“non mi freghi”

MANUALE SU COME DIFENDERSI DALLE TRUFFE

CONTROLLO DEL VICINATO
INSIEME

Federconsumatori
Provincia di Modena APS

Questa guida è rivolta sia alle potenziali vittime di questi odiosi reati, sia a tutti quegli operatori pubblici e privati, parenti o amici, che possono assumere un ruolo importante nella loro prevenzione e tutela.

IL FENOMENO

Le truffe a danno dei cittadini sono in costante aumento ed hanno assunto caratteristiche molto diversificate, in quanto possono avvenire in contesti differenti, con modalità variegate e coinvolgere soggetti diversi.
I trucchi attraverso i quali i truffatori raggirano e derubano le persone sono sempre più elaborati.
È importante, quindi, saper riconoscere le situazioni più a rischio, avere consapevolezza dei fattori che possono caratterizzare un tentativo di truffa e, di conseguenza, dei comportamenti da tenere.

Aderiscono all'iniziativa

Con il supporto di:

AIMAG

Con il patrocinio di:

Unione delle Terre d'argine

UNIVERSITAS STUDIORUM MUTINENSIS ET REGIENSIS 1175

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

LE TRUFFE PRESSO L' ABITAZIONE

I falsi funzionari

È forse la più classica delle truffe. Falsi funzionari di enti pubblici o privati si presentano presso l'abitazione, spesso di persone anziane, con diversi pretesti. L'obiettivo è prevalentemente il furto di denaro o di beni preziosi.

False identità assunte più frequentemente dai truffatori:

1) Operatore di fornitori di acqua, luce, gas, con il pretesto della lettura dei contatori o di verificare se si effettua la raccolta differenziata;
2) Funzionari INPS o dell'Agenzia delle Entrate, con l'espediente di dover controllare la posizione pensionistica o contributiva;
3) Assistenti sociali, con il pretesto di dover valutare le condizioni di salute o di vita della persona;
4) Funzionari del Catasto, con la scusa di dover misurare le dimensioni dell'abitazione;
5) Operatori delle forze dell'Ordine per verifiche di denaro o per presenza di sostanze pericolose all'interno dell'abitazione.

È, inoltre, frequente il caso in cui i truffatori siano in più di uno e utilizzino una delle due seguenti tecniche alternative: 1) Entrano entrambi nell'abitazione e, mentre uno distrae la persona, chiedendo ad esempio un bicchiere di acqua, l'altro cerca di rubare denaro o valori. 2) Entra in casa uno dei due con un pretesto, cercando di rubare un oggetto qualsiasi. In un secondo momento il complice, spacciandosi per un agente di polizia, si presenta presso l'abitazione chiedendo alla persona se riconosce l'oggetto e invitandola a controllare se manca altro. In questo caso è la stessa persona che mostra al malintenzionato dove conserva denaro o oggetti preziosi. Talvolta questi truffatori convincono la vittima a recarsi in Banca o all'Ufficio Postale per prelevare denaro.

COSA FARE

Innanzitutto, è importante sapere che non sussiste nessun obbligo di far entrare in casa operatori o funzionari di enti pubblici o privati, o di associazioni, senza aver verificato prima la loro reale identità. Ciò è possibile telefonando direttamente all'Ente o all'Associazione a cui detti funzionari dicono di appartenere o chiedendo l'aiuto delle forze di polizia, di parenti, amici o vicini. Il più delle volte può essere, infatti, sufficiente la richiesta di verifica dell'identità o la ricerca di un vicino o un parente per far allontanare questi truffatori, se si tratta di malintenzionati. É bene, inoltre, ricordare che, prima di procedere a controlli presso le abitazioni, gli Enti affiggono degli avvisi nel palazzo o sul cancello dell'abitazione o contattano direttamente e in anticipo gli abitanti per fissare un appuntamento. Occorre che le verifiche consigliate vengano fatte immediatamente, perché, una volta che il truffatore si è introdotto nell'abitazione, potrebbe reagire in modo imprevedibile nel caso in cui si accorga che l'abitante sta effettuando telefonate o chiedendo aiuto. Se i truffatori si trovano già in casa, è importante osservarli bene così da rilevare eventuali particolari utili alla loro identificazione, da riportare successivamente nella denuncia alle Forze dell'Ordine, e, qualora si allontanino con un mezzo di trasporto, cercare di rilevare il modello, la targa, e la direzione percorsa.

VENDITA PORTA A PORTA

La tecnica di vendita porta a porta è molto utilizzata da soggetti più disparati: dai “classici” venditori di aspirapolveri e prodotti per la casa agli agenti delle società di energia che vogliono proporre nuovi contratti, con tecniche di persuasione sempre più raffinate e insistenti. In questo caso però non è corretto parlare di vere e proprie truffe, ma di “proposte commerciali scorrette”.

COSA FARE

Come già ricordato, non è obbligatorio aprire la porta a chiunque suoni al campanello. Anche correndo il rischio di apparire maleducati, basta semplicemente dire che non si è interessati e chiudere la porta per evitare la maggior parte dei problemi e dei fastidi.
A riguardo, ricordiamo che nessun operatore della propria banca, assicurazione, compagnia del gas, della luce o del telefono è autorizzato a riscuotere denaro presso il vostro domicilio.

Se l'agente si presenta come incaricato di una certa società, verificare il cartellino identificativo che dovrebbe tenere a vista; in caso di dubbi è sempre bene fare prima una telefonata di conferma alla società o alle forze di polizia del territorio.

Se si decide di aprire la porta e di fare entrare l'agente non mostrare alcun documento (carta di identità codice fiscale, bolletta, vecchio contratto ecc.) che contenga i dati personali.

Se le proposte dell'agente suonano interessanti, è bene comunque non firmare nulla sul posto. Fatevi lasciare tutti i documenti utili per farvi un'idea più ragionata, sarete sempre in tempo a contattare voi stessi la società e stipulare il contratto in seguito.
In ogni caso, prima di firmare o di permettere che l'agente raccolga i vostri dati personali, leggete bene tutti i fogli, con attenzione, anche le clausole scritte in piccolo. In caso di dubbi chiedete spiegazioni e se non sono esaurienti non firmate. Se, in particolare, vi vengono sottoposti dei documenti in carta intestata di banche o finanziarie, siate scrupolosi nel leggere ogni riga.

Ricordarsi che:
Le promesse fatte a voce dall'agente non valgono nulla se non sono riportate nero su bianco nel contratto.

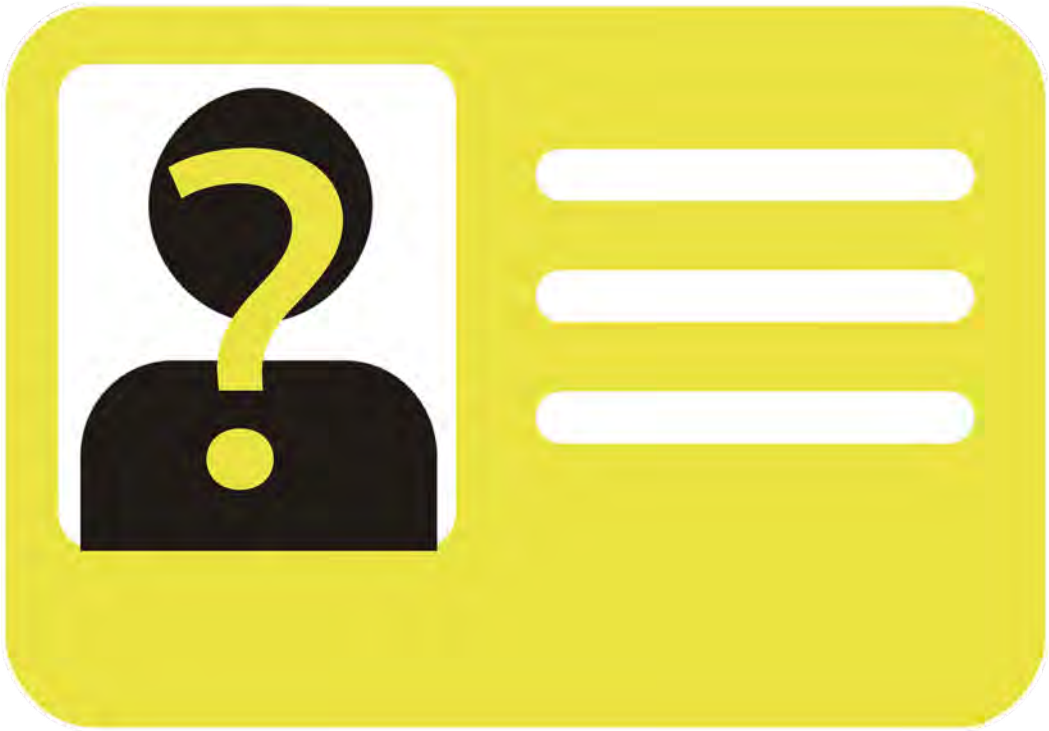
Qualsiasi persona, giovane o meno giovane, può essere vittima di un truffatore

Ma qual è l'identikit del truffatore?

Può essere un uomo o una donna, presentarsi da solo o in coppia. In genere è elegante, cordiale e rassicurante, nella maggior parte dei casi conosce il nome vostro e dei vostri parenti prossimi, in modo da conquistare la vostra fiducia.

Parla molto allo scopo di confondervi e raggiungere il suo obiettivo. Spesso finge di essere stato mandato da un parente o da un conoscente.

Può presentarsi presso le abitazioni in tuta da lavoro o in uniforme e mostrare un tesserino, spacciandosi per un addetto delle forze dell'ordine o un impiegato di enti pubblici o privati.



Altra tipologia di raggiro che negli ultimi anni è diventato sempre più aggressivo riguarda le truffe telefoniche, ossia le truffe che vengono perpetrate mediante l'utilizzo del telefono da soggetti che fingono di essere operatori di call center ed ingannano l'utente inducendolo inconsapevolmente ad attivare servizi non graditi o falsi.

Le stesse Forze di Polizia sottolineano come, riguardo al reato di truffa, una volta che questo è commesso risulta molto difficile individuare i responsabili e perseguirli. Pertanto è importante mettere in atto tutte le azioni volte a prevenirlo.

Lo strumento più utile a nostra disposizione per difenderci da tutte queste truffe è quello di essere informati su come avvengono e di conseguenza come comportarci.
Questa è una battaglia che non si combatte da soli ma uniti insieme.
E' un fenomeno che colpisce tantissime persone e sta diventando sempre più virale.
Aiutiamo a fare informazione e facciamoci aiutare.

INFORMAZIONI IMPORTANTI

Qualsiasi vendita di servizi o prodotti eseguita porta a porta è soggetta ad una autorizzazione (SCIA) richiesta al Comune ove la vendita avverrà.

Nella richiesta l'azienda deve comunicare la zona ove opereranno i suoi venditori, la data di inizio e fine e non per ultimo la tipologia di prodotti e servizi oggetto della vendita.

Come Controllo del Vicinato, nell'ambito di questa iniziativa, per migliorare le informazioni e quindi la sicurezza di tutti, abbiamo stipulato degli **accordi con i Comuni**, per potere ricevere queste autorizzazioni, **e anche con AIMAG/SINERGAS.**
Riceveremo da loro tutte le informazioni sulla presenza nei territori di tecnici per letture contatori, o per manutenzioni programmate e tutte queste importanti informazioni verranno smistate ed inviate direttamente ai vari gruppi di controllo del vicinato delle zone interessate.
Queste informazioni permetteranno di smascherare tutte le persone non autorizzate o i truffatori che si spacciano per venditori o finti tecnici.

Qualsiasi persona o famiglia può aderire alla rete del Controllo del Vicinato e quindi ricevere queste importanti informazioni.
Il Controllo del Vicinato è una grande rete di persone, supportata dalle Istituzioni, che cerca con ogni mezzo di tutelarsi da truffe e furti.

L'adesione è gratuita e semplice: per maggiori informazioni visitate il sito www.cdv.community
oppure inviate una mail a info@cdv.community
o, se preferite, telefonate alla nostra segreteria al numero 366 3369468.

TRUFFE TELEFONICHE - TELEMARKETING

Le truffe telefoniche più diffuse sono le cosiddette **"truffe del sì"**, poste in essere da call center che propongono offerte irripetibili e irrinunciabili. Spesso a seguito di queste chiamate, ci si ritrova inconsapevolmente e senza averlo mai richiesto con una domanda di cambio di operatore telefonico, del gas o energetico o con l'attivazione di determinate offerte a pagamento.

COSA FARE

1) Va anzitutto ricordato che **è nostro diritto sapere dove è stato reperito il nostro numero** (cioè il soggetto a cui abbiamo ceduto i dati per usi pubblicitari). Va quindi sempre chiesto come un certo operatore ha fatto ad avere il nostro numero di telefono: così facendo, molto spesso la telefonata si interrompe immediatamente. Anche se abbiamo dato il nostro consenso, esso può essere sempre revocato inviando una raccomanda A/R con la richiesta di cancellazione; **è possibile poi fare una segnalazione al Garante della Privacy.**

2) Il consumatore ha diritto di conoscere la numerazione dalla quale chiama l'operatore: meglio quindi munirsi di telefoni fissi in cui compare il numero del chiamante (nei cellulari questo appare sempre) e se vengono visualizzati prefissi strani o comunque numeri sconosciuti è consigliato non rispondere. Se invece si decide di "alzare la cornetta" e la telefonata risulta essere di un call center **MAI** dare informazioni personali o che riguardano le nostre bollette (es. POD e PDR) e **MAI** rispondere di Sì, per non incorrere nel fastidioso cambio di contratto da un operatore all'altro o accettazione all'acquisto di un prodotto.

Ricordiamoci sempre che un contratto telefonico è un contratto valido, non serve la nostra firma ma è sufficiente un semplice Sì.

TRUFFE BANCARIE TELEFONICHE: IL VISHING

Il Vishing (parola inglese creata dalla combinazione delle parole 'Voice' e 'Phishing') è una truffa telefonica in cui i truffatori cercano di indurre la vittima a divulgare informazioni personali, finanziarie o di sicurezza o a trasferire loro del denaro.

COME PUOI DIFENDERTI?

Attenzione alle chiamate telefoniche indesiderate o da numeri strani.

Segnarsi il numero del chiamante e avvisarlo che verrà richiamato essendo tu ora occupato, così da prendere tempo e verificare online di che numero si tratta e se ci sono casistiche di truffe legate a questo numero.

Per verificare la loro identità: cerca il numero di telefono dell'organizzazione e contattali direttamente.

Non validare il chiamante nel dare credito al truffatore utilizzando il numero di telefono che ti è stato fornito (potrebbe trattarsi di un numero falso o contraffatto).

I truffatori spesso trovano le tue informazioni online (ad es. attraverso i social media). Non presumere che chi chiama sia autentico solo perché possiede questi dati.

Non condividere il numero segreto PIN della tua carta di credito o di debito oppure la password del tuo conto online.
La tua banca non ti chiederà mai tali dettagli telefonicamente.

Non trasferire denaro su un altro account a richiesta. La tua banca non ti chiederà mai di farlo telefonicamente.

Se pensi che sia una finta chiamata allo scopo di truffa, segnalalo immediatamente alla tua banca e alla Pubblica Sicurezza.

REGISTRO DELLE OPPOSIZIONI

Attualmente non ci sono regole severe ed efficaci che mettano un freno all'aggressività dei molti operatori ma è sicuramente utile iscriversi al Registro Pubblico delle Opposizioni (per ora l'iscrizione è possibile solo per la numerazione fissa, anche se non presente in elenco telefonico, ma a breve sarà disponibile anche per i numeri di cellulare).

Il Registro Pubblico delle Opposizioni è un servizio gratuito, patrocinato dal Ministero dello Sviluppo Economico, che permette di rendere pubblica la propria volontà di non essere contattati a scopi promozionali dai call center.
Gli operatori commerciali, quindi, prima di procedere alle telefonate, dovrebbero verificare se la numerazione è presente nel Registro e, in caso positivo, astenersi dal molestare il cittadino. Purtroppo ciò non sempre accade, ma se si è iscritti al Registro e le telefonate continuano ad arrivare, si ha un'arma in più: far presente all'operatore la nostra iscrizione, che la telefonata che sta facendo è del tutto illegale e pertanto potrà essere denunciato al Garante della Privacy. Se ciò non fosse sufficiente, si potrà presentare un ricorso allo stesso Garante chiedendo la cancellazione dei dati personali ed indicando il numero dell'utenza telefonica sulla quale sono state ricevute le chiamate promozionali, le date, l'ora delle chiamate e la società i cui prodotti sono stati pubblicizzati.
L' arma migliore rimane la prevenzione. Ricordiamoci che quando firmiamo il consenso ai dati, necessario per fruire di un servizio, non abbiamo l'obbligo di mettere altre firme (o *flaggare* caselle in più) per fini commerciali o per la cessione di dati a terzi.
Infine, concediamo con parsimonia il nostro numero di telefono ed evitiamo accuratamente di metterlo a disposizione sui social-network.

Registro Pubblico delle Opposizioni (RPO): come iscriversi

L'utente può richiedere l'iscrizione, l'aggiornamento dei dati e la revoca al RPO tramite quattro modalità:

- web (compilazione di un modulo elettronico)
- telefono (chiamata al numero verde RPO)
- email (invio tramite posta elettronica di un apposito modulo)
- raccomandata

L'operatore di telemarketing che utilizza i dati presenti negli elenchi telefonici pubblici è tenuto a verificare tramite il RPO le liste dei potenziali contatti, tramite una serie di servizi disponibili sul sito. **www.registrodelleopposizioni.it**

TRUFFE TRAMITE MAIL: IL"PHISHING"

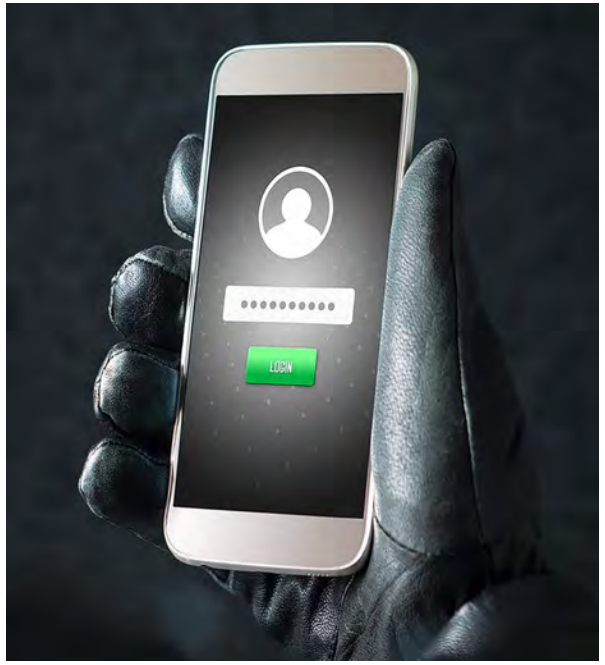
La parola *phishing* deriva dall'inglese "pescare" ed è la strategia più utilizzata dagli hacker (molte volte dilettanti) per truffare gli utenti sottraendo loro dati sensibili e credenziali che, in alcuni casi, consentono l'accesso ai risparmi presenti su carte e conti correnti.
Alla luce di questo, diventa importante comprendere cos'è il *phishing* e conoscere le astuzie che permettono di prevenire questa tipologia di truffa. Il *phishing* risale al lontano 1987, ma è sempre maggiormente sfruttato dai malfattori, che adoperano tutti i sistemi possibili, dagli SMS, ai Social, alle mail, per "pescare" le loro vittime.

Gli espedienti illecitamente usati sono sempre di più e altrettanto numerose sono le strategie ideate per compiere l'inganno.
Alla luce di queste considerazioni, è importantissimo comprendere cos'è il *phishing* e in particolare imparare quei trucchi che permettono di riconoscere e prevenire queste truffe così da proteggere le proprie credenziali, carte e conti correnti.
Lo strumento maggiormente utilizzato per la diffusione di queste truffe sono le email, molte delle quali presentano in linea di massima la medesima struttura, anche se è possibile identificare l'intento fraudolento ed evitare di essere "pescati".
Spesso le mail in questione presentano errori grammaticali palesi (essendo inviate da persone straniere che usano traduttori online) e tale caratteristica costituisce un campanello d'allarme da non sottovalutare.
Spesso sono presenti degli inviti a fornire le proprie credenziali e i dati sensibili, spacciandoli per necessari, ad esempio, per risolvere problemi, documenti in scadenza, ecc. Al fine di permettere l'inserimento dei dati, nelle mail sono presenti dei link o allegati file (Trojan) sui quali si è esortati a cliccare, passaggio, quest'ultimo, che consentirà ai malfattori di compiere l'inganno.

In molti casi le email si presenteranno sotto falso mittente, come nomi di aziende e marchi noti estranei all'inganno e utilizzati in maniera illecita come espediente.

E' indispensabile accertare la veridicità della comunicazione ricevuta, non affidarsi a quei messaggi che presentano le caratteristiche appena esposte ed evitare in qualsiasi circostanza l'inserimento di dati personali.

COME COMPORTARSI E PRECAUZIONI DA PRENDERE



In caso di truffa, esistono metodi di pagamento che consentono alle Forze dell'Ordine di risalire all'identità del malvivente. Tra questi, i bonifici bancari o sistemi di pagamento come PayPal e Hype, che tengono traccia delle transazioni in denaro.
Al contrario, i vaglia postali o le ricariche di carte ricaricabili, così come servizi quali Western Union e Moneygram, sono tipologie di pagamenti preferiti da chi vuole ingannare i compratori, poichè non permettono forme sicure di tracciamento.

Spesso raggiri di questo tipo riguardano somme modeste, per le quali la vittima tende a non richiedere livelli elevati di sicurezza.

Per proteggersi bastano dei semplici accorgimenti:

1) **non fornire in nessun modo password e/o dati sensibili a terzi non conosciuti;**
2) **non utilizzare password semplici come la data di nascita o nome e cognome: la password deve essere almeno di 6 cifre in numeri, lettere e caratteri speciali;**
3) **non cliccare su links conosciuti;**
4) **non scaricare file di cui non si conosce il contenuto o l'esatta provenienza;**
5) **fare pagamenti, se si ha la possibilità, utilizzando PayPal o altri metodi tracciabili;**
6) **non aprire mail dal contenuto insolito o provenienti da persone o aziende non conosciute;**
7) **cambiare spesso le diverse password che usiamo per tutelare i dati personali;**
8) **controllare sempre i propri movimenti bancari e delle carte di credito;**

TRUFFE WEB

Oggigiorno realizzare delle truffe su Internet è relativamente semplice: basta registrare un sito Web con domini quali .com, .net, .org, dando dati falsi, costruire un negozio virtuale online, vendere prodotti a prezzi convenienti e di marche conosciute oppure, oggi molto di moda, vendere false assicurazioni. In questi casi, il malvivente aspetta che qualcuno abbocchi all'esca, acquistando i prodotti e pagandoli con la carta di credito. La vittima, nella migliore delle ipotesi non riceverà nulla, nella peggiore si troverà rubati i dati della carta di credito cha ha inserito. Per i domini .it (Italia) e .eu (Europa) vengono verificati i dati del registrante e per questo è molto difficile poterli falsificare.

Altra tipologia tra le tantissime, è quella dei falsi affitti online, spesso di case per vacanza. La strategia non è nuova, ma negli ultimi anni i metodi di questa truffa si sono raffinati per riuscire a colpire con più puntualità.

Attenzione alle piattaforme di vendita online: non sotto tutte uguali. Prima di perfezionare un acquisto **assicuratevi che il sito sia attendibile.**

Fate una ricerca in rete, confrontatevi con le esperienze di altri utenti, leggete i commenti.

Verificate se il negozio abbia una sede legale e un numero di telefono.

Utilizzate i siti ufficiali del prodotto che avete intenzione di acquistare: eviterete di ricevere a casa della merce contraffatta.

Altra popolare truffa online è la frode **sui biglietti**, in cui i consumatori sono indotti a comprare biglietti falsi per eventi sportivi, concerti e altro. Spesso i biglietti che vengono poi inviati hanno codici a barre contraffatti o sono copie duplicate di biglietti legittimi. Altre volte, non viene inviato alcun biglietto.

Ransomware: gli hacker, con diverse modalità, fanno scaricare alla vittima un software autoinstallante, detto *malware*, che opererà poi su un computer o su un sistema di computer limitando l'accesso ai loro file. In tali casi viene normalmente richiesto il pagamento di un riscatto per sbloccare i file. Il pagamento di questa forma di riscatto spesso viene richiesto sotto forma di *bitcoin*.
Quasi sempre però, anche una volta pagato, non si riceve la chiave per sbloccare i file.

COME COMPORTARCI E PRECAUZIONI DA PRENDERE

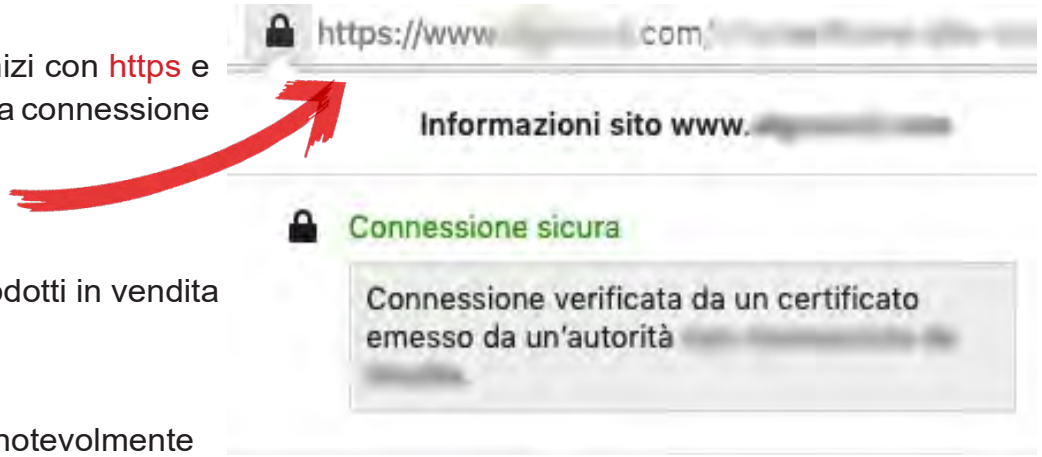
Ogni sito che si visita deve SEMPRE riportare i dati dell'azienda proprietaria del sito e deve ASSOLUTAMENTE riportare: partita IVA, indirizzo della sede, numeri di telefono e mail.

La normativa prevede che in ogni sito aziendale di una società di capitale (S.r.l., S.p.A.) almeno nella home page siano riportati i dati dell'azienda e la Partita I.V.A: un sito che non pubblica queste basilari informazioni vuole nascondere qualcosa ed è sanzionabile.

IN PARTICOLARE I SITI DI ECOMMERCE (VENDITE ONLINE) DEVONO OBBLIGATORIAMENTE SEMPRE RIPORTARE:

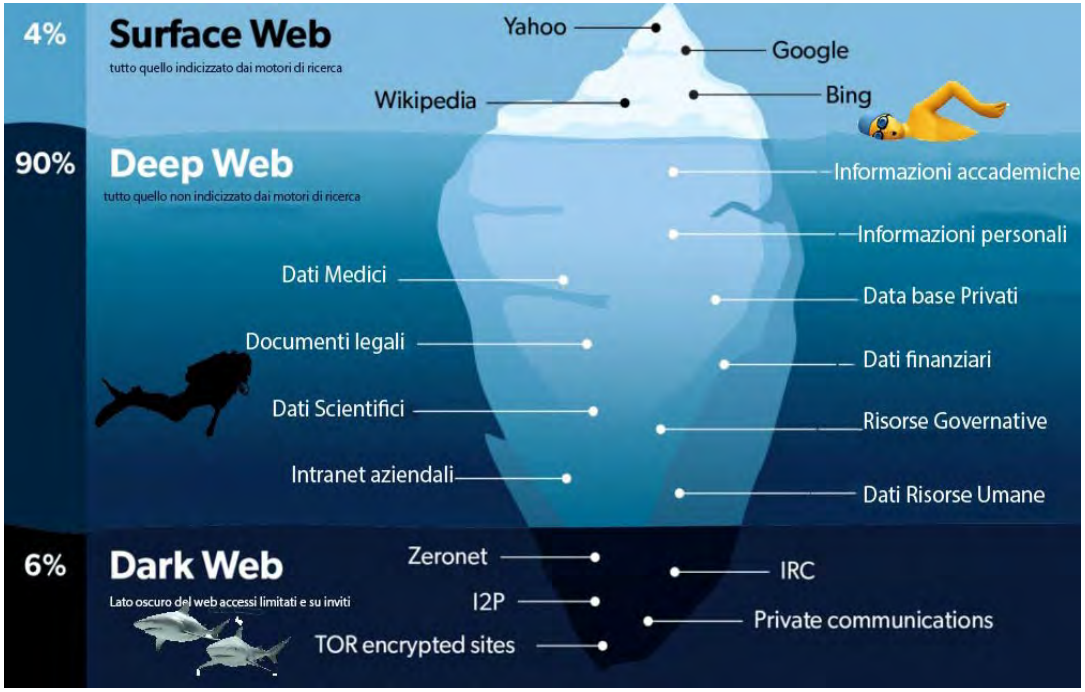
- il nome dell'azienda, la denominazione e la ragione sociale;
- il domicilio o la sede legale;
- gli estremi che permettono di contattare il venditore in maniera rapida ed efficace quali telefono e indirizzo mail;
- il numero di iscrizione al registro delle imprese;
- il numero di Partita IVA o altro numero di identificazione che viene considerato equivalente nello Stato membro (solo nel caso in cui il prestatore svolga un'attività soggetta ad imposta).

Il sito che vende online prodotti DEVE essere in possesso del certificato di sicurezza SSL.
Per verificarlo basta controllare che l'URL della pagina visualizzata inizi con https e che compaia un lucchetto CHIUSO: ciò significa che viene utilizzata una connessione crittografata e le informazioni sono probabilmente al sicuro.



Se il sito chiede di scaricare un software dedicato per acquistare i prodotti in vendita NON FARLO ASSOLUTAMENTE

DIFFIDARE SEMPRE dall'acquisto in siti dove i prodotti sono a prezzi notevolmente più bassi rispetto alla media: occorre fare verifiche su altri siti prima di acquistarli.



Internet è diviso in tre zone; *surface web*, *deep web* e *dark web*

1) Surface Web, anche detto Web di superficie: rappresenta tutte quelle pagine web e quei documenti che vengono indicizzati dai motori di ricerca, circa il 4% di tutto quello che è contenuto nel web. Spesso siamo sicuri che Google potrà sempre trovare tutto quello che ci occorre. Purtroppo però, frequentemente, dopo aver visionato tutte le pagine proposte, non siamo soddisfatti del risultato ottenuto. Eppure abbiamo sempre sentito parlare dell'efficacia dell'indicizzazione delle informazioni di Google, della sua grossa potenzialità essendo anche da sempre il primo motore di ricerca del web … del Surface Web.

2) Deep Web, anche detto web profondo: è quella parte del web che i motori di ricerca tradizionali non indicizzano ma comunque il suo contenuto è accessibile senza particolari software.

All'interno di questa area molto estesa (circa il 90% del totale del web) possiamo trovare:

Contenuti dinamici, come ad esempio pagine scritte con linguaggi server site ASP, PHP, ecc, o siti gestiti attraverso un form o un'interrogazione, oppure creati come risposta alla compilazione di un *form* o una *query* avviata dall'utente sul sito;

Hidden pages: pagine che non contengono elementi di collegamenti ipertestuali che potrebbero portare la pagina a essere indicizzata;

Siti con accesso ristretto o limitato, come pagine private, che per essere visualizzate richiedono qualche forma di login (mail, social network, cloud), oppure pagine il cui accesso è ristretto da strumenti tecnici come l'uso del *Robots Exclusion Standard* (robots.txt) e/o Reti Private;

Pagine web linkate attraverso linguaggio di script o pagine web accessibili solo attraverso link prodotti da linguaggio *javascript* o linguaggi dinamici;

Siti recenti, o siti con contenuti non testuali.

3) Dark Web, anche detto web oscuro: è quella parte del web che non è accessibile attraverso i normali programmi, ma che richiede l'impiego di accorgimenti e programmi particolari. Sostanzialmente, possiamo definirlo come la porzione di internet che è intenzionalmente nascosta dai motori di ricerca, utilizzando indirizzi IP nascosti.

Sul Dark Web si trova, si vende e si compra di tutto, specialmente beni/servizi illegali come droga, armi, denaro contraffatto, finti titoli di studio, sicari, materiale pedopornografico, identità rubate, conti in banca fittizi, ecc.

Esistono anche usi legittimi del Dark Web: ad esempio, le persone che vivono sotto regimi totalitari e non hanno libero accesso a internet usano il Dark Web per comunicare con il mondo esterno (la BBC, ad esempio, ha aperto una sua pagina sul Dark Web per renderla disponibile a tutti nel mondo).

Per segnalare truffe, frodi, abusi o furti telefonare al 112

Federconsumatori
Provincia di Modena APS

Per avere supporto e consulenza telefonare allo 059 260384 (orari ufficio)

CONTROLLO DEL VICINATO
INSIEME

Per avere informazioni sul controllo del vicinato e su questa iniziativa:
telefonare al numero 366 3369468 (segreteria)
oppure visitare il sito www.cdv.community
e.mail: info@cdv.community

Questo manuale è parte integrante del progetto “non mi freghi”

Redatto in collaborazione tra Controllo del Vicinato INSIEME e Federconsumatori

Con il Patrocinio oneroso dei Comuni delle Terre D'Argine