Banca Regionale di Sviluppo SpA

GUIDA

REGOLE DI SICUREZZA PER UN CORRETTO USO DEL SERVIZIO HOME BANKING

SETTEMBRE 2016

Sommario

Banca Regionale di Sviluppo SpA

Premessa

La presente guida ha lo scopo di raccoglie e sintetizzare le principali regole di sicurezza che ciascun cliente deve conoscere per poter utilizzare in sicurezza del servizio di Home Banking della Banca Regionale di Sviluppo SpA.
La guida non può essere considerata come una raccolta esaustiva ed esauriente delle regole di sicurezza a cui il cliente deve attenersi.L'evoluzione continua dell'informatica, da intendersi sia in accezione positiva(nuovi sviluppi informatici di hardware e software),sia negativa (aumento dei rischi potenziali di attacchi criminali di tipo informatico), ha come conseguenza la necessità di monitorare e, di adeguare di conseguenza, la presente Guida in considerazione dei rischi legati all'utilizzo del canale internet.Leconsiderazioni ed i consigli elencati in questaguida si limitano pertantoad individuare quelle elementari "misure di sicurezza"da rispettare nell'utilizzo della rete Internet.
Occorre sempre tenersi aggiornati sulle possibili truffe e sui nuovi suggerimenti per contrastarle, collegandosi ad alcuni siti istituzionali,impegnati nel contrasto a frodi informatiche (ad es. polizia di stato, polizia postale), ovvero da cui si possono ottenere aggiornamenti sulle regole di comportamento per un corretto uso di internet (Netiquette):

http://www.poliziadistato.it/articolo/17734-Rischi_e_pericoli_del_web_come_difendersi/

https://www.commissariatodips.it/da-sapere/per-i-cittadini-e-i-ragazzi/internet-qualche-precauzione.html

https://www.commissariatodips.it/da-sapere/per-i-cittadini-e-i-ragazzi/internet-rischi-e-minacce.html

https://it.wikipedia.org/wiki/Netiquette

Il significato di alcuni termini informatici è riportato alla fine del documento nella sezione Glossario.

Regole generali per una maggiore sicurezza nella navigazione internet

- ✓ Rifletti bene prima di pubblicare qualsiasi cosa in rete. Ricorda che, fotografie, video, commenti, messaggi ed altre informazioni personali possono essere visti da sconosciuti e potrebbero rimanere in rete per sempre;
- ✓ Proteggi le tue informazioni personali ed evita che siano rese pubbliche e visibili a tutti;
- ✓ Evita la diffusione dei propri dati personali sui social network, mail e telefono
- ✓ Scegli con cura le password per le tue aree personali (scegli quelle con lunghezza adeguata, utilizza lettere maiuscole, minuscole e caratteri speciali, non lasciarle incustodite e non divulgarle ad altri, evita di usare la stessa password per siti diversi, non usare password con propri dati personali o di familiari facilmente rintracciabili in rete (es. data nascita, nomi persone care, ecc.);
- ✓ Diffida delle persone conosciute in rete ed evitalo scambio di informazioni personali con queste persone;
- ✓ Nelle chat, nei blog, nei forum, nei giochi non dare mai il tuo nome, cognome, indirizzo, numero cellulare o numero di casa. Chi chatta con te potrebbe non essere chi dice di essere e nascondere le vere intenzioni;
- ✓ Non scaricare programmi se non ne conosci la provenienza, potrebbero contenere malware che danneggiano il dispositivo o che rendono accessibili anche le tue informazioni riservate;
- ✓ Attento ai falsi messaggi allarmistici, offerte imperdibili, richieste di aiuto, promesse di ricariche, regali, vincite, diffida di tutti questi messaggi;
- ✓ Sui social controlla bene chi può vedere il tuo profilo e le tue informazioni esponendoti in situazioni che potrebbero sfuggire dal tuo controllo.
- ✓ Cancella sempre la cache e la cronologia della navigazione di internet;
- ✓ Non scaricare files o documenti non sicuri provenienti da fonti/siti non sicuri e conosciuti
- ✓ Non scaricare files o documenti non sicuri provenienti da mail con mittenti non conosciuti ovvero da mail di mittenti conosciuti ma su argomenti o temi inaspettati. In caso di dubbi richiedere sempre la conferma al mittente del messaggio
- ✓ Fai attenzione a eventuali peggioramenti delle prestazioni generali (rallentamenti, apertura di finestre non richieste, ecc.) o a qualsiasi modifica improvvisa delle impostazioni di sistema, che possono indicare infezioni sospette.
- ✓ Durante la navigazione in internet, installa solo programmi di cui puoi verificare la provenienza.
- ✓ Aggiorna costantemente sistema operativo e applicativi del computer, installando solo gli aggiornamenti ufficiali disponibili sui siti web delle aziende produttrici.
- ✓ Diffida di qualsiasi messaggio, anche se apparentemente autentico, ricevuto tramite e-mail, sms, social network, etc. che ti invita a scaricare documenti o programmi in allegato. Potrebbero contenere dei malware che si installano sul tuo pc.
- ✓ Diffida di qualunque richiesta di dati relativi a carte di pagamento, chiavi di accesso all'home banking o altre informazioni personali ricevute su qualsiasi canale digitale (posta elettronica, sms, etc.). La tua banca e qualunque altra Autorità non ti chiederanno mai queste informazioni, anche in ragione di presunti motivi tecnici o di sicurezza.

Regole sull'uso e gestione di Hardware/ dispositivi elettronici

- ✓ Tieni il tuo dispositivo ben protetto con programmi antivirus, sistemi di firewall per filtrare e proteggere la propria connessione;
- ✓ Tieni aggiornato sempre il tuo software (ad es. pur in presenze di un buon programma Antivirus, il mancato aggiornamento ti espone a notevoli rischi);
- ✓ Installa e mantieni aggiornati software di protezione (antivirus e antispyware), ed effettua delle scansioni periodiche del tuo hard disk;
- ✓ Se noti un peggioramento delle prestazioni del tuo device (ad. es. rallentamenti della velocità del device, apertura di programmi o finestre non richieste), procedi ad un controllo antivirus del device;
- ✓ Fai utilizzo delle procedure di aggiornamento automatico dei programmi antivirus e delle patch dei programmi utilizzati (ad. es. Word, Excel, ecc.);
- ✓ Non utilizzare dispositivi (tablet, Iphone, ecc.) con Jail Break;
- ✓ Non utilizzare Sistemi operativi obsoleti dichiarato dal produttore non più aggiornati (ad. es. il Sistema Operativo Windows XP è stato dichiarato "out of support" (fuori manutenzione) a partire dalla date del 08/04/2014);
- ✓ Utilizzo di sistema operativo con licenza ufficiale, aggiornato secondo le ultime versioni/release rilasciate dal produttore del software;
- ✓ Cambia la password standard di Amministratore fornita dal produttore del modem;
- ✓ Abilita la protezione più robusta per consentire il collegamento al modem in modalità wi-fi;
- ✓ Inserisci una password complessa per consentire il collegamento al tuo wi-fi;
- ✓ Non divulgare la password di Amministratore del modem e del collegamento wi-fi;
- ✓ Modifica periodicamente le password del modem e wi-fi;
- ✓ Prima di collegare qualsiasi dispositivo al proprio device (ad. es. PC) verifica la non presenza di file contagiati con i programmi antivirus;
- ✓ Evita di utilizzare tastiere senza fili (wireless) perché potenzialmente non sicure in quanto le sequenze di caratteri digitati possono essere suscettibili di essere spiate per carpire dati sensibili come password e numeri di carte di credito

Banca Regionale di Sviluppo SpA

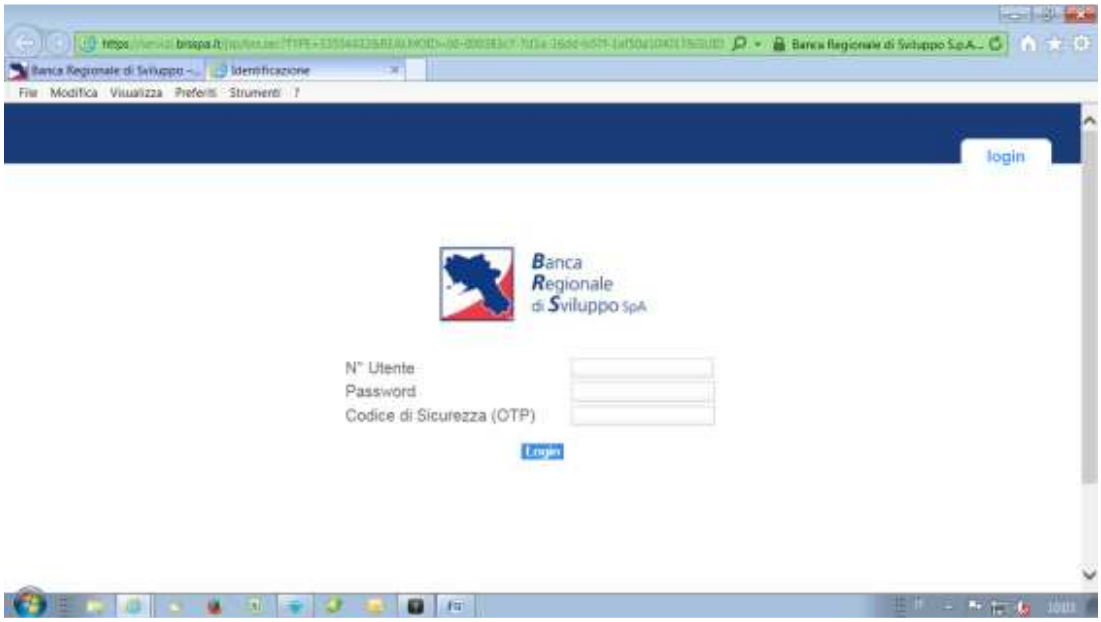
Regole di comportamento per collegarsi al sito Home Banking della Banca

- ✓ Cerca di utilizzare sempre il tuodispositivo per il collegamento al Servizio di Home Banking. Evita l'uso di PC o dispositivi pubblici (hotel aeroporti, negozi che offrono collegamenti ad internet, ecc.) o di terzi.
- ✓ Cancella sempre la cache e la cronologia della navigazione di internet prima e dopo esserti collegato al Servizio Home banking della Banca;
- ✓ Utilizza sempre lo stesso browser dedicato per i collegamenti alla tua Banca (ad esempio se per la navigazione uso sempre Internet Explorer, posso utilizzare altro browser – MozzillaFirefox, Chrome od altro – per le transazioni su Home Banking). Il browser prescelto per queste transazioni on line preferibilmente deve essere privo di componenti aggiuntivi;
- ✓ Evitadi collegarti al sito della banca mediante link da te salvati nella lista dei "preferiti" o tramite motori di ricerca (Google, Libero, ecc.);
- ✓ Per connetterti al sito della tua banca, scrivi direttamente l'indirizzo internet della BRS (***https://brsspa.it***) nella barra di navigazione. Non cliccare mai su link presenti su e-mail e sms, che potrebbero invece condurti su siti contraffatti, molto simili a quelli originali.
- ✓ Non utilizzare reti di collegamento pubbliche di fonti dubbie non protette o non sicure (wi-fi pubbliche o negozi che offrono servizi di collegamento ad internet a pagamento);
- ✓ Utilizza una connessione ad internet sicura da casa. Se usi la connessione con modem wi-fi verifica che la rete sia protetta da password complesse con adeguato protocollo WPA;
- ✓ Cambia di frequente la password complessa del modem che utilizzi per la connessione;
- ✓ Non collegarsi mai al sito della Banca attraverso link provenienti da qualsiasi fonte (esempio messaggio posta elettronica) . La banca non invia mai messaggi del genere né richiede il cambio delle credenziali via mail.
- ✓ Controllare che il collegamento al sito della Banca sia sempre protetto dalla presenza dell'apposito lucchetto chiuso e dal protocollo di sicurezza "***https://*** " prima di inserire le proprie credenziali

- ✓ Prima di inserire le credenziali di accesso al Servizio di Home banking, accertati della presenza del colore verde nella barra di navigazione. Specificamente il colore apparirà nei modi seguenti a seconda del browser utilizzato sull'indirizzo internet di collegamento al servizio della banca:

Internet Explorer (IE):

La schermata di BRS quando si utilizza il browser IE mostrerà una **"colorazione verde"**di tutto l'indirizzo web della pagina del nostro sito, del lucchetto e del nome della banca.



Chrome:

La schermata di BRS quando si utilizza il browser Chrome mostrerà una **"colorazione verde"**solo del lucchetto, del nome della banca e della stringa "**https**" dell'indirizzo.

MozillaFirefox:

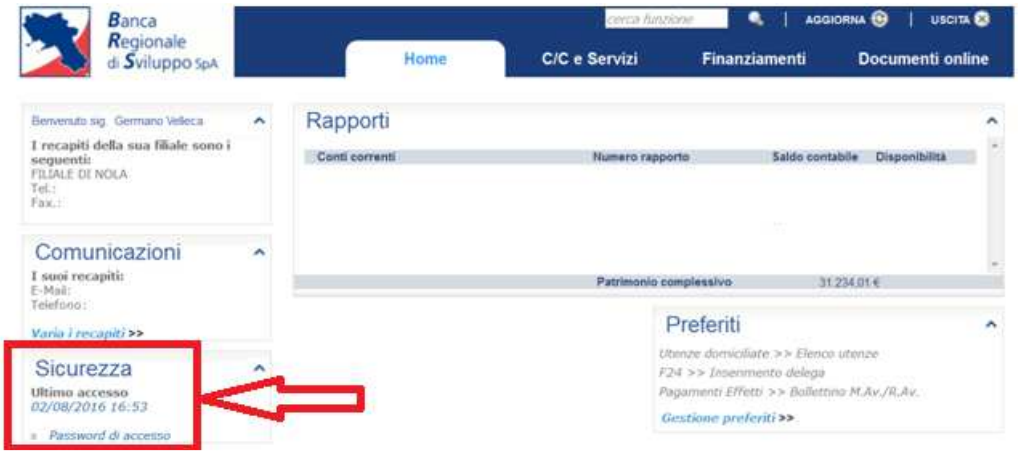
La schermata di BRS quando si utilizza il browser Mozilla mostrerà una **"colorazione verde"**solo del lucchetto e del nome della banca.

Safari:

La schermata di BRS quando si utilizza il browser Safari mostrerà una **"colorazione verde"**solo del lucchetto e del nome della banca.

- ✓ Verifica l'autenticità della connessione con la tua banca, controllando con attenzione il nome del sito nella barra di navigazione. Se è presente, "clicca" due volte sull'icona del lucchetto o sulla i d'informazione

- ✓ Annota la data ed ora del tuo ultimo collegamento. Verifica che essa corrisponda a quanto riportato nella Home Page del tuo Internet Banking (riquadro "Sicurezza") non appena hai ultimato l'accesso. In caso di mancata coincidenza procedi subito al blocco delle tue credenziali e contatta immediatamente i tuo referenti di filiale.



- ✓ Utilizzare il blocco computer con password quando ci si allontana dalla postazione in uso
- ✓ Non lasciare attiva la propria sessione di lavoro di collegamento al proprio Home Banking una volta terminata l'operatività on line;
- ✓ Ricordati di effettuare il log out (Uscita) della sessione di collegamento al Servizio Home Banking una volta completata l'operatività

- ✓ Controlla regolarmente le movimentazioni del tuo conto corrente per assicurarti che le transazioni riportate siano quelle realmente effettuate e utilizza eventuali strumenti di notifica delle operazioni svolte se messi a disposizione dalla tua banca.
- ✓ Se riscontri problemi o anomalie nei servizi di Home Banking rivolgiti alla tua banca, che potrà fornirti chiarimenti ed informazioni utili.

Banca Regionale di Sviluppo SpA

Regole di comportamento per corretta gestione delle password

- ✓ Utilizza sempre password complesse cambiandole di frequente (ad esempio leggi i consigliindicati da microsoftsul tema alla pagina web https://www.microsoft.com/it-it/security/online-privacy/passwords-create.aspx);
- ✓ Non comunicare a nessuno la propria password;
- ✓ Non utilizzare l'opzione per il salvataggio delle credenziali e delle password automatiche sul tuo Browser. Di seguito alcuni suggerimenti per i principali programmi internet più in uso. Per ogni ulteriore chiarimento ed aggiornamento verificare i consigli proposti dal produttore del singolo software utilizzato:


Internet Explorer:
Clicca sul menu "Strumenti" e seleziona la voce "Opzioni Internet"- Clicca sulla voce "Contenuto" e clicca sul tasto "Impostazioni" nel riquadro "Completamento automatico" – disattiva le spunte presenti nelle varie voci specificamente quella indicata come "Nome utente e password sui moduli", conferma premendo il tasto "OK".


MozillaFirefox:
Cliccare sul menù "Strumenti" ed attivare "Opzioni" - Cliccare quindi sulla voce "Sicurezza"e verifica che sia disattiva la voce "Ricorda i dati di accesso ai siti".


Chrome:
Cliccare sul menù in alto a destra, selezionare "Impostazioni", scegliere in basso "Mostra Impostazioni avanzate". In "Password e moduli" deselezionare la casella accanto alla voce "Richiedi di salvare le tue password web".


Safari:
Cliccare sul menù "Safari", scegliere "Preferenze" e poi selezionare "Password". Verificare che non sia attivo la modalità "Riempimento automatico di nomi utente e password".

- ✓ Non salvare i tuoidati segreti di accesso all'Home Banking sul computer o sul telefonino o su altri dispositivi ovvero nel portafoglio/telefono facilmente rintracciabili;
- ✓ Per la creazione di una password numerica è opportuno non utilizzare codici facilmente associabili alla propria persona, come ad esempio la data di nascita, oppure troppo banali (ad esempio 12345678).
- ✓ Modifica la password di accesso ai servizi online frequentemente ed immediatamente se ritieni che qualcuno ne sia venuto in possesso.
- ✓ La password di default, assegnata in fase di primo accesso o di richiesta nuova password deve essere sostituita subito;

Banca Regionale di Sviluppo SpA

Conoscere il Phishing

Definizione

Il phishing è un sistema di acquisizione fraudolenta dei dati riservati di alcuni utenti mediante l'invio di e-mail aventi l'obiettivo di allarmare il destinatario.

Come funziona

Il Cliente riceve nella sua casella di posta elettronica una e-mail che ad un utente superficiale sembra provenire da una fonte/mittente ufficiale (ad. es. il tuo Istituto di Credito, il tuo fornitore di energia elettrico, qualcuno che si spaccia o utilizza una mail di un tuo carissimo amico, ecc.).
Nella mail viene richiesto con motivazioni pretestuose di inserire i propri dati personali ovvero di collegarsi al sito della Banca/azienda attraverso un link riportato nel testo della mail. Il link collegherà l'utente ad una pagina web che è stata clonata graficamente dai pirati informatici, il cui unico scopo è quello di sottrarre le credenziali di accesso dell'utente al sito ufficiale. Le credenziali acquisite ingannevolmente consentiranno ai malfattori di collegarsi fraudolentemente al sito della Banca/Azienda.

Suggerimenti per evitare il phishing

Di seguito alcuni suggerimenti che possono evitare a chiunque di cascare nella trappola del phishing.

1. per nessuna ragione verranno richiesti dagli Istituti di Credito o dai siti di commercio elettronico tramite e-mail richieste d'inserimento di codici segreti, numeri di carta elettroniche,ecc.);
2. un tipico messaggio di "phishing"contiene, generalmente, nel corpo del testo dell'e-mail unlink al quale l'utente è inviato a collegarsi. La pagina che verrà visualizzata attivando il linksi troverà su di uno spazio web abusivo, anche se graficamente analogo al sito originale;
3. è consigliabile mantenere aggiornato il proprio sistema di protezione che, oltre adifendere dai virus che circolano in rete, alleggerirà anche le problematiche legate allospamming e al phishing;
4. è consigliabile imparare a riconoscere le email false. Di solito contengono l'indirizzo del mittente in formato web (es.: nome.cognome@dominio), non sono personalizzate e dichiarano intenti non ben specificati (es: risoluzione di fantomatici problemi di sicurezza, adesioni ad 'imperdibili' offerte, riscossione di vincite) o spesso usano anche toni "intimidatori", come le minacce di sospensione del servizio in caso di mancata risposta;
5. è fondamentale non cliccare sui link e non aprire files allegati;
6. i siti web proposti da email sospette non vanno visitati, neppure per brevi periodi. La stessa precauzione vale per i files allegati che non devono essere mai letti e salvati sul proprio PC.
7. nonrispondere mai alla email di spamming e phishing né cliccare sul collegamento riportato nella mail per richiedere la cancellazione della propria mail dalla lista dei destinatari.
8. e'sempre consigliabile segnalare l'accadutoverificatosi.Nel caso in cui si riceva un'email sospetta, è raccomandabile informare subito la propriaFiliale o in alternativa, denunciare l'accaduto all'Autorità Giudiziaria o di Polizia.Le segnalazioni possono attivare contromisure immediate per proteggere gli altri clienti.

9. Usa sempre il buon senso:se una email ti appare sospetta, diffida e cerca un sistema per verificare l'autenticità (ad esempio chiama il referente della filiale della tua Banca o il tuo amico che ti ha inviato la mail)

Credenziali per utilizzo dell'Home Banking di Banca Regionale di Sviluppo

Il sistema di sicurezza adottato dalla Banca richiede l'utilizzo contemporaneo di tre credenziali:

1. N° Utente
   Detto anche UserIDo Codice Cliente è il codice numerico assegnato al cliente dalla banca all'atto della sottoscrizione del contratto di Servizio Home banking.

2. Password
   E' la password numerica,composta di 9 caratteri numerici, consegnata dal cliente in busta chiusa che consente il primo accesso. La password di primo accesso fornita dalla Banca deve essere cambiata dal cliente appena effettuato il primo accesso. Per ovvi motivi di sicurezza,si suggerisce di provvedere a cambiare la password anche più volte in un mese.

3. Codice di Sicurezza (OTP -One Time Password)

   E' il codice numerico di 6 caratteri causali variabile ogni 60 secondi visualizzabile sulla chiavetta personale (Dispositivo di sicurezza) consegnata al cliente dalla BRS all'atto della conclusione del contratto di attivazione del Servizio. La chiavetta personale ha una scadenza riportata sul retro della stessa. Alla data di scadenza il cliente deve chiedere la consegna di una nuova chiavetta personale.
   Il codice di sicurezza OTP è richiesto in fase di accesso all'area riservata ovvero ogni volta che si effettua una disposizione (ad esempio inserimento di una disposizione di bonifico) o una variazione di dati rilevati (ad esempio cambio dei dati presenti nella rubrica dei beneficiari dei bonifici)

Glossario

Antivirus	E’ un software programmato per funzionare su un computer atto a prevenire, rilevare ed eventualmente rendere inoffensivi codici dannosi, noti anche come malware, Un antivirus non ha solo la funzione di eliminazione dei programmi malevoli ma ha anche una funzione preventiva, impedendo che un virus possa entrare in un sistema ed infettarlo.
Blog	Sito web personale concepito principalmente come contenitore di testo (per es. come diario o come organo di informazione indipendente), aggiornabile dal singolo utente in tempo reale grazie ad apposito software.
Browser	Programma che consente di navigare ed interagire con le pagine web, i testi, le immagini ed altri elementi multimediali che formano internet o una rete locale.
Bug	Identifica un errore nella scrittura di un software (codice sorgente).
Cache	E’ un sistema attraverso il quale l’utente di internet salva sul disco rigido file temporanei relativi ai siti visitati. Questo permette di velocizzare in maniera significativa l'accesso ai siti più visitati, perchépermette al computer di richiamare i file salvati invece che scaricarli ogni volta da internet.
Chat	Servizio offerto da Internet, che permette mediante apposito software una ‘conversazione’ fra più interlocutori costituita da uno scambio di messaggi scritti che appaiono in tempo reale sul monitor di ciascun partecipante.
Chrome	Applicazione Web Browser
Componente aggiuntivo	Sono componenti di software in grado di aggiungere nuove caratteristiche e funzionalità al Browser.
Crittografia	E’ una tecnica di cifratura dei dati e del traffico scambiati in una rete (ad es. internet, una rete privata, ecc.).
Cronologia navigazione	La cronologia esplorazioni include le informazioni archiviate dal programma internet (Browser) in un PC mentre si naviga sul Web. Queste informazioni includono i dati che si immettono nei moduli, le password ed i siti visitati.
Device	Unità hardware, dispositivo elettronico (ad esempio dispositivi e apparecchi ad alta tecnologia e di piccole dimensioni quali smartphone, e-book reader, tablet PC ecc.).
Dominio	Nome alfabetico che identifica un’entità logica accessibile in rete Internet.
Firewall	E’ un componente per la sicurezza informatica con lo scopo di controllare gli accessi alle risorse di un sistema filtrando tutto il traffico che tale sistema scambia con l'esterno (es. internet). La protezione del firewall può essere rivolto ad un singolo computer o ad una rete di computer (ad esempio

	computer presenti in un'azienda).
Forum	Servizio Internet che permette di inviare e leggere messaggi su un argomento specifico, che restano a disposizione per i commenti altrui.
Internet Explorer	Applicazione Web Browser
Jail Break	E' una procedura non autorizzata che permette di installare su un device Apple (iPhone, iPad e iPod touch) meccanismi di distribuzione di applicazioni e pacchetti di applicazioni, non firmati, alternativi al canale ufficiale AppStore.
Link	Indicaun collegamento tra pagine diverse internet (collegamento ipertestuale). Ad esempio il link presente in una mail o in un documento se cliccato dall'utente, avvia il programma di internet che consente di collegarsi all'indirizzo della pagina web. Se non si è sicuri il link può essere uno strumento di perpetrare frodi informatiche (Phishing, Spamming, ecc.).
Malware	Programma informatico, documento informatico o messaggio di posta elettronica in grado di apportare danni a un sistema informatico.
MozzillaFirefox	Applicazione Web Browser
Opera	Applicazione Web Browser
Password Complesse	Sono protezioni più robuste che consentono di effettuare transazioni ed operazioni online più sicure.
Patch	E' una porzione di software progettata per aggiornare o migliorare un programma software. Può prevedere la risoluzione di vulnerabilità di sicurezzae altri bug generici, tali patch vengono anche chiamati fix o bugfix.
Phishing	Invio di e-mail per acquisire fraudolentemente dati personali quali numero di carte di credito, credenziali di accesso all'Home Banking.
Safari	Applicazione Web Browser
Sistemi operativi	E' un insieme di componenti software, che rende utilizzabile (operativo) il device/computer e/o altri apparati e dispositivi informatici.
Social	Servizio informatico on line che permette la realizzazione di reti sociali virtuali. Si tratta di siti internet o tecnologie che consentono agli utenti di condividere contenuti testuali, immagini, video e audio e di interagire tra loro.
Spamming	è l'invio anche verso indirizzi generici, non verificati o sconosciuti, di messaggi ripetuti ad alta frequenza o a carattere di monotematicità tale da renderli indesiderati (generalmente sono commerciali, offensivi ovvero anche a scopi di frode). Può essere attuato attraverso qualunque sistema di comunicazione, messaggi di posta elettronica, chat, forum, Facebook e altri

servizi di rete sociale.

WPA	E’ un protocollo di crittografia per lo scambio sicuro di dati tra il modem e il dispositivo (PC, Tablet, Iphone, ecc.).