

Informatica per il Turismo

Nozioni di sicurezza informatica

Sicurezza nella Posta Elettronica

Vengono definiti **Spam** i cosiddetti messaggi spazzatura, ovvero quelli contenenti informazioni pubblicitarie di ogni genere.

Queste mail ovviamente non richieste costituiscono una notevole **perdita di tempo e di denaro**.

Gli indirizzi vengono reperiti all'interno di newsgroup o chat o in molti altri modi.

I Virus e la Posta Elettronica

La più diffusa preoccupazione riguardo l'uso della posta elettronica è la possibilità di ricevere via e-mail virus informatici in grado di distruggere i dati memorizzati sul nostro computer.

Alcuni Virus sono innocui e si limitano a creare solo effetti di disturbo, altri sono molto pericolosi perché possono

- cancellare file,
- rallentare il funzionamento del computer,
- ridurre lo spazio disponibile nella memoria principale,
- segnalare falsi funzionamenti.

Nei casi più gravi riescono a distruggere la file allocation table (FAT) e rendere il disco inutilizzabile.

I Virus e la Posta Elettronica

Essendo programmi i Virus **non possono** diffondersi attraverso semplici **messaggi di testo**. Quindi i messaggi di solo testo sono sempre sicuri.

Un **potenziale rischio** sono i **file allegati ai messaggi**.

Tramite gli allegati o attachment possono diffondersi due tipi di Virus:

- **Programmi eseguibili**, caratterizzati dall'estensione **.exe**
- **e macrovirus** inseriti in documenti **word o excel**.

I Virus e la Posta Elettronica

Per difendersi dal primo tipo di Virus basta fare attenzione a non aprire gli allegati inviati magari da persone che non si conoscono, è opportuno aprirli solo dopo che si è accertati della provenienza.

Allo stesso modo è sempre bene diffidare dei messaggi che arrivano da persone conosciute ma che hanno qualcosa di strano.

Capita di ricevere e-mail che avvertono che ci sono dei Virus che girano sulla rete, spesso queste e-mail sono degli scherzi e si chiamano Virus Hoax.

I Virus e la Posta Elettronica

I Virus meno conosciuti sono le Macro, a proposito di Word e Excel.

Trattasi di sequenze di operazioni che vengono impacchettate in un unico comando. In questo modo è possibile associare ad alcuni documenti particolari comandi, in modo che all'apertura del documento si producano determinate azioni.

I macrovirus sono difficili da individuare.

La Firma Digitale

La firma digitale consente ai destinatari dei messaggi di posta elettronica di verificare l'identità del mittente.

Per inviare i messaggi con la firma digitale è necessario ottenere un **ID Digitale**; gli **ID digitali** vengono rilasciati da autorità di certificazione indipendenti, alle quali bisogna fare esplicita richiesta.

Cosa sono i termini Cookie e Cache

- **Cookie:** (letteralmente biscottino) si definiscono quei file che vengono memorizzati sul disco fisso dell'utente navigatore da alcuni siti web.

Mentre l'utente visita un certo sito, vengono creati questi piccoli file in modo da fornire informazioni al gestore del sito ai successivi accessi.

Cosa sono i termini Cookie e Cache

- **Cache:** si definisce quella parte dell'hard disk dove vengono memorizzati i file temporanei internet. Essi non sono altro che le pagine web appena visitate memorizzate nel computer.

Per esempio se si visita spesso la stessa pagina la sua visualizzazione risulta più veloce perché può essere aperta direttamente da disco.

Sicurezza

- E' necessario che l'informazione che transita sulla rete sia riservata e non possa essere quindi captata e utilizzata da terze persone.
- E' necessario che le parti che procedono allo scambio di informazioni siano sicure dell'identità della rispettiva controparte.

Cos'è un sito protetto?

I siti protetti sono quei siti che possono garantire la sicurezza delle informazioni scambiate grazie all'implementazione di alcuni protocolli.

I protocolli di comunicazione sviluppati sono:

- Transport Layer Security (TLS) e il suo predecessore Secure Sockets Layer (SSL)
- HTTPS (HyperText Transfer Protocol over Secure Socket Layer)
- S-HTTP (Secure-HTTP)

TLS e SSL

- Protocolli crittografici che permettono una comunicazione sicura dal sorgente al destinatario (*end-to-end*) su reti TCP/IP (come ad esempio Internet)
- Forniscono
 - autenticazione
 - integrità dei dati
 - cifratura
- Operano al di sopra del livello di trasporto.

SSL

E' un protocollo sviluppato da Netscape ed è attualmente il più utilizzato.

Consente di ottenere una connessione sicura tra Client e Server provvedendo:

- alla cifratura dei dati
- all'autenticazione del server
- al controllo dell'integrità dei dati
- eventualmente all'identificazione del Client.

HTTPS

- HyperText Transfer Protocol over Secure Socket Layer (HTTPS) è il risultato dell'applicazione di un protocollo di crittografia asimmetrica al protocollo di trasferimento di ipertesti HTTP.
 - Un livello di crittografia/autenticazione come il Secure Sockets Layer (SSL) o il Transport Layer Security (TLS) si interpone tra il protocollo TCP e HTTP trasparentemente all'utente.
 - HTTPS usa il livello di crittografia per cifrare l'intera comunicazione.
- Viene utilizzato per garantire trasferimenti riservati di dati nel web, in modo da impedire intercettazioni dei contenuti.
- Il metodo che si riferisce a questa tecnologia è *https*
 - Per controllare che un sito è protetto è necessario controllare che nella barra dell'indirizzo figuri il predetto metodo *https*.

S-HTTP

È uno standard per la sicurezza proposto dal W3C (Consorzio che standardizza le applicazioni relative al web) che consente:

- L'autenticazione del server
- La crittografia dei dati inviati per i singoli messaggi (e non per l'intera connessione)

SSL e S_HTTP

SSL e S_HTTP sono protocolli che non si escludono a vicenda ma possono essere integrati.

Nome Utente e Password

Nella maggior parte dei siti protetti è necessario **identificarsi presso il server** prima di fornire i propri dati.

Nel sito verrà visualizzata una pagina dove inserire il proprio **nome utente** e **la propria password**.

Una volta che l'utente è stato riconosciuto verrà abilitato per usufruire dei servizi che offre il sito.

Certificato digitale di identificazione

I certificati digitali sono gli equivalenti elettronici di passaporti, carte d'identità, ecc.

Presentando il vostro certificato digitali si è sicuri della vostra identità.

Le Autorità di Certificazione si occupano di garantire l'identità di un soggetto.

Certificato digitale di identificazione

Un certificato digitale si avvale di una coppia di chiavi elettroniche: la chiave pubblica del proprietario, e la chiave privata dell'Autorità di Certificazione.

Oltre la chiave pubblica del proprietario bisogna avere altre informazioni: il nome del proprietario, la data di scadenza della chiave pubblica, il nome dell'emittente, il numero di serie del Certificato Digitale, la firma digitale dell'emittente.

La Crittografia

La crittografia è una scienza nata per scopi militari che studiava come mascherare le informazioni senza farle cadere in mano nemiche.

Si basa su algoritmi che sulla base di una chiave rendono il messaggio indecifrabile.

Frodi e utilizzo di Carte di Credito su Internet

Negli ultimi anni si sono sviluppati sul Web una serie di servizi, come l'e-commerce o l'home banking che presuppongono lo scambio di informazioni riservate come il numero della carta di credito.

Per questo motivo è necessario che l'informazione che transita sulla rete sia riservata e non possa essere quindi captata e utilizzata da terze parti.

I Virus

- I **Virus** sono quei programmi contenenti istruzioni potenzialmente dannose, in grado di introdursi in altri programmi modificandone il comportamento per l'utente.
- Possono trasmettersi attraverso lo scaricamento di file infetti con estensione .exe da un sito il cui server non risulti sicuro.

I Virus

Sono in grado di interferire con funzioni basi del computer:

- Creazione o cancellazione di file e cartelle.
- Agiscono sulla tabella di allocazione dei file.
- Agiscono sul settore boot, ovvero la parte del disco che contiene il programma per il caricamento del sistema operativo nella memoria RAM.

Cos'è un Firewall

I Firewall (letteralmente muri di fuoco) sono dei computer o anche solo dei programmi che hanno la funzione di filtrare tutta l'informazione che passa tra un computer o una rete e l'esterno.

I firewall permettono di bloccare tentativi di accesso al sistema da Internet e i *virus Trojan* che dall'interno di un computer e una rete aprono una porta di comunicazione con l'esterno o i *virus worm* che spediscono all'esterno dati importanti relativi a password e codici di accesso riservati.