con la collaborazione di

SICURAMENTE ONLINE

Piccola Guida - Consigli utili per una navigazione sicura

PENSI CHE IL **PHISHING**

SIA SOLO UN TIPO DI PESCA?

PENSI CHE I **COOKIE**

SIANO SOLO BISCOTTI?

PENSI CHE UN **VIRUS**

SIA SOLO UN RAFFREDDORE?

Internet è una risorsa fondamentale per la nostra vita quotidiana, ci consente di accedere facilmente e rapidamente ad ogni tipo di informazione e semplifica molte operazioni, tra cui la comunicazione tra due o più persone.

E' fondamentale che tutti gli internauti sappiano navigare in modo sicuro e responsabile. Dalla tutela della sicurezza e della privacy al caricamento di contenuti inappropriati o illeciti, senza dimenticare le frodi online, le domande e i dubbi sulla navigazione sicura emergono soprattutto tra gli adulti, preoccupati per il modo in cui i loro figli affrontano queste problematiche.

Partendo dall'analisi della situazione attuale Adoc e Cittadinanzattiva, in collaborazione con Google, vogliono porsi come obiettivo quello salvaguardare l'utente/consumatore attraverso una iniziativa volta a informare e formare i consumatori all'utilizzo di strumenti e accortezze per una navigazione sicura e responsabile in Rete.

A tale scopo è stato predisposto un corso di formazione rivolto ad un target adulto, al fine di fornire delucidazioni e linee guida sulle buone pratiche da adottare per una navigazione sicura e consapevole.

PROTEGGI IL **DISPOSITIVO** CHE UTILIZZI PER ACCEDERE AD INTERNET

Che si tratti di un personal computer, di un tablet o di uno smart phone, è sempre buona prassi proteggere il dispositivo che utilizzi per accedere alla rete internet, in modo da salvaguardare i tuoi dati personali. L'accesso al tuo dispositivo può avvenire:

- **Da parte di persone fisiche**, facilmente individuabili (famigliari, colleghi di lavoro, addetti alle pulizie, ecc.) che potrebbero, legittimamente o non, avere accesso al tuo dispositivo.
- **Da parte di persone che accedono tramite la rete**, difficilmente identificabili.

A tale scopo esistono tanti accorgimenti e strumenti che puoi utilizzare per proteggerti dai rischi che la rete può celare, sfruttandone al meglio le opportunità, come ad esempio il blocco dello schermo o del dispositivo, quando non devi più utilizzarlo.

Si può predisporre anche il blocco automatico quando il dispositivo entra in stand-by, operazione che si rivela particolarmente importante per cellulari e tablet - che è più facile vengano smarriti e trovati da persone che non devono accedere alle informazioni personali - e i computer situati in spazi comuni.

I cellulari e i tablet offrono invece la possibilità di impostare il blocco tramite PIN o sequenza, in modo tale da proteggere ancora meglio i dati personali.

UTILIZZA GLI **STRUMENTI DI SICUREZZA** SUL BROWSER

Esistono diversi strumenti per proteggere le tue informazioni durante la navigazione online:

- **La navigazione in incognito**, che permette di non registrare le tue visite ai siti web o i tuoi download nelle cronologie di navigazione e dei download. Alcuni browser hanno questa opzione nel menu, altri invece richiedono la digitazione di una combinazione di tasti.

Alcuni browser permettono, inoltre, di creare un collegamento sul desktop per accedere al browser direttamente in incognito;

- **La gestione dei cookie,** per accettare solo alcuni cookie e respingerne altri, utilizza le impostazioni nel tuo browser (ad esempio Google Chrome, Internet Explorer o Mozilla Firefox).

Puoi anche utilizzare il browser per disabilitare completamente i cookie, tuttavia molti siti web non funzioneranno correttamente se decidi di farlo.

DIFENDITI DAI **MALWARE**

Per malware s'intende un programma software progettato per danneggiare intenzionalmente un computer o dispositivo mobile. I malware comportano un duplice rischio: il danneggiamento del dispositivo e dei dati in esso contenuti e la possibilità che qualcuno possa venire a conoscenza di informazioni riservate e addirittura utilizzarle fingendo di essere te (furto d'identità online). Pertanto è importante che tu sappia come puoi difenderti dai malware.

Per difenderti dai malware è utile adottare alcuni accorgimenti:
- **Aggiornamenti costanti** dei sistemi operativi, programmi software, browser, plug-in e antivirus che utilizzi, poiché a volte le versioni meno recenti hanno problemi di sicurezza su cui fanno leva i criminali informatici per avere facile accesso ai tuoi dati;
- **Attenzione ai contenuti che scarichi**:

• *Pop up:* costituiti da finestre che compaiono automaticamente durante la navigazione e che a volte inducono a installare software dannosi con l'inganno;

• *Script ActiveX e Applet Java:* estensioni, dette anche "componenti aggiuntive", che forniscono funzionalità accessorie durante la navigazione (ad es. animazione ed interattività all'interno di un sito web). Le proposte di installazione di queste estensioni devono essere ben valutate dall'utente, poiché possono essere fonti di rischio in quanto sono spesso usati per effettuare degli attacchi. Quindi l'utente, prima di mandarli in esecuzione, deve accertarsi di essere su un sito conosciuto, che faccia riferimento ad un marchio

importante. Talvolta tali script possono attivarsi anche involontariamente, quindi è utile prestare attenzione alla loro eventuale presenza in modo tale da disattivarli.

• *Plug-ins:* può capitare che, all'apertura di una pagina web, venga richiesta l'installazione di un plug-in che il dispositivo ancora non possiede. Prima di installarlo, è consigliabile assicurarsi che sia effettivamente necessario e che il sito che si sta usando per scaricarlo sia conosciuto, poiché anche questi software possono essere usati per attività malevole.

• *Programmi che scarichi:* prima di scaricare un programma si può verificarne la reputazione tramite lo store, è possibile consultare l'appstore integrato nel telefono o nel browser o il sito web dello sviluppatore. Si può così verificare anche la reputazione dello sviluppatore leggendo le opinioni di altri utenti. È utile cercare anche nella rete recensioni o commenti relativi al programma in questione. Se le informazioni raccolte sono negative sarebbe opportuno evitare il download.

In generale, è consigliabile non aprire file di tipo sconosciuto (inclusi gli allegati a mail di persone che non si conoscono o che sembrano strane!) e non seguire messaggi di avviso o di errore (i cosiddetti "prompt") che chiedono di aprire un file. Nel caso in cui un malware impedisca di uscire da una pagina, ad esempio aprendo più volte un messaggio di richiesta di download, può essere d'aiuto l'utilizzo dell'applicazione Task Manager o Monitoraggio Attività del computer per chiudere il browser.

- **Installare sul pc:**

• *un programma antivirus;*

• *un programma antispyware;*

• *un firewall personale sempre attivo.*

- **Tenere al sicuro i dati importanti che non vogliamo perdere**, impostando adeguatamente le opzioni di salvataggio e backup delle informazioni sulle unità di archiviazione interne ed esterne. E' importante tenere i dati separati dal sistema operativo e dai programmi, poiché, se in seguito ad un grave crash causato da un malware dovesse essere necessario formattare il disco e reinstal-

lare il sistema operativo, si può effettuare l'operazione senza il pericolo di perdere i dati, poiché questi ultimi si trovano su un altro disco fisso. Non è necessario avere materialmente due hard disk all'interno del pc: è sufficiente *partizionare* (suddividere) l'unico disco presente. Controlla se sul tuo dispositivo ci sono già due dischi fissi (molti sistemi vengono venduti con il disco fisso già suddiviso in due partizioni). Un'altra soluzione, altrettanto (se non più) sicura, è di salvare dati e documenti importanti all'interno di un sistema di cloud sicuro, al quale puoi accedere solamente attraverso una username e password sicura.

PROTEGGI LE TUE **PASSWORD**

La password è la chiave "virtuale" che ti permette di entrare negli account personali. È molto importante impostarla in modo tale che ad essa non si possa risalire facilmente, soprattutto quando questa permette l'accesso a dati personali o informazioni riservate e importanti.
La password deve essere:
- **facile da ricordare, difficile da indovinare**;
- **abbastanza lunga** (ad es. almeno 8-10 caratteri);
- **costituita da parole che non siano di uso comune**;
- **non costituita da dati facilmente reperibili** (ad es. data di nascita, numero di telefono, targa automobilistica);
- **preferibilmente alfanumerica**, con caratteri minuscoli e maiuscoli, numeri, simboli e segni di interpunzione;
- **diversa per ogni account**, per scongiurare il pericolo che, se malauguratamente scoperta, dia accesso a tutti gli account personali.

Inoltre, è buona prassi:
- **aggiornare regolarmente le password** degli account particolarmente importanti;
- **verificare**, se il servizio utilizzato lo permette, **tutti gli accessi** per controllare se sono tutti riconducibili ai tuoi ingressi o se ci sono accessi sospetti;
- **non comunicare le password tramite mail**;
- **diffidare di mail di servizi utilizzati** (ad es. banche, gestori mail, social network) che chiedono di inviare la password o rimandano a link nei quali inserirla;
- **disattivare l'opzione "ricorda password"** se utilizzi un computer che non è il tuo;
- **appuntare la password solo se necessario** e in modo tale che

sia riconoscibile solo da te, ad esempio salvandola sul telefono con il nominativo di una persona, anziché sotto la voce "password mail";
- **non inserire mai la tua password né i tuoi dati dopo aver cliccato su un link contenuto in un'email.** Accedi al sito direttamente dal web digitandone l'indirizzo;
- **non comunicare le password dei tuoi account personali** (mail, social network, ecc.) ad altri, compresi amici e parenti. Comunicare la tua password significa dare la possibilità a qualcuno di utilizzare i tuoi account in una maniera che potresti non approvare. Ad esempio, nel caso della mail o dei social network, chi vi accede potrebbe leggere i tuoi messaggi personali o spacciarsi per te.

È consigliabile configurare sempre le opzioni di recupero della password, fondamentali nel caso in cui venga dimenticata. I servizi offrono la possibilità di recuperarla tramite diverse modalità.

PROTEGGI GLI **ACCOUNT** PERSONALI

È molto importante proteggere gli account personali, in quanto un utilizzo da parte di terzi potrebbe comportare seri rischi, che potrebbero sfociare ad esempio nel furto d'identità. Per quanto concerne la sicurezza degli account personali, oltre ai consigli elencati nella sezione "Proteggi le tue password" è utile adottare alcuni accorgimenti:

- **Utilizzo di servizi crittografati:** è consigliabile usare servizi che supportino la *crittografia SSL* (protocollo che configura un percorso di comunicazione protetto tra computer). Se il servizio che stai utilizzando supporta la crittografia SSL, i dati inviati a e dal sito dovrebbero essere protetti dai malintenzionati. I servizi che utilizzi hanno questo servizio se l'indirizzo inizierà con *https* e nella barra in fondo al tuo browser comparirà una piccola icona di un lucchetto. La crittografia SSL è necessaria nelle pagine web con accesso ai dati personali come nome e cognome, indirizzo, codice fiscale, codice della carta di credito ecc. Esempi di pagine in cui è fondamentale questa funzione sono quelle delle banche con accesso all'area personale, siti di compravendita online, caselle di posta elettronica contenenti dati importanti. Prima di inserire i tuoi dati su un sito controlla sempre che la pagina web sia crittografata!
- **Connessioni sicure:** è sconsigliato accedere ad un account personale quando si è connessi a reti WiFi Pubbliche e libere. In particolare, sarebbe opportuno non digitare la password, in quanto non si può sapere se la rete utilizzata è sicura. Ci sono programmi chiamati "sniffer di rete" che vengono usati dagli hacker per intercettare il traffico di dati;
- **Attenzione ai siti fake:** il sito fake (dall'inglese "fake": "falso") è una pagina web finta, identica - per quanto riguarda la grafica e i contenuti - a quella di un sito originale, ma che ha piccolissime dif-

ferenze nell'indirizzo, come ad esempio un punto o una lettera (ad es. il sito fake di www.adoc.org potrebbe essere www.a.doc.org). Il sito fake viene utilizzato dai malintenzionati per rubare i dati dell'utente. I malintenzionati possono farti arrivare alla pagina fake tramite diverse strategie (attraverso un link inviato tramite mail o messaggi privati, ecc.).
Questa tecnica offre la possibilità di rubare le credenziali di accesso di ogni sito web che richieda l'autenticazione degli utenti attraverso username e password.
Alla luce di quanto detto è opportuno controllare sempre i siti che prevedono l'accesso all'area personale tramite password prima di inserire i dati: verifica che l'indirizzo sia scritto correttamente.
- **Attenzione alle truffe di phishing:** il Phishing è un tipo di truffa informatica finalizzata all'acquisizione, per scopi illegali, di dati riservati. Il phisher manda alle ipotetiche vittime email che sembrano provenire da siti commerciali o istituzioni come le Poste o la propria banca, nelle quali vengono richiesti dati personali. Il phisher può anche rimandare l'utente, tramite un link, a un sito fake, in cui gli si chiede di inserire i dati personali o le password per l'accesso all'area personale del sito falsificato.
In generale, bisogna diffidare sempre dalle comunicazioni da parte delle istituzioni via email, in quanto queste ultime non utilizzano tale mezzo per richiedere dati sensibili. *Quando si riceve una email che chiede dati personali, è sempre una truffa.*
Altri esempi di phishing sono:
- mail inviate dal gestore di posta elettronica utilizzato, che chiedono di rispondere inviando i tuoi dati personali o di accesso alla casella;
- mail che chiedono soldi con promesse di vincere grosse somme di denaro;
- mail che invitano a pagare qualcosa che non è mai stato comprato;
- mail recanti offerte di lavoro e/o di collaborazione da parte di società sconosciute.

In generale è bene:
- *non inviare mai dati personali* quali coordinate bancarie, password etc. via email;
- *non inserire mai la tua password dopo aver cliccato su un link contenuto in un'email.* Accedi al sito direttamente dal web digitandone l'indirizzo;
- *verificare che l'anti-virus blocchi i siti di phishing* o installare una barra degli strumenti del browser che segnali eventuali attacchi di phishing;
- *segnalare le frodi di phishing.* Quasi tutti i fornitori di servizi email consentono di segnalare episodi di phishing e mail sospette. La segnalazione bloccherà l'invio di altre mail da parte del mittente e consentirà ai team che si occupano dei comportamenti illeciti di fermare simili attacchi.

- Social network, social forum e blog: qualche attenzione in più. Particolare attenzione va poi posta ai social network, social forum e blog. Se da un lato offrono l'opportunità di creare reti sociali, condividere interessi e accrescere le proprie conoscenze, dall'altro celano dei rischi, tra questi la possibilità che qualcuno se ne appropri indebitamente.
Utilizza i social networks e similari con attenzione e responsabilità. In particolare:
• *imposta le opzioni per la privacy nel modo corretto;*
• *fai attenzione ai link ricevuti nei messaggi o nelle chat da parte di altri utenti: non sempre questi contenuti sono autentici!*
• *diffida di quegli applicativi che richiedono l'autorizzazione ad accedere ai tuoi dati personali e alla lista dei tuoi indirizzi mail;*
• *digita l'indirizzo del social network direttamente dal tuo browser o usa l'impostazione "preferiti" per evitare il phishing;*
• *ricorda che tutto ciò che viene pubblicato in un social network potrebbe rimanere per sempre su Internet, anche dopo la cancellazione del tuo profilo;*
• *Il mondo online è reale quanto lo è il mondo offline e su di esso valgono le stesse regole di rispetto e educazione. Comportati bene e richiedi che gli altri facciano altrettanto.*

- Casella di posta elettronica: qualche attenzione in più

• Difendersi da Spam - Mail Bombing

Lo spam consiste nell'utilizzo illecito di sistemi di messaggistica elettronica per l'invio indiscriminato di messaggi non richiesti dall'utente che li riceve. Di solito si tratta di mail commerciali e spesso pubblicizzano servizi e prodotti illegali. Altre volte invece, sono utilizzate per veicolare truffe attraverso attività di phishing.
Per proteggersi dallo spam è consigliabile:
- utilizzare le impostazioni di sicurezza della tua casella di posta per segnalare e mettere in "quarantena" le mail di spam;
- leggere prima di selezionare o deselezionare le opzioni relative all'invio di materiale pubblicitario o altre tipologie di aggiornamento, e verificare l'utilizzo delle tue informazioni sui termini e condizioni del servizio;
- per non confermare la correttezza e l'esistenza del tuo indirizzo email: non rispondere mai allo spam e stai attenti ai links che promettono di "cancellarti" a meno che non si conosca il sito: gli spammer usano spesso questi metodi per essere certi che la casella di posta sia ancora attiva. Non causerebbero, quindi, una cancellazione ma uno spam maggiore.

• Sicurezza degli allegati

Gli allegati alle email sono diventati uno strumento pratico ed efficiente per ricevere e inviare documenti. Purtroppo, però, essi sono spesso usati per veicolare malware.
Per tale motivo è consigliabile:
- usare molta cautela quando si aprono gli allegati, anche se sembrano provenire da una persona conosciuta. Se è possibile, contattare con altri mezzi coloro che hanno inviato l'allegato prima di aprirlo, la stessa cautela va usata per tutte quelle email che sembrano provenire dal tuo ISP o da società di software che dicono di avere in allegato patch o software antivirus, poiché gli ISP e le società non inviano patch o software via e-mail;
- non aprire gli allegati provenienti da indirizzi mail sconosciuti;
- effettuare sempre una scansione prima di aprire gli allegati, almeno per quelli provenienti da persone sconosciute.

PROTEGGI LA TUA **FAMIGLIA** ONLINE

La rete offre ai ragazzi tante opportunità, permette di accrescere le loro conoscenze, mantenere i contatti con gli amici vicini e lontani, conoscerne di nuovi. Accanto alle opportunità si celano, però, anche dei rischi, come la possibilità che i ragazzi siano esposti a contenuti non appropriati, o che diventino vittime di cyberbullismo, frodi o adescamento, o che si isolino dal mondo reale, rinchiudendosi in quello virtuale. Tali rischi possono essere arginati grazie alla supervisione di un adulto di riferimento e all'utilizzo di alcuni strumenti forniti dalla rete.
Per evitare che i ragazzi siano esposti a contenuti non adatti a loro è possibile adottare i seguenti accorgimenti:
- **Installare un filtro sul pc che controlla i contenuti del pc o di una rete specifica**, mostrando solo quelli consentiti in base alle impostazioni. Esistono diverse tipologie di filtri famiglia:
• *il filtro del browser o browser specializzati*
• *modello walled garden: la biblioteca di casa*
• *programma installato su PC che filtra i contenuti*
• *servizio fornito dall' ISP: il parental control*
• *i server DNS*
• *motori di ricerca con controllo dei contenuti*
Le tipologie di filtro elencate presuppongono che l'adulto abbia un po' di dimestichezza con le nuove tecnologie, poiché non tutti gli adulti li conoscono o sanno come installarli.
Se il filtro è sicuramente consigliato per quanto riguarda i più piccoli, va ponderato bene il tipo di utilizzo che se ne può fare se i ragazzi sono più grandi, poiché essi spesso hanno le competenze tecniche per "aggirarlo" e possono essere ulteriormente invogliati a farlo se il grado di rigidità del filtro è troppo elevato, in quanto impedisce di soddisfare quelle curiosità tipiche dell'età adolescen-

ziale. Un filtro troppo rigido, inoltre, potrebbe portarli a reperire le informazioni a cui sono interessati in maniera alternativa, utilizzando un pc senza filtri di un amico o connettendosi da un internet point, rendendo così impossibile la supervisione dell'adulto. Quindi è fondamentale adattare il filtro all'età del minore. Inoltre è consigliabile condividere con il minore la scelta di installare il filtro, spiegandogli le motivazioni e i vantaggi che ne conseguiranno.
È fondamentale tenere presente che il filtro non garantisce una protezione al 100%. Quindi si rivela utile affiancarlo ad altre strategie di protezione.

- Supervisionare la loro attività online e dialogare con loro per:

• responsabilizzarli nell'utilizzo della rete;
• aiutarlia sviluppare un senso critico nei confronti di ciò che vedono online;
• spiegargli i possibili rischi ai quali potrebbero essere esposti;
• incoraggiarli a segnalare eventuali contenuti che potrebbero turbarli.

Adescamento online

Molto spesso i minori mantengono online i contatti con persone che conoscono nella vita reale, ma può accadere che facciano amicizia con persone che non hanno mai visto. In quest'ultimo caso si può celare il rischio di "grooming" (dall'inglese grooms: "cura"), termine con il quale si indica l'adescamento online di un minore da parte di un adulto potenziale abusante, che avviene principalmente tramite le chat.
Per evitare che un minore incorra in tale rischio è importante:
- *informarlo* sul possibile pericolo, mettendolo in guardia su quanto sia facile creare una falsa identità online e la conseguente possibilità che chi è online non è detto che sia chi dice di essere;
- *controllare* il modo in cui utilizza la rete;
- *spiegargli i motivi* per i quali non deve mettere online o scambiare con persone conosciute in rete dati personali o foto, anche se si pensa che queste siano amiche e che ci si possa fidare di loro;
- *dirgli di segnalare all'adulto* se riceve una proposta di incontro offline o se gli viene richiesto l'invio di foto o video da parte di

qualcuno conosciuto online;
- *dirgli di non fissare appuntamenti* con persone conosciute online o, se si desidera davvero conoscerle, comunicarlo all'adulto e andarci con lui o, se l'età lo consente, lasciare al ragazzo la possibilità di scegliere con chi andare e incontrare il soggetto in luoghi pubblici e sicuri preventivamente comunicati all'adulto;
- informare il minore sulla possibilità di *rivolgersi alle Autorità* o ad associazioni di tutela dei minori se è vittima di adescamento.

Cyberbullismo

Il termine cyberbullismo indica una serie di comportamenti assunti in rete, messi in atto da un singolo o da un gruppo, finalizzati a danneggiare una persona.
In genere la vittima prescelta è una persona che non riesce a reagire e a difendersi e le azioni ai danni di quest'ultima vengono reiterate nel tempo.
Tale fenomeno spesso è difficile da rilevare per gli adulti, poiché la maggior parte delle volte è consumato solo in rete.
Per combattere il cyberbullismo è fondamentale agire su due fronti: quello della potenziale vittima e quello del potenziale abusante.
- **Prima regola: rispetto.** Gli adulti di riferimento (genitori, insegnanti, educatori, ecc.) devono insegnare ai ragazzi il rispetto per gli altri sia "online" che "offline". È importante far capire loro che offese e pettegolezzi feriscono anche in rete e che tali comportamenti non sono tollerati in alcun caso.
- **Tieni sotto controllo l'attività online dei minori.** È importante che l'adulto controlli che uso fanno i ragazzi della rete, e, in particolar modo nei casi in cui il loro comportamento si modifica negativamente quando sono online, cerchi eventuali segni di cyber bullismo.
- **Insegna al minore a tenere al sicuro i propri dati.** Suggerire ai ragazzi di tenere al sicuro i dati di accesso agli account personali o altre informazioni che potrebbero renderli vittime di episodi di cyberbullismo.
- **Gli atti di cyberbullismo devono essere denunciati.** Bisogna incoraggiare i ragazzi a denunciare immediatamente eventuali atti

di cyberbullismo subiti, chiedendo aiuto ad un adulto di fiducia, in modo da bloccare tempestivamente l'attività dell'abusante.

Se il minore è vittima di cyberbullismo è importante:
- **Agire subito.** Non bisogna aspettare nell'eventualità che tali atti cessino senza alcun intervento, è importante mostrare al minore sostegno e protezione;
- **Consiglia al minore di ignorare i messaggi e le provocazioni.** I cyberbulli cercano una reazione da parte delle vittime che è importante non offrire per non alimentare tali comportamenti;
- **Cerca di individuare l'identità del bullo** per denunciarlo e segnalarlo ai siti in cui sono avvenuti tali atti. Molti siti, in seguito alla segnalazione bloccano l'utente. Verifica che il servizio utilizzato abbia questa opzione;
- **Conserva le prove.** È importante salvare mail, messaggi e immagini inviate dal cyberbullo nell'eventualità che possano servire alle autorità per le indagini.

Per segnalare atti di cyberbullismo e altre situazioni di pericolo o di grave disagio che riguardano un minore, adulti e ragazzi possono chiamare il 114 Emergenza Infanzia, la linea di emergenza del Dipartimento per le Pari Opportunità gestita da Telefono Azzurro.
In generale, per la richiesta di informazioni o per segnalazioni di violazione online di norme penali è possibile contattare la Polizia Postale e delle Comunicazioni agli indirizzi e-mail degli uffici di tutta Italia.

ACQUISTA IN SICUREZZA ONLINE

E-commerce

l termine e-commerce, o commercio elettronico, indica l'acquisto di beni o servizi tramite internet. Sebbene tale forma di acquisto presenti tanti vantaggi, spesso può celare anche dei rischi. È fondamentale che il consumatore sia informato ed utilizzi il commercio elettronico conoscendo tutte le regole del gioco, in modo da poterne trarre grandi vantaggi.

Come si acquista on line

Quando il consumatore acquista online effettua un ordine al professionista, il quale è obbligato ad eseguire l'ordinazione entro 30 giorni dal giorno successivo in cui ha ricevuto l'ordine del consumatore.

In caso d'indisponibilità del bene o del servizio, il professionista deve informare il consumatore entro 30 giorni. Inoltre, il professionista è tenuto a corrispondere le intere somme eventualmente già versate dal consumatore. Il professionista non può adempiere alla prestazione fornendo beni e servizi diversi da quelli ordinati anche nel caso in cui si tratti a beni o servizi di importo uguale o superiore a quelli richiesti dal consumatore. Solo in caso di consenso esplicito del consumatore il professionista potrà fornire beni o servizi diversi da quelli ordinati. L'assenza di risposta del consumatore non può mai essere interpretata come consenso implicito.

Quando il contratto consiste nell'acquisto di beni è opportuno che al momento della consegna della merce il consumatore ne verifichi tempestivamente l'integrità. Qualora il pacco appaia visibilmente danneggiato è opportuno che il consumatore rifiuti la consegna o lo accetti con riserva sulla bolla di consegna. Se non lo fa perde il diritto di sostituzione del bene o di risarcimento del danno da trasporto.

Nel caso in cui i pacchi siano integri esternamente e quindi la merce sarà controllata in un secondo momento, è sempre opportuno accettare la merce con riserva e scrivere sulla bolla di consegna "accetta con riserva".

I sistemi di pagamento

Anche se esiste la possibilità di pagare prima, contestualmente o dopo la consegna della merce, molti venditori pretendono il pagamento anticipato escludendo tutte le altre forme di pagamento.
Le modalità più diffuse di pagamento degli acquisti on line sono:

- PayPal
- Carta di credito
- Carta prepagata
- Bonifico
- Contrassegno

Acquistare on line in sicurezza: alcuni consigli

- *Trasparenza delle informazioni:* prima di acquistare verifica sempre le politiche di vendita, le condizioni del recesso, i tempi di consegna, la presenza di costi aggiuntivi, i costi di spedizione;
- *I dati del venditore:* verifica che sul sito siano presenti tutti i dati che permettono di identificare il venditore. In particolare devono essere indicati il nome e l'indirizzo dell'azienda, diffida di indicazioni parziali o poco chiare che non permettono di risalire al venditore;
- *Usa in maniera appropriata le carte di credito:* verifica che il sito garantisca un'adeguata protezione dei dati al momento del pagamento, rappresentata da un sistema di protezione della trasmissione dei dati SSL (socketsecurelock). Lo si può riconoscere se sul sito è presente, di solito nella parte bassa dello schermo, un lucchetto chiuso. La presenza di un lucchetto aperto indica che il sito non è sicuro e la transazione non è adeguatamente protetta;
- *Protezione dati personali:* presta particolare attenzione che i dati personali richiesti siano in linea con la normativa sulla privacy. I dati richiesti dovrebbero essere unicamente quelli utili a finalizzare l'acquisto;
- *Mezzi di pagamento:* utilizza mezzi di pagamento più sicuri, da preferire le carte prepagate ed il contrassegno. Evita i mezzi di pa-

gamento che non permettono di essere bloccati e/o contestati (bonifico o moneytransfer);
• *Conserva la documentazione:* conserva con cura copia degli ordini effettuati e di tutte le comunicazioni intercorse.

I diritti dei consumatori che acquistano on line

Il commercio elettronico è disciplinato come "contratto di acquisto a distanza" ed è regolato dal Codice del Consumo (D.Lgs 206/2005), articoli 45 e seguenti. Il Codice del Consumo riconosce diritti ben precisi al consumatore che acquista on line che, in caso di mancato rispetto da parte del venditore, possono essergli contestati.
La legge pone particolare attenzione all'obbligo del professionista di fornire tutta una serie di informazioni prima della conclusione del contratto, in particolare, il consumatore deve ricevere queste informazioni:
• *Identità del professionista;*
• *Caratteristiche essenziali del bene e del servizio prescelto;*
• *Prezzo del bene e del servizio incluse le imposte e le tasse;*
• *Spese di consegna;*
• *Modalità di pagamento di consegna del bene o della prestazione del servizio o di ogni altra forma di esecuzione del contratto;*
• *Esistenza del diritto di recesso o di esclusione dello stesso;*
• *Modalità di esercizio del diritto di recesso e restituzione del bene;*
• *Costo per l'utilizzo della forma di comunicazione a distanza;*
• *Durata di validità dell'offerta o del prezzo;*
• *Durata minima del contratto in caso di contratti per la fornitura dei prodotti o la prestazione di servizi ad esecuzione continuativa e periodica.*

ATTENZIONE: LA GARANZIA LEGALE DI CONFORMITA' (ARTICOLI 128 E SEGUENTI DEL CODICE DI CONSUMO) SI APPLICA ANCHE AI CONTRATTI A DISTANZA E QUINDI AGLI ACQUISTI ON LINE.
IL CONSUMATORE CHE ACQUISTA ON LINE HA GLI STESSI DIRITTI DI CHI ACQUISTA IN UN NEGOZIO!

Come tutelarsi in caso di controversie

Per le controversie relative ai contratti a distanza la competenza territoriale è del giudice del luogo di residenza o domicilio del consumatore.

Nel caso di controversia transfrontaliera, cioè nel caso in cui il venditore non risieda nello stesso paese del consumatore, il consumatore può rivolgersi al Tribunale del luogo del proprio domicilio se ricorrano due condizioni:

1. Il commerciante deve esercitare la propria attività commerciale o professionale nello Stato membro di residenza del consumatore oppure dirigere con qualsiasi mezzo (ad esempio internet) la propria attività verso lo Stato membro;
2. Il contratto oggetto della controversia deve rientrare nell'ambito di queste attività.

Oltre alla via legale giudiziaria, i consumatori che dovessero incappare in controversie con il venditore possono anche attivare composizioni extragiudiziali delle controversie tramite la Conciliazione presso la Camera di Commercio se l'impresa ha sede legale in Italia, tramite le conciliazioni trasfrontaliere EEJNet se il consumatore o l'impresa si trovano in paesi diversi dell' Unione Europea.

Il social shopping

Il "social shopping" è una tipologia di commercio elettronico basata sui concetti di "gruppi d'acquisto" e "deal del giorno". Il gruppo d'acquisto ("groupbuying") è un concetto che indica un tipo di commercio in cui si offrono prodotti e servizi a prezzi notevolmente ridotti, a condizione che un numero minimo di clienti effettui l'acquisto. Il "deal del giorno" ("deal of the day") o "affare del giorno" è una caratteristica del social shopping, che consiste nella vendita di un prodotto unico per un periodo di tempo limitato ad un prezzo scontato.

Il Couponing: la forma di social shopping più diffusa in Italia

Il couponing consiste nell'acquisto di gruppo tramite coupon. I siti più noti che lo propongono sono: Groupalia, Groupon e Let's Bo-

nus. Il consumatore può trarre grandi risparmi dal couponing poiché ha la possibilità di acquistare prodotti o servizi spesso a prezzi "stracciati". Tuttavia, i problemi in cui può incappare sono molti e a volte configurano delle vere e proprie truffe.
Anche se non vi è ancora una normativa specifica che regola il couponing, questi acquisti rientrano nella tipologia di contratti a distanza e, pertanto, anche in questi casi si applica la disciplina prevista dal Codice del Consumo per e-commerce.

Come tutelarsi in caso di controversie

Nel caso in cui si verifichino problemi con il coupon, il rimborso della somma versata o il risarcimento per eventuali inadempienze va richiesto direttamente al sito internet di social shopping. E' opportuno inviare un reclamo al sito di social shopping e per conoscenza al professionista.
Il consumatore ha diritto di ricevere indietro la somma versata e può rifiutare eventuali altre forme di rimborso che spesso vengono offerte dal sito di social shopping (ad esempio un altro coupon o bonus).
Nei casi in cui il reclamo del consumatore non basti per risolvere le controversie, si applicano al couponing le stesse tutele elencate per il commercio on line.

SEGNALA CONTENUTI ILLECITI E ATTIVITA' ILLEGALI

È importante denunciare contenuti illeciti e attività illegali presenti nella rete. Se sei già stato vittima di una truffa, sarai facilitato nelle pratiche di denuncia e recupero del danno subito. Nel caso in cui non avessi subito danno alcuno, denuncia comunque la truffa: eviterai che altra gente ci caschi.

Scopri quali sono i vari strumenti di segnalazione
Serviti dei servizi di segnalazione di attività illecite o contenuti inappropriati già disponibili all'interno dei social network o altri servizi che utilizzi. Diversi social media come YouTube, Facebook, Twitter o Google + offrono la possibilità di segnalare tali contenuti o attività, in modo da aiutarli ad eliminarli e a offrire un servizio migliore. Se durante la navigazione su queste pagine ti imbatti in contenuti inappropriati segnalali tramite gli appositi comandi.
Di seguito trovi i link dei rispettivi social media per le segnalazioni:
-**YouTube:**http://www.youtube.com/yt/policyandsafety/it/reporting.html;
-**Facebook:**https://it-it.facebook.com/help/263149623790594;
-**Twitter:**http://support.twitter.com/articles/93896-come-segnalare-violazioni;
-**Google+:**https://support.google.com/webmasters/answer/93713?hl=it.

Utilizza il servizio di denuncia frode offerto dai siti web delle comunità dei commercianti. Solitamente i siti di e-commerce contengono una sezione dedicata alla denuncia delle truffe. Se ti accorgi di un post chiaramente fraudolento, segnalalo e contatta il servizio frode dell'assistenza clienti.

Spargi la voce

Quando si è vittime di una truffa è importante comunicarlo alla comunità per evitare che altri utenti vengano truffati. A tale scopo la rete offre diversi strumenti: esistono numerosi blog, forum e comunità online che permettono di denunciare una frode subita e di avvertire gli altri consumatori. Grazie a questi siti ci si può documentare sui truffatori e leggere le testimonianze di altre persone vittime di frodi.

Segnala email sospette e truffe

Molti fornitori di servizi email hanno dei filtri antispam o una sezione spam nella casella della posta ricevuta. Se le e-mail truffa o di phishing non sono trasferite automaticamente in queste sezioni possono essere spostate manualmente selezionando la voce "Sposta in Spam" o "Segna come Spam" presenti sulle pagine della casella di posta. Di solito, grazie a questa operazione, il fornitore viene allertato automaticamente. La segnalazione bloccherà l'invio di altre mail da parte del mittente e consentirà ai team che si occupano dei comportamenti illeciti di fermare simili attacchi.

Contatta la Polizia Postale o la guardia di finanza per denunciare reati informatici

Se ti imbatti in qualsiasi tipo di contenuto illecito o attività illegale è fondamentale esporre denuncia presso l'ufficio locale della Polizia postale (http://www.commissariatodips.it/).

Per segnalazioni di frodi informatiche e tecnologiche, puoi rivolgerti anche al GAT – Nucleo Speciale Frodi Telematiche della Guardia di Finanza (mail: sos@gat.gdf.it).