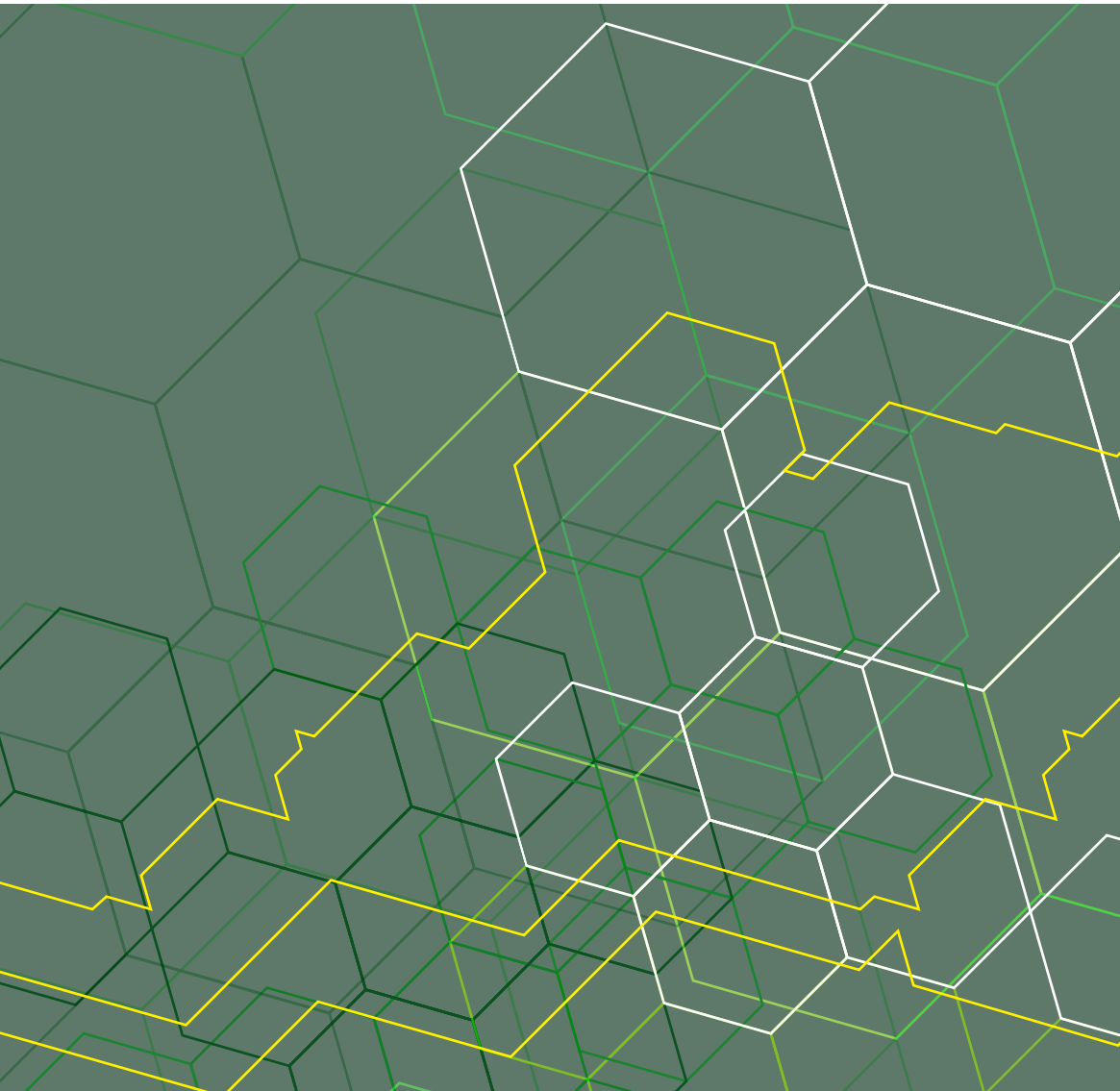
CAMERA DI COMMERCIO
INDUSTRIA, ARTIGIANATO
E AGRICOLTURA DI NAPOLI

giada

Guida all'Acquisto Sicuro sul Web



giada

Guida all'Acquisto Sicuro sul Web

ADOC Napoli e Campania
ASSOCIAZIONE DIFESA E ORIENTAMENTO DEI CONSUMATORI

Camera di Commercio Industria Artigianato
e Agricoltura di Napoli

Questa pubblicazione fa parte del progetto

Sportello on-line GIADA
Guida all'Acquisto Sicuro sul Web

realizzato da

ADOC Napoli e Campania
ASSOCIAZIONE DIFESA E ORIENTAMENTO DEI CONSUMATORI

con il contributo finanziario di

Camera di Commercio Industria Artigianato
e Agricoltura di Napoli

Responsabile del progetto per ADOC

Luciana del Fico

Referente del progetto per CCIAA Napoli

Caterina Casalino

progetto grafico Paolo Vigorito

indice

Viaggiare sicuri lungo l'autostrada globale della Rete. E'questo l'obiettivo pienamente centrato dalla guida sintetica al commercio online realizzata dall'Adoc Napoli e Campania con il contributo della Camera di Commercio partenopea.

Uno strumento agile e di immediata consultazione per chi non ha ancora allacciato le cinture di sicurezza durante la navigazione e vuole saperne di più sulle regole e sul funzionamento delle applicazioni e sugli utilizzi più recenti.

Grazie ad un linguaggio semplice e conciso, questo vademecum è un lasciapassare utilissimo per la quotidiana attività d'impresa e non solo. Le apposite sezioni dedicate alla trasparenza nelle contrattazioni e alla qualità dei beni e servizi che si scambiano su Internet, nonché le precise avvertenze sulla responsabilità del venditore nelle transazioni e sui diritti dell'acquirente sul web, sono tracce fondamentali di un cammino comune che l'ente camerale intende percorrere in piena sintonia con il mondo dei consumatori.

Educare all'utilizzo consapevole e responsabile delle tecnologie legate ad Internet è un impegno che vede coinvolta direttamente la rappresentanza istituzionale del mondo delle imprese e dei consumatori.

E'una battaglia di civiltà e di progresso che insieme all'Adoc siamo consapevoli di combattere ogni giorno quando ognuno di noi accende il pc e si collega con il mondo e con il futuro a portata di click.

Maurizio Maddaloni

Presidente Camera di Commercio Industria Artigianato e Agricoltura di Napoli

Imparare a navigare in Internet, non è per tutti una cosa sempre facile. Spesso cimentarsi con motori di ricerca, e-mail, virus e chi ne ha più ne metta, diventa una sfida con il computer, per riuscire a destreggiarsi tra comandi da dare e procedure da seguire.

Non si può negare, però, che una volta divenuti abili nella navigazione si resta affascinati da questo enorme patrimonio di informazioni, cultura e conoscenza in continua evoluzione che è il web. In questi ultimi anni, ormai sta diventando uso comune anche l'utilizzo del commercio on-line, così come il servizio offerto da molti istituti di credito per collegarsi al proprio conto corrente bancario anche da casa, appunto via internet.

Tramite i nostri sportelli ADOC ci siamo resi conto però che queste opportunità non sono utilizzate da un pubblico vasto, anzi sono ancora viste con diffidenza da molti utenti.

Si è pensato quindi di proporre una Guida per imparare a capire dove possono nascondersi i pericoli che possono derivare da un uso poco attento di un servizio che, se usato con accortenza, può invece diventare un aiuto per chi non ha la possibilità di raggiungere di persona un locale commerciale per fare un acquisto. Così, seguendo le nostre indicazioni e avvertenze sarà possibile contattare quel tale produttore di vino o di prodotti caratteristici della Campania o di un'altra Regione, collegandosi al sito web. Si potrà fare un ordine comodamente da casa, seduti davanti al computer, navigando tra le pagine del catalogo on-line di quel commerciante o di quel produttore, facendo i dovuti confronti e le scelte con calma.

Ciò significa essere al passo con i tempi, aquistando on line in sicurezza e tranquillità i prodotti o i servizi che più ci aggradano.

Nel commercio elettronico valgono le stesse regole legali che per il commercio tradizionale, in merito al diritto di recesso e/o di ripensamento. La conoscenza dei propri diritti, infatti ci mette anche nelle condizioni di valutare se quel venditore on-line è corretto o meno, se ha messo in evidenza tutte le dovute informazioni per il Consumatore.

In linea con l'obiettivo del progetto la Guida sarà disponibile on-line sul sito dell'ADOC Napoli e Campania WWW.ADOC-CAMPANIA.IT *nella sezione dedicata al progetto Giada.*

Ringrazio la Camera di Commercio di Napoli, che ha avuto la sensibilità di promuovere un progetto come il nostro, rivolto all'utilizzo responsabile delle nuove tecnologie, ma anche promotore di nuove forme di commercio e servizi a disposizione dei Consumatori. Ringrazio, infine anche il Comitato Tecnico Scientifico per il lavoro svolto e il gruppo di lavoro per la dedizione e la professionalità avuta in tutte le fasi del progetto.

Luciana del Fico
Presidente ADOC Napoli e Campania

la rete

CHE COS'È?

E'un insieme di computer e/o dispositivi (stampanti, unità disco, smartphone) collegati tra di loro. Il principale scopo di una rete è quello di condividere o scambiare informazioni (es.: *file, directory* etc.) e/o dispositivi.

TIPI DI RETE

Le reti si possono classificare in tre grandi categorie:

- LAN - Local Area Network
- MAN - Metropolitan Area Network
- WAN - Wide Area Network

LAN - LOCAL AREA NETWORK

LAN o rete locale è, come si intuisce dal nome, una rete che copre un'area limitata a pochi chilometri, appunto "locale". Principalmente utilizzata in una casa, in uffici di uno o più piani o in aziende ubicate in più palazzine adiacenti. Di solito i dispositivi di una rete sono collegati tra loro tramite cavi (di tipo *UTP*), ma possono collegarsi anche tramite Wireless, ossia collegamento "senza fili", in questo caso non parleremo più di LAN, ma di WLAN (Wireless Local Area Network). Ad una WLAN potranno collegarsi solo dispositivi che supportano questo tipo di tecnologia conosciuta anche come *Wi-Fi*.

MAN - METROPOLITAN AREA NETWORK

MAN o rete metropolitana, si riferisce ad una rete estesa ad un perimetro cittadino. In pratica è come se pur trovandosi in diversi punti di una città i dispositivi si trovino nella stessa LAN. Di solito il collegamento utilizzato per questo tipo di rete è la fibra ottica. Un esempio pratico di MAN è FastWeb.

WAN - WIDE AREA NETWORK

WAN o rete geografica, è un insieme di LAN e MAN collegate tra loro in un'ampia area geografica tramite linee telefoniche, con fibre ottiche o collegamenti satellitari. La rete WAN più conosciuta è INTERNET.

UN PO'DI STORIA

Come predecessore di Internet viene indicato il progetto ARPANET (Advanced Research Projects Agency Network) finanziato negli anni sessanta dal Ministero della Difesa statunitense. Il progetto assegnato alla società BBN (Bolt, Beranek and Newman) fu realizzato con la collaborazione di quattro università americane, l'Università della California di Los Angeles, l'SRI di Stanford, l'Università della California di Santa Barbara e l'Università dello Utah. La rete fu terminata fisicamente nel 1969 quando i quattro poli furono collegati fra loro. Durante gli anni settanta, ARPANET continuò a svilupparsi estendendosi anche oltre oceano, dove iniziarono a nascere altre reti in Francia, Inghilterra e Norvegia.

All'inizio degli anni '80, la Difesa statunitense si ritirò dal progetto isolando la sua rete (MILNET) ed ARPANET iniziò ad essere denominata come Internet.

La vera rivoluzione, però, ci fu nel 1991 quando il ricercatore del CERN di Ginevra, Tim Berners-Lee, definì il protocollo *HTTP*, un linguaggio che permette la lettura semplificata dei dati trasmessi. Nel 1993 nacque il primo browser dando così il via al WWW (World Wide Web).

il browser

CHE COS'È?

Il browser (in italiano: navigatore) è un programma che consente agli utenti di accedere al World Wide Web (WWW). Un browser permette di visualizzare, ma non di modificare le pagine dei siti web. In pratica, ha la funzione di interpretare il linguaggio *HTML* (codice usato per la scrittura di pagine web) e di tradurlo in immagini, audio, link, parole e tutto quello che costituisce una pagina web.

COME FUNZIONA

Tale programma permette di accedere a qualsiasi oggetto si desideri recuperare inserendo un "indirizzo", detto *URL*, che contiene tutte le informazioni necessarie per l'operazione richiesta.

TIPI DI BROWSER

Per navigare in Internet è necessario installare un browser. Attualmente esistono diversi browser in commercio, più o meno utilizzati. I più conosciuti sono:

- Internet Explorer
- Mozilla Firefox
- Google Crome
- Opera
- Safari

La scelta di un browser è molto importante, in quanto è il programma che ci fa navigare in Internet, dove possiamo incontrare virus e truffe. Un utente, in base ai propri gusti e alla propria esperienza potrà scegliere quale browser utilizzare.

I BROWSER PIÙ SICURI

"Non esiste un browser più sicuro di un altro". Questo è quanto è emerso dai vari studi e dai numerosi test effettuati sui diversi browser presenti oggi sul mercato.

I test hanno dimostrato che tutti i browser presentano delle falle, anche se quelli più noti (Internet Explorer e Mozilla Firefox) vengono presi di più di mira dai *cracker*, proprio per la maggior diffusione e quindi, per questi sono stati rilevati più *buchi* di sicurezza rispetto ad altri. C'è, però, da dire che le società Mozilla (Firefox) e Microsoft (Internet Explorer) sono tra le più veloci a fornire soluzioni alle vulnerabilità scoperte.

CONSIGLI PER NAVIGARE IN SICUREZZA

In conclusione, la scelta del browser viene fatta in base ai propri gusti, l'importante è aver installata sempre l'ultima versione. In genere, l'aggiornamento è un'azione che avviene in automatico all'apertura del browser.

Inoltre, è consigliabile abilitare sempre sul proprio browser il blocco dei pop-up, impostando correttamente le preferenze presenti nella sezione apposita del browser.

e-mail

CHE COS'È?

L'e-mail (electronic mail) è un servizio di posta elettronica disponibile in Internet che permette lo scambio di messaggi tra due o più utenti.
La caratteristica principale che ha permesso la diffusione della posta elettronica è la rapidità nel ricevere qualsiasi tipo di messaggio, in modo più veloce ed economico rispetto all'utilizzo del classico servizio postale. Per poter utilizzare la posta elettronica bisogna prima di tutto creare un proprio *account e-mail*.

ACCOUNT E-MAIL

Una casella di posta (*o account e-mail*) è individuata dall'indirizzo utente@dominio, formato da tre campi:

- utente
- @ (chiocciola, si legge at o presso)
- dominio

Utente

È scelto personalmente dal proprietario dell'indirizzo di posta al momento della creazione dell'account e-mail. Può essere formato da lettere, numeri e alcuni caratteri speciali.
Il nome utente è univoco per ciascun dominio, motivo per cui è possibile che al momento della creazione del nostro indirizzo di posta ci venga chiesto di modificare il nome utente poiché quello scelto è già in uso.

@

Serve da separatore tra il nome utente e il dominio, è necessario per i *server* che gestiscono la posta ad individuare dove finisce il nome utente e dove inizia il dominio, in modo da poter indirizzare correttamente il messaggio.

Dominio

è il fornitore che offre il servizio di posta (es.: alice.it, tiscali.it, yahoo.com, gmail.com), quindi anch'esso viene scelto dal proprietario della casella di posta.

CREARE UN ACCOUNT

Oggi sono davvero tanti i siti che permettono di creare una casella di posta elettronica ed ogni utente può possedere uno o più indirizzi e-mail, anche su siti diversi. Quando ci si collega ad un sito che offre questo servizio, nella sezione mail, si richiede di inserire i propri dati per accedere alla casella e-mail con un bottone/link *Entra* o *Login*.

Se non si ha ancora un indirizzo, un link *Sei un nuovo utente? Registrati* dà la possibilità di creare un nuovo account, accedendo ad un modulo di registrazione. E'necessario compilare tutti i campi richiesti (nome, cognome, indirizzo, data di nascita, etc...) e ad un certo punto scegliere un nome utente *user* e una parola chiave *password*. Queste ultime informazioni sono importanti per accedere alla casella e-mail, poiché in genere serviranno a creare l'indirizzo di posta elettronica.
Si consiglia dunque di scegliere un nome utente appropriato; la password invece dovrà rispettare alcune regole, a volte decise dal gestore del sito (ad esempio: essere minimo di 6 caratteri alfanumerici, ovvero potrà contenere solo lettere e/o numeri, per un massimo di 16 caratteri).
Terminata la compilazione del modulo, si conclude la creazione dell'account cliccando sul bottone a disposizione per completare la registrazione.
Generalmente, viene presentato un messaggio di avvenuta registrazione ed è consigliabile salvare, o meglio stampare, e conservare la pagina di riepilogo contenente tutti i dati: l'indirizzo e-mail, la password di accesso, i dati anagrafici, e gli indirizzi dei server SMTP e POP, indispensabili per accedere alla casella e-mail direttamente tramite un client di posta elettronica.

GESTIRE UN ACCOUNT E-MAIL

Un utente che possiede un account e-mail può ricevere messaggi nella sua casella di posta e può inviare messaggi ad altri utenti, contenenti anche uno o più file allegati alla e-mail.

RICEVERE MESSAGGI

La posta può essere letta via web direttamente su sito del dominio o tramite appositi client di posta (es.: Outlook), su cui è possibile configurare uno o più account di posta, che in maniera automatica o manuale si collegano all'account di posta replicando i messaggi sul proprio pc.
Quando ci si collega al sito, inserendo i propri dati (user e password) nella maschera di login, si accede al proprio account di posta elettronica.
Tutte le mail contenute nell'account sono suddivise per cartelle:

- Posta in arrivo
- Posta inviata
- Bozza
- Cestino

E'possibile, inoltre, creare cartelle personali per conservare le e-mail, definendone il nome che si desidera; poi, selezionando i messaggi dalla Posta in arrivo, si può scegliere di spostare tali

messaggi nella cartella. Nella cartella Posta in arrivo, saranno visualizzati i messaggi ricevuti, quelli non letti saranno identificati con colore o stile diverso (in grassetto o evidenziati).

INVIARE MESSAGGI

Per inviare un nuovo messaggio di posta, selezionare l'opzione "Nuovo" (o "Scrivi nuovo messaggio"). Si presenterà un modulo, diviso in due sezioni: l'intestazione e il corpo del messaggio. Queste costituiscono la struttura di un messaggio di posta.

Intestazione

Contiene obbligatoriamente: l'e-mail del mittente del messaggio

Campo A

L'e-mail di uno o più destinatari del messaggio
e altre informazioni opzionali, così descritte:

Campo OGGETTO

si può scrivere un titolo o una frase riassuntiva del contenuto del messaggio.

Campo CC (Carbon Copy)

È possibile inserire uno o più indirizzi e-mail in copia di conoscenza. I destinatari (Campo A:) sono a conoscenza che il messaggio è stato inoltrato anche a questi altri indirizzi. In particolare, i destinatari presenti in CC, ricevono la e-mail solo a scopo informativo.

Campo BCC (Blind Carbon Copy) o CCN (Copia Conoscenza Nascosta)

È possibile inserire uno o più indirizzi e-mail, che riceveranno una copia di conoscenza del messaggio, ma a differenza di ciò che accade nel campo CC, il loro indirizzo non sarà visibile agli altri destinatari dell'e-mail.

Campo Rispondi A

È possibile specificare un indirizzo e-mail, diverso da quello relativo al mittente, al quale eventualmente inviare messaggi di risposta.

Corpo

Rappresenta il contenuto del messaggio. Una volta visualizzato un messaggio ricevuto, si può: rispondere al mittente, scegliendo "Rispondi" (o "Reply"), rinviare il messaggio ad altri destinatari, scegliendo "Inoltra" (o "Forward"). E'possibile rimuovere eventuali allegati presenti nel messaggio o aggiungerne di nuovi.

ALLEGARE DOCUMENTI

E'possibile allegare documenti, foto, immagini ad un messaggio di posta, utilizzando il bottone o il link "Allega". Questo servizio permette di cercare sul proprio pc il file da allegare alla mail; ogni dominio fissa un peso massimo da rispettare per gli allegati.

SICUREZZA DELLA POSTA ELETTRONICA

La posta elettronica, per il semplice fatto che rappresenta il mezzo più efficace e veloce per lo

scambio delle informazioni, è anche il mezzo più utilizzato per la diffusione di virus, spam, phishing ed altri scopi malevoli. Di seguito sono riportati alcuni tipi di *attacchi* che possono verificarsi tramite e-mail, il phishing verrà trattato in un capitolo a parte.

SPAM

Un messaggio di posta elettronica inviato con lo scopo di promuovere, pubblicizzare o informare l'utente di un prodotto o un servizio, viene considerato spam.
Spesso, però, si tratta di messaggi inviati all'utente, a seguito di un suo consenso, cioè l'utente stesso ha dato esplicito consenso a voler ricevere informazioni su quel prodotto/servizio. E'consigliabile, perciò, ogni qualvolta si effettua una registrazione ad un servizio on-line, leggere attentamente la normativa della privacy associata, ove è possibile trovare informazioni riguardo al trattamento dei dati personali.

VIRUS, MALWARE, TROJAN

Un messaggio di posta elettronica può essere inviato anche con il solo scopo di crear danni all'utente, con l'invio di virus, malware e trojan. Generalmente, il mezzo utilizzato da queste applicazioni sono gli allegati (ad esempio file applicativi, il cui nome ha estensione .exe). E'consigliabile non aprire gli allegati, provenienti da indirizzi e-mail non conosciuti; sebbene oggi esistono anti-virus sempre più all'avanguardia, per garantire un livello di sicurezza abbastanza elevato.

COME DIFENDERSI

Ecco alcuni consigli per il corretto utilizzo di una casella di posta:

- *Apertura dei messaggi*
  Fare attenzione nell'aprire messaggi di posta elettronica, scaricare ed aprire allegati di cui non si conosce il mittente; in caso di dubbio è meglio cancellarli.
- *Non rispondere alle mail di spam*
  Spesso, in queste mail, si offre la possibilità di disattivare la ricezione dei suddetti messaggi; in pratica questa tecnica è utilizzata dallo spammer per accertarsi che l'indirizzo a cui ha inviato la mail sia valido.
- *Disattivare l'opzione anteprima*
  In quasi tutti i programmi di posta elettronica, è offerta l'opzione di leggere il messaggio ricevuto senza aprirlo, ma spesso anche la sola anteprima *apre* l'e-mail, dando così la possibilità ad eventuali virus di attivarsi o inviare allo spammer la conferma che l'indirizzo è valido ed utilizzato.
- *Limitare la diffusione del proprio indirizzo e-mail*
  Evitare di scrivere il proprio indirizzo e-mail su forum (gruppi di discussione) o siti Internet che non sono di vostro interesse o che non frequentate regolarmente; esistono

programmi, utizzati dagli spammer che “cercano” in Rete indirizzi validi.
Creare un indirizzo alternativo per registrarsi a forum, newsletters e community può essere utile.

- *Utilizzare i filtri antispam*
  Quasi tutti i programmi di posta elettronica forniscono gratuitamente un servizio di filtri in grado di riconoscere ed eliminare la posta non desiderata.
- *Evitare le “catene di S. Antonio”*
  Non rispondere a quelle mail che chiedono di rispedire il messaggio ad un certo numero di persone “promettendo” fortuna o mala sorte, o quelle di casi di gente disperata. Il più delle volte, sono storie inventate per ottenere una convalida dell’indirizzo e-mail ed ottenere nuovi indirizzi.

Nel dubbio, visitate il sito HTTP://ATTIVISSIMO.BLOGSPOT.COM/P/INDICE-DELLE-INDAGINI-ANTIBUFALA.HTML .
Una valida arma di difesa contro lo spam, spesso, può essere semplicemente un pò di buon senso e il saper mettere in dubbio ciò che si riceve.

il phishing

CHE COS'È?

Il phishing (letteralmente si traduce "pescare") è un'attività illecita usata per il furto d'identità, con lo scopo di "pescare", rubare informazioni personali, come numero di conto corrente, numero di carta di credito o altri dati privati della "vittima".

COME FUNZIONA

Nella maggior parte dei casi, questo tipo di attacco avviene tramite messaggi di posta elettronica fittizi, a volte vengono utilizzate anche finestre di pop-up o schermate di login fasulle.
Nal caso delle e-mail, di solito, un messaggio di phishing riporta loghi, contenuti, suggerimenti e quant'altro riguardi la società utilizzata per la frode (nella maggior parte dei casi si tratta di Poste Italiane o Banche), suggerendo di cliccare un bottone o un link che indirizza ad una pagina, molto simile graficamente, ma contraffatta, a quella del sito di riferimento. Qui viene richiesto di inserire i propri dati personali, ad esempio, informazioni come:

- *nome utente e password*
- *codice fiscale*
- *numero di carta di credito*
- *numero del conto bancario*
- *codice pin (codice di identificazione personale)*

L'utente "vittima", credendo di fornire informazioni ad un'azienda credibile, rende noti invece i propri dati al truffatore, cadendo nella sua trappola.

COME DIFENDERSI

Navigando in Rete è facile essere "pescati" da phisher intenzionati a rubare la nostra identità o i nostri dati sensibili, è bene quindi prestare piccoli accorgimenti per non "abboccarre" a truffe ingannevoli.

Browser Aggiornato

La prima cosa da fare è aggiornare il proprio browser perché i nuovi browser hanno un filtro anti-phishing che non permettono l'apertura di pagine web non sicure.

Siti Web Sicuri

In caso si utilizzi la propria carta di credito o il proprio numero di conto corrente, è importante notare che nella pagina web, in basso a destra ci sia un'icona a forma di lucchetto chiuso e che nella barra degli indirizzi dopo "http" compaia una ***S***: HTTPS://. Se l'indirizzo del sito, infatti, non è preceduto da HTTPS (la "***S***" vuol dire "sicuro", sta per transazione criptata, quindi sicura)

indica che la pagina non è sicura ed è dunque consigliabile non inserire alcuna informazione personale. Attenzione che molti siti contraffatti mostrano l'icona del lucchetto all'interno della pagina, invece che sulla barra di stato, proprio con lo scopo di ingannare chi vi accede.

Servizi Bancari

Alcuni istituti bancari permettono di controllare il proprio conto corrente da casa, cioè on-line, e inoltre mettono a disposizione un servizio SMS che avvisa in tempo reale i propri clienti dei movimenti compiuti.

Inoltre, per l'accesso on-line, alcune banche forniscono i propri clienti di un portachiavi (token) che genera numeri casuali che vengono richiesti al momento dell'accesso al sito. Quando una persona scopre di spese a suo carico effettuate da terzi, la prima cosa da fare è telefonare alla propria Banca per comunicare l'accaduto e per bloccare la propria carta, poi esporre denuncia presso la Polizia Postale. Comunque la vittima della frode avrà diritto ad un rimborso.

Maggiori informazioni e/o suggerimenti relativi ai conti bancari on-line sono esposti nel capitolo apposito. È importante ricordare che nessun Istituto Bancario richiede tramite e-mail informazioni personali.

certificati ssl e tsl

CHE COSA SONO?

L'SSL (Secure Sockets Layer) o il TSL (Transport Layer Security) sono dei protocolli di crittografia che permettono le comunicazioni tra un client ed un server in modo sicuro.
L'utilizzo dei certificati è utilizzato principalmente dalle banche, per transazioni on-line e per i siti di e-commerce (commercio elettronico).

COME FUNZIONANO

Quando si naviga in rete, il problema della sicurezza riguarda tutte le informazioni, soprattutto quelle relative al commercio elettronico o quelle coinvolte in una transazione economica; in pratica, non si ha mai la certezza con chi si sta *parlando* e ciò rende diffidenti nell'inviare informazioni.
I siti web che hanno necessità di effettuare delle transazioni sicure verso i propri utenti creano dei certificati digitali, che sono rilasciati o validati da società, pubbliche o private, chiamate Certification Authority.
Dopo uno scambio di certificati, i dati trasmessi viaggiano in un canale preferenziale in modo che nessun altro, all'infuori del client e del server, possano leggere, intercettare o modificare il contenuto dei dati.
Il certificato digitale funge, dunque, da documento di riconoscimento del sito-web e fornirà all'utente *fiducia* nell'Autorità di Certificazione che lo ha emesso. Quando l'utente accede ad un sito, per effettuare una transazione sicura, il certificato digitale viene attivato in maniera automatica dal browser che è in grado di riconoscerne anche la validità.
In pratica, l'attivazione della transazione sicura è facilmente verificabile con qualsiasi browser in quanto la URL del sito cambierà in automatico da http ad **HTTPS** (es.: HTTPS://WWW.MIOSITO.IT).
Di solito, nel momento in cui si lascia l'area sicura, il browser presenta all'utente un messaggio avvisando che da quel momento in poi le informazioni sensibili che verranno inserite sono a rischio.
In caso di certificati scaduti o non validati da una Authority, il browser segnalerà l'anomalia del certificato; si può scegliere, a proprio rischio e pericolo se continuare la connesione o meno.

IN BREVE

- L'SSL e il TSL garantiscono trasmissioni sicure tra due computer.
- Per attivare una connessione sicura è necessario disporre di un certificato; preferibilmete validato da una Certificate Authority.
- Nel caso di inserimento di dati sensibili nel web assicurarsi sempre che la transazione sia sicura. Un comunicazione è sicura quando nella barra degli indirizzi, il nome del sito è preceduto da HTTPS (con il browser Internet Explorer è presente un lucchetto chiuso in basso a destra).
- Attenzione ai sito dove il browser segnala che il certificato offerto è scaduto o non validato.

conto bancario on-line

CHE COS'È?

La Banca on-line (o anche Home Banking) è un servizio ormai offerto da tutte le banche per la gestione del proprio conto corrente. Questo sistema, è stato adottato dalle banche "tradizionali", ma soprattutto ha permesso la nascita di banche che operano totalmente on-line, le quali, riducendo i costi di filiali, sportelli ed altre spese, spesso riescono ad offrire notevoli vantaggi rispetto alle banche "tradizionali".

I principali servizi offerti sono:

- movimenti di conto corrente e saldo
- bonifici e giroconti
- pagamento bollettini di conti correnti postali/imposte/tasse/RAV
- pagamento ricariche di telefoni mobili
- domiciliazione delle utenze convenzionate
- estratto conto delle carte di credito
- gestione titoli

COME ATTIVARE IL SERVIZIO

Per attivare il servizio di home banking è possibile recarsi nella propria filiale e chiedere informazioni in merito. In caso di banche on-line, di solito, è sempre attivo un numero verde dove si è seguiti fino all'apertura del conto.

COME ACCEDERE AL SERVIZIO

Generalmente le banche forniscono un codice cliente e un pin per accedere al pannello di gestione del conto bancario.

Di solito i conti on-line hanno quasi sempre due pin, uno per l'accesso al conto e l'altro per la convalida delle operazioni, questo per aumentare il livello di sicurezza.

Alcune banche, come secondo pin forniscono all'utente un portachiavi (token), associato al proprio conto. Il token genera un codice temporaneo ogni 60 secondi da inserire al momento in cui viene richiesto.

Per accedere al conto on-line, dunque, è necessario andare sul sito della propria banca ed autenticarsi con i proprio dati personali:

- *Codice Cliente o Codice Conto*: assegnato dalla Banca al momento dell'attivazione;
- *PIN*: codice numerico segreto;
- *Secondo PIN*: alcune banche richiedono al login anche il secondo codice per l'accesso, per altre è necessario prima di eseguire un'operazione.

Di solito, al primo accesso viene chiesto di modificare il codice pin, assegnato dalla banca al momento dell'attivazione; dopo aver impostato un nuovo codice personale, questo potrà essere utilizzato per i successivi accessi al sito bancario.

UTILIZZARE IL CONTO BANCARIO ON-LINE IN SICUREZZA

Le banche on-line sono dotate di sistemi di protezione molto avanzati per impedire a chiunque di accedere a dati sensibili dei propri clienti. Una delle falle più grosse nella sicurezza dell'home banking è dovuta proprio a "disattenzioni" degli utenti.

Quindi, come per tutto quello che riguarda Internet, è consigliato seguire delle semplici regole:

- Non accedere al conto online da computer pubblici o condivisi.
- Digitare sempre l'indirizzo del sito web della propria banca e non cliccare mai su link ricevuti via e-mail o presenti sul web, potrebbero reindirizzare a siti cloni.
- In caso di una connessione sicura (HTTPS://), cliccando due volte sul lucchetto o sulla chiave che appare in basso a destra del browser (Internet Explorer), è possibile visualizzare il certificato che mostra la genuinità del sito.
- Le informazioni con cui si accede ai servizi della propria banca (codice utente, PIN, etc...) sono strettamente personali, ed è bene custodirli con molta attenzione.
- Un istituto bancario non richiede mai dati sensibili dei propri utenti telefonicamente, via e-mail o sms; questi mezzi sono utilizzati solo per fornire informazioni.
- Una volta terminate le operazioni online, occorre sempre chiudere la connessione cliccando su esci, logout (o uscita).
- In caso di furto/smarrimento dei codici di accesso occorre subito bloccare i codici, denunciare l'accaduto alle Autorità competenti e quindi inviare una copia alla banca.
- Attivare, se previsti, i meccanismi di sicurezza aggiuntivi, come: le notifiche via SMS o e-mail delle operazioni effettuate.
- Controllare regolarmente l'estratto conto, in questo modo ci si può assicurare che le operazioni riportate siano quelle realmente effettuate. In caso contrario, bisogna contattare subito la Banca, tramite il servizio call center o recandosi direttamente in filiale.
- Non abilitare mai il salvataggio automatico della password, né sul sito né sul browser.

e-commerce e aste on-line

CHE COSA SONO?

E-Commerce, o commercio elettronico, è la compravendita on-line di un servizio o un bene tra venditore e acquirente.

Aste on-line, è un'asta in linea, in rete. Proprio come nelle aste vere e proprie, il bene viene messo all'asta dal venditore ad un prezzo minimo; gli acquirenti, a partire dal prezzo di partenza, fanno un'offerta superiore; allo scadere del tempo (anch'esso imposto dal venditore), il miglior offerente (chi ha fatto l'offerta più alta) si aggiudica il bene. E'un'asta, ma il tutto avviene on-line. Il più diffuso sito d'aste on-line è e-Bay.

CONSIGLI PER EFFETTUARE ACQUISTI ON-LINE

L'ostacolo maggiore al commercio elettronico è sicuramente rappresentato dal timore dell'utente di essere truffato, ad esempio ricevendo merce diversa da quella visionata e ordinata on-line o addirittura non ricevendola affatto. Per questi motivi molti utenti sono diffidenti a fornire via web informazioni relative alla propria carta di credito.

Tale apprensione diffusa può derivare da una cattiva informazione: quando si desidera fare compere on-line, oltre a prestare la normale attenzione come acquirente, è consigliabile seguire alcune semplici regole.

SICUREZZA DEL "NEGOZIO"

Innanzitutto è sempre meglio acquistare da siti che godono di una certa "fama", cioè quei siti che sono notoriamente affidabili per il commercio elettronico. Se si è alle prima esperienze, ci si può anche far indicare i siti dove parenti, amici o conoscenti hanno già acquistato qualcosa con esiti andati a buon fine.

Una buona prassi è effettuare un'indagine avvalendosi di motori di ricerca per trovare opinioni in merito al negozio on-line presso cui si vuole fare un acquisto.

Altra cosa da verificare è se il negozio on-line da noi scelto permette di fare transazioni in modalità sicura. Si consiglia, dunque, di controllare nella sezione "Termini e Condizioni" del sito o nella pagina di acquisto, se sono utilizzati canali di trasmissione sicuri come l'SSL, il TSL o il SET (Secure Electronic Transaction). Diffidate dei siti che non offrono una connessione

sicura, in questi casi, scegliete, se è possibile, di pagare in contrassegno, in modo da poter verificare la merce al momento della consegna.
Esistono alcuni loghi presenti su un sito di e-commerce che garantiscono la trasparenza e la correttezza del negozio nel trattamento dei dati personali; assicurano, cioè, il rimborso integrale della cifra in caso di uso improprio dei dati bancari dell'utente. Un esempio sono i loghi: Fianet Trusted Shops, Webcert e Webtrust.

GARANZIE E DIRITTO DI RECESSO

Ricordarsi sempre di esaminare lo stato della merce al momento della consegna ed indicare sulla ricevuta del corriere eventuali irregolarità. Segnalarle, se presenti, anche al venditore e chiedere una sostituzione o il rimborso del prodotto.

Diritto di Recesso

Anche quando si acquista un prodotto online esiste per il consumatore il diritto di recesso. Per esercitare tale diritto è necessaria la consegna del bene entro dieci giorni (sette nel resto dell'Unione Europea), inviando una raccomandata con avviso di ricevimento al venditore e nello stesso termine restituire il prodotto a vostre spese.
Il venditore ha l'obbligo di restituirvi le somme versate entro breve tempo, e comunque non oltre trenta giorni dalla data in cui è venuto a conoscenza del recesso.
Se avete pagato con carta di credito, la società emittente è obbligata a restituirvi la somma eventualmente addebitata per errore o per frode (da parte del venditore o di terzi).
Questo è quanto previsto dal decreto legislativo n° 185 del 1999.
Se il venditore non risponde alla richiesta di rimborso, è bene rivolgersi all'associazione dei consumatori ADOC per avere assistenza per far valere i propri diritti oppure direttamente all'ufficio di Polizia Postale, responsabile delle indagini sulle frodi relative a siti Web.

Garanzie

A tutte le vendite si applica la garanzia europea di conformità.
Il consumatore è assistito dalle stesse garanzie previste per le compravendite tradizionali: garanzia di conformità prestata dal venditore (obbligatoria), garanzia di buon funzionamento prestata dal produttore.
La garanzia vale per due anni dal momento della consegna e può essere fatta valere entro due mesi dalla scoperta del problema, il consumatore può chiedere la sostituzione o la riparazione del prodotto, e solo se queste sono difficoltose o impossibili si può chiedere la diminuzione del prezzo o la risoluzione del contratto (con restituzione del denaro al cliente e del prodotto al venditore).

ACQUISTO E PAGAMENTO

Gli acquisti on-line, nella maggior parte dei casi, si svolgono tramite un carrello elettronico. Un carrello elettronico è semplicemente una pagina web che permette di gestire gli acquisti dell'utente durante lo shopping on-line. Permette quindi la visualizzazione e la scelta degli

articoli nelle varie versioni, il controllo della disponibilità, la scelta della modalità di pagamento, il tipo di trasporto e la registrazione dell'indirizzo al quale inviare la spedizione fisica.
Si ricorda che i dati inseriti nel carrello non sono impegnativi, quindi è possibile in qualsiasi momento cancellare i dati, rimuovere gli articoli dal carrello e rinunciare all'acquisto.
E'buona norma, se possibile, procurarsi i riferimenti del venditore quali l'indirizzo della sede commerciale, il recapito telefonico e l'indirizzo di posta elettronica, così da poterlo contattare direttamente per ogni tipo di problema.
E'importante, inoltre, conservare l'e-mail di conferma dell'acquisto che il venditore vi invia dopo aver fatto l'ordine e il pagamento, in quanto è l'unico documento che dimostra la transazione avvenuta.
Esistono svariati metodi di pagamento on-line, tra cui:
Contrassegno; *Bonifico Bancario*; *Vaglia* o *Bollettino Postale*; *PayPal*; *Carte di Credito*.
E'preferibile comunque utilizzare una carta prepagata per tutti i tipi di pagamento on-line.

PayPal

La PayPal, una società del gruppo Ebay, è il sistema di pagamento più diffuso. E'un vero e proprio intermediario di pagamento e offre garanzie al consumatore. Con PayPal è possibile associare al proprio conto una carta di credito (o prepagata ricaricabile) Visa, Visa Electron e MasterCard, o utilizzando il proprio saldo.
La registrazione è gratuita; è necessario solo un indirizzo e-mail per la notifica delle transazioni eseguite. Per maggiori dettagli consultare il sito HTTP://WWW.PAYPAL.IT.

Carte di Credito

Un altro metodo comodo e veloce per effettuare acquisti su Internet è la carta di credito.
Accettata da quasi tutti i negozi on-line, per utilizzarla è sufficiente inserire il numero della propria carta, il nome del titolare e la data di scadenza. In alcuni casi viene richiesto anche il numero di sicurezza di 3 o 4 cifre stampato sul fronte o sul retro della carta.
Molte banche offrono un servizio gratuito che notifica via SMS ogni transazione effettuata con la propria carta. Per i più diffidenti, esiste una vasta offerta di carte prepagate ricaricabili, accettate quasi ovunque.

PRATICI CONSIGLI PER E-BAY

Per sicurezza, prima di iniziare un'asta è consigliabile leggere tutte le clausole ad essa relative e qualora fosse possibile, richiedere l'invio di alcune foto dell'oggetto in questione.
E'consigliato informarsi sulla "reputazione" del venditore presente su e-Bay, prima di procedere con l'acquisto. Ciò è possibile consultando il suo Punteggio di Feedback.
Verificando, infatti, il Feedback che il venditore ha ricevuto nelle transazioni eseguite e leggendo i commenti lasciati dai precedenti acquirenti, si può avere una maggiore sicurezza sulla serietà del "negoziante".
Un venditore che riceve molti Feedback positivi viene contrassegnato come "Power Seller": questo garantisce un'affidabilità riconosciuta da altri utenti e dal sistema e-Bay.

IN BREVE

- Acquistare da siti Internet conosciuti, meglio ancora se qualche parente o amico ha già effettuato acquisti sul sito da voi scelto.
- Confrontare il prezzo del prodotto anche su altri siti Internet.
- Diffidare, a meno di evidenti garanzie, dai prezzi troppo bassi rispetto al valore commerciale del prodotto.
- Preferite siti che offrono transazioni sicure nella fase di pagamento HTTPS://
- Verificare l'esistenza del venditore, l'esattezza dei dati riguardanti la sede sociale, l'indirizzo ed il numero telefonico.
- Leggere sempre le condizioni generali di contratto, in particolare le disposizioni che regolano la spedizione e l'eventuale restituzione e le indicazioni che regolano l'accesso al diritto di recesso.
- Accertarsi sull'ammontare delle spese di spedizione e informarsi su chi grava il rischio per smarrimento durante la spedizione.
- Stampare i documenti della vendita (descrizione del prodotto, ordine, le attestazioni dell'ordine e di pagamento, etc.).
- Nelle aste on-line: accertatevi che sia concesso dalla casa d'asta il diritto di recesso.

SEDI PROVINCIALI ADOC CAMPANIA

Sede Regionale e Provinciale
Piazzale Immacolatella Nuova, 5 (interno porto) 80133 Napoli
tel. 081.2252411/420/435 · *fax* 081.5534453
web www.adoc-campania.it · *e-mail* info@adoc-campania.it

Sede Provinciale di Avellino
Via Fratelli Bisogno, 27/a 83100 Avellino
tel. 0825.33477 · *fax* 0825.25024/0825.683901/0825.250219

Sede Provinciale di Benevento
Piazza S. Donato, 2 82100 Benevento
tel. 0824.42719 / 0824.21743 · *fax* 0824.29434/0824.29289

Sede Provinciale di Caserta
Via Roma, 66 81100 Caserta
tel. 0823.320279 / 0823.344328 · *fax* 0823.320501/0823.455932/0823.216339
e-mail adoccaserta@hotmail.com

Sede Provinciale di Salerno
Via Renato De Martino, 10 84124 Salerno
tel. 089.488111 · *fax* 089.234488
e-mail adoc.salerno@virgilio.it

Contattateci per conoscere tra le altre Sedi quella a voi più vicina.

WIKIPEDIA

Il lettore alle prime armi potrà effettuare delle ricerche usando un sito di facile consultazione che è Wikipedia.
Nata dal progetto della Wikimedia Foundation, un'organizzazione senza scopo di lucro, è un'enciclopedia libera. La sua principale caratteristica è di permette a chiunque di collaborare, dando la possibilità di inserire/modificare una pagina relativa ad un certo argomento, mediante un sistema aperto di modifica e pubblicazione. Le inserzioni degli utenti, solo dopo essere state inserite, vengono esaminate dai collaboratori del progetto per verificarne la veridicità ed essere eventualmente modificate e/o cancellate.

HTTP://IT.WIKIPEDIA.ORG/WIKI/WIKIPEDIA

LA RETE	HTTP://IT.WIKIPEDIA.ORG/WIKI/RETE_DI_CALCOLATORI
LAN	HTTP://IT.WIKIPEDIA.ORG/WIKI/LOCAL_AREA_NETWORK
MAN	HTTP://IT.WIKIPEDIA.ORG/WIKI/METROPOLITAN_AREA_NETWORK
WAN	HTTP://IT.WIKIPEDIA.ORG/WIKI/WIDE_AREA_NETWORK
BROWSER	HTTP://IT.WIKIPEDIA.ORG/WIKI/BROWSER
E-MAIL	HTTP://IT.WIKIPEDIA.ORG/WIKI/E-MAIL
SPAM	HTTP://IT.WIKIPEDIA.ORG/WIKI/SPAM
VIRUS	HTTP://IT.WIKIPEDIA.ORG/WIKI/VIRUS_(INFORMATICA)
MALWARE	HTTP://IT.WIKIPEDIA.ORG/WIKI/MALWARE
TROJAN	HTTP://IT.WIKIPEDIA.ORG/WIKI/TROJAN
PHISHING	HTTP://IT.WIKIPEDIA.ORG/WIKI/PHISHING
SSL – TSL	HTTP://IT.WIKIPEDIA.ORG/WIKI/SECURE_SOCKETS_LAYER
CERTIFICATI	HTTP://IT.WIKIPEDIA.ORG/WIKI/CERTIFICATO_DIGITALE
HOME BANKING	HTTP://IT.WIKIPEDIA.ORG/WIKI/HOME_BANKING
TRADING ON-LINE	HTTP://IT.WIKIPEDIA.ORG/WIKI/TRADING_ONLINE
E-COMMERCE	HTTP://IT.WIKIPEDIA.ORG/WIKI/E-COMMERCE
E-BAY	HTTP://IT.WIKIPEDIA.ORG/WIKI/E-BAY

GLOSSARIO

File
in italiano "archivio" è un contenitore di infomazioni (documento Word, Excel, immagine, audio)

Directory
in italiano "cartella" è un contenitore di file

Cavo UTP (Unshielded Twisted Pair)
cavo non schermato utilizzato comunemente per il collegamento nelle reti

Wireless
collegamento in rete "senza fili"

Wi-Fi
tecnologia per il collegamento senza fili.

HTTP (HyperText Transfer Protocol)
un linguaggio che permette la lettura semplificata dei dati trasmessi in rete

HTML (HyperText Markup Language)
linguaggio usato per la scrittura di pagine web

URL (Uniform Resource Locator)
è l'indirizzo di una risorsa in Internet (siti, documenti, immagini etc. etc.)

Cracker
persona che commette crimini informatici

Pop-up
pagina web che si apre in maniera automatica, di solito utilizzata per la pubblicità in Internet

Account
casella di posta elettronica

Server
un computer utilizzato per fornire servizi ad altri computer

Login
procedura di autenticazione che richiede un nome utente (user) ed una parola chiave (password)

PIN (Personal Identification Number)
codice di identificazione personale

SET (Secure Electronic Transaction)
è un protocollo per le transazioni sicure con carte di credito sviluppato da Visa e Mastercard

DL n° 185 del 1999
link ufficiale per i dettagli sul decreto HTTP://WWW.PARLAMENTO.IT/PARLAM/LEGGI/DELEGHE/99185DL.HTM

Feedback
valutazione, commento, opinione, in caso di commercio elettronico, che un acquirente lascia su un venditore (o viceversa) in seguito ad una transazione. Possono essere positivi, negativi o neutri.

finito di stampare nel mese di ottobre 2010 da
Tipografia IRIDE s.r.l. Arzano, Napoli