competenze multimediali fanno già ampiamente parte dei piani di studio, e alcune organizzazioni e aziende propongono già moduli complementari in materia. Tuttavia, ci sono delle lacune, in particolare per quanto riguarda il quadro giuridico o l'aggiornamento dei rischi. Questo aspetto è diventato evidente anche di recente durante una lezione a distanza, quando ospiti indesiderati si sono intromessi disturbando la classe virtuale. Grazie ad una rapida azione di sensibilizzazione lanciata su vari canali, è stato possibile diffondere efficacemente le informazioni necessarie al riguardo.

A partire dall'anno scolastico 2021/2022, inoltre, il Canton Berna proporrà un corso di formazione generale sul tema "media digitali" a partire dalla 1ª media. Oltre alle visite personali nelle scuole, questo progetto comprende anche materiali didattici specifici disponibili online. Nell'estate 2020, per esempio, sul sito della Polizia cantonale bernese è stato pubblico un quiz destinato ai giovani sul tema del sexting e del cyberbullismo. Anche questo progetto è stato realizzato in collaborazione con la magistratura dei minorenni, gli insegnanti e le direzioni scolastiche. D'altronde, questo tipo di offerte è in piena espansione e viene attualmente elaborato e coordinato grazie allo scambio con altre organizzazioni.

Le esperienze fatte finora mostrano che la cooperazione interna ed esterna nell'ambito del lavoro di prevenzione, e specialmente nel caso della cybercriminalità, è estremamente utile perché i diversi partner coinvolti nell'elaborazione di soluzioni possono apportare il loro contributo grazie alle loro innumerevoli considerazioni e riflessioni al riguardo. È proprio nell'ambito della cooperazione con partner in seno ai corpi di polizia che importanti informazioni provenienti dal campo investigativo confluiscono nei progetti di prevenzione e contribuiscono così a migliorare la qualità dei prodotti. In definitiva, tutte le misure elaborate mirano non solo a sensibilizzare il maggior numero possibile di cittadini, allievi, dipendenti di aziende e comuni e a metterli in guardia dalla cybercriminalità, ma anche di diffondere in modo coerente e professionale le varie misure di protezione elaborate in comune.

123RF/Elnur Amikishiyev

L'ammontare dei danni causati dai cyberdelitti può essere notevole.

“L’importante è attirare l’attenzione e suscitare l’interesse.”

Intervista a Denise Nick, direttrice, e a Manuel Specker, consulente senior dell’agenzia Partner & Partner (Winterthur) su strategia, difficoltà e sfide della campagna di prevenzione “Sicurezza digitale”.

Denise Nick

Manuel Specker

m.a.d.

Attualmente state realizzando una campagna il cui obiettivo è aiutare i cittadini a migliorare la loro sicurezza digitale, mandato affidatovi da polizia, Confederazione e rappresentanti del mondo economico. Con un argomento così arido, dovete quindi far passare un messaggio e tenere conto di molte esigenze diverse. Cosa prevale: l’entusiasmo o lo sgomento?

Denise Nick (DN): Chiaramente l’entusiasmo. Non è raro che diverse organizzazioni partecipino ad un tale progetto. Ma è sempre emozionante vedere come collaborano fra di loro, come si suddividono i ruoli, gli iter decisionali, i processi. Secondo noi, inoltre, la sicurezza digitale non è un argomento arido. Astratto, sì, perché potrebbe non essere così familiare. È vero, noi tutti usiamo questi dispositivi, e ancora di più in questo periodo in cui prevale il telelavoro. Ma siamo prevalentemente semplici utenti con poca dimestichezza in materia di sicurezza digitale.

Manuel Specker (MS): È inoltre alquanto interessante vedere come un buon coordinamento fa la differenza quando sono coinvolte così tante organizzazioni. Con relativamente pochi mezzi, si può essere presenti su molti canali. Questa condizione offre un enorme potenziale per raggiungere molte persone. Normalmente, per avere una tale quantità di destinatari si devono impiegare mezzi considerevoli.

Ci sono restrizioni alla realizzazione di una campagna quando è la polizia ad affidarvi il mandato?

DN: No. La sicurezza digitale non è un argomento trattato specificatamente dalla polizia. Per quanto riguarda lo stile e il tono, occorre certamente mantenere una certa serietà, ma non è nulla di straordinario.

Come procedete per realizzare una campagna?

DN: Si inizia con il leggere, leggere molto …

MS: All’inizio è sempre importante farsi un’idea dell’effetto e degli obiettivi che si vogliono raggiungere. Poi, si confronta il tutto con la situazione attuale per determinare quanto è già noto. A questo punto, si delineano piano piano i principi di base della campagna. Qui si tratta di definire chi raggiungere attraverso quali canali e come questi ultimi interagiscono. Ci chiediamo dove si trova il punto di convergenza tra un tema e il suo destinatario, come fornire ulteriori informazioni e a quale momento lanciare la campagna. Si tratta inoltre di stabilire quali contenuti trasmettere, e in particolare quale linguaggio e tono utilizzare, aspetto importante soprattutto nel caso di una campagna di prevenzione. Bisogna trovare il giusto mix per raggiungere l’obiettivo. Insieme al committente, si affronta poi la questione di come veicolare e visualizzare i messaggi.

DN: La fase di ricerca iniziale è estremamente importante per un tema come questo. Esiste già un’enorme quantità di riflessioni, scritti e pubblicazioni realizzati da varie istituzioni. Non ha senso reinventare i contenuti. Prima, però, abbiamo dovuto preparare il terreno per creare una base accurata e selezionare l’essenziale.

Sarebbe stato più facile elaborare voi stessi i contenuti?

DN: No, la nostra posizione di partenza è buona. Dato che i contenuti sono già noti, possiamo concentrarci completamente sul modo di veicolare il messaggio.

A cosa si deve fare attenzione in questo frangente?

DN: I contenuti devono essere facili da capire e suscitare l’interesse. Si tratta di affrontare il tema e informarsi senza però esagerare e avere la sensazione che la materia sia complicata e si stia prendendo la direzione sbagliata.

E come procedete?

MS: Sapendo che il tema è importante, possiamo già partire dal presupposto che la popolazione possieda certe conoscenze di base in materia e che non si dovranno fornire molti chiarimenti. La sfida consiste nel trasmettere le istruzioni in modo tale da consentire all’utente di memorizzare facilmente i singoli passi. Così facendo, infondiamo la fiducia necessaria che l’obiettivo può

essere raggiunto rapidamente e agevolmente, predisponendo così l'utente a mettere effettivamente in pratica le conoscenze acquisite. Il trucco sta nel non dare l'impressione di salire in cattedra, né nell'annoiare, ma nel far sì che si impari ad aiutare se stessi.

DN: È come per gli altri temi di prevenzione. Vogliamo ottenere un cambiamento di comportamento nelle persone. Tutto questo va bene, ma occorre dapprima preparare il terreno in modo da rendere possibile questo cambiamento. Per questa campagna abbiamo quindi previsto di creare una pagina di destinazione, dove si descrive in modo semplice e comprensibile ciò che si deve fare, su cui l'utente arriva dopo aver cliccato su un link. Qui, le persone interessate trovano rapidamente le informazioni desiderate.

Come fate a convincere il pubblico destinatario dei vantaggi di cambiare comportamento?

DN: Ricorriamo ad analogie presenti nella vita quotidiana, cioè paragoniamo cose note con il mondo digitale. Questo è l'elemento chiave della campagna e dei temi da divulgare. Presentiamo situazioni in cui di solito ci si protegge e poi applichiamo il comportamento adottato alla sicurezza digitale, senza puntare il dito, ma piuttosto facendo leva sull'umorismo o sull'effetto sorpresa.

Che ruolo svolge appunto l'umorismo in campagne del genere?

MS: È importante trovare un equilibrio tra la serietà e la comicità di un argomento. Se si vuole solo essere divertenti, si corre il rischio di non prendere il tema con sufficiente serietà. È quindi da evitare. Questa campagna tratta il tema della sicurezza. Bisogna quindi veicolarlo con una certa serietà.

Cosa si deve assolutamente evitare in una campagna di prevenzione?

DN: Ci sono delle regole di base. Nel frattempo sappiamo che minacciare è alquanto controproducente. Per responsabilizzare le persone e fare in modo che agiscano, si deve evitare di creare allarmismo e far leva sulla paura.

Vi è mai capitato di dover scartare un progetto perché vi siete resi conto che l'approccio scelto non funziona?

DN: Questo capita probabilmente per ogni processo, non appena si inizia a pensare al "come". Definiamo di volta in volta diverse vie da seguire, diversi approcci per la realizzazione. Succede spesso di non arrivare da nessuna parte o di rendersi conto che una delle vie scelte non è praticabile. A volte si finisce per scegliere una via imprevista che ha invece il potenziale necessario. Bisogna solo mettersi in moto. All'inizio abbiamo davanti a noi tutti i tasselli del mosaico – la situazione di partenza, la definizione dell'obiettivo, il briefing, la grafica e il testo – poi poco a poco appare il quadro complessivo.

Recentemente avete presentato le immagini della campagna. Naturalmente ci sono state discussioni, anche se avevamo già scelto la via da seguire. Il percorso che porta al mosaico finito è ovviamente irto di ostacoli...

DN: È sempre eccitante vedere cosa succede quando si fa una prima proposta. Alcune persone la guardano e dicono: "Sì, capisco di cosa si tratta, ci sta bene". Altri hanno invece un approccio più scientifico ed esigono che tutto sia chiaro e senza ambiguità. Per noi, questo di solito è un arricchimento, come nel vostro caso, perché ci rendiamo conto delle differenze con cui si può percepire un'immagine. Ad un certo punto, però, arriva il momento in cui si deve decidere, in cui si deve smettere di prendere in considerazione tutte le opinioni e scendere a compromessi. Altrimenti questo va a scapito del messaggio che si vuole veicolare. A furia di voler essere corretti, l'immagine finisce per non essere più ben capita dal pubblico destinatario. L'importante è attirare l'attenzione e suscitare l'interesse. Il lavoro di approfondimento permette poi di definire con precisione tutti i dettagli che saranno minuziosamente corretti, ma durante il primo contatto bisogna a volte anche lasciar correre e fare a meno di concetti complicati.

La campagna si focalizza principalmente sui media sociali. Questo è compatibile con la polizia?

DN: I media sociali sono il canale ideale per stabilire il contatto con la popolazione e avvicinarsi alla gente. Lo vediamo qui a Winterthur. La polizia comunale usa i media sociali con dimestichezza e la sua presenza su TikTok è notevole. Questo approccio è in sintonia con la nuova generazione. I nativi digitali difficilmente leggono i volantini. Non si accorgerebbero nemmeno dell'esistenza di molti argomenti con cui invece vengono in contatto grazie ai media sociali. Questi canali permettono di trasmettere i temi con rapidità e in piccole quantità. I media sociali consentono alla polizia di dare un'immagine di se stessa completamente diversa. Se non si è toccati da un problema, si hanno pochi contatti con la polizia. Quindi non ci si rende assolutamente conto che è molto più disponibile e aperta di quanto pensi.

Per cosa è più sulle spine in vista della "Settimana di sensibilizzazione" di maggio?

DN: Una cosa mi interessa moltissimo: disponete di una rete enorme con moltissimi moltiplicatori. È fantastico quando si possono attivare così tanti canali. Ma bisogna anche orchestrare il tutto. In definitiva, questa è la sfida posta dalla campagna. Tutti devono contribuire e fare la cosa giusta al momento giusto. Questo richiede una buona organizzazione e informazioni intelligibili, in modo che sia chiaro per tutti quale materiale è disponibile dove e quando, e come verrà utilizzato. Una sfida non certo semplice da affrontare, ma è quello che ci piace.

Signora Nick, signor Specker, grazie mille per l'istruttiva intervista!

(Intervista a cura di Beatrice Kübli)

Nuovi membri in seno alle commissioni

Hanno rassegnato le loro dimissioni dalle commissioni della PSC quattro persone sostituite da quattro nuovi membri.

Commissione di esperti

Da tempo membro impegnato in seno alla Commissione di esperti della PSC, Bruno Lüthi – autorevole esperto in materia di sicurezza integrale, sicurezza amministrativa e protezione antieffrazione (e molto altro ancora!) – ha lasciato la Commissione di esperti per raggiunti limiti d'età in quanto andrà in pensione. Ringraziamo sentitamente Bruno per il know-how messoci a disposizione e il suo dinamismo di cui abbiamo approfittato per molti anni. A lui e al FC Thun facciamo inoltre i nostri migliori auguri per un futuro da trascorrere ancora più intensamente insieme!

Commissione di progetto

Purtroppo, la Commissione di progetto ha dovuto accomiatarsi da Kasi Bischoff, in quanto è stato chiamato ad assolvere altre mansioni in seno alla Polizia comunale di Winterthur. Per oltre quattro anni, Kasi ha rappresentato i corpi delle polizie comunali nella Commissione di progetto, la quale è stata felice di avere al suo interno il rappresentante di un corpo di polizia comunale così moderno e innovativo come quello di Winterthur. Ringraziamo vivamente Kasi Bischoff per i suoi suggerimenti sempre benvenuti, la sua partecipazione costruttiva, senza dimenticare il suo costante buon umore, e gli auguriamo tutto il meglio nella sua nuova funzione!

E siamo lieti di dare un cordiale benvenuto a **Thomas Egloff,** nuovo membro in seno alla Commissione del progetto. Anche Thomas rappresenterà i corpi delle polizie comunali, e siamo sicuri che non mancherà di portare molti suggerimenti e idee utili provenienti dalla Polizia comunale di Winterthur. Benvenuto Signor Egloff!

Abbiamo anche dovuto prendere congedo da Roland Hübner della POLCANT di Appenzello Interno che rappresentava il concordato Ostpol per la polizia criminale. Roland è stato con noi per molti anni, e per conto del suo piccolo corpo di polizia ha rappresentato con fervore e grande spirito d'iniziativa tutta la Svizzera orientale. Auguriamo a Roland tutto il meglio per il suo nuovo percorso professionale e lo ringraziamo per la sua sempre gradita collaborazione!

Il concordato Ostpol sarà ora rappresentato da **Stephan Kühne,** capo della polizia criminale della POLCANT sangallese. Diamo un cordiale benvenuto a Stephan Kühne in seno alla Commissione di progetto, felici di poter contare su questo fattivo sostegno proveniente dall'Est!

Infine, ma non per questo meno importante, Stefan Grieder, ex capo della polizia criminale della POLCANT svittese, si è dimesso dalla sua funzione di rappresentante del Concordato della Svizzera centrale, poiché assumerà il comando della POLCANT nidvaldese in primavera 2021. Ci congratuliamo vivamente con Stefan per la sua nuova funzione e per questa nuova sfida, e lo ringraziamo vivamente per il suo impegno pluriennale e la sua collaborazione costruttiva in seno alla CP!

Siamo lieti di dare il benvenuto a **Jürg Wobmann,** capo della polizia criminale della POLCANT lucernese, in seno alla Commissione di progetto in veste di nuovo rappresentante della polizia criminale della Svizzera centrale! Ci rallegriamo sin d'ora di continuare l'eccellente rapporto di collaborazione con le POLCANT nel cuore della Svizzera.


m.a.d.

Markus Friedli, responsabile del reparto Consulenza e Progetti della POLCANT bernese


m.a.d.

Cap. Thomas Egloff, MLaw, Capodivisione


m.a.d.

Stephan Kühne, capo della polizia criminale della POLCANT sangallese


m.a.d.

Jürg Wobmann, capo della polizia criminale della POLCANT lucernese

Bruno Lüthi sarà sostituito da **Markus Friedli,** a cui siamo lieti di dare il più cordiale benvenuto nella Commissione di esperti!

Markus Friedli, responsabile del reparto Consulenza e Progetti della POLCANT bernese, non è affatto un novellino in materia di prevenzione, in quanto si dedica da anni alla protezione antieffrazione e alla prevenzione della criminalità anche in molti altri settori. Siamo lieti che Markus Friedli condivida le sue conoscenze specialistiche con i membri della Commissione di esperti!

Il paradosso della prevenzione...

... potrebbe essere riassunto così: meglio funziona, più si potrebbe credere, erroneamente, che non sia affatto necessaria. Perché i danni che dovrebbe impedire non si verificano effettivamente, e spesso la minaccia non è né visibile, né tangibile. I montanari, invece, temono ciò che *potrebbe* accadere se non si fossero costruiti i paravalanghe che li proteggono. E lo temono anche quando sono ben ancorati: o perché sono stati testimoni dell'ultima valanga, o perché conoscono i racconti di tali catastrofi e hanno ogni giorno davanti agli occhi la montagna innevata, cioè la minaccia. Neppure una persona che passeggia in riva al lago in una sera d'estate, circondata da migliaia di zanzare ma senza essere punta una sola volta, non metterebbe mai in dubbio l'effetto preventivo del suo spray antizanzare, specialmente se *ogni* volta che *non* lo aveva messo era stata punta. I danni subiti ci aprono gli occhi: riconoscere la minaccia significa riconoscere il valore della prevenzione.

Là fuori, tuttavia, sono numerose le nuove minacce non facilmente riconoscibili, di fronte alle quali non si può attingere dalle proprie esperienze personali o familiari, come nel caso di una pandemia. Per disporre di una prevenzione efficace, bisogna in questo caso basarsi su informazioni che si trovano al di fuori del proprio bagaglio di esperienze. Rapidamente emerge allora un altro paradosso della prevenzione: quanto più sono io stesso vulnerabile perché faccio parte di un gruppo a rischio e dunque di una minoranza, tanto più approfitto degli sforzi di prevenzione messi in atto dalla collettività, mentre la maggioranza meno vulnerabile ne beneficia solo molto indirettamente e forse a lungo termine. Inoltre quest'ultima subisce soprattutto le restrizioni apportate al suo stile di vita abituale di cui soffre. Queste sono brutte notizie per la maggior parte delle persone, motivo per cui molti sono inclini a minimizzare o addirittura a negare la minaccia, considerando i messaggeri come uccelli del malaugurio. D'altro canto, se si venisse d'improvviso colpiti duramente dal virus, a chi ci si vorrebbe rivolgere: a "verità24.ch" o a un vero e proprio ospedale?

Per quanto riguarda la cybercriminalità, il tema di questo numero di INFO PSC, è ancora tutta un'altra una storia. La maggior parte delle persone non conosce veramente le varie minacce di cui stiamo parlando. Ma non appena le conoscenze in materia si diffonderanno rapidamente e su larga scala e si organizzeranno corsi formazione al riguardo, la prevenzione andrà a vantaggio di tutti, senza paradossi. Ne beneficeranno le persone private perché sapranno individuare le trappole che i truffatori tendono in Internet ed evitare così di perdere i loro averi. E ne approfitterà anche l'intera economia, perché da un lato saprà difendersi dagli attacchi informatici diretti e, dall'altro, potrà continuare a contare sulla stabilità finanziaria dei suoi clienti e partner, anch'essi in grado di difendersi. In questo caso, proteggere il singolo significa anche protegge la collettività, e viceversa.

Infine, un ultimo esempio di paradosso della prevenzione, ossia il cambiamento climatico. Contrariamente alle valanghe, alle pandemie e alle zanzare, probabilmente non sarà proprio possibile in questo caso aspettare che si verifichino dei danni per poter ottenere dati empirici affidabili e quindi sviluppare misure preventive efficaci per il futuro. Si dovrebbe piuttosto evitare che accada qualcosa che non si è mai visto prima. Ci sono molte evidenze che indicano che incombe una catastrofe, ma non ci sono prove. Per la prima volta, si dovrebbe tornare alla ragione non per via dei *danni subiti,* ma *utilizzando la ragione.* Si può ipotizzare che si stia ancora festeggiando sul ponte superiore del transatlantico, mentre l'iceberg (l'ultimo?) ha già squarciato lo scafo. Dovremo però aspettare per vedere se questo è vero. Citiamo in questa sede la celebre frase di un capo indiano del popolo dei Cree: "Solo dopo che l'ultimo albero sarà stato abbattuto. Solo dopo che l'ultimo fiume sarà stato avvelenato. Solo dopo che l'ultimo pesce sarà stato catturato. Soltanto allora scoprirai che il denaro non si mangia." Fino ad allora: indossare la mascherina, proteggersi dai virus, e quando il telefono squilla... non rispondere!

Volker Wienecke
Contatto: redaktion@skppsc.ch

“Non si faccia ricattare!” Tutto ciò che dovreste sapere sulla sextortion

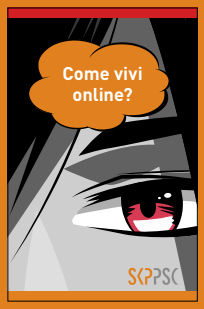
È veramente terribile il momento in cui le persone realizzano di essere ricattate con immagini o video intimi. I cosiddetti casi di sextortion possono assumere varie forme. Possono verificarsi in seguito ad una conversazione a sfondo erotico in una chat o arrivare come spam nella propria casella di posta elettronica. Entrambi i modi operandi sfruttano il fatto che le vittime vogliono evitare la pubblicazione di immagini o video compromettenti (presumibilmente) esistenti o il loro invio ad amici e conoscenti. Motivo per cui pagano un riscatto. In entrambi i casi, tuttavia, il messaggio di prevenzione è chiaro: *Keep calm and don't pay!*

“Rendimenti da sogno? No, perdite da incubo!”

Tutto ciò che dovreste sapere sulle truffe sugli investimenti online

Sempre più spesso, i truffatori e le truffatrici pubblicizzano nuove forme d'investimento apparentemente lucrative sulle loro presunte piattaforme d'investimenti o sui loro siti di trading online. Ma chi investe su questi siti, ha solo da perderci! Il nuovo opuscolo della PSC spiega in modo comprensibile come avvengono tipicamente le truffe sugli investimenti online, come ci si dovrebbe informare prima di investire per esempio in criptovalute e cosa si dovrebbe fare se si è già perso denaro investendo su questi siti falsi. L'opuscolo contiene inoltre consigli generali su come capire per tempo se un'offerta è seria o molto probabilmente fraudolenta. L'opuscolo è stato prodotto grazie al prezioso contributo di EBAS (“eBanking – ma sicuro!”).

“Come vivi online?”



Il mini-pieghevole in formato carta di credito informa i giovani in modo breve e conciso su come comportarsi in Internet e come reagire a comportamenti scorretti e irrispettosi. Il mini pieghevole completa la serie Safebook, con i suoi opuscoli approfonditi, destinata a giovani, genitori ed educatori.

Le tre pubblicazioni si trovano all'indirizzo seguente: www.skppsc.ch → Download → Opuscoli + pieghevoli

LA CRIMINALITÀ CON UN TOCCO DI COMICITÀ

Per portare un po' di leggerezza nel contesto spesso opprimente e triste della lotta alla criminalità, in futuro vorremmo pubblicare un piccolo contributo umoristico (delle nostre lettrici e dei nostri lettori!) nel nostro bollettino INFO PSC. Potrebbe trattarsi di una poesia, un aneddoto tratto dalla vita quotidiana della polizia, una barzelletta o una vignetta sul tema. Chi si sente interpellato, non esiti a dare libero sfogo alla sua creatività e ad inviare la sua proposta a info@skppsc.ch!

“Cybercriminalità”, di Mario Capitanio, Berna

SKPPSC

Prevenzione Svizzera della Criminalità
Casa dei Cantoni
Speichergasse 6
Casella postale
CH-3001 Berna

www.skppsc.ch