

Dispensa di Sicurezza Informatica (Parte 3)

CAPITOLO 6 – COMUNICAZIONI

- **Cifrare e Decifrare un Messaggio di Posta Elettronica**

- I messaggi di posta elettronica, nella loro forma tradizionale, vengono trasmessi **in chiaro** attraverso la rete. Chiunque intercetti la comunicazione lungo il percorso può leggerne il contenuto.
- Per garantire la riservatezza e la protezione della privacy della comunicazione email, è necessario **cifrare il messaggio**.
- La cifratura rende il messaggio incomprensibile a chiunque non possieda la **chiave di decodifica**.

- **La "Firma Digitale"**

- La firma digitale è uno strumento che affronta il problema dell'identificazione del mittente in una comunicazione digitale. Poiché è facile creare un messaggio di posta elettronica facendolo sembrare provenire da qualcun altro, è necessaria una soluzione per **garantire l'identità del mittente**.
- Una firma digitale applicata a un documento elettronico garantisce tre aspetti fondamentali:
 - **Integrità:** Il destinatario può verificare che il documento non sia stato alterato dopo la firma. Non può aggiungere né creare contenuto facendolo risultare firmato dal mittente.
 - **Autenticità:** Permette di accertare l'identità del mittente del documento.
 - **Non ripudiabilità:** Il mittente non può negare di aver inviato il documento che ha firmato.
- Tecnicamente, la firma digitale si basa su un sistema a **due chiavi** (crittografia asimmetrica): una **chiave privata** (segreta, usata per firmare) e una **chiave pubblica** (condivisa, usata per verificare). Il processo coinvolge l'utilizzo di una funzione di **Hash** sul documento per ottenere una stringa univoca (impronta digitale), che viene poi cifrata con la **chiave privata** del mittente per ottenere la firma digitale. Il destinatario utilizza la **chiave pubblica** del mittente per decifrare la firma e confrontarla con l'hash calcolato sul documento ricevuto. Se coincidono, la firma è valida e il documento non è stato alterato.

- **Identificare Possibili Messaggi Fraudolenti e Indesiderati**

- Internet è un mezzo per uno scambio massiccio di informazioni. Purtroppo, questo include anche messaggi indesiderati o fraudolenti.
- **Junk mail** o **Spam**: posta indesiderata ricevuta in modo indiscriminato, spesso a scopo pubblicitario.

- **Messaggi fraudolenti:** messaggi che cercano di indurre i destinatari a fornire informazioni sensibili, spesso a scopo di lucro o per acquisire informazioni riservate. Il **phishing** è uno degli esempi più comuni.
- Quando si ricevono questi messaggi, è consigliabile cancellarli immediatamente **senza aprirli** e, soprattutto, **senza rispondere**, per evitare di confermare che l'indirizzo email è attivo.
- **Phishing: Caratteristiche e Come Riconoscerlo**
 - Il **phishing** è una truffa online che cerca di carpire informazioni sensibili come numeri di carte di credito, password, dati personali o finanziari.
 - Tipicamente, avviene tramite un'**email** che sembra provenire da un sito web legittimo (es. una banca, un servizio online) e che contiene un **link**. Questo link reindirizza l'utente a un **sito web fasullo**, quasi identico a quello originale, creato appositamente per ingannare. L'utente, credendo di essere sul sito legittimo, inserisce le proprie credenziali o dati sensibili, che vengono così rubati.
 - Per riconoscere un tentativo di phishing:
 - **Controllare la qualità del messaggio:** Spesso contengono errori grammaticali o offerte irreali.
 - **Verificare i dettagli del mittente:** Passare il mouse sul nome del mittente nella casella di posta può rivelare l'indirizzo email reale. Un indirizzo email non corrispondente al dominio ufficiale dell'organizzazione è un forte indizio di frode.
 - **Esaminare attentamente i link:** Non fare clic sui link sospetti. Passare il mouse sopra un link (senza cliccare) mostra l'URL di destinazione. Se l'URL reale non corrisponde al dominio atteso, è probabile che sia un sito fraudolento.
 - **Verificare l'autenticità del sito web:** Per attività sensibili come acquisti o operazioni bancarie, assicurarsi che l'indirizzo web inizi con **https://** e che sia presente l'icona del **lucchetto**. L'HTTPS e il lucchetto indicano che la connessione è cifrata e il sito è autenticato tramite un certificato digitale. Cliccando sul lucchetto si possono vedere i dettagli del certificato.
 - **Controllare il nome del dominio:** Assicurarsi che il nome del dominio nella barra degli indirizzi sia corretto.
 - **Pharming:** Una tecnica più subdola del phishing. Anziché ingannare l'utente con un link falso, il pharming **reindirizza automaticamente** il traffico da un sito legittimo a uno fasullo, modificando la configurazione del server DNS o il file hosts del computer dell'utente. L'utente potrebbe non accorgersi del reindirizzamento se non controlla scrupolosamente l'indirizzo e il certificato.
- **Rischio di Infettare il Computer con un Allegato o File Eseguitabile**
 - Gli allegati di posta elettronica e i file scaricati dal web rappresentano uno dei principali vettori di infezione per i malware.

- Prima di aprire un allegato, specialmente da mittenti sconosciuti, è fondamentale essere certi della sua sicurezza. È consigliabile sottoporlo a una **scansione antivirus**.
- Alcuni tipi di file sono particolarmente rischiosi, specialmente quelli eseguibili (.com, .exe, .vbs) o quelli che possono contenere macro dannose (.doc, .xls, .ppt). Le macro nei documenti Office dovrebbero essere disattivate per impostazione predefinita.
- **Importanza di Non Divulgare Informazioni Riservate o Personali**
 - Le reti sociali e i servizi online sono strumenti potenti per connettersi, ma comportano anche il rischio di **condividere eccessivamente informazioni personali**.
 - È importante essere consapevoli che le informazioni che si pubblicano online (come foto, video, opinioni) potrebbero essere visibili non solo agli amici ma anche a estranei.
 - Bisogna essere cauti nel condividere dettagli che potrebbero compromettere la privacy o la sicurezza. Questo include informazioni sulla propria posizione (tramite GPS dello smartphone), opinioni politiche o religiose, o altri dati sensibili.
- **Rivedere le Impostazioni del Proprio Account (Social Network)**
 - Controllare e regolare le **impostazioni sulla privacy** sui social network è cruciale per gestire chi può vedere i propri contenuti e contattarci.
 - Le piattaforme offrono diverse opzioni per limitare la visibilità dei post, delle foto, delle informazioni del profilo.
 - È possibile definire chi fa parte della propria rete di "amici" o contatti e impostare autorizzazioni specifiche per diversi gruppi.
 - Sulle principali piattaforme (Facebook, Twitter, Google+), le impostazioni si trovano generalmente nella sezione "Profilo" o "Account".
- **Potenziati Pericoli Connessi all'Uso dei Siti di Reti Sociali**
 - L'uso dei social network espone a diversi rischi, tra cui:
 - **Cyberbullismo:** Atti di prepotenza, molestie o intimidazione online.
 - **Contenuti Inappropriati:** Esposizione a materiale offensivo o dannoso.
 - **Divulgazione di Informazioni Personali:** Condivisione involontaria o consapevole di dati che possono causare danni o sfruttamento.
 - **Furto d'Identità:** Creazione di profili falsi per scopi fraudolenti.
 - **Link o Messaggi Fraudolenti:** Diffusione di phishing o altre truffe tramite la piattaforma.
 - È importante segnalare comportamenti inappropriati o contenuti dannosi alla piattaforma stessa o alle autorità competenti.
- **Sicurezza di Messaggistica Istantanea e VoIP**
 - Anche i servizi di messaggistica istantanea e le applicazioni VoIP (Voice over IP, per chiamate via internet) presentano rischi per la sicurezza.

- File o link ricevuti tramite questi servizi possono contenere malware.
- Il VoIP, essendo basato su protocolli internet, è vulnerabile a diversi attacchi tipici del web.
- Vulnerabilità specifiche del VoIP includono: **SPIT** (Spam over IP Telephony), intercettazione delle chiamate (eavesdropping), **vishing** (phishing vocale), hacking della linea VoIP, e problemi di **privacy** dovuti al traffico non sempre cifrato.
- Le stesse precauzioni di cifratura valide per l'email sono applicabili per garantire la confidenzialità nella messaggistica istantanea e nel VoIP. L'utilizzo di sistemi crittografici migliora la sicurezza.
- **Implicazioni dell'Uso di Applicazioni Provenienti da "App Store" Non Ufficiali**
 - Scaricare e installare applicazioni da sorgenti diverse dagli store ufficiali (come Google Play o Apple App Store) comporta rischi significativi.
 - Le app negli store ufficiali sono generalmente sottoposte a controlli di sicurezza, anche se non sono esenti da rischi. Le app non ufficiali spesso non hanno verifiche e aumentano la probabilità di scaricare **malware**, di subire furti di credenziali o accessi non autorizzati ai dati.
- **Comprendere il Termine "Autorizzazioni dell'Applicazione"**
 - Quando si installa un'applicazione su un dispositivo mobile, questa richiede specifiche **autorizzazioni** per accedere a determinate funzionalità o dati del dispositivo.
 - Queste richieste non sono sempre chiare o facilmente comprensibili per l'utente.
 - È fondamentale comprendere a quali dati e funzionalità l'app sta chiedendo accesso prima di concedere l'autorizzazione. Ad esempio, un'app che chiede "Lettura stato e identità del telefono" può accedere al numero di telefono, all'IMEI (codice identificativo unico del dispositivo) e sapere quando si ricevono chiamate.
 - Alcune autorizzazioni, come l'accesso alla posizione, ai contatti, al microfono o alla fotocamera, possono rivelare informazioni molto private. È importante valutare se l'app necessita realmente di tali permessi per funzionare. I sistemi operativi moderni consentono di rivedere le autorizzazioni concesse alle app installate.
- **Misure Precauzionali in Caso di Perdita o Furto di Dispositivo Mobile**
 - Gli smartphone contengono un'enorme quantità di dati personali e rappresentano un valore. La loro perdita o il furto sono eventi seri dal punto di vista della sicurezza e della privacy.
 - Misure precauzionali consigliate:
 - Conservare in un luogo sicuro le informazioni identificative del dispositivo (modello, marca, colore, IMEI/IMSI).
 - Abilitare e configurare le funzionalità di **localizzazione remota** e blocco/cancellazione dei dati offerte dal sistema operativo (es. "Trova il mio telefono").

- In caso di perdita o furto, **sporgere denuncia** alle autorità di Polizia.
- **Contattare immediatamente l'operatore telefonico** per richiedere il blocco della SIM e del telefono tramite il codice IMEI. Il blocco IMEI impedisce al telefono di connettersi alle reti mobili nazionali.

CAPITOLO 7 – GESTIONE SICURA DEI DATI

- **Modi Comuni per Assicurare la Sicurezza Fisica di Computer e Dispositivi Mobili**
 - Oltre alla sicurezza logica (password, crittografia), la **sicurezza fisica** è fondamentale per proteggere i dati. Avere accesso fisico a un dispositivo rende molto più facile violare la sua sicurezza.
 - Metodi per garantire la sicurezza fisica includono l'uso di **controlli elettronici di accesso** (dove applicabile) e sistemi di protezione fisica come i **cavi di sicurezza** (es. stile Kensington) e lucchetti per ancorare i dispositivi, specialmente in luoghi pubblici.
 - Catalogare e registrare la posizione dei dispositivi può aiutare in caso di smarrimento o furto.
- **Effettuare Copie di Sicurezza (Backup) per Ovviare alla Perdita di Dati**
 - Perdere dati a causa di furto, smarrimento, malfunzionamenti o errori umani è un rischio concreto.
 - La soluzione principale per proteggersi dalla perdita di dati è effettuare **copie di sicurezza**, comunemente chiamate **Backup**.
 - Un backup è utile solo se può essere ripristinato ("Restore") in caso di necessità.
 - Una procedura di backup efficace deve essere:
 - **Regolare**: Eseguita con una frequenza adeguata alla velocità con cui i dati cambiano.
 - **Automatica**: Per garantire la regolarità e minimizzare gli errori umani.
 - **Memorizzata Esternamente/Off-site**: Le copie devono essere conservate su un supporto separato o in una posizione geograficamente diversa dall'originale per proteggersi da disastri locali (incendi, alluvioni).
- **Caratteristiche e Tipi di Backup**
 - Esistono diverse strategie per effettuare backup:
 - **Backup Completo (Full Backup)**: Copia l'intero set di dati selezionato ogni volta che viene eseguito. È il più semplice da ripristinare ma richiede più spazio e tempo.
 - **Backup Incrementale**: Copia solo i file che sono cambiati dall'ultimo backup (sia completo che incrementale). Richiede meno tempo e spazio del completo o differenziale, ma il ripristino è più complesso (richiede l'ultimo completo + tutti gli incrementali successivi).
 - **Backup Differenziale**: Copia solo i file che sono cambiati dall'ultimo backup completo. Il ripristino richiede l'ultimo backup completo e solo l'ultimo backup differenziale.

- **Effettuare la Copia di Sicurezza dei Dati**
 - Il backup può essere eseguito su vari tipi di supporti:
 - **Unità disco/dispositivo locale:** Un secondo hard disk interno o esterno.
 - **Unità esterna:** Hard disk esterni, chiavette USB, CD/DVD.
 - **Servizio su Cloud:** Archiviazione online fornita da terzi (es. Microsoft OneDrive, Google Drive). Il cloud offre scalabilità e accessibilità.
 - I sistemi operativi (come Windows 7, descritto nelle fonti) offrono strumenti integrati per pianificare ed eseguire backup, permettendo di selezionare i file o le cartelle da includere.
- **Ripristinare i Dati da una Copia di Sicurezza**
 - In caso di perdita o danneggiamento dei dati originali, è possibile ripristinarli dalla copia di sicurezza.
 - La procedura di ripristino (su Windows 7, ad esempio) prevede l'utilizzo dello strumento di backup e ripristino per selezionare i file o le cartelle da recuperare e la posizione in cui ripristinarli.
- **Distinguere tra Cancellare ed Eliminare i Dati in Modo Permanente**
 - La semplice cancellazione di un file spostandolo nel Cestino/Cestino o la formattazione di un disco **non elimina permanentemente** i dati.
 - Queste operazioni si limitano a marcare lo spazio occupato dai file come disponibile per essere sovrascritto. I dati originali rimangono sul supporto fino a quando non vengono effettivamente sostituiti da nuovi dati.
 - Esistono **software di recupero dati** in grado di recuperare file cancellati in modo standard anche dopo molto tempo.
 - La cancellazione dei dati eseguiti a livello locale sul proprio dispositivo non garantisce che copie degli stessi dati non rimangano su backup, su servizi cloud o siano state condivise con altri su reti sociali o forum.
- **Motivi per Eliminare in Modo Permanente i Dati**
 - La principale ragione per eliminare i dati in modo permanente è la **sicurezza e la privacy**.
 - È assolutamente essenziale assicurarsi che i dati personali o sensibili vengano distrutti in modo irrecuperabile prima di cedere, vendere o rottamare un computer o dispositivo di archiviazione.
 - La semplice cancellazione standard non è sufficiente per questo scopo.
- **Metodi Più Comuni per Distruggere i Dati in Modo Permanente**
 - Per garantire l'irrecuperabilità dei dati, si possono utilizzare diverse tecniche:
 - Per documenti cartacei o memorie ottiche (CD/DVD): utilizzare **distruggidocumenti** che sminuzzano o tagliano il supporto.
 - Per memorie magnetiche (hard disk): utilizzare apparecchi chiamati **"degausser"** che smagnetizzano completamente il disco.

- Per cancellare i dati sui dischi rigidi in modo software: utilizzare **programmi specifici** che scrivono dati casuali (sovrascrivono) più volte sullo spazio del disco. Alcuni programmi consentono anche di cancellare in modo sicuro lo spazio libero. La distruzione fisica del supporto è un'altra opzione efficace.