Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF
Centro nazionale per la cibersicurezza NCSC

eBanking ma sicuro!
Lucerne University of Applied Sciences and Arts
HOCHSCHULE LUZERN
FH Zentralschweiz

iBarry

SKPPSC
Schweizerische Kriminalprävention
Prévention Suisse de la Criminalité
Prevenzione Svizzera della Criminalità

Ihre POLIZEI
Votre POLICE
La vostra POLIZIA
Kantonale und Städtische Polizeikorps
Corps de police cantonaux et municipaux
Corpi di polizia cantonali e comunali

Comunicato stampa, 26 aprile 2021

Settimana nazionale di sensibilizzazione per una maggiore sicurezza digitale

Negli ultimi anni le segnalazioni di ciberincidenti in Svizzera sono aumentate nettamente (fig. 1). La settimana nazionale di sensibilizzazione alla sicurezza digitale, che si terrà dal 3 al 7 maggio 2021, punta ad accendere i riflettori sui pericoli e a spiegare come proteggersi. L'iniziativa è sostenuta da importanti partner tra cui figurano autorità e attori del mondo scientifico ed economico.

Come nel resto del mondo, anche in Svizzera il coronavirus ha accelerato la diffusione della digitalizzazione: molti lavorano da casa, effettuano un maggior numero di acquisti online o approfittano più spesso delle offerte digitali. Di conseguenza, aumentano le possibilità di trovarsi confrontati con ciberincidenti, ma vi è anche maggiore consapevolezza. Le segnalazioni alla polizia e al Centro nazionale per la cibersicurezza (NCSC) sono così aumentate, stabilizzandosi a un livello più alto. A crescere sono stati soprattutto i casi di frode e di phishing (fig. 2): durante la pandemia, date le maggiori vendite tramite i siti di e-commerce, si sono registrati soprattutto casi di phishing concernenti la presunta consegna di pacchi. Sul fronte delle truffe, invece, sono comparsi casi di false donazioni per le vittime del coronavirus o di ordini di mascherine fasulli.

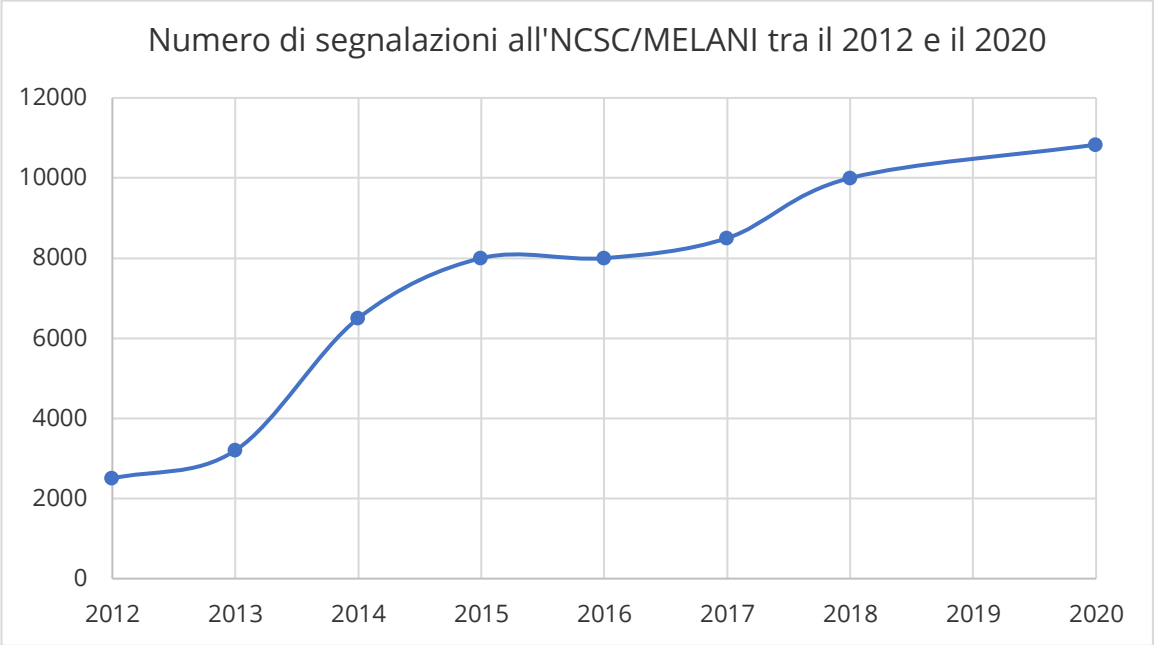

Figura 1: aumento del numero di segnalazioni di ciberattacchi all'NCSC nel periodo 2012–2020. Copyright: NCSC, 2021

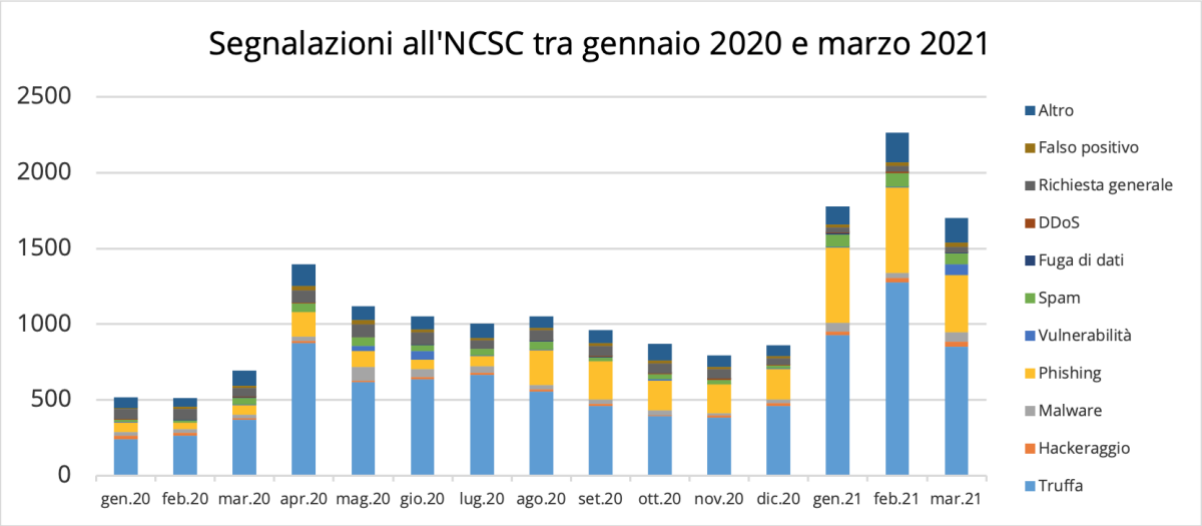

Figura 2: numero di segnalazioni di ciberattacchi all'NCSC 2020/2021. Copyright: NCSC, 2021

Settimana nazionale di sensibilizzazione con partner importanti

L'obiettivo della settimana nazionale di sensibilizzazione è quello di attirare l'attenzione su questo argomento. Allo stesso tempo, però, si vuole anche mostrare che, con alcuni semplici strumenti e piccoli accorgimenti, è possibile aumentare notevolmente la propria sicurezza online (ad es. password forti, aggiornamento regolare dei software e cautela nello spazio digitale).

L'iniziativa è promossa dalla Prevenzione Svizzera della Criminalità (PSC) in collaborazione con l'NCSC, la piattaforma «eBanking – ma sicuro!» della Scuola universitaria professionale di Lucerna (HSLU), la piattaforma per la sicurezza informatica iBarry di Swiss Internet Security Alliance (SISA) nonché i corpi di polizia di Cantoni e città.

La campagna di sensibilizzazione si svolgerà dal 3 al 7 maggio 2021 e sarà accompagnata da iniziative su diversi canali online e offline. Nella stessa settimana (giovedì 6 maggio) ricorrerà anche la giornata mondiale della password. La campagna sarà sostenuta dalle testimonianze di personalità note del mondo economico e politico.

L'elemento centrale della campagna è il sito web www.S-U-P-E-R.ch, che offre consigli e suggerimenti concernenti la sicurezza dei dati, gli aggiornamenti di sicurezza, la protezione dai virus, le password e il comportamento corretto sul web. Presenta anche una panoramica dei rischi nello spazio digitale, insieme a misure preventive da adottare e norme di comportamento. Vi sarà inoltre la possibilità di partecipare a webinar gratuiti su vari temi.

Cinque temi principali legati alla cibersicurezza in un'unica parola

Nel corso della settimana di sensibilizzazione, ogni giorno sarà dedicato a un tema. Le iniziali dei vari temi compongono la parola chiave «S-U-P-E-R», che aiuterà gli internauti a ricordare rapidamente come navigare in modo sicuro:

- **S per Salvare** – lunedì 3 maggio 2021
  Salvate regolarmente i vostri dati su almeno due supporti.
- **U per Usare** – martedì 4 maggio 2021
  Aggiornate regolarmente il sistema operativo, i programmi e le app all'ultima versione disponibile.

- **P per Proteggere** – mercoledì 5 maggio 2021
  Assicuratevi che sul vostro dispositivo sia installato un programma antivirus costantemente aggiornato.
- **E per Elaborare** – giovedì 6 maggio 2021
  Eseguite l'accesso ai siti web utilizzando esclusivamente password forti.
- **R per Ridurre** – venerdì 7 maggio 2021
  Riducete il rischio di truffe nello spazio digitale agendo sempre con un po' di sana diffidenza.

La prevenzione è lo strumento più efficace

«Individuare i casi di cibercriminalità è difficile e spesso non porta a grandi risultati». Per questo Fabian Ilg, esperto di cibercriminalità e direttore della PSC, è convinto che «una campagna simile aiuti a fare in modo che questi incidenti non avvengano».

Anche se le segnalazioni di ciberincidenti sono in aumento, il numero dei casi non denunciati rimane elevato. «Segnalare gli attacchi è importante, perché in questo modo si aiuta l'NCSC a valutare più rapidamente la situazione, riconoscere tempestivamente le nuove tendenze e adottare misure di contrasto», afferma Florian Schütz, delegato federale alla cibersicurezza e direttore dell'NCSC. Daniel Nussbaumer, presidente della SISA, aggiunge: «con questa settimana di sensibilizzazione vogliamo attirare l'attenzione dei media e della popolazione su questo tema, perché la prevenzione è lo strumento più efficace.»

I ciberattacchi possono essere di vari tipi: i malviventi si infiltrano ad esempio nei computer o negli smartphone per compiere atti illegali all'insaputa dei proprietari oppure per entrare in possesso e abusare di informazioni personali, dati delle carte di credito e credenziali di accesso, o ancora per usurpare l'identità dei malcapitati. «Ai pirati informatici non manca la fantasia, sono esperti e spesso organizzati a livello internazionale», afferma Fabian Ilg, «è quindi importante mettere in guardia la popolazione sui rischi e fornire loro supporto e informazioni al riguardo, perché proteggersi da questi attacchi in realtà è davvero semplice.»

Maggiori informazioni

www.S-U-P-E-R.ch

Materiale illustrativo

Cliccare qui per scaricare il materiale illustrativo*

Partner organizzativi

Prevenzione Svizzera della Criminalità
«eBanking – ma sicuro!» – una piattaforma indipendente della Scuola universitaria di Lucerna
Centro nazionale per la cibersicurezza NCSC
iBarry – La piattaforma per la sicurezza in Internet

Contatto per domande generali da parte dei media

Fabian Ilg, direttore della Prevenzione Svizzera della Criminalità (PSC)
Casa dei Cantoni
Speichergasse 6
3001 Berna
e-mail: fi@skppsc.ch
Tel.: +41 31 511 00 08

* Il materiale illustrativo non può essere modificato e l'uso è consentito solo per il resoconto della settimana di sensibilizzazione.

Contatti (in ordine alfabetico)

Le persone indicate di seguito sono a disposizione per domande e interviste sui temi indicati ai fini del resoconto della settimana di sensibilizzazione.

Marcus Beyer
Security Awareness Officer di Swisscom (Svizzera) SA
- Sicurezza informatica
- Cyber security awareness
- Ciber-resilienza nelle imprese

e-mail: marcus.beyer@swisscom.com
Tel.: +41 58 221 12 18 / +41 79 307 81 33

Andreas Hölzli
Direttore del Centro di competenza Cyber Risk di Mobiliare Svizzera Società d'assicurazioni SA
- Ciberassicurazione per privati, PMI e imprese
- Ciberattacchi contro PMI

Persona di contatto: Jürg Thalmann, portavoce
e-mail: media@mobiliar.ch
Assente dal 30.4 al 7.5.2021

Chantal Billaud
Vicedirettrice della Prevenzione Svizzera della Criminalità (PSC)
- Criminologia e psicologia
- Meccanismi di truffa in ambito informatico

e-mail: cb@skppsc.ch
Tel.: +41 31 511 00 09

Fabian Ilg
Direttore della Prevenzione Svizzera della Criminalità (PSC)
- Prevenzione in ambito di cibersicurezza
- Fenomeni di cibercriminalità

e-mail: fi@skppsc.ch
Tel.: +41 31 511 00 08

Ivan Bütler
Fondatore e presidente del CdA di Compass Security
- Hackeraggio etico ed esempi in Svizzera/presso aziende svizzere
- L'avanzata dei ciber-rischi

e-mail: ivan.buetler@compass-security.com
Tel.: +41 79 250 06 28

Centro nazionale per la cibersicurezza (NCSC)
- Cifre e fatti del Servizio nazionale di contatto dell'NCSC
- Attacchi malware
- Cosa fare in caso di attacco o di sospetto
- Cosa ci riserva il futuro?

e-mail: ncsc-media@gs-efd.admin.ch

André Duvillard (parla tedesco e francese)
Delegato della Rete integrata Svizzera per la sicurezza (RSS)
- Politica svizzera in ambito di sicurezza
- Collaborazione tra i responsabili della sicurezza in Svizzera
- Perseguimento penale e criminologia

e-mail: andre.duvillard@gs-vbs.admin.ch
Tel.: +41 58 464 21 13

Dr. iur. Daniel Nussbaumer
Capo della cibersicurezza presso T-Systems e presidente della Swiss Internet Security Alliance
- Cibercriminalità e prevenzione
- Rischi e opportunità della digitalizzazione

e-mail: daniel@swiss-internet-security-alliance.ch
Tel.: +41 79 672 32 05

Ten Serdar Günal Rütsche
Capo della divisione Cybercrime presso la polizia cantonale di Zurigo e direttore di NEDIK (rete di supporto digitale alle indagini sulla criminalità informatica)
- Criminalità digitale e cibercriminalità

e-mail: gus@kapo.zh.ch
Tel.: +41 44 247 22 00, assente dal 19 al 23.4.2021

lic. iur. Stephan Walder
Sostituto procuratore capo, Ministero pubblico II, del Cantone ZH, cibercriminalità
- Perseguimento penale e situazione giuridica

e-mail: stephan.walder@ji.zh.ch
Tel.: +41 44 247 31 40

Oliver Hirschi
Docente di sicurezza informatica e direttore della piattaforma «eBanking – ma sicuro!», Scuola universitaria professionale di Lucerna (HSLU)
- Attacchi di forza bruta inclusa demo live
- Perizie su password, e-banking e furti d'identità
- Furti d'identità

e-mail: oliver.hirschi@hslu.ch
Tel.: +41 41 757 68 58

Anonimo
- Vittima di una truffa tramite annunci

e-mail: medien@skppsc.ch
Tel.: +41 52 269 16 64 (Sig.ra Honegger)
Assente dal 5 al 15.5.2021

Brevi interviste e dichiarazioni

Le presenti interviste possono essere utilizzate solo per il resoconto della settimana di sensibilizzazione. Per utilizzarle in altri contesti o apportare modifiche alle dichiarazioni è necessario contattare le persone interessate.

Situazione generale: «La cibersicurezza è sempre più importante»

Florian Schütz, delegato federale alla cibersicurezza, direttore dell'NCSC

Perché con l'emergenza COVID-19 vi è stato un aumento delle segnalazioni?
L'NCSC ha rilevato un sensibile aumento delle segnalazioni, ma il numero effettivo di ciberattacchi è cresciuto solo lievemente. Dal nostro punto di vista, quindi, l'aumento delle segnalazioni è dovuto alla maggiore sensibilità di aziende e privati. Abbiamo però constatato che spesso gli attacchi fanno riferimento alla pandemia.

Quali sono al momento le minacce più frequenti?
Seguiamo sempre con attenzione i tipi di minacce più frequenti, anche perché la situazione può cambiare molto velocemente. Esistono svariati tipi di minacce, ma tra queste il phishing è una delle più note e, in un certo senso, un classico. In questo caso i criminali cercano di ottenere dalle vittime informazioni personali, come password o dati della carta di credito, inviando e-mail o SMS falsi. Questi messaggi possono sembrare molto professionali e spesso non sono immediatamente riconoscibili.

Cosa si dovrebbe fare se si è vittima di un attacco o si ha un sospetto?
Dipende dal tipo di attacco, ma in generale l'importante è agire il più in fretta possibile per evitare ulteriori danni, ad esempio bloccando la carta di credito o informando altre potenziali vittime. Inoltre, bisognerebbe segnalare il caso al Centro nazionale per la cibersicurezza (NCSC) e, se la vittima ha subito danni finanziari, sporgere denuncia presso le autorità di polizia competenti.

Che ruolo svolge la cibersicurezza in Svizzera?
La crescente digitalizzazione ha portato in primo piano anche la cibersicurezza. A livello federale ha un ruolo centrale nella politica estera e nella politica in materia di sicurezza e sta diventando sempre più rilevante anche per la piazza economica e la popolazione svizzera.

Tema della prevenzione: «Più siamo informati, minori sono le possibilità di successo dei pirati informatici.»

Daniel Nussbaumer, presidente della Swiss Internet Security Alliance (SISA) con la piattaforma per la prevenzione iBarry.ch

Perché le autorità e l'economia puntano tanto sulla prevenzione nel ciberspazio?
La persecuzione penale nel ciberspazio è aumentata sensibilmente. Si riesce sempre più spesso e sempre meglio a chiamare i colpevoli a rispondere delle proprie azioni. Dal momento, però, che i responsabili dei reati digitali sono sparsi in tutto il mondo e la persecuzione penale a livello internazionale è complessa e non sempre possibile per la mancanza di accordi, è importante che la popolazione sia informata sui pericoli.

La prevenzione non riesce sempre a stare al passo dei malviventi?
Vi sono tanti tipi di malviventi. Alcuni meno fantasiosi e altri che si inventano ogni volta nuovi stratagemmi per aggirare i controlli. Questi ultimi sono effettivamente più difficili da contrastare con la prevenzione. Per questo anche la prevenzione utilizza tecniche diverse: da un lato, spieghiamo quali sono i trucchi utilizzati dagli impostori, dalle false richieste di assistenza alla truffa dell'amore fino alle e-mail di phishing; dall'altro dimostriamo come, nonostante le storie raccontate dai criminali cambino, le tecniche con le quali cercano di ingannarci sono sempre simili, perché conoscono i nostri punti deboli.

Potrebbe essere più preciso?
Per prima cosa catturano l'interesse delle loro vittime tramite una richiesta di amicizia sui social media, un'e-mail, un messaggio, un annuncio, una telefonata o un finto ordine a un'azienda. Una volta ottenuta l'attenzione, cercano di impedire alle potenziali vittime di riflettere e fare i necessari accertamenti. Nella maggior parte dei casi per raggiungere questo scopo le mettono sotto pressione, ad esempio con e-mail, messaggi e chiamate, dando poco tempo o fornendo presunte prove per evitare che le vittime facciano delle verifiche.

La prevenzione quindi serve?
È sempre difficile dimostrare l'efficacia della prevenzione. Economia e autorità, però, hanno già investito molto nell'informazione e constatiamo che gli svizzeri sono sempre più consapevoli dei rischi presenti su Internet. Dobbiamo però sensibilizzarli ancora di più sul comportamento corretto da tenere sul web. Per questo abbiamo aderito anche alla campagna S-U-P-E-R.ch.

Tema Salvare: «Pensate al vostro smartphone.»
Fabian Ilg, direttore della PSC

La maggior parte delle persone sa che è necessario effettuare il backup dei propri dati su un supporto esterno, giusto?
È possibile, ma una cosa è la teoria, un'altra è la pratica. Secondo le nostre stime circa un terzo della popolazione svizzera non effettua il backup dei propri dati.

La perdita dei dati è davvero così frequente?
Pensate al vostro smartphone: può capitare di perderlo, che venga rubato o che si rompa. In questi casi, se non sono stati salvati altrove, i dati al suo interno andranno persi. Molti, però, se ne rendono conto soltanto quando si trovano in queste situazioni. E spesso è molto spiacevole.

Cosa bisognerebbe fare esattamente?
Sarebbe buona abitudine salvare regolarmente i propri dati su un disco rigido esterno o su cloud. Effettuare il backup dei dati su un disco esterno, però, può richiedere tempo e quindi scoraggia molte persone. Sui sistemi operativi più diffusi sono già installati programmi di backup molto semplici da usare che risolvono il problema. Su www.S-U-P-E-R.ch abbiamo raccolto le principali informazioni al riguardo.

Tema Usare gli aggiornamenti: «Il software non è perfetto.»

Ivan Bütler, fondatore di Compass Security

Perché gli aggiornamenti sono così importanti?
I software non sono perfetti e hanno sempre dei punti deboli. Gli aggiornamenti servono a risolvere questo problema. Chi non tiene aggiornati i propri dispositivi rischia quindi che queste vulnerabilità vengano sfruttate dagli hacker. I pirati informatici, infatti, sono sempre alla ricerca di falle di questo tipo e quando le trovano riescono molto facilmente a penetrare nei sistemi e a provocare danni.

In che misura l'hackeraggio attraverso software obsoleti è un problema per i privati?
Quando si parla di hackeraggio la minaccia più grande per i privati è l'estorsione: gli hacker accedono ai dati dall'esterno e li codificano, in modo tale che il proprietario non vi abbia più accesso. Dopo di che chiedono un riscatto in cambio dello sblocco dei dati. Spesso dopo il pagamento della somma richiesta ovviamente non succede niente, quindi si finisce per perdere sia i soldi che i dati.

Tema Proteggere: «È come a casa, bisogna chiudere le porte.»

André Duvillard, delegato della Rete integrata Svizzera per la sicurezza

Ormai tutti abbiamo installato dei programmi per proteggere i nostri dispositivi, giusto?
Purtroppo no: l'impressione è che il numero di utenti che hanno un antivirus stia diminuendo o, se non altro, che questo aspetto sia trascurato.

Come fanno esattamente i malware e i virus a penetrare un sistema?
È l'utente ad aprire le porte: se non ci si protegge, è sufficiente cliccare su un link o effettuare un download per far entrare nel sistema malware e virus. Le ripercussioni poi possono essere molto diverse: il sistema può ad esempio diventare molto lento o bloccarsi completamente. Gli hacker possono rubare dati o prendere il controllo del computer o dello smartphone.

Cosa si può fare concretamente?
È come a casa, bisogna chiudere le porte in modo che non entri nessuno. Sul computer possiamo farlo attraverso programmi specifici, ad esempio gli antivirus. Inoltre, è necessario controllare regolarmente se siamo stati «infettati» attraverso un'analisi del sistema. Sul sito web www.S-U-P-E-R.ch trovate una panoramica dei programmi di sicurezza disponibili per i diversi sistemi operativi. Non dimentichiamo che anche gli smartphone possono e devono essere protetti.

Tema Elaborare: «Non è necessario cambiare sempre le password.»

Oliver Hirschi, docente e direttore della piattaforma «eBanking – ma sicuro!» della Scuola universitaria professionale di Lucerna

Cosa rende una password sicura?
In generale l'obiettivo è fare in modo che un hacker non riesca a scoprire la password facilmente andando per tentativi. Quindi, più la password è lunga e complessa, minori saranno le sue probabilità di successo.

Come si fa a scegliere quella giusta?
La prima cosa da fare è scegliere una password forte e sul sito www.S-U-P-E-R.ch sono elencate le principali regole da seguire. In secondo luogo si dovrebbe avere una password diversa per ogni account. Così facendo non sarà necessario cambiare costantemente la password, come affermano spesso in molti. Inoltre si può fare ricorso ai cosiddetti password manager, alcuni dei quali sono presentati anche sul nostro sito web.

Quali rischi si corrono scegliendo una password debole?
Scoprire che ci hanno rubato la password di un servizio sul quale sono salvati i dati di un mezzo di pagamento può essere molto spiacevole, perché significa che gli hacker possono avere accesso a queste informazioni e farne un uso illecito. Oppure, se riescono ad avere accesso al dispositivo possono rubare dati o installare malware.

Tema Ridurre: «Tutti possiamo cadere in trappola.»

Chantal Billaud, vicedirettrice della PSC

Tutti possiamo essere vittime di un caso di truffa online?
Sì, anche se la maggior parte delle persone è convinta che non ci cascherebbe mai. Le segnalazioni di truffa che riceviamo ogni giorno non vengono mai da persone particolarmente ingenue o stupide. Le vittime appartengono a ceti sociali diversi.

Come si fa a cadere in trappola?
Tutti abbiamo dei momenti di debolezza in cui siamo particolarmente vulnerabili e abbiamo bisogno di approvazione, attenzione, intimità o semplicemente di denaro. I trucchi escogitati dai truffatori fanno sempre leva su uno di questi punti deboli. Quindi, adottando queste tecniche fraudolente su un elevato numero di potenziali vittime online, i criminali hanno maggiori possibilità di trovare qualcuno che cada in trappola. Se poi le vittime vengono messe sotto pressione facendo credere loro che l'offerta è limitata, la maggior parte rischia di cadere in trappola.

Come ci si può proteggere?
A volte è sufficiente essere informati: se sappiamo che sulla rete qualsiasi notizia può essere alterata e che spesso vengono diffuse informazioni false con l'intento di ingannare le persone, forse è più facile non credere ciecamente a tutto, ad esempio che un militare americano di stanza in Afghanistan voglia sposare proprio me. Una volta acquisita questa consapevolezza, i profili e le offerte vengono guardate con occhio critico. Possedere competenze circa l'utilizzo dei media e informarsi può quindi aiutare a proteggersi dalle truffe.