



PROTEGGI I TUOI BAMBINI ONLINE

GUIDA A COME DIFENDERE L'ESPERIENZA DIGITALE DEI
TUOI BAMBINI

LOREDANA BOTEZATU, RAZVAN LIVINTZ
ESPERTI COMUNICAZIONE E ANALISI MINACCE ELETTRONICHE

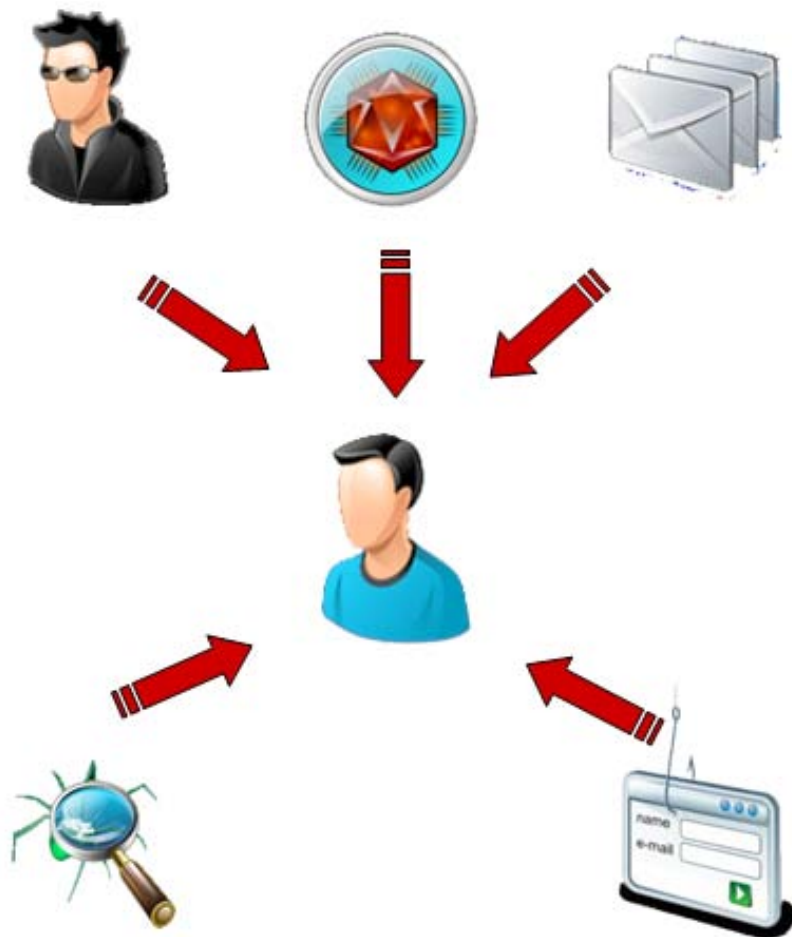
FAMIGLIA, GENITORI E INSEGNANTI



Indice

- Indice.....2
- I bambini e il Web3
- I maggiori rischi e pericoli per i bambini* 4
 - Dipendenza online.....4
 - Ciber-bullismo.....4
 - Esposizione a contenuti inappropriati.....5
 - Incoraggiare una condotta poco etica5
 - Azioni Illegali.....5
- Minacce per i sistemi e per i dati* 6
 - Malware6
 - Phishing e furto di identità6
 - Spam7
- Consigli per una navigazione sicura7
- Consigli per bambini e ragazzi* 8
- Consigli per i genitori*..... 8
- Consigli per gli insegnanti*..... 10
- BitDefender ti aiuta a proteggere i tuoi bambini.....11

I bambini e il Web



Ci sono molte più probabilità per i ragazzi che per gli adulti di cadere in trappole su Internet.

La produzione di massa e la facilità d'accesso hanno trasformato i computer in beni di largo consumo, mentre le connessioni a Internet ad alta velocità stanno diventando uno standard sia per le utenze domestiche che aziendali. Un cambiamento significativo si è verificato nella nostra vita quotidiana, dove e-mail, messaggeria istantanea, social networking, blog, acquisti online, ecc... sono divenute azioni regolari.

Considerando che l'utente medio trascorre fino a cinque ore (a volte anche di più) di fronte a un computer, sia a lavoro che a casa, è probabile che i bambini inizino a familiarizzare con i PC sin da piccoli. Dall'altro lato per esempio, i nonni che vivono distanti, ora possono fare gli auguri di "Buon Natale" ai propri nipoti attraverso video-chat.

I bambini sono affascinati da Internet e la maggior parte di loro risulta essere estremamente abile quando si tratta di utilizzare un computer. Non c'è strumento più divertente o più facile per loro per fare amicizia, giocare o scambiare informazioni, sia a fini scolastici, sia per divertimento. Una conversazione iniziata dopo scuola, può facilmente continuare on-line, via chat, o sul "campo di battaglia" del gioco di ruolo online del momento.

Nonostante i suoi evidenti benefici di comunicazione, Internet può anche essere un luogo pericoloso. Può essere utilizzato per diffondere una vasta gamma di minacce, quali virus, worm, Trojan, per furti di password, keylogger, adware, per attacchi di phishing o spam e-mail. Può condurre alla diffusione di contenuti inappropriati, come la pornografia o materiale discriminatorio, e talvolta può essere veicolo di comportamenti non etici, come plagio o imbrogli.

A causa della loro età e della naturale curiosità per sperimentare cose nuove, i giovani possono facilmente trovarsi in situazioni delicate sulla rete. Per questo motivo, è importante per loro poter avere una buona guida fin dall'inizio e scoprire tutti gli aspetti positivi e negativi che Internet ha in serbo.

“I malintenzionati su internet non devono essere considerati come il problema di qualcun’altro. Loro sono anche un tuo problema “, avverte Catalin Cosoi, Ricercatore Esperto di BitDefender® “se non si tiene conto di alcune semplici linee guida sulla sicurezza, pensate allo scopo di proteggere i tuoi figli e la tua famiglia”, aggiunge Cosoi.

I maggiori rischi e pericoli per i bambini

Dipendenza online

La dipendenza online si manifesta attraverso l’uso compulsivo della messaggeria istantanea, dei social network o dei giochi, e può alterare il comportamento sociale dei bambini e il loro sviluppo, così come la loro condizione fisica.

Se i genitori non controllano costantemente le attività su Internet e la quantità di tempo trascorso davanti al computer, aumentano le possibilità che bambini e adolescenti si ritirino sempre più in un universo virtuale e si isolino dal mondo reale, impossibilitati o non desiderosi di interagire socialmente con gli altri in maniera non virtuale.



Il cyber-bullismo non dovrebbe essere sottovalutato quando si tratta della sicurezza online dei propri bambini

Ciber-bullismo

Il ciber-bullismo viene descritto come una situazione in cui un bambino o un adolescente è più volte tormentato, minacciato, vessato, umiliato, imbarazzato o in altro modo attaccato da un altro bambino o adolescente attraverso messaggi di testo, e-mail, chat o qualsiasi altro tipo di tecnologia digitale.

Questo tipo di comportamento è di solito ricorrente, divenendo una minaccia credibile. Le ragioni alla radice di tutto ciò possono essere rabbia, vendetta o frustrazione, ma a volte i ragazzi lo fanno anche per divertimento o per combattere la noia.



Lo spam può esporre i bambini a contenuti inappropriati

Esposizione a contenuti inappropriati

Il materiale pornografico o discriminatorio è un altro dei rischi che i genitori dovrebbero prendere in seria considerazione. Senza la supervisione diretta, o una soluzione di sicurezza in grado di bloccare contenuti non appropriati, la curiosità potrebbe portare i bambini a cercare in rete film e immagini violente o sessualmente esplicite.

Allo stesso modo, in assenza di un filtro adeguato, i bambini potrebbero imbattersi in materiali che violano norme sociali, religiose, culturali o di altro tipo e standard, o in contenuti che mostrano loro attività illecite. I bambini possono anche accidentalmente scoprire queste cose tramite messaggi pubblicitari indesiderati visualizzati da diversi siti web.

Incoraggiare una condotta poco etica

Senza una guida, i bambini e gli adolescenti potrebbero essere tentati di plagiare o imbrogliare quando devono completare i loro progetti o compiti a casa.

Azioni Illegali

Se le interazioni online dei bambini sono poco sorvegliate, uno degli errori più frequenti che potrebbe avere implicazioni giuridiche è la condivisione di contenuti protetti da copyright.

Poiché la maggior parte di tale contenuto si trova su siti pirata o su piattaforme di condivisione di file, può accadere che i computer ed i dati verranno compromessi nel processo. Come illustrato nella Panoramica BitDefender sulle minacce online, [Bitdefender's E-Threat](#) queste fonti sono anche responsabili di un gran numero di infezioni, poiché diffondono malware assieme ai contenuti piratati.



Un sito web per bambini, apparentemente innocente, viene invece utilizzato per diffondere malware.

Minacce per i sistemi e per i dati

Malware

Per malware si intende qualsiasi tipo di programma per computer creato con un intento maligno e con l'obiettivo di manomettere il funzionamento del computer, rendere inutilizzabili le informazioni memorizzate, rubare i dati personali a scopo di lucro, ecc...

Nell'esempio qui a sinistra, un trojan sfrutta la ricerca fatta su Twitter per trovare maniere interessanti per l'intrattenimento dei bambini. Invece di trovare un sito Web con giochi e attività per bambini, i genitori che cliccano sull'indirizzo accorciato che viene visualizzato, sono reindirizzati verso pagine con diversi tipi di malware, compresi spyware. Senza una adeguata soluzione di sicurezza, qualsiasi sistema è a rischio.

Phishing e furto di identità

Questi termini si riferiscono al meccanismo che i criminali informatici utilizzano per indurre le persone a cedere i propri dati personali (es. numeri di carta di credito, PIN, ecc...). Per ottenere queste informazioni, creano copie di rinomate pagine Web (banche, applicazioni per social media, autorità statali, ecc.). Credendo erroneamente di trovarsi sui veri siti, gli utenti inseriranno i propri dati e si esporranno direttamente al rischio di frodi finanziarie.

Inoltre, i dati inseriti sulle pagine dei social network, blog e community sono sempre a rischio. Un indirizzo e-mail o una foto sono sufficienti per ottenere un profitto in maniera disonesta alle spalle di qualcun'altro. Due casi noti a riprova di questi schemi sono: un biglietto di auguri natalizi di una famiglia apparso in una pubblicità di alimentari, e una immagine rubata di un bambino utilizzata in uno schema fraudolento per una presunta adozione.

Spam

Il termine Spam si riferisce alla ricezione di e-mail indesiderate inviate a grandi gruppi di persone, in genere per promuovere diversi prodotti. Queste e-mail vengono utilizzate anche come esche in attività dannose più complesse, come il phishing, ma possono anche esporre i bambini a contenuti non adatti, come la pornografia.

Consigli per una navigazione sicura



Almeno la metà della nostra interazione quotidiana con i computer ruota attorno al World Wide Web. Ciò è probabilmente dovuto al fatto che questo sia percepito come un ambiente amichevole per lo scambio di diversi tipi di contenuti e per interagire. Da questo punto di vista, Internet rappresenta probabilmente uno degli strumenti educativi più preziosi del 21mo secolo, essendo allo stesso tempo il più grande database di conoscenza umana, e uno degli strumenti di comunicazione più complesse ed efficaci.

Come già spiegato in precedenza, con l'utilizzo di questo prezioso mezzo di comunicazione, i ragazzi possono inavvertitamente essere esposti a contenuti inadeguati, o possono diventare bersagli per coloro che mirano a farne un uso illegale per scopi pornografici, finanziari o di altra natura. Fortunatamente, queste situazioni indesiderabili possono e devono essere facilmente evitate da bambini, genitori e insegnanti, attraverso aperte discussioni sui vari aspetti relativi alla sicurezza online e alle misure necessarie per la sicurezza. Per quanto riguarda il momento ideale per avviare questo tipo di conversazione, dipende da quanto precocemente i PC diventato parte della vita dei bambini. La cosa importante è che prima che questi arrivino a utilizzare il computer, siano consapevoli delle minacce che l'interazione su Internet pone.



Parla sempre con i tuoi figli, spiega loro le tue preoccupazioni sulla loro sicurezza su internet e ascoltare quello che dicono.

Consigli per bambini e ragazzi

Non permettere al computer di impossessarsi della tua vita, di incidere sul tuo rendimento scolastico, o di sostituirsi ai momenti con i tuoi amici e familiari.

Quando crei un profilo per unirti ad una comunità online, chiedi aiuto ai tuoi genitori per fare un elenco delle persone di fiducia che saranno autorizzate a contattarti.

È sempre possibile interrompere le conversazioni online che mettono a disagio; se qualcuno o qualcosa sul web ti fa sentire spaventato, confuso, intrappolato, offeso o minacciato, parlane con i tuoi genitori e chiedi loro consiglio.

Non condividere informazioni su di te e la tua famiglia con persone che non conosci o di cui non ti fidi. Non accettare di incontrare persone sconosciute che ti hanno contattato online e assicurati di riferire ai tuoi genitori di qualsiasi tentativo di approccio diretto che ti viene fatto online.

Stai molto attento su quali foto e video decidi di caricare online - devi sapere che una volta pubblicati - non sarai più in grado di controllare completamente come verranno utilizzati.

Quando vuoi comprare qualcosa online, ed è necessario utilizzare una carta di credito, chiedi ai genitori il permesso e l'assistenza.

Fai attenzione quando scarichi giochi gratuiti e applicazioni, queste possono avere malware o contenuti inappropriati.

Consigli per i genitori

Qui presentiamo alcune idee per i genitori che vogliono prendere parte attiva nella vita online e offline dei propri figli.



Provate a spendere del tempo online assieme ai vostri bambini e aiutateli nelle loro ricerche, progetti e interessi. Questi momenti assumono un valore ancora maggiore quando potete dar loro alcune linee guida.

Cercate di scoprire quanto più possibile sulle esigenze informatiche e di Internet dei vostri figli e cercate di risolvere insieme i misteri del mondo cibernetico. Prendetevi il tempo per discutere delle minacce che Internet rappresenta per loro così come per l'intera famiglia.

Se possibile, posizionate il computer di famiglia in un luogo dove potete tenere un occhio sul monitor nel caso le circostanze lo richiedessero. Insieme con i vostri bambini, ricercate il loro nome su Internet e vedete che cosa viene fuori. Potreste trovare cose interessanti fatte dai vostri figli come i blog, o le comunità in cui sono direttamente attivi e vedere quali informazioni potete trovare su di loro e su tutta la famiglia. Ciò potrebbe dare ai vostri figli un senso di responsabilità e fargli capire che le loro azioni avranno ripercussioni su tutti i membri della famiglia.

Quando i bambini creano un loro profilo in una comunità online, aiutateli a utilizzare le funzioni di tutela della privacy. Create un elenco di persone di fiducia abilitate a contattarli. Incoraggiateli a limitare la quantità di informazioni esposte solo ad un certo numero di persone che si conoscono e di cui si fidano, e assicuratevi di sapere quali amici online il vostro bambino frequenta, proprio come si farebbe nella vita reale.

Insieme con i vostri figli, impostate alcune regole in materia di utilizzo del computer e del web, sottolineando le ragioni di sicurezza che potrebbero farvi preoccupare - l'obiettivo è quello di diventare un alleato di vostro figlio nella nostra lotta per la sicurezza.

Utilizzate un antivirus dotato di "Controllo Genitori" con tutte le impostazioni per il controllo dell'utilizzo del Web e delle varie applicazioni, nonché la capacità di filtro Web, posta elettronica e messaggia istantanea per determinate parole chiave.

Consigliate ai vostri figli di non rispondere alle e-mail che contengono messaggi di spam, contenuti osceni e aggressivi e, inoltre, consigliate loro di non inviare questo tipo di e-mail. Insegnate loro la responsabilità che hanno verso gli altri utenti all'interno di una comunità online, così come le regole essenziali della netiquette.

Consigli per gli insegnanti

Insieme con i genitori, voi come insegnanti, dovete essere consapevoli degli interessi online dei vostri studenti in modo da individuare e promuovere le caratteristiche forti e distintive di ogni generazione.

Assicuratevi di sapere quali filtri sono installati nei PC della vostra scuola e discutete con gli studenti perché queste misure di sicurezza sono così importanti per la scuola e per loro come persone.

Coinvolgete gli studenti nelle attività online, utilizzando il computer come uno strumento per scopi didattici. Incoraggiate gli studenti ad usare il computer e Internet come strumenti di ricerca, sottolineando l'importanza del lavoro originale e creativo. Assicuratevi che utilizzino applicazioni legittime e spiegate loro l'importanza dei diritti d'autore.

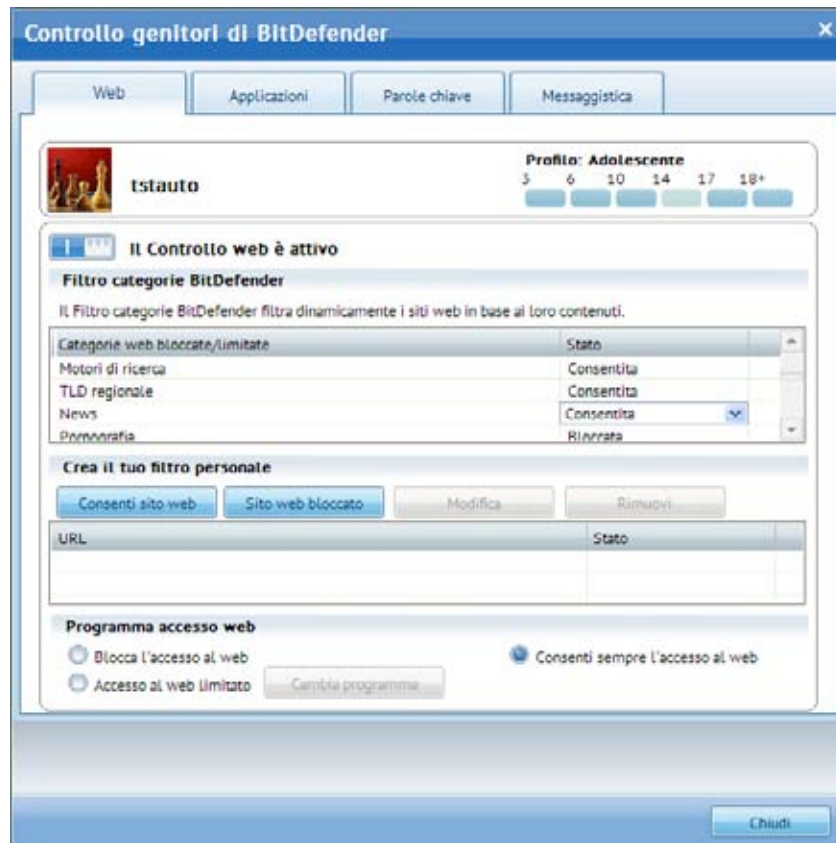
Assicuratevi che i vostri studenti comprendano come azioni apparentemente innocenti su Internet potrebbero nascondere intenzioni pericolose, e che i malintenzionati potrebbero utilizzare una grande varietà di metodi per ingannare gli utenti.

Spiegate ai vostri studenti le ragioni per cui non dovrebbero accettare di incontrare persone che non conoscono, e perché è così importante discutere sempre con i genitori di questo tipo di proposte che ricevono online.

Coinvolgete i genitori nelle attività scolastiche degli studenti e metteteli direttamente in contatto con le autorità coinvolte nella protezione dei bambini da attività illecite - pornografia online, droga o il furto di dati personali.



BitDefender ti aiuta a proteggere i tuoi bambini



Il modulo Controllo Genitori di BitDefender offre un modo semplice per proteggere l'attività online dei tuoi figli.

Il modulo Controllo Genitori di BitDefender offre opzioni di monitoraggio e controllo sia per le attività Web, sia per le varie applicazioni che i vostri figli utilizzano quotidianamente. Il Controllo Genitori prevede tre livelli di restrizione personalizzabili - bambino, adolescente e adulto, in base all'età dell'utente.

La componente **Controllo Web** consente - come genitore o insegnante - di filtrare il Web, la posta elettronica e le chat per determinare le parole chiave non consentite. In altre parole, sarai tu a decidere quali siti il bambino può o non può visitare in base al tipo di contenuto visualizzato o con quali contatti può chattare.

L'opzione per **L'accesso al Web Limitato** (Pianifica Orario) consente o blocca l'accesso a Internet nei momenti stabiliti. L'interfaccia intuitiva ricalca un calendario. Con un clic, ogni casella limita l'accesso a Internet per un determinato utente; se la stessa casella viene cliccata due volte, la restrizione viene rimossa.

La componente **Controllo Applicazione** consente di definire un rigoroso calendario in base al quale l'adolescente può accedere ad applicazioni specifiche - come giochi o programmi personalizzati, se ci riferiamo ad un computer di famiglia. È possibile impostare un ciclo orario o giornaliero, o bloccare completamente l'accesso a un determinato software o applicazione.

Il Controllo per la Messaggiera Instantanea permette di bloccare o consentire i diversi interlocutori via chat, mentre il Controllo Parole Chiave aiuta a limitare l'accesso al Web, e-mail e chat basandosi sulle parole chiave.

Un'altra caratteristica importante del Controllo Genitori è che i genitori possono ricevere una notifica via e-mail ogni volta che il servizio blocca un'attività che il bambino ha tentato di eseguire o possono consultare un log con la storia dei siti web a cui il bambino ha avuto accesso. Solo l'amministratore di sistema, quindi il genitore, può apportare modifiche nella sezione Controllo Genitori. Queste impostazioni possono essere protette con una password.

BitDefender con il suo Controllo Genitori sono disponibili per il download per 30 giorni di prova gratuiti su: <http://www.bitdefender.it/solutions>.

Seguici su:



Le informazioni e i dati presenti in questo documento rappresentano l'attuale opinione di BitDefender® sugli argomenti trattati al momento della pubblicazione. Questo documento e le informazioni presenti non devono essere interpretati in alcun modo come impegno o accordo di qualsiasi sorta per BitDefender.

Sebbene ogni precauzione sia stata presa nella preparazione di questo documento, l'editore, gli autori e i collaboratori non si assumono alcuna responsabilità per eventuali errori e/o omissioni. Tantomeno, si assumono responsabilità per eventuali danni derivanti dall'uso delle informazioni contenute nel presente documento. Le informazioni qui presenti sono soggette a modifiche senza preavviso. BitDefender, l'editore, gli autori e i collaboratori non garantiscono la pubblicazione di ulteriori documenti relativi ai contenuti qui presenti, o la pubblicazione di qualsiasi altra informazione futura.

Questo documento e i dati contenuti al suo interno sono solo a scopo informativo.

BitDefender, l'editore, gli autori e i collaboratori non forniscono alcuna garanzia, espressa, implicita o per legge, per quanto riguarda le informazioni contenute in questo documento.

Il contenuto del documento può non essere adatto per ogni tipo di situazione. Nel caso in cui assistenza a livello professionale fosse richiesta, si prega di richiedere la consulenza di un professionista. BitDefender, l'editore, gli autori e i collaboratori non sono responsabili per danni derivanti da questo documento.

Il fatto che un individuo o organizzazione, il lavoro di un singolo o collettivo, compresi materiali stampati, documenti elettronici, siti web, ecc... siano indicati in questo documento come una citazione e/o fonte di informazioni non implica che BitDefender, l'editore, gli autori e i collaboratori condividono le informazioni o le raccomandazioni che queste persone, organizzazioni, opere individuali o collettive, compresi i materiali stampati, documenti elettronici, siti web, ecc possono fornire. Informiamo i lettori che BitDefender, l'editore, gli autori e i collaboratori non possono garantire l'accuratezza delle informazioni qui presentate dopo la data di pubblicazione, includendo, ma non limitandosi a, indirizzi Web e collegamenti internet elencati nel documento, i quali potrebbero essere stati modificati o rimossi fra il momento in cui questo lavoro è stato scritto e pubblicato, ed è il momento in cui viene letto.

I lettori sono interamente responsabili al fine di rispettare tutte le leggi internazionali sul copyright derivanti dal presente documento. Fermi restando tutti i diritti coperti da copyright, nessuna parte di questo documento può essere riprodotta, memorizzata o inserita in un sistema di recupero dati, o trasmessa in qualsiasi forma e con qualsiasi mezzo (elettronico, meccanico, fotocopia, registrazione o altro), o per qualsiasi scopo, senza il permesso scritto di BitDefender. BitDefender può avere brevetti, domande di brevetto, marchi, copyright o altri diritti di proprietà intellettuale relativi all'oggetto del presente documento. Salvo quanto può essere espressamente previsto in un contratto di licenza scritto con BitDefender, il presente documento non fornisce alcuna licenza su tali brevetti, marchi, copyright o altra proprietà intellettuale.

Copyright © 2010 BitDefender. Tutti i diritti riservati.

Tutti i nomi di altre società e prodotti citati nel presente documento sono solo a scopo identificativo e sono di proprietà di, e possono essere marchi, dei rispettivi proprietari.