Fondazione "Città Solidale" Onlus

SENTIRSI SICURI ONLINE

Nel web si nascondono numerosi pericoli: i principali sono sicuramente il rischio di **truffa** e quello di **violazione della privacy**, ma ne esistono tanti altri che spesso non si considerano. Per questo motivo occorre innanzitutto informarsi bene sulle insidie della rete, poi bisogna prendere le dovute precauzioni e adottare dei comportamenti per un uso corretto e responsabile di internet.

Vediamo insieme quali sono i rischi e poi le strategie da adottare per proteggersi quando si naviga in rete.

Secondo le statistiche della Polizia, ormai un crimine su cinque viene commesso online. Si tratta, quindi, di veri e propri **reati penali** che è utile conoscere per non diventarne vittime.

Ecco quali sono i principali rischi che si corrono navigando online:

- **Phishing**: si tratta di un sistema che approfitta della vulnerabilità del tuo dispositivo per installare virus nascosti al fine di rubarti dati sensibili, come ad esempio PIN e altri dati personali. Il virus si installa aprendo mail dannose - spesso camuffate da comunicazioni provenienti da istituti bancari o simili - oppure cliccando su banner pubblicitari ingannevoli o siti pericolosi.
- **Truffe**: sempre cliccando su banner pubblicitari ingannevoli capita spesso anche di imbattersi in siti che richiedono dati personali all'utente per riscuotere un premio. Si tratta ovviamente di una truffa, reato di cui si può essere vittime anche su siti di e-commerce oppure anche attraverso annunci di privati. Succede spesso, ad esempio, nel settore dei viaggi, dove vengono venduti finti pacchetti vacanze o affittate case che non esistono.
- **Furti d'identità**: sono frequenti sui social network, dove alcune persone si impossessano dell'identità di qualcuno allo scopo di diffamarlo, denigrarlo o distribuire password o numeri di telefono. A volte le vittime sono personaggi pubblici la cui identità viene rubata per cercare di metterli in cattiva luce compiendo atti illeciti, come la pubblicazione di post compromettenti o ingiuriosi, screditando così il loro nome, oppure per ottenerne dei benefici.
- **Utenti pericolosi**: navigando in rete, utilizzando i social network e soprattutto le chat, ci si può imbattere in persone con cattive intenzioni come hacker, pedofili, maniaci o individui che fingono di essere qualcun altro con lo scopo di danneggiare in qualche modo la vittima di turno.
- Da non sottovalutare, in questo senso, è anche il pericolo di essere diffamati o di diventare vittime del **cyberbullismo**, fenomeno che interessa soprattutto i giovani: sui social network si può rischiare, infatti, che vengano pubblicate foto o video per ridicolizzarci e denigrarci, oppure può capitare che qualcuno, magari nascosto dietro a un nickname falso, ci insulti o riveli pubblicamente fatti o dati che ci riguardano, violando così la nostra privacy.

5 STRATEGIE PER DIFENDERSI SUL WEB

Abbiamo analizzato quali sono i principali pericoli del web. Vediamo adesso 5 strategie da adottare per difendersi da queste minacce e prevenire ogni possibile rischio.

1. **Installare un antivirus**

Per proteggersi da phishing e software malevoli il primo passo è quello di installare sul proprio computer un **antivirus valido e sempre aggiornato**. È opportuno, poi, navigare sempre in modalità protetta, disabilitando tutti quegli accessori del browser, come ad esempio i java script, che di solito vengono usati proprio per carpire informazioni e dati sensibili. Altri importanti accorgimenti da seguire sono: non aprire mai email provenienti da mittenti sconosciuti e comunque non cliccare mai sui link contenuti al loro interno.

Non fidatevi delle mail nelle quali compare il nome della vostra banca: in genere in questi messaggi viene chiesto di inserire i propri dati o i propri codici bancari per un problema riguardante il sistema di internet banking o per un aggiornamento dei vostri dati. Si tratta, appunto, di tentativi di phishing: le banche non inviano mai questo tipo di comunicazioni ai clienti via email, quindi non bisogna mai cliccare su link sospetti o fornire i propri dati.

2. Non fidarsi in chat

Quando si conosce una persona in una chat, ma anche attraverso applicazioni di messaggistica istantanea come **Skype**, **WhatsApp** e **Messenger**, bisogna fare attenzione a confidare cose personali, a rivelare i propri dati e anche a inviare proprie foto. Dall'altra parte dello schermo potrebbe nascondersi un truffatore o un malintenzionato che potrebbe utilizzare ciò che gli dite o inviate per scopi illeciti, incluso il diffondere le vostre foto in rete senza la vostra autorizzazione.

3. Attenzione a cosa si scarica

Quando si effettua il download di un programma o un file dal web bisogna stare sempre in guardia in quanto potrebbe trattarsi di **virus**, uno **spyware** o di un altro **software malevolo**. Inoltre, ogni volta che si condivide o si scarica qualcosa in rete bisogna considerare il problema del copyright: il materiale in questione, infatti, potrebbe appartenere a qualcuno che potrebbe rivendicarlo e chiederne i diritti.

4. Non condividere informazioni personali sui social network

Spesso, per rubare l'identità di qualcuno il ladro si serve proprio delle informazioni che la persona in questione ha già condiviso sui social. Più dati personali si pubblicano e più è alto il rischio di subire un furto d'identità. Bisogna dunque **evitare di inserire data di nascita, indirizzo, luogo di lavoro o scuola frequentata**. Inoltre, quando si pubblicano le proprie foto bisogna considerare che poi resteranno in rete e sarà molto difficile eliminarle o controllarle, e chiunque potrà scaricarle e usarle per creare un nuovo profilo fingendo di essere la persona della foto. Queste avvertenze valgono anche per i minori, che andrebbero controllati costantemente per evitare che forniscano dati personali a sconosciuti.

5. Sottoscrivere una polizza di tutela legale cyber

Stipulare un'assicurazione che copra le eventuali spese legali per difendersi dai reati commessi o subiti sul web è un ottimo metodo per tutelare sé stessi e la propria famiglia e per poter così navigare in rete con una protezione in più.