



Manuale ECDL Full Standard

Modulo IT Security



www.micertificoecl.it

SOMMARIO

CAPITOLO 1 – CONCETTI DI SICUREZZA	1
Distinguere tra dati e informazioni.....	2
Comprendere i termini “crimine informatico” e “hacking”.....	2
Riconoscere le minacce dolose e accidentali ai dati.....	3
Riconoscere le minacce ai dati provocate da circostanze straordinarie.....	4
Riconoscere le minacce ai dati provocate dall'uso del cloud computing.....	4
Comprendere le caratteristiche fondamentali della sicurezza delle informazioni.....	5
CAPITOLO 2 – MALWARE	13
Comprendere il termine “malware”.....	14
Riconoscere diversi modi con cui il malware si può nascondere	14
Riconoscere i tipi di malware infettivo e comprendere come funzionano.....	14
Riconoscere i tipi di malware e comprendere come operano.....	15
Comprendere come funziona il software anti-virus e quali limitazioni presenta.....	15
Comprendere che il software anti-virus dovrebbe essere installato su tutti i sistemi informatici	16
CAPITOLO 3 – SICUREZZA IN RETE	21
Comprendere il termine “rete” e riconoscere i più comuni tipi di rete.....	21
Comprendere che la connessione ad una rete ha implicazioni di sicurezza.....	22
Comprendere il ruolo dell'amministratore di rete.....	23
Comprendere la funzione e i limiti di un firewall in ambiente personale e lavorativo	23
Attivare, disattivare un firewall personale.....	24
CAPITOLO 4 – CONTROLLO DEGLI ACCESSI	29
Identificare i metodi per impedire accessi non autorizzati ai dati.....	29
Comprendere il termine “one-time password” ed il loro utilizzo tipico	30
Comprendere lo scopo di un account di rete	30
CAPITOLO 5 – USO SICURO DEL WEB	35
Completamento automatico e salvataggio automatico nella compilazione di un modulo	35
Eliminare dati privati da un browser	36
Utilizzare una connessione di rete sicura per le attività in rete.....	36
CAPITOLO 6 – COMUNICAZIONI	39
Cifrare e decifrare un messaggio di posta elettronica	40
La “firma digitale”.....	40
Identificare possibili messaggi fraudolenti e indesiderati.....	41
CAPITOLO 7 – GESTIONE SICURA DEI DATI.....	51
I più comuni modi per assicurare la sicurezza fisica di computer e dispositivi mobili	51
Effettuare copie di sicurezza per ovviare alla perdita di dati da computer e dispositivi mobili	52
Le caratteristiche di una procedura di copie di sicurezza	52

Capitolo 1 – Concetti di sicurezza

Riferimento Syllabus 1.1.1	<i>Distinguere tra dati e informazioni.</i>
Riferimento Syllabus 1.1.2	<i>Comprendere i termini "crimine informatico" e "hacking".</i>
Riferimento Syllabus 1.1.3	<i>Riconoscere le minacce dolose e accidentali ai dati provocate da singoli individui, fornitori di servizi, organizzazioni esterne.</i>
Riferimento Syllabus 1.1.4	<i>Riconoscere le minacce ai dati provocate da circostanze straordinarie, quali fuoco, inondazioni, guerre, terremoti.</i>
Riferimento Syllabus 1.1.5	<i>Riconoscere le minacce ai dati provocate dall'uso del cloud computing, quali controllo dei dati, potenziale perdita di riservatezza (privacy).</i>
Riferimento Syllabus 1.2.1	<i>Comprendere le caratteristiche fondamentali della sicurezza delle informazioni, quali: confidenzialità, integrità, disponibilità.</i>
Riferimento Syllabus 1.2.2	<i>Comprendere i motivi per proteggere le informazioni personali, quali evitare il furto di identità o le frodi, mantenere la riservatezza.</i>
Riferimento Syllabus 1.2.3	<i>Comprendere i motivi per proteggere informazioni di lavoro su computer e dispositivi mobili, quali evitare furti, utilizzi fraudolenti, perdite accidentali di dati, sabotaggi.</i>
Riferimento Syllabus 1.2.4	<i>Identificare i principi comuni per la protezione, conservazione e controllo dei dati e della riservatezza, quali: trasparenza, scopi legittimi, proporzionalità delle misure in rapporto ai danni.</i>
Riferimento Syllabus 1.2.5	<i>Comprendere i termini "soggetti dei dati" e "controllori dei dati", e come si applicano nei due casi i principi di protezione, conservazione e controllo dei dati e della riservatezza.</i>
Riferimento Syllabus 1.2.6	<i>Comprendere l'importanza di attenersi alle linee guida e alle politiche per l'uso dell'ICT, e come fare per ottenerle.</i>
Riferimento Syllabus 1.3.1	<i>Comprendere il termine "ingegneria sociale" e le sue implicazioni, quali accesso non autorizzato a sistemi informatici, raccolta non autorizzata di informazioni, frodi.</i>
Riferimento Syllabus 1.3.2	<i>Identificare i metodi applicati dall'ingegneria sociale, quali chiamate telefoniche, phishing, shoulder surfing (spiare alle spalle), al fine di carpire informazioni personali.</i>
Riferimento Syllabus 1.3.3	<i>Comprendere il termine "furto di identità" e le sue implicazioni personali, finanziarie, lavorative, legali.</i>
Riferimento Syllabus 1.3.4	<i>Identificare i metodi applicati per il furto di identità, quali acquisire informazioni a partire da oggetti e informazioni scartati (information diving); uso di dispositivi fraudolenti di lettura (skimming); inventare uno scenario pretestuoso (pretexting).</i>
Riferimento Syllabus 1.4.1	<i>Comprendere gli effetti di attivare/disattivare le impostazioni di sicurezza relative alle macro.</i>
Riferimento Syllabus 1.4.2	<i>Comprendere i vantaggi e i limiti della cifratura. Comprendere l'importanza di non divulgare o perdere la password, la chiave o il certificato di cifratura.</i>
Riferimento Syllabus 1.4.3	<i>Cifrare un file, una cartella, una unità disco.</i>



Riferimento Syllabus 1.4.4	<i>Impostare una password per file quali: documenti, fogli di calcolo, file compressi.</i>
Contenuti della lezione	Distinguere tra dati e informazioni; Comprendere i termini "crimine informatico" e "hacking"; Riconoscere le minacce dolose e accidentali ai dati; Riconoscere le minacce ai dati provocate da circostanze straordinarie; Riconoscere le minacce ai dati provocate dall'uso del cloud computing ; Comprendere le caratteristiche fondamentali della sicurezza delle informazioni; Comprendere i motivi per proteggere le informazioni personali; Comprendere i motivi per proteggere informazioni di lavoro su computer e dispositivi mobili; Identificare i principi comuni per la protezione, conservazione e controllo dei dati e della riservatezza; Comprendere i termini "interessato" e "responsabili del trattamento"; Comprendere l'importanza di attenersi a linee guida e politiche per l'uso dell'ICT e come fare per ottenerle; comprendere il termine "ingegneria sociale" e le sue implicazioni; Identificare i metodi applicati dall'ingegneria sociale, al fine di carpire informazioni personali; Comprendere il termine "furto di identità" e le sue implicazioni personali, finanziarie, lavorative, legali; Identificare i metodi applicati per il furto di identità; Comprendere l'effetto di attivare/disattivare le impostazioni di sicurezza delle macro; Comprendere i vantaggi e i limiti della cifratura e l'importanza di non divulgare o perdere la password, la chiave o il certificato di cifratura; Cifrare un file, una cartella, una unità disco; Impostare una password per file.

2

Distinguere tra dati e informazioni

Nelle attività umane più semplici le informazioni vengono rappresentate e scambiate secondo le tecniche naturali tipiche delle attività stesse: la lingua, scritta o parlata, disegni, figure, numeri, ecc.

Nei sistemi informatici invece le informazioni vengono rappresentate per mezzo di **dati** (numeri, testo, immagini o altro) che di per sé rappresentano fatti o eventi non organizzati e quindi privi di significato.

Organizzando però i dati in modo da renderli comprensibili, e cioè associandoli ad una interpretazione, si ottengono delle **informazioni**.

Ad esempio il numero "42" di per sé non costituisce informazione, ma se associato ad una interpretazione, ad esempio "*numero civico*" diventa informazione.

Comprendere i termini "crimine informatico" e "hacking"

Il **crimine informatico** è un'attività criminale attuata utilizzando strumenti informatici come computer e la rete Internet. Esempi di crimine informatico sono la frode informatica, il furto d'identità o l'accesso non autorizzato a sistemi informatici.

Spesso, l'opinione pubblica associa al "crimine informatico" il termine "**hacking**", collegandovi la pratica di accedere illegalmente ai sistemi altrui allo scopo di carpire dati riservati o danneggiarne il funzionamento. L'hacking comprende in realtà una serie di attività perfettamente lecite svolte anche a livello professionale: i sistemi informatici vengono infatti sottoposti a specifici e costanti test al fine di valutarne e comprovarne la sicurezza e l'affidabilità.



L'hacking è quindi l'attività volta a studiare in modo approfondito le caratteristiche tecniche dei sistemi di computer, con l'obiettivo di individuarne limiti e difetti, fino al punto di essere in grado di modificarli e migliorarli.

 **APPROFONDIMENTO**

Rientrano nel reato di "crimine informatico" anche le seguenti attività:

- **Intercettazione** (di dati informatici verso, da o all'interno di un sistema informatico)
- **Interferenze di dati** (danneggiamento, cancellazione, deterioramento, alterazione o soppressione di dati informatici)
- **Riproduzione non autorizzata** (di programmi protetti o topografie di prodotti a semiconduttore)
- **Diffusione di virus e malware**

La repressione dei crimini informatici è attuata in Italia attraverso la **Polizia postale** e il **C.N.A.I.P.I.C.** (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche). A livello europeo dall'**EC3** (European Cybercrime Center) un apposito centro dell'**EUROPOL** (European Police Office) focalizzato sui crimini ad opera di gruppi organizzati a scopo di frode online, adescamento in rete e lo sfruttamento sessuale dei bambini, nonché gli attacchi a infrastrutture critiche e sistemi informativi della UE.

Per quanto attiene all'hacking, chi lo pratica può essere definito in due modi: chi sfrutta le sue conoscenze per cercare le eventuali vulnerabilità di sistemi e reti per porvi rimedio è detto **hacker**; viceversa chi sfrutta le stesse conoscenze per utilizzare il sistema informatico a proprio vantaggio, per rubarne i dati o danneggiarlo è identificato come **cracker**.

Nota: il termine "hacking" è stato qui definito unicamente in rapporto alla sicurezza informatica. In realtà tale termine è utilizzato anche in altri contesti. Ad esempio, si parla di hacking anche quando si altera il funzionamento dell'hardware di un componente al fine di ottenere incrementi prestazionali, oppure di rimuovere delle limitazioni di un prodotto alterando il firmware o il software dello stesso.

3

Riconoscere le minacce dolose e accidentali ai dati

In generale, quando si parla di sicurezza dei dati aziendali, si è portati a pensare che ogni possibile minaccia possa essere attuata solo mediante attacchi informatici via Internet. Spesso invece molti atti dannosi vengono provocati dall'interno da parte di persone che, per i motivi più vari, hanno occasione di entrare in azienda e di accedere al sistema informativo aziendale.

Si pensi ad esempio ai fornitori di servizi quali i manutentori dell'hardware o dell'infrastruttura di rete o dei tecnici informatici che devono intervenire sui computer degli utenti o sui server aziendali per installare o aggiornare programmi. Queste persone, per ovvie esigenze tecniche, devono operare con accesso amministrativo e dunque con il massimo dei permessi offerti dal file system. Ciò porta inevitabilmente ad avere libero accesso non solo ai programmi, ma anche ai dati, esponendoli al rischio di copia, modifica o cancellazione, sia accidentale, che volontaria.

Le minacce ai dati possono anche derivare da persone esterne non tecniche, quali clienti, fornitori o semplici ospiti che accedano alla rete aziendale o scolastica tramite computer o altri dispositivi portatili, ad esempio tramite Wi-Fi. Ancora peggio, se tramite un computer di un utente lecito lasciato incustodito e non bloccato da una password.

 **APPROFONDIMENTO**

Sebbene il focus di questo argomento sia stato portato sulle minacce esterne, non va dimenticato che gli aggressori più pericolosi sono in genere gli utenti interni perché conoscono molti dei codici e delle misure di sicurezza utilizzate. E' infatti evidente che un utente interno per svolgere la sua mansione deve poter accedere al sistema informativo e quindi per disattenzione, ripicca o vendetta può provocare una perdita dei dati o appropriarsene e farne un uso non corretto.



Riconoscere le minacce ai dati provocate da circostanze straordinarie

Nessuno può impedire il verificarsi di calamità naturali. **Terremoti, tempeste, inondazioni, fulmini e incendi** possono causare danni gravi ai computer, che possono risultare in perdita di informazioni, tempi di inattività o perdite di produttività. I danni all'hardware possono inoltre danneggiare altri servizi essenziali.

Le difese che è possibile predisporre contro le calamità naturali non sono molte.

L'approccio migliore consiste nel preparare in anticipo dei piani di ripristino e di emergenza.

In questa categoria rientrano anche minacce quali **sommosse, guerre e attacchi terroristici** che pur avendo origine umana sono classificate come calamità.

4



APPROFONDIMENTO

Le aziende, soprattutto di grandi dimensioni, in cui la perdita dei servizi a supporto del business causerebbe il blocco totale o parziale dell'attività (ad esempio, banche, providers telefonici, assicurazioni, ecc.) predispongono un **Business Continuity Plan** (in italiano "piano di continuità aziendale") all'interno del quale sono presenti le misure di **Disaster recovery** che definiscono con estrema precisione tutte le strategie di ripristino delle funzioni aziendali nel caso di eventi straordinari come quelli citati.

Riconoscere le minacce ai dati provocate dall'uso del cloud computing

Il **cloud computing** è il recente trend nel mondo IT che ha permesso di spostare l'elaborazione e la memorizzazione dei dati dai PC aziendali alle grandi server farm remote utilizzando la rete Internet.

Mediante il *cloud computing* le applicazioni ora possono essere distribuite alle aziende sotto forma di servizi web, ottenendo così importanti riduzioni di costi grazie al risparmio sulle infrastrutture e al mantenimento delle risorse di elaborazione che in questo modello gravano unicamente sul provider.

Insieme a questi, e ai molti altri vantaggi, si vanno tuttavia palesando alcune preoccupazioni sulla sicurezza in quanto i meccanismi tradizionali di protezione dei dati risultano inefficienti o inutili.

Innanzitutto aderendo ad un contratto di *cloud computing* un'azienda perde il controllo sui dati fisici, dato che è quasi impossibile stabilire dove siano realmente immagazzinati. Inoltre, la memorizzazione di dati sensibili espone l'utente a potenziali problemi di violazione della privacy. Un provider scorretto potrebbe accedere ai dati personali e condurre ricerche di mercato o catalogare gli utenti. Naturalmente, in questo contesto la crittografia può essere d'aiuto.



APPROFONDIMENTO

Sebbene ad oggi (2014) non esista ancora uno standard vero e proprio per la sicurezza del *cloud computing* nel 2009 si è costituita un'organizzazione no-profit chiamata **Cloud Security Alliance** (CSA) con la missione di promuovere l'uso delle migliori pratiche per fornire garanzie di sicurezza all'interno del *cloud computing* e di fornire supporto formativo sull'uso dello stesso.



Comprendere le caratteristiche fondamentali della sicurezza delle informazioni

La sicurezza delle informazioni, secondo i principali istituti di standardizzazione, coincide con l'assicurare requisiti di **Confidenzialità**, **Integrità** e **Disponibilità**.

Per **Confidenzialità** (o Riservatezza) si intende che l'informazione deve essere accessibile solo a chi è autorizzato a conoscerla e che le informazioni devono essere protette sia durante la trasmissione che durante la memorizzazione.

L'**Integrità** implica che le informazioni devono essere trattate in modo che siano difese da manomissioni e modifiche non autorizzate.

La **Disponibilità** invece impone che l'informazione sia sempre disponibile alle persone autorizzate quando necessario.

5

APPROFONDIMENTO

La norma ISO/IEC 27002:2013 "Information Technology - Security techniques - Code of practice for information security management" è il documento di riferimento sul tema della sicurezza dell'informazione. Essa riconosce (tra l'altro) che legare il tema della sicurezza dell'informazione esclusivamente ad aspetti puramente tecnologici può essere limitativo: un ruolo altrettanto importante viene svolto quindi da una adeguata gestione dei controlli e delle procedure (sistemi di monitoraggio, prevenzione e ripristino dati), il che significa un coinvolgimento complessivo e articolato, ai vari livelli, di tutte le strutture dell'organizzazione.

La norma citata descrive gli obiettivi di sicurezza dell'informazione mediante il paradigma **C.I.A.** (Confidentiality, Integrity, Availability) traducibile in italiano nel modello **C.I.D.** (Confidenzialità, Integrità, Disponibilità).

Comprendere i motivi per proteggere le informazioni personali

Con l'uso di dispositivi mobili come *tablet* e *smartphone* la protezione dei dati personali ha assunto un'importanza decisamente più rilevante rispetto al passato.

È infatti evidente che se qualcuno entra in possesso di dati riservati, come le credenziali di accesso alla posta elettronica o a una rete sociale, ne può fare un uso illegale facendo ricadere la colpa sull'ignaro derubato. Ancora peggio se un malintenzionato riesce a impossessarsi delle credenziali di home banking o dei dati della carta di credito: può utilizzarli a proprio vantaggio creando talvolta seri danni economici.

APPROFONDIMENTO

Furti di identità, frodi, danneggiamento della propria immagine o della propria reputazione sono rischi da prendere sempre in considerazione. Un uso sicuro di Internet e dei suoi servizi si basa quindi sulla consapevolezza di questi rischi per ridurre i quali è fondamentale tenere riservate e protette le informazioni personali.

Comprendere i motivi per proteggere informazioni di lavoro su computer e dispositivi mobili

La forza di una azienda è nelle informazioni in suo possesso, nel come riesce a gestirle e a renderle profittevoli. Alla base di tutto quindi, per ragioni commerciali o legali, c'è la protezione delle informazioni, a garanzia dei rapporti con clienti, fornitori e interlocutori vari.



In particolare la protezione dei dati dei clienti o di tipo finanziario è ancora più rilevante in quanto ogni azienda è penalmente responsabile di un loro uso illegale.

Per tutte le ragioni citate e per gestire con profitto il proprio business, ogni azienda deve mettere in atto tutte le misure necessarie per proteggere i propri dati in modo da prevenirne il furto, la perdita accidentale, l'uso improprio o il sabotaggio.

Identificare i principi comuni per la protezione, conservazione e controllo dei dati e della riservatezza

6

La facilità di accesso e manipolazione delle informazioni resa possibile dall'ICT ha portato a legiferare sulla tutela del trattamento dei dati personali cercando di mediare tra due esigenze contrastanti:

- *La tutela della riservatezza* - cioè il controllo dell'interessato sull'utilizzo delle informazioni che lo riguardano da parte di terzi;
- *La necessità di rendere sempre disponibili i dati per ragioni di legalità e trasparenza*- cioè l'inammissibilità dell'anonimato per questioni di sicurezza.

La direttiva **95/46/CE** e la legge italiana **675/1996**, hanno stabilito il quadro di riferimento normativo iniziale poi sfociato nel **D.L. 196/2003** comunemente conosciuto come "Codice della privacy".

Nonostante la complessità della materia, tutte queste leggi e regolamenti si ispirano ad alcuni principi di base tra i quali spiccano:

- **Trasparenza**
- **Legittimità**
- **Proporzionalità**

La tabella che stai vedendo dettaglia i contenuti di ciascun principio liberamente sintetizzato dal codice della Privacy italiano.

PRINCIPIO	DESCRIZIONE
Trasparenza	<ul style="list-style-type: none"> ✓ L'attività di raccolta dati deve essere manifesta e dichiarata; ✓ Devono essere descritti i motivi e le finalità; ✓ Devono essere dichiarate le procedure adottate per il rispetto delle regole; ✓ Devono essere comunicate le modalità di contestazione.
Legittimità	<ul style="list-style-type: none"> ✓ La raccolta ed il trattamento possono essere consentiti solo se: <ul style="list-style-type: none"> - Perseguono fini legittimi - Non violano i diritti dell'interessato
Proporzionalità	<ul style="list-style-type: none"> ✓ I dati personali raccolti devono essere adeguati, pertinenti e non eccedenti le finalità per cui sono raccolti; ✓ Devono essere accurati e mantenuti aggiornati



APPROFONDIMENTO

Molti aggiornamenti sono intervenuti a modificare la 196 dal 2003 ad oggi, ed è anche stata approvata dalla commissione europea (25 gennaio 2012) una proposta di regolamento che una volta approvato in via definitiva andrà a sostituire non solo la 95/46/CE ma anche tutte le specifiche normative dei 28 paesi membri e quindi anche del codice della Privacy italiano.



Comprendere i termini “interessato” e “responsabili del trattamento

Il codice in materia di protezione dei dati personali italiano (D.L. 196/2003) nel suo **articolo 4** definisce i termini utilizzati dalla legge. Per gli scopi di questo argomento si riportano le seguenti:

- **“Interessato”**: la persona fisica cui si riferiscono i dati personali;
- **“Responsabile”**: la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

Per l'*interessato* si applicano i diritti riportati nell'**articolo 7** liberamente sintetizzato nella tabella sottostante.

D.L. 196/2003 - Articolo 7	
Comma 1	Essere informato sull'esistenza di dati personali e di averne comunicazione in forma intellegibile.
Comma 2	Conoscere l'origine di tali dati, le finalità e modalità del trattamento, gli estremi del titolare del trattamento e i soggetti ai quali possono essere comunicati tali dati.
Comma 3	Ottenere cancellazione, aggiornamento, rettifica e integrazione dei dati.
Comma 4	Opporsi, per motivi legittimi, al trattamento dei propri dati personali a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

7

Per il *responsabile* si applicano molti doveri che si possono però sintetizzare nei due principi di “**Conservazione**” e “**Sicurezza**” di seguito visualizzati.

D.L. 196/2003	
Principio di conservazione	I dati raccolti devono essere conservati per un tempo non superiore al necessario per gli scopi per i quali sono raccolti.
Principio di sicurezza	<ul style="list-style-type: none"> ✓ I dati devono essere conservati in modo sicuro e al riparo da intrusioni esterne; ✓ Sono obbligatorie misure di sicurezza come: <ul style="list-style-type: none"> – Protezioni fisiche; – Protezioni procedurali; – Protezioni tecniche: <ul style="list-style-type: none"> ➢ Protezione da intrusioni ➢ Protezione da infezioni ➢ Protezione da perdite di dati

Comprendere l'importanza di attenersi a linee guida e politiche per l'uso dell'ICT e come fare per ottenerle

Ogni giorno **privati** e **aziende** hanno a che fare con molteplici rischi alla sicurezza dei propri dati. Se però nell'uso in ambito privato è sufficiente conoscere i pericoli per evitarli, in ambito lavorativo le problematiche sono decisamente maggiori. Il maggior livello di interconnessione, l'utilizzo di molti più tipi di software con procedure integrate e la necessità di accedere a base dati da parte di molti addetti, richiede una gestione delle risorse informatiche e delle procedure anche in rapporto alla sicurezza.

Ogni azienda quindi analizza l'utilizzo delle proprie tecnologie ICT e, seppure a diversi gradi di complessità in rapporto alle proprie strutture e dimensioni, stila un documento che formalizza le linee guida a cui ciascun dipendente deve attenersi nell'uso delle risorse informatiche aziendali e delle relative procedure.



La disponibilità di tale documento viene poi comunicata a tutto il personale con l'indicazione di dove reperirlo (solitamente nella intranet aziendale) in modo che ciascuno possa agevolmente prenderne visione.

Comprendere il termine “ingegneria sociale” e le sue implicazioni

L'**ingegneria sociale** (dall'inglese “*Social engineering*”) è quel ramo della sicurezza delle informazioni che si occupa di manipolare psicologicamente delle persone al fine di compiere azioni o carpire informazioni riservate. Questa tecnica viene a volte utilizzata, al posto delle usuali tecniche di hacking, per aggirare sistemi di protezione dei dati sempre più sofisticati e difficilmente penetrabili.

8

Le implicazioni legate all'ingegneria sociale possono essere riassunte nei tre punti visualizzati:

- **Raccolta di informazioni** (che possono essere confidenziali o di valore)
- **Frode** (cioè utilizzare le informazioni raccolte per commettere una truffa)
- **Accesso non autorizzato ai dati** (cioè accedere a dati di terzi con credenziali rubate).

Identificare i metodi applicati dall'ingegneria sociale, al fine di carpire informazioni personali

Sono molti i mezzi che l'ingegneria sociale utilizza per carpire informazioni. Uno di questi è la classica **chiamata telefonica** che si presenta come sondaggio anonimo che partecipa a un'estrazione di premi; oppure con l'annuncio che è stato rilevato un guasto ai propri impianti, ma risolvibile chiamando una fantomatica assistenza tecnica.

Un'altra tecnica oggi molto diffusa è quella del **phishing**: una pratica basata sull'invio di messaggi di posta elettronica ingannevoli. Ad esempio il *phisher* si finge un dipendente bancario o delle poste e, informando il malcapitato del blocco del proprio conto o della carta di credito per rilevamento di intrusioni, chiede le sue credenziali per poterle verificare e procedere allo sblocco. Ovviamente si tratta di un trucco per entrarne in possesso.

Un'ulteriore tecnica, a cui sovente non si fa caso, è chiamata **shoulder surfing** cioè “spiare dietro le spalle”. Consiste nel carpire le credenziali immesse dall'utente di un servizio spiandolo direttamente.



APPROFONDIMENTO

Ulteriori mezzi utilizzati dall'ingegneria sociale sono i seguenti:

Dumpster diving.

Tecnica d'indagine basata sull'analisi della spazzatura prodotta dalla vittima. Scontrini, ricevute, giornali, riviste, ogni singolo oggetto può essere utile per ricostruire lo stile di vita o la abitudini del potenziale truffato.

Eavesdrop

Tecnica che consiste nell'origliare, cioè ascoltare una conversazione di nascosto, un dialogo sottovoce, o un colloquio a cui non si dovrebbe far parte.

Wiretap

Meglio nota come intercettazione, si attua attraverso il telefono ma soprattutto tramite mezzi di messaggistica istantanea, VoIP, e posta elettronica con strumenti di sniffing del traffico, hacking del canale di comunicazione, utilizzo di microspie, ecc.



Comprendere il termine “furto di identità” e le sue implicazioni personali, finanziarie, lavorative, legali

Il furto d'identità consiste nell'ottenere indebitamente le informazioni personali di un soggetto al fine di sostituirsi in tutto o in parte al soggetto stesso e compiere azioni illecite in suo nome o ottenere credito tramite false credenziali.

Come si può intuire il furto d'identità ha implicazioni enormi. Si va dalla perdita di credibilità, alla responsabilità di azioni criminose, dalle perdite finanziarie alle responsabilità legali.

Identificare i metodi applicati per il furto di identità

Alcuni metodi utilizzati per il furto d'identità adottano tecniche di ingegneria sociale quali il **Dumpster diving** e il **Phishing**. Come già visto, il primo consiste nel frugare tra la spazzatura della vittima per cercare riferimenti a dati sensibili, mentre il secondo consiste nel fingersi qualcun altro proponendosi come persona autorevole dotato del diritto ad avere le sue credenziali.

Altri metodi sono più specifici, ad esempio la tecnica chiamata “**skimming**” consiste nella clonazione di una carta di credito attraverso l'apparecchiatura elettronica utilizzata negli esercizi commerciali per pagare i beni acquistati.



APPROFONDIMENTO

Rientra nella tecnica di **skimming** anche l'acquisizione di immagini o filmati di oggetti su cui sono impressi dei dati sensibili, per esempio la carta di credito o il PIN del bancomat. Per questa ragione, quando si preleva da un bancomat è importante non solo nascondere la digitazione del PIN, ma anche stare attenti che non ci siano webcam posizionate sopra la tastiera o il terminale ATM non appaia “diverso dal solito”.

Comprendere l'effetto di attivare/disattivare le impostazioni di sicurezza delle macro

Strumenti di produttività come elaboratori di testo o fogli elettronici consentono l'utilizzo di un linguaggio di programmazione con il quale scrivere **macro** che possono essere eseguite automaticamente al verificarsi di un evento, oppure alla pressione di una combinazione di tasti.

Le macro possono essere strumenti molto utili in grado di automatizzare molte azioni ripetitive, ma possono contenere codice malevolo in grado di causare danni, anche gravi, al computer.

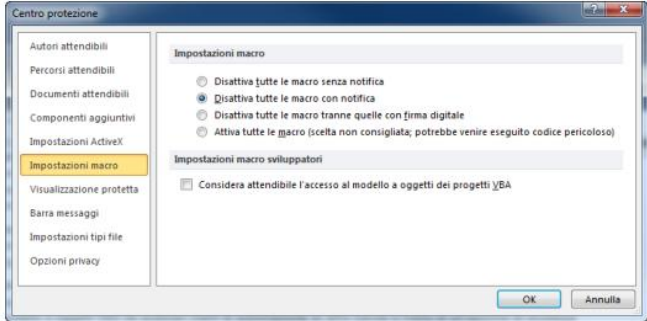
Per questa ragione, per poter essere utilizzate, le macro devono essere **attivate**. Ad esempio, in Office 2010, il rilevamento di una macro all'apertura di un file causa la comparsa di un avviso di sicurezza sulla barra messaggi che chiede se si desidera abilitarne il contenuto.

Abilitare il contenuto consente l'esecuzione delle macro con i vantaggi che esse procurano, ma espone il computer a rischi.

Per non sbagliare, la cosa migliore è attivare le macro dei documenti di cui si è certi della provenienza e lasciare disattivate le altre.



 **APPROFONDIMENTO**



Nelle applicazioni Office che supportano l'esecuzione di macro le relative impostazioni di sicurezza si attuano dal "**Centro protezione**" accessibile da *File > Opzioni > Centro protezione*. L'impostazione **Disattiva tutte le macro con notifica** è l'impostazione predefinita e consente di disattivare le macro ma ricevere avvisi di sicurezza se vengono rilevate. In questo modo, è possibile scegliere se abilitare le macro caso per caso. Sono poi

disponibili altre opzioni: una più restrittiva e due più permissive.

Comprendere i vantaggi e i limiti della cifratura e l'importanza di non divulgare o perdere la password, la chiave o il certificato di cifratura

Quando si parla di crittografia è necessario distinguere tra la crittografia **simmetrica** utilizzata per i documenti prodotti da MS Office, da quella **asimmetrica** utilizzata nella firma digitale o nella trasmissione di informazioni.

La crittografia simmetrica utilizza la stessa chiave per cifrare e decifrare il file e in ambiente *Office* viene generalmente indicata come "*Password*".

Proteggere un file con la crittografia impedisce a malintenzionati di accedere ai contenuti del documento, tuttavia espone anche al rischio che l'utente si dimentichi la password e quindi non sia più in grado di aprire il file. La password va quindi custodita in modo da poterla ritrovare in caso di necessità.

Nella crittografia asimmetrica si utilizzano due chiavi: una *privata* ed una *pubblica* disponibili attraverso un *ID digitale*. Ad esempio, nella cifratura di un messaggio il mittente utilizza la **chiave pubblica del destinatario** per codificare le informazioni da inviare; il destinatario utilizza **la propria chiave privata** per decodificare le informazioni ricevute.

In questo contesto la perdita di un ID digitale comporta l'impossibilità del proprietario di accedere ai messaggi crittografati mediante la propria chiave pubblica ed inoltre la possibilità di firmare o cifrare nuovi messaggi.

L'approfondimento di questo argomento contiene altre importanti informazioni.

 **APPROFONDIMENTO**

La sottrazione o la scoperta di una password di crittografia comporta la perdita di confidenzialità del documento che potrà ovviamente essere decifrato e letto. La scelta di una buona password e l'attenzione alla sua conservazione bastano tuttavia ad evitare il problema.

Nel caso di sottrazione o perdita di un ID digitale invece è fondamentale procedere alla **revoca** dello stesso in modo che il malintenzionato non possa spacciarsi per il legittimo proprietario in rete. La revoca del certificato lo rende invalido, ed è definitiva. La relativa procedura è normalmente definita dall'autorità che lo ha emesso.



Cifrare un file, una cartella, una unità disco

Tutti i sistemi operativi moderni offrono funzionalità crittografiche applicabili a file, cartelle e persino intere unità. Windows non fa eccezione, anche se tali funzionalità sono disponibili solo in alcune versioni.

Per crittografare un file o una cartella basta aprire una finestra di *Esplora risorse* e posizionarsi sul file o cartella che si desidera proteggere. Accedendo alle sue proprietà attraverso il menu *File* o il *menu contestuale* si può utilizzare il pulsante **Avanzate** della scheda *Generale* per visualizzare la finestra di dialogo “*Attributi avanzati*”.

La selezione dell'opzione “**Crittografa contenuto per la protezione dei dati**” e la conferma su tutte le finestre di dialogo aperte, completeranno la procedura.

Per la crittografia di un intero disco, Windows mette a disposizione la funzionalità **BitLocker**. Per attivarla, nelle edizioni di Windows che la supportano, basta andare nel **Pannello di controllo**, selezionare la categoria **Sistema e sicurezza** ed infine **Crittografia unità BitLocker**. La finestra di dialogo che si apre mostrerà le unità su cui è possibile attivare la funzionalità.

Un clic sul link **Attiva BitLocker** avvierà la procedura guidata che chiederà la password di cifratura e la modalità di salvataggio della chiave per recuperare il contenuto dell'unità se si dimenticasse la password.



APPROFONDIMENTO

Sebbene le procedure indicate siano estremamente semplici e alla portata di tutti, le conseguenze di errori, guasti e mancanza di backup possono causare perdita di accesso irreversibile alle strutture crittate. Leggere con attenzione gli omonimi argomenti ampiamente spiegati nella guida in linea di Windows prima di applicare la crittografia. Un esempio di precauzione è il backup del certificato che viene creato automaticamente la prima volta che si cripta un file o una cartella. Tale backup, tra l'altro, è indispensabile per concedere ad altri il permesso di accesso alle strutture crittate.

Sia la crittografia di file e cartelle che quella applicata da BitLocker si applicano unicamente ai dischi residenti. File estratti da tali dischi e copiati su supporti esterni sono decrittati automaticamente. Esiste tuttavia la possibilità di criptare anche unità esterne, come chiavette o memorie flash di vario tipo, mediante la funzionalità **BitLocker To Go**. Si rimanda alla guida in linea per ogni ulteriore informazione.

Impostare una password per file

Per proteggere un file da accessi indesiderati è necessario impostare sul file una password di apertura. Ad esempio, usando un'applicazione Office come Word, Excel o PowerPoint 2010 è necessario:

- Accedere alla scheda **File** e selezionare il comando **Informazioni**.
- Fare clic sul pulsante **Proteggi tipodidocumento** per aprire il relativo menu e selezionare il comando **Crittografa con password**.
- Nella finestra che appare inserire e poi confermare la password di apertura del documento.

Nel caso di archivi compressi la password di protezione è possibile solo usando programmi di terze parti in quanto **Cartelle compresse** di Windows non offre questa possibilità.



 **APPROFONDIMENTO**

L'impostazione di una password di apertura (con crittografia) è disponibile anche mediante la seguente procedura:

- Accedere alla scheda **File** e selezionare il comando **Salva con nome**.
- Nella finestra di dialogo omonima aprire il menu **Strumenti** (accanto al pulsante Salva) e selezionare il comando **Opzioni generali**.
- Nella finestra che appare inserire e poi confermare la **password di lettura**.

Questo metodo consente anche di impostare una password di modifica, cioè una password da fornire se si desidera modificare il file. L'applicazione della sola password di modifica non crittografa il documento.

Per rimuovere la password basta ripetere la procedura usata per crearla cancellando la password.

12



Capitolo 2 – Malware

Riferimento Syllabus 2.1.1	<i>Comprendere il termine "malware". Riconoscere diversi modi con cui il malware si può nascondere nei computer, quali: trojan, rootkit e backdoor.</i>
Riferimento Syllabus 2.1.2	<i>Riconoscere i tipi di malware infettivo e comprendere come funzionano, ad esempio virus e worm.</i>
Riferimento Syllabus 2.1.3	<i>Riconoscere i tipi di malware usati per furto di dati, profitto/estorsione e comprendere come operano, ad esempio: adware (proposta di pubblicità attraverso banner e popup), ransomware (blocco doloso di un programma con lo scopo di chiedere un riscatto per sbloccarlo), spyware (software che invia ad un server remoto i dati di navigazione), botnet (software capace di prendere il controllo di una rete di computer), keylogger (software capace di inviare ad un server remoto i caratteri digitati su una tastiera) e dialer (software capace di cambiare la connessione del modem da un provider ad un altro).</i>
Riferimento Syllabus 2.2.1	<i>Comprendere come funziona il software antivirus e quali limitazioni presenta.</i>
Riferimento Syllabus 2.2.2	<i>Comprendere che il software antivirus dovrebbe essere installato su tutti i sistemi informatici.</i>
Riferimento Syllabus 2.2.3	<i>Comprendere l'importanza di aggiornare regolarmente vari tipi di software, quali: antivirus, browser web, plug-in, applicazioni, sistema operativo.</i>
Riferimento Syllabus 2.2.4	<i>Eseguire scansioni di specifiche unità, cartelle, file usando un software antivirus. Pianificare scansioni usando un software antivirus.</i>
Riferimento Syllabus 2.2.5	<i>Comprendere i rischi associati all'uso di software obsoleto e non supportato, quali: maggiori minacce da parte del malware, incompatibilità.</i>
Riferimento Syllabus 2.3.1	<i>Comprendere il termine "quarantena" e l'effetto di messa in quarantena file infetti/sospetti.</i>
Riferimento Syllabus 2.3.2	<i>Mettere in quarantena, eliminare file infetti/sospetti.</i>
Riferimento Syllabus 2.3.3	<i>Comprendere che un attacco da malware può essere diagnosticato e risolto usando risorse online quali: siti web di sistemi operativi, antivirus, fornitori di browser web, siti web di autorità preposte.</i>
Contenuti della lezione	Comprendere il termine "malware"; Riconoscere diversi modi con cui il malware si può nascondere; Riconoscere i tipi di malware infettivo e comprendere come funzionano; Riconoscere i tipi di malware e comprendere come operano; Comprendere come funziona il software anti-virus e quali limitazioni presenta; Comprendere che il software anti-virus dovrebbe essere installato su tutti i sistemi informatici; Comprendere l'importanza di aggiornare regolarmente i vari tipi di software; Eseguire e pianificare scansioni di specifiche unità, cartelle e file usando un software anti-virus; Comprendere i rischi associati all'uso di software obsoleto e non supportato; Comprendere il termine "quarantena" e l'operazione di mettere in quarantena file infetti/sospetti; Eliminare file infetti/sospetti; Utilizzo di risorse online per diagnosticare e risolvere un attacco malware.

13



Comprendere il termine "malware"

In passato quando si voleva far riferimento ad un software in grado di arrecare danni ad un computer si utilizzava il termine "Virus".

Lo sviluppo informatico ha però portato con se anche un generale incremento delle tipologie infettive tanto che il termine "virus" non si dimostrava più adeguato.

Pertanto, nel 1990 un ricercatore israeliano coniò il termine **Malware** (dalla contrazione delle parole inglesi "**MAL**icious **SOFT**WARE") per indicare genericamente un qualsiasi programma creato con il solo scopo di causare danni più o meno gravi a un sistema informatico o all'integrità dei dati che gestisce.

14

Questa parola ha dunque il significato letterale di "programma malevolo" ma è meglio traducibile in italiano con il termine "codice maligno".

Riconoscere diversi modi con cui il malware si può nascondere

Si distinguono molte categorie di malware, tra queste, nel gruppo definito "*ad occultamento*" troviamo:

- **Trojan** (o cavallo di troia): è un software che oltre ad avere delle funzionalità "lecite", utile per indurre l'utente ad utilizzarlo, contiene istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore.
- **Backdoor** (letteralmente "porta sul retro"): è un software pensato per creare un accesso nascosto al sistema che lo incorpora.
- **Rootkit** (letteralmente "Attrezzi da amministratore"): è un software clandestino progettato per nascondere l'esistenza di alcuni processi o programmi dai normali metodi di individuazione e di mantenere la continuità di accesso privilegiato al computer.



APPROFONDIMENTO

Spesso un programma malware è composto di più parti interdipendenti e rientra pertanto in più di una classe, inoltre la classificazione presentata non è da ritenersi esaustiva.

Riconoscere i tipi di malware infettivo e comprendere come funzionano

I malware di tipo infettivo sono noti più per il modo in cui si diffondono che per il loro comportamento specifico. In questa classe troviamo:

- **Virus**: sono parti di codice che si diffondono copiandosi all'interno di altri programmi, in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti.
- **Worm**: (letteralmente "verme") è simile ad un virus, ma a differenza di questo non necessita di legarsi ad altri eseguibili per diffondersi in quanto modifica il computer che infetta, in modo da venire eseguito ogni volta che si avvia la macchina e tenta di replicarsi sfruttando Internet, tipicamente a mezzo della posta elettronica.



Riconoscere i tipi di malware e comprendere come operano

La vera novità riguardo alla sicurezza è che il malware è diventato un business. Esistono organizzazioni attive a livello internazionale che hanno un unico obiettivo: fare soldi. Ecco quindi che, oltre alle tipologie già illustrate, vengono utilizzate anche le seguenti:

- **Spyware:** è un software usato per raccogliere informazioni dal sistema su cui viene installato al fine di trasmetterle ad un destinatario interessato. Le informazioni carpite possono andare dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente.
- **Adware:** sono programmi software che presentano all'utente messaggi pubblicitari durante l'uso. Possono causare danni quali rallentamenti del pc e rischi per la privacy in quanto comunicano le abitudini di navigazione ad un server remoto.
- **Keylogger:** sono dei programmi in grado di registrare tutto ciò che viene digitato sulla tastiera o che copia e incolla, consentendo il furto di password o di dati.
- **Dialer:** sono programmi che modificano il numero telefonico chiamato dalla connessione predefinita a Internet con uno a tariffazione speciale, allo scopo di trarne illecito profitto all'insaputa dell'utente.
- **Botnet:** è l'infezione di una rete informatica che viene controllata da remoto dal botmaster, che è in grado di utilizzare la rete stessa e i dispositivi ad essa collegati per svolgere attività non autorizzate.
- **Ransomware:** è un software malevolo che blocca il desktop dell'utente e invia delle richieste di pagamento di alcune somma di denaro per sbloccarlo.

15

Comprendere come funziona il software anti-virus e quali limitazioni presenta

Con le dovute differenze, nessun sistema operativo è immune dal malware. Per questa ragione è importante che ogni sistema installi un software antivirus.

Un antivirus ha due funzioni primarie:

- La prima, è quella di analizzare continuamente la memoria alla ricerca di comportamenti anomali o di uno schema virale sulla base della comparazione con un archivio contenente le "firme" dei malware conosciuti;
- La seconda, normalmente eseguita su richiesta utente o pianificata, è quella di controllare cartelle e file in modo da individuare e rendere innocui eventuali file portatori di infezione virale.

Un antivirus da solo, per quanto affidabile ed efficiente, non rappresenta una protezione totale contro il 100% dei virus informatici esistenti al mondo. Inoltre, per poter essere efficace, l'antivirus deve essere aggiornato con frequenza, in particolare l'archivio delle firme, in quanto nuovi malware vengono diffusi in continuazione.

Infine, va segnalato che un altro limite dei software antivirus, è che l'impiego di tecniche euristiche per scoprire virus non ancora presenti nel database delle firme, porta a volte a segnalare **falsi positivi**, cioè a indicare come virus programmi del tutto leciti.



 **APPROFONDIMENTO**

Bisogna ricordare che l'antivirus è in grado di eliminare soltanto i virus che riconosce (perché è presente la relativa firma nel database dei malware o perché l'analisi euristica ne rileva un comportamento anomalo). Quindi, tutti i nuovi virus (per nuovi si intendono sia virus che il proprio antivirus non riconosce, sia quelli che non sono ancora stati scoperti) possono passare completamente incosservati. Inoltre, l'antivirus riesce a intercettare il virus solo quando questo è entrato all'interno del computer e quindi ha già infettato un file o la memoria; a questo punto, a seconda del tipo di virus, può "disinfettare" il file o la memoria eliminando completamente il virus o in alcuni casi è costretto a mettere in "quarantena" il file contagiato ed eliminarlo per l'impossibilità di recuperare il file originario.

16

Comprendere che il software anti-virus dovrebbe essere installato su tutti i sistemi informatici

Non è vero che tutto il malware in circolazione è pensato esclusivamente per i sistemi operativi Windows, anche se questi, grazie alla loro diffusione, sono sicuramente i più bersagliati.

Va poi ricordato che anche i dispositivi mobili come tablet e smartphone sono computer a tutti gli effetti e quindi, anche per loro, è importante disporre di un prodotto antivirus.

Naturalmente, per i diversi sistemi operativi mobili, il grado di sicurezza intrinseco può variare sensibilmente in accordo con la facilità con cui si possono rimuovere le protezioni di sistema. Ad esempio, nei sistemi "Android" è possibile mediante la variazione di un semplice parametro di configurazione abilitare l'esecuzione di codice non preventivamente autorizzato.

In sintesi, anche i dispositivi mobili dovrebbero essere protetti da un buon antivirus. Ciò consentirebbe di evitare che "App" malevoli possano accedere alla rubrica e ai dati sensibili archiviati o inviare automaticamente SMS di abbonamento a linee erotiche o MMS "premium" il cui costo verrebbe inevitabilmente scalato dal credito della povera vittima.

 **APPROFONDIMENTO**

Esistono due pratiche che consentono di rimuovere tutti i vincoli presenti su un sistema operativo mobile: il **Jailbreak** per i sistemi iOS (Apple) e il **Rooting** per i sistemi Android. Effettuando queste attività l'utente può eseguire qualsiasi programma, anche se non approvato, e le App sono libere di agire con i massimi privilegi, compresi quelli per modificare file e impostazioni a proprio piacimento. È evidente che in queste condizioni un software antivirus diventa indispensabile.

Comprendere l'importanza di aggiornare regolarmente i vari tipi di software

Come già accennato in precedenza, è essenziale scaricare regolarmente gli aggiornamenti delle definizioni dei virus e del programma antivirus. Ciò permette al sistema di aggiornarsi contro i nuovi rischi. Attualmente tutti i software antivirus si aggiornano automaticamente, ma è bene controllare che lo facciano. Il mancato aggiornamento automatico potrebbe essere indice di un malfunzionamento, magari dovuto proprio ad un virus che cerca di impedire al programma di individuarlo.

La predetta procedura va altresì estesa al resto del sistema. Aggiornare il sistema operativo e le altre applicazioni installate sul personal computer non è una procedura oziosa, una perdita di tempo. Tutt'altro. Se si "naviga" in Rete utilizzando un sistema operativo non aggiornato, un browser obsoleto o dei plugin "superati", ci sono buone probabilità che il proprio sistema (ed i dati in esso conservati) possano diventare bersaglio di un malware.



www.micertificoeCDL.it

© Copyright AICA 2014 – 2019

I criminali informatici sono infatti soliti utilizzare pagine web che, una volta caricate dal browser, fanno leva sulle vulnerabilità note del browser stesso, dei plugin installati (Java, Flash Player, Silverlight, QuickTime, ...) o del sistema operativo per installare codice dannoso.

APPROFONDIMENTO

Mantenere aggiornato e attivo un programma antivirus e fare tutti gli aggiornamenti di sicurezza rilasciati dai produttori di software è sicuramente una buona cosa. Tuttavia, non va dimenticato che la prima difesa dai pericoli della rete è l'utente stesso: un utente attento ha molte meno possibilità di ritrovarsi col computer infetto. Prestare dunque attenzione quando si installano nuovi programmi o prima di cliccare un URL inviato via mail. È bene anche controllare i programmi che si avviano automaticamente. La maggior parte dei programmi malevoli vengono caricati all'avvio del computer. Se poi per le ragioni più varie si deve accedere ad ambienti di dubbia reputazione è caldamente consigliato la creazione di una "sandbox" (area virtuale isolata nel sistema) mediante apposita applicazione.

17

Eseguire e pianificare scansioni di specifiche unità, cartelle e file usando un software anti-virus

Ogni programma antivirus utilizza una specifica modalità per l'esecuzione di una scansione. Ad esempio, con AVG è possibile utilizzare sia l'icona del programma presente nell'area di notifica, sia la console principale del prodotto.

Nel primo caso si dispone di un'interfaccia sintetica e si sfruttano le opzioni impostate come predefinite.

Nel secondo caso si possono controllare molti più aspetti delle sue funzionalità e impostare molte opzioni stabilendo con precisione il livello di scansione desiderato. Ad esempio si può impostare l'analisi degli *archivi compressi*, dei *cookie di rilevamento* e, tra le *impostazioni aggiuntive*, dei file senza estensione piuttosto che quelli multimediali.

Ogni opzione influenza il numero dei file analizzati piuttosto che il tempo complessivo necessario alla scansione.

Al termine della scansione una finestra di riepilogo mostra i risultati dell'analisi.

APPROFONDIMENTO

La scansione di specifiche cartelle o file non presenta alcuna differenza logica rispetto alla scansione dell'intero computer se non l'ovvia selezione di tale elemento prima dell'avvio.

Tra le opzioni di scansione non va dimenticata la possibilità di impostare una pianificazione esecutiva della stessa in modo che con una certa frequenza, solitamente settimanale, venga eseguita l'attività. Impostando una pianificazione si evita di dimenticare il lancio dell'antivirus o la pigrizia di farlo e si migliora la sicurezza del sistema.

ATTENZIONE!

L'esecuzione di una scansione è un'attività "pesante" per il sistema, per questa ragione, in genere, gli antivirus utilizzano un'opzione per definire il grado di utilizzo delle risorse. Si va da una gestione ridotta delle stesse con tempi di scansione relativamente lunghi, ad un alto utilizzo di risorse con scansioni più veloci ma con il computer praticamente inusabile. Solitamente l'utilizzo da preferire è quello *dinamico* (sensibile all'utente) in cui l'antivirus che lo supporta, si adatta all'uso del computer che ne fa l'utente.



Comprendere i rischi associati all'uso di software obsoleto e non supportato

Si è già avuto modo di analizzare l'importanza di mantenere aggiornato il sistema e alcuni suoi elementi chiave, ma che dire di programmi "datati" e non più supportati dai relativi produttori?

In diverse occasioni, Microsoft, analizzando le informazioni sulle minacce provenienti da oltre un miliardo di sistemi in tutto il mondo, ha riportato i pericoli per la sicurezza derivanti dall'utilizzo di software obsoleti citando anche i principali malware in grado di sfruttare le carenze tecnologiche di tali prodotti.

18

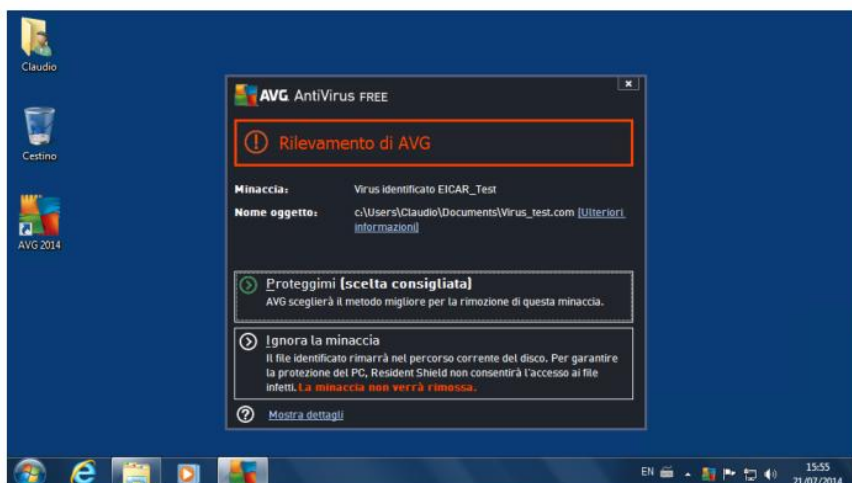
Inoltre, le falle alla sicurezza non sono l'unico aspetto del problema. L'utilizzo di prodotti datati, spesso non è in grado di rispondere adeguatamente alle esigenze in termini di flessibilità e mobilità imposte da un mercato in continua evoluzione ed è fonte di possibili incompatibilità con software più recenti.

Comprendere il termine "quarantena" e l'operazione di mettere in quarantena file infetti/sospetti

In generale, quando un software antivirus individua dei file contenenti del codice virale che non riesce a rimuovere chiede all'utente se intende metterli in **quarantena**, cioè **spostarli** in una apposita cartella creata dal software antivirus dove i file vengono codificati e salvati in una forma non eseguibile.

Naturalmente, se l'infezione riguarda un file importante di un'applicazione, questa può smettere di funzionare in tutto o in parte. Per questa ragione il file non viene eliminato ma solo reso inerte. L'idea alla base di questa scelta è quella di ipotizzare che futuri aggiornamenti del software possano rimuovere il virus consentendo poi il ripristino dei file nella sua posizione originale.

Nell'immagine di AVG visualizzata la voce "quarantena" non appare, ma rappresenta la scelta del programma se si seleziona l'opzione "Proteggimi".



 **APPROFONDIMENTO**
ATTENZIONE!

I file non restano in quarantena "a vita". Solitamente vengono cancellati automaticamente dopo 30 giorni oppure quando lo spazio a loro dedicato tende ad esaurirsi.

Eliminare file infetti/sospetti

Dopo aver messo in quarantena dei file, se non mancano file di dati e le applicazioni vengono eseguite correttamente, è possibile eliminare quei file dalla quarantena.

Ad esempio utilizzando AVG è necessario utilizzare il menu **Opzioni** e scegliere **Quarantena virus**. Nella finestra di dialogo diventa possibile visualizzare i dettagli di un file, eliminarlo o svuotare l'intera quarantena che eliminerà tutti i file presenti senza passare dal cestino.

19

 **APPROFONDIMENTO**

Nella gestione della quarantene di AVG, è anche possibile ripristinare un file nella sua posizione originale (o in altra cartella) oppure inviare ai suoi laboratori un file per l'analisi (nel caso di un falso positivo).

Utilizzo di risorse online per diagnosticare e risolvere un attacco malware

Una delle prime cose che tenta di fare un software dannoso è quella di disattivare l'antivirus installato. Se ci riesce, l'unico modo disponibile per diagnosticare il malware e tentare di risolvere il problema è quello di utilizzare uno scanner online.

Un'altra importante ragione è quella di avere un secondo parere sulla sicurezza del sistema durante la pulizia di un PC infetto.

Quasi tutte le aziende produttrici di antivirus offrono infatti sul proprio sito strumenti per cercare sul PC virus o malware, e alcune ne permettono anche la rimozione. In genere, si tratta di strumenti gratuiti e facili da usare che consentono a chiunque abbia una connessione internet di verificare velocemente la sicurezza del proprio Pc.

Altri tool sono disponibili nei siti dei produttori dei sistemi operativi e delle più importanti autorità nel campo della sicurezza.

 **APPROFONDIMENTO**

Ci sono pro e contro sull'utilizzo degli strumenti antivirus online. Di seguito ne sono riportati alcuni.

Vantaggi

- Forniscono un metodo alternativo per fronteggiare una minaccia esistente.
- Usano semplici interfacce con poche scelte.
- Non richiedono aggiornamenti

Svantaggi

- Possono solo rimuovere ciò che ha già infettato il PC (non esiste la protezione in tempo reale).
- Possono richiedere di installare un componente ActiveX.



- Possono richiedere l'uso di un browser specifico.
- Possono non rimuovere tutte le minacce.
- Potrebbero non essere in grado di selezionare quali cartelle o unità si desidera scansionare.
- Possono non eseguire la scansione di tutti i tipi di file.

Altre limitazioni

- Alcuni scanner individuano il virus ma chiedono di installare il prodotto dell'azienda per rimuoverlo o si fermano al primo rilevamento.
- Altri scanner individuano il virus e forniscono indicazioni di come cercare lo specifico "remover" costringendo l'utente ad una lunga e spesso difficile ricerca.
- Alcuni scanner richiedono la presenza di Java.

Alcuni software raccolgono informazioni sull'utente e non solo sui virus rilevati.



Capitolo 3 – Sicurezza in rete

Riferimento Syllabus 3.1.1	<i>Comprendere il termine "rete" e riconoscere i più comuni tipi di rete, quali LAN (rete locale), WLAN (rete locale wireless), WAN (rete geografica), VPN (rete privata virtuale).</i>
Riferimento Syllabus 3.1.2	<i>Comprendere che la connessione ad una rete ha implicazioni di sicurezza, quali malware, accessi non autorizzati ai dati, difesa della riservatezza.</i>
Riferimento Syllabus 3.1.3	<i>Comprendere il ruolo dell'amministratore di rete nella gestione delle operazioni di autenticazione, autorizzazione e assegnazione degli account all'interno di una rete; verifica e installazione di patch e aggiornamenti di sicurezza importanti; controllo del traffico di rete e trattamento del malware rilevato su una rete.</i>
Riferimento Syllabus 3.1.4	<i>Comprendere la funzione e i limiti di un firewall in ambiente domestico e di lavoro.</i>
Riferimento Syllabus 3.1.5	<i>Attivare, disattivare un firewall personale. Consentire o bloccare l'accesso attraverso un firewall personale a un'applicazione, servizio/funzione.</i>
Riferimento Syllabus 3.2.1	<i>Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti, quali: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) / WPA2 (Wi-Fi Protected Access 2), filtraggio MAC (Media Access Control), SSID nascosto (Service Set Identifier).</i>
Riferimento Syllabus 3.2.2	<i>Essere consapevoli che usando una rete wireless non protetta si va incontro ad attacchi da parte di intercettatori (eavesdropping), dirottatori di rete (network hijacking), violatori di comunicazioni private (man in the middle).</i>
Riferimento Syllabus 3.2.3	<i>Comprendere l'importanza di aggiornare regolarmente vari tipi di software, quali: antivirus, browser web, plug-in, applicazioni, sistema operativo.</i>
Riferimento Syllabus 3.2.4	<i>Comprendere il termine "hotspot personale".</i>
Contenuti della lezione	Comprendere il termine "rete" e riconoscere i più comuni tipi di rete; Comprendere che la connessione ad una rete ha implicazioni di sicurezza; Comprendere il ruolo dell'amministratore di rete; Comprendere la funzione e i limiti di un firewall in ambiente personale e lavorativo; Attivare, disattivare un firewall personale; Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti; Essere consapevoli che usando una rete wireless non protetta si rischia che i propri dati vengano intercettati da "spie digitali"; Comprendere il termine "hotspot personale"; Attivare, disattivare un hotspot personale sicuro, connettere in modo sicuro e disconnettere dispositivi informatici.

21

Comprendere il termine "rete" e riconoscere i più comuni tipi di rete

Una **rete di computer**, è un insieme di più elaboratori indipendenti ma interconnessi, in grado di scambiare e condividere informazioni attraverso mezzi trasmissivi differenti.



Le reti possono essere classificate in base a diversi criteri. Ad esempio, in base all'estensione geografica una rete può essere identificata come:

- **LAN** o *Local Area Network* quando si sviluppa in un'area fisica delimitata, come una o più stanze, un edificio o più edifici tra loro vicini; quando poi la rete utilizza, in toto o in parte, una copertura wireless, si parla di **WLAN** (cioè Wireless Local Area Network).
- **MAN** o *Metropolitan Area Network* se la rete si estende a un'intera area cittadina.
- **WAN** o *Wide Area Network* se la rete è geograficamente molto estesa e collega tra loro host e LAN utilizzando mezzi trasmissivi diversi che possono includere anche i satelliti.

22

Un particolare tipo di rete, non classificabile con le precedenti è la **VPN** o *Virtual Private Network*. Come suggerisce il nome, è una rete di telecomunicazioni privata, instaurata tra soggetti che utilizzano un sistema di trasmissione pubblico e condiviso, generalmente Internet.

Nelle VPN un apposito software si occupa di creare un "tunnel" sicuro attraverso la criptazione dei dati e l'autenticazione della comunicazione.

APPROFONDIMENTO

Le **reti locali** vengono realizzate tipicamente utilizzando un sistema di cablaggio strutturato con tecnologia *ethernet* e supportano velocità di 10/100 Mbit/s, o anche 1 Gbit/s, su cavi in rame dalle caratteristiche adeguate (CAT5 o superiore), o su fibra ottica. In molti casi, le LAN aziendali sono sostituite o integrate da reti wireless. Questo è vantaggioso negli edifici più vecchi, dove non esiste o non è possibile installare un impianto di cablaggio strutturato. Lo standard WLAN più diffuso è quello basato su specifiche IEEE 802.11 ma è più noto con il nome commerciale "Wi-Fi". La velocità tipica di una WLAN è di 54 Mbit/s.

Le **reti metropolitane** sono reti di trasporto che tipicamente operano su collegamenti Gigabit Ethernet e utilizzano la fibra ottica come mezzo trasmissivo. Comunemente queste reti operano a velocità fino a 150 Mbit/s.

Le **reti WAN** sono reti di trasporto che utilizzano linee di comunicazione dedicate e possono operare in un range di velocità compreso tra 1 e 100Gbit/s.

Comprendere che la connessione ad una rete ha implicazioni di sicurezza

Sono molti i vantaggi che derivano dall'uso di una rete: condivisione di risorse, trasferimento di file, centralizzazione di applicativi, ecc. Dalla rete però possono giungere anche delle minacce.

Attraverso la rete locale, ma specialmente da internet, è possibile che il computer venga infettato da **malware** che spesso viene scaricato attraverso la posta elettronica o da pagine web infette.

Attraverso la rete sono possibili **accessi non autorizzati** al computer dovuti a falle di sicurezza o infezioni virali.

Da ultimo, la rete può costituire un rischio anche per la **privacy** degli utenti connessi, in quanto i dati personali, se non adeguatamente protetti, possono essere acceduti da malintenzionati sfruttando una delle modalità precedenti.

A riprova di quanto affermato si riportano i dati forniti da un bollettino della sicurezza dei laboratori Kaspersky: un celebre produttore di antivirus, in cui sono messi in evidenza le percentuali di malware finanziario rispetto al totale rilevato in ciascuna nazione.



Nel 2013 c'è stato un aumento significativo della percentuale delle minacce informatiche finanziarie rispetto all'anno precedente. In particolare, hanno giocato un ruolo chiave i malware progettati per rubare denaro.

Comprendere il ruolo dell'amministratore di rete

L'amministratore di rete è la figura professionale che, nell'ambito di un ente o azienda, è preposta alla gestione tecnica della rete di computer. I suoi compiti possono variare in modo significativo in rapporto alle dimensioni dell'organizzazione e possono coinvolgere anche più persone.

Le attività a lui richieste sono davvero molte e spaziano dalla progettazione, realizzazione e controllo di LAN e WAN, alla implementazione di politiche di accesso alle strutture di rete.

In quest'ultimo contesto sono coinvolti nella gestione delle operazioni di autenticazione, autorizzazione e assegnazione degli account all'interno della rete.

Ciò significa stabilire per ogni utente l'accesso alle risorse necessarie quali file, cartelle, stampanti, Internet, ecc. in accordo con le politiche dell'ICT.

Naturalmente, poiché la definizione degli accessi è regolata attraverso delle "Access Control List" e queste a loro volta sono realizzate sulla base dell'account utente, è necessario che ogni utente che desidera l'accesso alla rete disponga di una propria User ID e relativa password.

Gli amministratori di rete sono coinvolti in modo proattivo anche nelle seguenti attività:

- Monitoraggio della rete.
- Test della rete per individuarne eventuali debolezze.
- Applicazione degli aggiornamenti necessari.
- Installazione e implementazione di programmi per la sicurezza.
- Individuazione dei "colli di bottiglia".

Comprendere la funzione e i limiti di un firewall in ambiente personale e lavorativo

Un firewall (letteralmente "muro tagliafuoco") è un componente di difesa frapposto tra un computer o una rete privata e Internet, allo scopo di evitare intrusioni e accessi non autorizzati.

Va detto subito che è opportuno distinguere tra **firewall perimetrali**, utilizzati con apparati dedicati nelle aziende a protezione della LAN; e **firewall personali**, solitamente realizzati mediante software in ambito personale.

Il compito primario di un firewall è quello di monitorare il traffico di rete e filtrarlo in base ad **opportune regole** che garantiscano la sicurezza di tutti i dati in entrata e in uscita, da e verso la rete o il computer, bloccando ciò che si ritiene pericoloso o indesiderato. Da questa definizione si evince che il suo principale punto di forza è paradossalmente anche la sua maggior debolezza. Se le regole non sono ben programmate, il suo funzionamento non solo non sarà efficace, ma potrebbe anche impedire un uso legittimo della rete.

A differenza del firewall perimetrale, quello personale consente di proteggere solamente il PC sul quale è installato a meno che altri PC si connettano ad Internet attraverso il PC che ne fa uso.

Un'altra differenza è che il personal firewall può anche interagire con l'utente del PC chiedendo conferma di alcune azioni potenzialmente pericolose, come ad esempio permettere o impedire a un particolare programma di connettersi a Internet.



Tra i limiti di un personal firewall è bene annoverare che:

- In molti casi la sua configurazione è gestita da impostazioni predefinite, quindi poco flessibili, per non lasciare ad utenti inesperti un impegno decisamente complesso;
- Dato che è installato sul sistema che protegge, un attacco al personal firewall compromette l'intero sistema come ha dimostrato il worm Witty;
- Una volta che il sistema è stato compromesso da un malware questo può manipolare anche il funzionamento del firewall.

Attivare, disattivare un firewall personale

24

Si è già detto che un personal firewall è un programma installato nel PC da proteggere. Questo programma può essere fornito da terze parti o già presente nel sistema operativo.

Nel caso di Windows, il personal firewall è chiamato "**Windows Firewall**" ed è attivato all'installazione del sistema per impostazione predefinita.

In caso di necessità, ad esempio se si desidera attivare un firewall di terze parti, è possibile disattivare Windows Firewall mediante la seguente procedura:

- Aprire il **Pannello di controllo**
- Selezionare **Sistema e sicurezza** quindi **Windows Firewall**
- Sul lato sinistro della finestra selezionare **Attiva/Disattiva Windows Firewall**
- Nella finestra *Personalizza impostazioni* selezionare l'opzione **Disattiva Windows Firewall (scelta non consigliata)** per i tipi di rete desiderati, quindi, concludere con **OK**.

Con procedura analoga è possibile riattivarlo.

Quando è attivo, *Windows Firewall* blocca la maggior parte dei programmi per garantire una maggior sicurezza, tuttavia, per un corretto funzionamento, alcuni programmi potrebbero aver bisogno di comunicare attraverso il firewall.

Lo sblocco di tali programmi si attua nel seguente modo:

- Accedere alla finestra di *Windows Firewall* come visto in precedenza
- Sul lato sinistro della finestra selezionare **Consenti programma o funzionalità con Windows Firewall**
- Nella finestra *Programmi consentiti* premere il pulsante **Modifica Impostazioni**
- Selezionare la casella di controllo del programma o funzionalità da attivare
- Selezionare la casella di controllo dei percorsi di rete su cui si desidera consentire le comunicazioni, quindi concludere con **OK**.

Con procedura analoga è possibile bloccare la comunicazione ad un programma o funzionalità sbloccata in precedenza.

APPROFONDIMENTO

In Windows Firewall per aggiungere alla lista dei programmi consentiti un programma non compreso nell'elenco basta premere il pulsante **Consenti un altro programma** (disponibile nella finestra Programmi consentiti) e selezionarlo dalla lista nella finestra che appare.

Concludere con **Aggiungi** e quindi **OK**.



Riconoscere diversi tipi di sicurezza per reti wireless e i loro limiti

Il problema principale delle reti senza filo è la sicurezza. Se la rete non è adeguatamente protetta un malintenzionato potrebbe facilmente intercettare i dati in transito. Per questa ragione è opportuno proteggerne l'accesso con una chiave di sicurezza e cifrare i dati scambiati.

Negli anni si sono resi disponibili diversi standard di sicurezza crittografica:

- **WEP** (Wired Equivalent Privacy). Nasce nel 1999 come primo standard con lo scopo di fornire una sicurezza comparabile a quella delle reti cablate, da cui il nome. Seri difetti nella particolare implementazione dell'algoritmo crittografico e chiavi troppo brevi, resero però necessaria una sua revisione. Lo standard è ancora disponibile per supportare i dispositivi meno attuali, ma il suo utilizzo è sconsigliato perché relativamente facile da violare.
- **WPA e WPA2** (Wi-Fi Protected Access). Disponibili rispettivamente nel 2003 e 2004 mettono a disposizione una maggiore sicurezza. WPA2 è più sicuro di WPA, ma non è supportato da alcune schede di rete meno recenti.

25

Per aumentare la sicurezza, si può aggiungere ai sistemi di autenticazione e crittografia appena visti un controllo hardware dei computer che si collegano.

Questa protezione si realizza utilizzando il **MAC address**, ossia l'indirizzo fisico di ogni scheda di rete (sia cablata che wireless). Dato che tale indirizzo è univoco al mondo, è possibile utilizzarlo in apposite "Access control List" all'interno degli apparati di rete. Ciò garantisce l'accesso alla rete ai soli dispositivi registrati.

Da ultimo, è bene sapere che, in generale, i router impostano in modo predefinito il broadcasting (ovvero la diffusione) del proprio **SSID**. Acronimo di Service Set Identifier, l'SSID è il nome col quale una rete Wi-Fi si presenta ai suoi utenti.

Dato che in genere tale nome è impostato sul modello di dispositivo, si finisce per fornire al potenziale attaccante anche l'hardware con cui ha a che fare. È pertanto possibile modificare nelle impostazioni di configurazione del router tale diffusione, senza che ciò abbia impatto sui device che già utilizzano la rete.



APPROFONDIMENTO

Utilizzando i MAC address, in teoria un dispositivo con un Mac address differente non verrà connesso alla rete senza fili anche se il proprietario conosce la chiave di sicurezza.

In realtà, questo metodo non è del tutto sicuro, infatti esistono dei software in grado di modificare il Mac address della scheda di rete di un dispositivo.

Come si può capire da quanto detto in precedenza, nessun metodo rende sicura al 100% una rete senza fili, tuttavia utilizzando più metodi in combinazione si raggiunge un buon grado di sicurezza.

Si rammenta inoltre che il mancato uso di una chiave di sicurezza ha portato nel passato alla nascita di un'attività illegale chiamata "**Wardriving**" (Acronimo composto da "Wireless Access Revolution" e "driving") che consisteva nell'intercettare reti Wi-Fi, in automobile o a piedi con un laptop, solitamente abbinato ad un ricevitore GPS per individuare l'esatta locazione della rete trovata ed eventualmente pubblicarne le coordinate geografiche su un sito web, o per accedere abusivamente ad una connessione ad internet.

Essere consapevoli che usando una rete wireless non protetta si rischia che i propri dati vengano intercettati da "spie digitali"

Alla luce di quanto si è detto finora, appare evidente che se una rete wireless non viene protetta da uno o più dei metodi presentati in precedenza è possibile che un malintenzionato possa guadagnarne l'accesso e utilizzarla per i propri scopi senza che il legittimo proprietario ne venga a conoscenza.



Tra le tipologie di attacco, l'intercettazione è sicuramente la più applicata con una delle sue varianti quali:

- Il **wardriving** già citata in precedenza
- L'**eavesdropping** che consiste nel catturare passivamente i segnali radio e cercando di decodificare i dati trasmessi

Altre tipologie di attacco possibili sono:

- **Network hijacking** che consiste nell'entrare nell'account di qualcuno senza conoscerne le credenziali ma "rubando" il suo cookie di sessione
- **Man in the middle** quando l'attaccante si frappone tra due parti comunicanti tra di loro e si sostituisce ad uno di essi in modo da poter leggere, inserire o modificare messaggi a piacere.

26

Comprendere il termine "hotspot personale"



Tutti i possessori di uno smartphone conoscono sicuramente il termine "*tethering*", malamente traducibile in italiano con l'espressione "*incatenamento*".

Tale termine individua la funzionalità che consente al telefono di trasformarsi in un **gateway** per offrire connettività Internet a device che ne sono sprovvisti. La connessione può avvenire wireless (Bluetooth o Wi-Fi) oppure con un cavetto USB. Quando la connessione si attua a mezzo Wi-Fi, il telefono diventa a tutti gli effetti un **Access Point**. In altri termini il telefono crea un **hotspot**.

Il termine **Personal Hotspot**, è stato coniato da Apple per iOS per indicare l'utilizzo della tecnologia di Tethering con Wi-Fi in modo da condividere la connessione dati di iPhone e iPad con altri dispositivi e computer senza necessità di connessione fisica.

Su dispositivi di altre aziende questa modalità assume nomi leggermente diversi quali ad esempio **Portable Wi-Fi hotspot**.

APPROFONDIMENTO

Per riferimento si fornisce di seguito una breve interpretazione di alcuni termini utilizzati nella spiegazione del termine "Personal hotspot".

Gateway - Nelle reti più semplici (come nel caso in esame) è un dispositivo che ha il compito di veicolare tutto il traffico diretto all'esterno verso la rete Internet.

Access Point - è un dispositivo di telecomunicazioni che permette all'utente mobile di accedervi in modalità wireless direttamente tramite il suo terminale, se dotato di scheda wireless.

Hotspot - Indica un luogo in cui è presente una connessione a Internet Wi-Fi.



Attivare, disattivare un hotspot personale sicuro, connettere in modo sicuro e disconnettere dispositivi informatici

La procedura di abilitazione di un hotspot personale varia a seconda del modello di smartphone utilizzato. Ad esempio su iPhone 3G può essere attuata come segue:

- Nel menu principale toccare **Impostazioni**
- Toccare la voce **Hotspot personale**
- Attivare l'interruttore **Hotspot personale**
- Se l'interruttore del servizio Wi-Fi o del servizio Bluetooth è impostato su *Spento* ne viene proposta l'attivazione
- Il menu **Password Wi-Fi** presente in *Hotspot personale* permette di impostare una password di accesso alla rete Wi-Fi.

27

Al termine del collegamento è importante chiudere correttamente la connessione con queste operazioni:

- Nel menu principale toccare **Impostazioni**
- Toccare la voce **Generali**
- Selezionare la voce **Rete**;
- Selezionare la voce **Hotspot personale**
- Toccare l'interruttore riportandolo sulla posizione **Spento**.

Dopo aver abilitato l'hotspot basta andare sul dispositivo da collegare e cercare la rete Wi-Fi. Ad esempio su un computer con Windows 7 effettuare quanto segue:

- Dall'area di notifica presente nell'angolo in basso a destra aprire il pannello delle connessioni di rete
- Individuare la rete generata dall'iPhone e cliccare sul pulsante **Connetti**
- Inserire nella finestra popup che appare la password creata nel menu Hotspot personale dell'iPhone
- Attendere la notifica della connessione.
- La disconnessione avviene con analoga procedura ma utilizzando il pulsante **Disconnetti**.



Capitolo 4 – Controllo degli accessi

Riferimento Syllabus 4.1.1	<i>Identificare i metodi per impedire accessi non autorizzati ai dati, quali: nome utente, password, PIN, cifratura, autenticazione a più fattori.</i>
Riferimento Syllabus 4.1.2	<i>Comprendere il termine "one-time password" e il suo utilizzo tipico.</i>
Riferimento Syllabus 4.1.3	<i>Comprendere lo scopo di un account di rete.</i>
Riferimento Syllabus 4.1.4	<i>Comprendere che per accedere alla rete sono necessari un nome utente e una password, e che è importante disconnettere l'account, al termine del collegamento.</i>
Riferimento Syllabus 4.1.5	<i>Identificare le comuni tecniche di sicurezza biometrica usate per il controllo degli accessi, quali impronte digitali, scansione dell'occhio, riconoscimento facciale, geometria della mano.</i>
Riferimento Syllabus 4.2.1	<i>Riconoscere buone linee di condotta per la password, quali scegliere le password di lunghezza adeguata e contenenti un numero sufficiente di lettere, numeri e caratteri speciali; evitare di condividerle, modificarle con regolarità, scegliere password diverse per servizi diversi.</i>
Riferimento Syllabus 4.2.2	<i>Comprendere la funzione e le limitazioni dei software di gestione delle password.</i>
Contenuti della lezione	Identificare i metodi per impedire accessi non autorizzati ai dati; Comprendere il termine "one-time password" ed il loro utilizzo tipico; Comprendere lo scopo di un account di rete; Accesso alla rete con nome utente e password, e blocco dell'account quando non viene usato; Identificare le comuni tecniche di sicurezza biometriche usate per il controllo degli accessi; Riconoscere buone linee di condotta per la password; Comprendere la funzione e le limitazioni dei software di gestione delle password.

29

Identificare i metodi per impedire accessi non autorizzati ai dati

Si definisce **autenticazione** il processo tramite il quale un sistema informatico, verifica l'identità di un altro computer, software o utente che vuole accedere alle proprie risorse autorizzandolo ad usufruire dei servizi associati.

In pratica, un sistema di elaborazione, progettato per essere usato soltanto da *utenti autorizzati*, deve essere in grado di rilevare ed escludere i *soggetti non autorizzati*. L'accesso ad esso, dunque, viene garantito solo dopo aver eseguito con successo una procedura di autenticazione, di solito attraverso un **nome utente** e una **password** personale. L'esempio citato è la comune procedura di autenticazione che conosciamo come "*login*".

Quando il processo di autenticazione deve essere più rigido, i metodi di autenticazione devono diventare più sofisticati ed adottare tecniche a più fattori. Si pensi ad esempio al prelievo di denaro da un bancomat: richiede una tessera a microchip e la digitazione di un **PIN**.



In generale, si può affermare che i metodi di autenticazione utilizzabili da un essere umano sono classificabili in tre classi in base a:

- **Qualcosa che conosce** (es. password o PIN)
- **Qualcosa che ha** (es. tesserino identificativo o smart card)
- **Qualcosa che è** (es. impronta digitale, vocale o retinica, calligrafia o altri identificatori biometrici)

Quando poi il processo di autenticazione non coinvolge in maniera diretta un essere umano, ad esempio nella trasmissione dei dati, un altro pilastro fondamentale è la **crittografia**.



APPROFONDIMENTO

30

Quando si utilizza più di un metodo di autenticazione per accedere ad una funzionalità/servizio si parla di **Autenticazione forte**.

Comprendere il termine “one-time password” ed il loro utilizzo tipico

L'espressione “One-Time Password” identifica una password “usa e getta” che può essere usata una sola volta; cioè valida per una singola transazione o per la sola sessione di lavoro fino alla disconnessione.

La password OTP risolve le problematiche di sicurezza legate all'utilizzo di password tradizionali, agendo in particolar modo nell'ambito della protezione contro gli attacchi con replica.

Infatti, se un potenziale intruso riuscisse ad intercettare una OTP che è stata già utilizzata per accedere a un servizio o eseguire una transazione, non sarà in grado di riutilizzarla, in quanto non più valida.

Le password OTP possono essere rese note all'utente in molti modi:

- A mezzo di una chiavetta con display, oggi molto usata nell'home banking.
- Attraverso apposito software che gira su cellulare.
- Attraverso la messaggistica SMS.
- Per mezzo di una scheda stampata in possesso dell'utente.

Comprendere lo scopo di un account di rete

Per comprendere lo scopo di un account di rete è necessario prima distinguere tra **reti paritetiche** e **reti client/server**.

Nelle **reti paritetiche** tutti i computer svolgono funzioni simili, l'autenticazione degli utenti avviene localmente e le risorse condivise sui vari computer sono accessibili in base alle impostazioni delle singole macchine.

Nelle **reti client/server** il server si occupa dell'autenticazione degli utenti anche su tutti i client e centralizza i permessi di accesso alle risorse di tutta la rete.

Nelle organizzazioni aziendali per ragioni di sicurezza e facilità di manutenzione, le reti client/server sono basate su un **dominio**, cioè un insieme di computer che vengono amministrati come un'unità con regole e procedure comuni.



www.micertificoecdl.it

© Copyright AICA 2014 – 2019

Ed è proprio nell'ottica del dominio che entra pesantemente in gioco l'**account di rete**. Attraverso l'account l'amministratore della rete può stabilire esattamente a quali risorse avrà accesso, limitando la visibilità delle informazioni aziendali in base al ruolo ricoperto dall'utente.

APPROFONDIMENTO

Un account di rete all'interno di un dominio ha importanti differenze rispetto ad un account locale di un computer. Ad esempio permette il login degli utenti in qualsiasi computer del dominio utilizzando le stesse credenziali e mantenendo gli stessi diritti rispetto alle risorse condivise.

Accesso alla rete con nome utente e password, e blocco dell'account quando non viene usato

31

Per fare in modo che solo gli utenti autorizzati possano accedere alle risorse di rete è necessario che ciascun utilizzatore disponga di proprie credenziali d'accesso, nella forma di "*nome utente*" e "*password*".

L'accesso può avvenire in fase d'avvio del computer o in un momento successivo dopo la sconnessione di un utente.

Dopo il login l'utente avrà accesso alle risorse locali del proprio profilo e a tutte le risorse condivise a cui è abilitato.

Per questa ragione è opportuno che in caso di allontanamento temporaneo dal PC provveda a bloccare lo schermo per impedire ad altre persone l'uso del computer e l'accesso ai dati contenuti. La sessione corrente resterà attiva e tutte le applicazioni continueranno a funzionare, ma occorrerà immettere la password per usare nuovamente il computer.

Lo schermo può essere bloccato manualmente mediante sequenze di tastiera o automaticamente usando l'opzione di blocco dello screen saver.

A conclusione della propria attività e se il PC deve essere usato da altri, procedere allo scollegamento dell'account invece dello spegnimento.

APPROFONDIMENTO

Windows 7 consente di cambiare utente senza attuare la sconnessione dell'utente corrente. Va però rilevato che tale funzionalità potrebbe essere bloccata dall'amministratore. Inoltre, è bene riflettere su vantaggi e svantaggi di questa procedura. Il vantaggio è l'immediatezza dell'operazione che permette ad altro utente che debba accedere al proprio account per un tempo molto limitato, di farlo senza interrompere l'attività corrente.

Gli svantaggi invece sono diversi. Cambiare utente senza sconnettere quello corrente mantiene bloccate le risorse in uso riducendo quelle disponibili per il nuovo utente (in particolare le risorse di memoria potrebbero essere critiche). In secondo luogo, se il nuovo utente dovesse spegnere per errore il computer, tutte le modifiche non salvate nel primo account verrebbero perse.

Identificare le comuni tecniche di sicurezza biometriche usate per il controllo degli accessi

L'uso delle password non è l'unico sistema sicuro per accedere ad un computer. In alcuni casi, si possono utilizzare **tecniche biometriche**, cioè basate sull'univocità di una caratteristica fisica umana.



Sicuramente, la tecnica biometrica più utilizzata è la scansione di **un'impronta digitale**: molti notebook ma anche altri dispositivi mobili ne sono provvisti.

In generale, nell'informatica tradizionale non si adottano altre tecniche, ma nel campo della autenticazione degli accessi fisici in locali protetti e in molti altri campi che riguardano la sicurezza, si possono utilizzare anche le seguenti:

- **Scansione della retina**, basata sull'analisi della struttura dei vasi sanguigni sul fondo dell'occhio.
- **Riconoscimento facciale**, basato sull'analisi della geometria del volto come, i lati della bocca, gli zigomi, la posizione del naso, il profilo degli occhi, ecc.
- **La geometria della mano**, basata sulle misure della mano, la lunghezza delle dita e la curvatura del palmo.

32

Tra le ulteriori tecniche è possibile citare anche le seguenti:

- **Il colore e la dimensione dell'iride**,
- **Le caratteristiche della voce**,
- **Il riconoscimento della firma**.

Riconoscere buone linee di condotta per la password

Per garantire la privacy dei propri dati e la sicurezza delle reti una password deve essere gestita in modo corretto e rispondere a criteri oggettivi di robustezza.

La prima cosa, benché ovvia, consiste nel mantenerla segreta e ciò implica non scriverla su un foglietto da incollare al monitor o sotto la tastiera. Se serve, va annotata e conservata in un luogo sicuro per futura referenza.

Inoltre è importante cambiarla con regolarità per vanificare una sua eventuale scoperta da parte di malintenzionati che adottano una delle tecniche esaminate in precedenza.

Infine, per potersi definire "robusta" e quindi difficilmente attaccabile deve avere una lunghezza non inferiore a 8 caratteri e utilizzare una combinazione di lettere maiuscole, minuscole, numeri e simboli speciali.



APPROFONDIMENTO

Ulteriori suggerimenti per la robustezza di una password possono essere i seguenti:

- Non deve essere riconducibile ad un soggetto fisico.
- Non deve essere una parola del dizionario o il nome di un parente o amico.
- Può utilizzare anche il carattere [spazio].

Va poi notato che una password andrebbe cambiata con una certa frequenza per vanificare eventuali falle nella sua segretezza, e soprattutto, è importante utilizzare password diverse a fronte di servizi diversi, per impedire che la scoperta di una password possa compromettere contemporaneamente tutti i servizi utilizzati.

ATTENZIONE!

L'uso di lettere accentate, se da un lato può aumentare la complessità della password, crea potenziali problemi se l'accesso deve avvenire su computer diversi con differenti lingue di tastiera o sistemi operativi.



Comprendere la funzione e le limitazioni dei software di gestione delle password

Il numero dei siti che richiedono password continua a salire, e certo non è facile ricordarsi decine o centinaia di password.

Uno studio americano del 2012 mostra che il 58% dei navigatori usa almeno 5 password uniche, ed il 30% più di 10, ma la maggior parte si lamenta dell'eccessiva fatica quando devono creare e ricordare nuove password. Per questo le persone spesso tendono ad usare la stessa password per più siti. Uno studio del 2013 di McAfee e Intel ha rilevato che il 74% del campione usava la stessa password per tutti i siti.

Se questo è il problema, quale può essere la soluzione? Al di là delle tecniche per ricordare più o meno facilmente una password è possibile ricorrere ad un **Password manager** ossia ad un programma specializzato per conservare in sicurezza le password nel computer o nel cloud.

33

La sicurezza è garantita dalla cifratura di tutti i dati.

Un programma di questo tipo permette di **ricordare soltanto un'unica password**: quella di accesso al database del programma. Questa password è chiamata **Master password** e la sua "robustezza" è ovviamente fondamentale.

Una volta posto in uso il password manager si incarica di compilare automaticamente i campi nome utente e password e questo consente di scegliere password sicure, lunghe, complesse e casuali diverse per ogni sito.



APPROFONDIMENTO

Esistono tre tipi di password manager: integrati nel browser; online e desktop con versioni gratuite e a pagamento. Le versioni online e desktop offrono anche funzionalità aggiuntive, come la creazione di password casuali, la memorizzazione di altre informazioni sensibili e i promemoria per cambiare le password periodicamente. Le versioni online hanno anche il vantaggio di consentire l'accesso alle proprie informazioni utilizzando dispositivi diversi (PC, Tablet, Smartphone, ecc.).



Capitolo 5 – Uso sicuro del web

Riferimento Syllabus 5.1.1	<i>Selezionare impostazioni adeguate per attivare, disattivare il completamento automatico, il salvataggio automatico quando si compila un modulo.</i>
Riferimento Syllabus 5.1.2	<i>Eliminare dati privati da un browser, quali cronologia di navigazione, cronologia di scaricamento, file temporanei di Internet, password, cookie, dati per il completamento automatico.</i>
Riferimento Syllabus 5.2.1	<i>Essere consapevoli che alcune attività in rete (acquisti, transazioni finanziarie) devono essere eseguite solo su pagine web sicure e con l'uso di una connessione di rete sicura.</i>
Riferimento Syllabus 5.2.2	<i>Identificare le modalità con cui confermare l'autenticità di un sito web, quali: qualità del contenuto, data corrente, validità URL, informazioni sulla società o sul proprietario, informazioni di contatto, certificato di sicurezza, validazione del proprietario del dominio.</i>
Riferimento Syllabus 5.2.3	<i>Comprendere il termine "pharming".</i>
Riferimento Syllabus 5.2.4	<i>Comprendere la funzione e i tipi di software per il controllo del contenuto, quali software per il filtraggio di internet, software di controllo genitori.</i>
Contenuti della lezione	Completamento automatico e salvataggio automatico nella compilazione di un modulo; Eliminare dati privati da un browser; Utilizzare una connessione di rete sicura per le attività in rete; Identificare le modalità con cui confermare l'autenticità di un sito web; Comprendere il termine pharming; Comprendere la funzione e i tipi di software per il controllo del contenuto.

35

Completamento automatico e salvataggio automatico nella compilazione di un modulo

Il **completamento automatico** e il **salvataggio delle password** di accesso ad un sito sono funzioni molto comode, ma rappresentano una minaccia per la privacy se il computer è utilizzato in modalità condivisa da più persone. Per questo motivo, queste funzionalità possono essere abilitate o disabilitate a seconda dei casi.

Per impostare questa funzionalità in Internet Explorer bisogna accedere alle **Opzioni Internet** del menu **Strumenti**. Dopo aver selezionato la scheda **Contenuto** è necessario premere il pulsante **Impostazioni** della sezione *Completamento automatico*. Nella finestra di dialogo che si apre è possibile togliere o mettere il segno di spunta dall'opzione "**Moduli**" o "**Nome utente e password sui moduli**" e quindi confermare le scelte con **OK** due volte.





APPROFONDIMENTO

L'opzione **Richiedi salvataggio password** (subordinata a "Nome utente e password sui moduli") attiva per default, se disattivata, consente il salvataggio automatico delle password senza alcun prompt.

Eliminare dati privati da un browser

Durante l'esplorazione del web Internet Explorer memorizza informazioni quali: File temporanei Internet, Cookie, Cronologia di navigazione, Password Web salvate e altro ancora.

36

Queste informazioni possono essere cancellate per liberare spazio disco o per mantenere la propria privacy.

Per eliminare questi dati basta aprire il menu **Sicurezza** e selezionare **Elimina cronologia esplorazioni**. Nella finestra di dialogo che si apre, selezionare o deselezionare le caselle di controllo di fianco a ciascuna categoria di informazioni che si desidera eliminare, quindi premere il pulsante **Elimina**.



APPROFONDIMENTO

Se non si desidera memorizzare i dati di navigazione citati è possibile utilizzare la funzionalità **InPrivate Browsing**. Questa modalità di esplorazione attivabile dal menu **Sicurezza** apre una nuova finestra nella quale si potranno aprire tutte le schede desiderate. Alla chiusura della finestra tutti i dati accumulati verranno eliminati automaticamente.

Utilizzare una connessione di rete sicura per le attività in rete

Ogni utente utilizza Internet per le attività più varie. Si può navigare tra le pagine dei notiziari preferiti, ascoltare una canzone, visualizzare un filmato, utilizzare i servizi di un sito web, ecc. Queste attività si fanno con molta serenità, senza troppo preoccuparsi della sicurezza.

La navigazione sul web è resa possibile grazie al protocollo HTTP che però ha la caratteristica di trasmettere tutti i dati in chiaro e quindi a rischio di intercettazione.

Ci sono però attività online che richiedono una maggiore attenzione, come fare acquisti o eseguire transazioni bancarie. In questi casi è opportuno accertarsi di essere posizionati su pagine web sicure.

Per questa ragione è stato creato anche il protocollo **HTTPS** (Hyper Text Transfer Protocol over Secure socket layer) che trasmette i dati attraverso un canale cifrato al fine di garantire che solamente il client, cioè il browser, e il server, cioè il sito web, siano in grado di conoscere il contenuto della comunicazione.

È pertanto essenziale per la sicurezza dei dati trasmessi che quando si utilizza il web per un pagamento, ci si accerti che il browser utilizzi il protocollo HTTPS.



www.micertificoecdl.it

© Copyright AICA 2014 – 2019

HTTPS richiede che il server si autentichi nei confronti del client presentandogli il proprio certificato digitale in modo che il client possa controllare la validità della relativa firma digitale. Se supera questo controllo, il browser visualizza sulla propria interfaccia **l'icona di un lucchetto**.

La presenza di questo simbolo rientra tra gli elementi indispensabili a classificare una pagina come sicura.



APPROFONDIMENTO

Naturalmente l'utilizzo del protocollo HTTPS non risolve tutti i problemi della sicurezza e soprattutto non risolve i problemi di affidabilità del sito. Nelle attività di acquisto on line (e-commerce) è sempre possibile incorrere in piccole truffe, spesso legate alla mancata consegna della merce o alla ricezione di beni diversi da quelli ordinati. Se poi l'azienda si trova all'estero e non risponde alle mail di sollecito, le possibilità di ricorso o di recupero del denaro sono pressoché nulle. Che fare quindi? Utilizzare siti noti ed autorevoli è sicuramente un buon inizio. Utilizzare un motore di ricerca per trovare informazioni sull'azienda che si intende utilizzare e verificare la presenza di pareri di altri utilizzatori può essere un altro importante suggerimento.

37

Identificare le modalità con cui confermare l'autenticità di un sito web

Navigando in Internet c'è il rischio di imbattersi in minacce sempre nuove. I cyber criminali, infatti, stanno diventando sempre più abili nel porre in essere raggiri e truffe di ogni tipo. In particolar modo, un mezzo efficace per tentare di sottrarre preziosi dati personali è la "falsificazione" di pagine web ufficiali. Fortunatamente, esistono alcuni indizi rivelatori che possono farci evitare di cadere in qualche imbroglio.

Innanzitutto la qualità dei contenuti. Se già la pagina principale contiene errori di vario genere, oppure non è precisa nella spiegazione dei servizi o prodotti che offre, è meglio non fidarsi.

Un secondo indicatore è dato dalla presenza di numeri di telefono e indirizzi validi. Se non c'è alcun modo di contattare l'azienda senza l'uso di internet, potrebbe essere un'avvisaglia. Molto importante è anche il controllo dell'URL. Verificare che non ci siano numeri presenti o mancanti o che parte dell'indirizzo contenga una numerazione IP, o ancora, con suffisso diverso dall'atteso (ad esempio ".com" invece di ".it").

E' poi evidente che se il sito chiede dati personali e/o pagamento di somme di denaro, la connessione deve essere sicura e quindi il protocollo sia impostato a "https://" e deve essere presente l'icona del lucchetto con il quale verificare il certificato di sicurezza assegnato al sito.



APPROFONDIMENTO

Ulteriori tecniche d'indagine per determinare l'autenticità di un sito possono essere le seguenti:

- Cercare il nome della società con un motore di ricerca. Potrebbero saltar fuori recensioni o qualche informazione sul fatto che si tratti di una truffa.
- Controllare i dati di registrazione del sito web della società. A volte è possibile trovare il nome ed eventuali informazioni su chi ha registrato il sito web, che si consiglia di usare per ulteriori ricerche. È opportuno osservare, inoltre, quando è stato creato il sito e quando scade. Se è stato creato da poco e scadrà a breve, è possibile che si tratti di una copertura temporanea per mettere in atto qualche truffa. Un buon sito per far ciò è <http://whois.domaintools.com>.



Comprendere il termine pharming

Il **pharming** è una tecnica di cracking che ha finalità simili al phishing, ovvero indirizzare una vittima verso un server web "clone" appositamente attrezzato per carpire i dati personali della vittima. Si attua però mediante una tecnica più sofisticata in quanto fa sì che, digitando l'indirizzo di un sito web lecito, si venga diretti verso un altro sito web, identico a quello lecito ma falso.

Questa operazione si attua modificando opportunamente la traduzione dell'URL nel corrispondente indirizzo IP attuato dal DNS. Ad esempio, digitando **www.ferrari.com** questo viene convertito nel corrispondente indirizzo IP **2.18.240.184**.

38

La tecnica del pharming modifica il riferimento e fa sì che l'indirizzo alfanumerico corrisponda a un IP diverso: quello del sito clone.

L'utente non ha modo di accorgersi della differenza se non controllando nel certificato digitale della pagina che utilizza il protocollo HTTPS il **Percorso certificazione**.



APPROFONDIMENTO

I siti che intendono ingannare l'utente non possono utilizzare un certificato del sito che vogliono impersonare perché non hanno la possibilità di cifrare in modo valido il certificato, che include l'indirizzo, in modo tale che risulti valido alla destinazione. Solo le **Certification Authority** possono generare certificati validi con un'URL incorporata in modo che il confronto fra l'URL apparente e quella contenuta nel certificato possa fornire un metodo certo per l'identificazione del sito. Molto spesso questo meccanismo non è noto agli utenti di Internet ed è causa di varie frodi dovute ad un uso non corretto del browser e non ad una debolezza del protocollo HTTPS.

Comprendere la funzione e i tipi di software per il controllo del contenuto

Dato che è impossibile controllare cosa viene pubblicato su Internet, esistono software in grado di filtrarne i contenuti. In particolar modo, questi filtri vengono utilizzati a livello aziendale per evitare lo scaricamento illegale e le violazioni di copyright tipiche di file audio, video e programmi, o l'accesso alle reti sociali per evitare che i dipendenti perdano tempo in "chiacchierate senza fine".

L'applicazione di questi filtri raggiunge anche altri scopi; ad esempio, migliora la sicurezza riducendo la probabilità di prendere dei virus e migliora le prestazioni della rete evitando l'inutile consumo di banda.

A livello privato esiste un'altra importante categoria di filtri che va sotto il nome di "Controllo genitori" o "Parental control". Questo tipo di software consente di filtrare i contenuti e di programmare i tempi di accesso a Internet per i propri figli nonché di mantenere il log delle attività svolte per eventuale referenza.



www.micertificoeecd.it

© Copyright AICA 2014 – 2019

Capitolo 6 – Comunicazioni

Riferimento Syllabus 6.1.1	<i>Comprendere lo scopo di cifrare, decifrare un messaggio di posta elettronica.</i>
Riferimento Syllabus 6.1.2	<i>Comprendere il termine "firma digitale".</i>
Riferimento Syllabus 6.1.3	<i>Identificare i possibili messaggi fraudolenti o indesiderati.</i>
Riferimento Syllabus 6.1.4	<i>Identificare le più comuni caratteristiche del phishing, quali: uso del nome di aziende e di persone autentiche, collegamenti a falsi siti web, uso di loghi e marchi falsi, incoraggiamento a divulgare informazioni personali.</i>
Riferimento Syllabus 6.1.5	<i>Essere consapevoli che è possibile denunciare tentativi di phishing alle organizzazioni competenti o alle autorità preposte.</i>
Riferimento Syllabus 6.1.6	<i>Essere consapevoli del rischio di infettare un computer o un dispositivo con malware attraverso l'apertura di un allegato contenente una macro o un file eseguibile.</i>
Riferimento Syllabus 6.2.1	<i>Comprendere l'importanza di non divulgare su siti di reti sociali informazioni riservate o informazioni personali che permettono l'identificazione.</i>
Riferimento Syllabus 6.2.2	<i>Essere consapevoli della necessità di applicare e di rivedere con regolarità le impostazioni del proprio account su una rete sociale, quali riservatezza dell'account e propria posizione.</i>
Riferimento Syllabus 6.2.3	<i>Applicare le impostazioni degli account di reti sociali: riservatezza dell'account e propria posizione.</i>
Riferimento Syllabus 6.2.4	<i>Comprendere i pericoli potenziali connessi all'uso di siti di reti sociali, quali cyber bullismo, adescamento (grooming), divulgazione dolosa di informazioni personali, false identità, link o messaggi fraudolenti o malevoli.</i>
Riferimento Syllabus 6.2.5	<i>Essere consapevoli che è possibile denunciare usi o comportamenti inappropriati della rete sociale al fornitore del servizio o alle autorità preposte.</i>
Riferimento Syllabus 6.3.1	<i>Comprendere l'importanza di non divulgare su siti di reti sociali informazioni riservate o informazioni personali che permettono l'identificazione.</i>
Riferimento Syllabus 6.3.2	<i>Comprendere l'importanza di non divulgare su siti di reti sociali informazioni riservate o informazioni personali che permettono l'identificazione.</i>
Riferimento Syllabus 6.4.1	<i>Comprendere le possibili implicazioni dell'uso di applicazioni provenienti da "app store" non ufficiali, quali malware per dispositivi mobili, utilizzo non necessario delle risorse, accesso a dati personali, bassa qualità, costi nascosti.</i>
Riferimento Syllabus 6.4.2	<i>Comprendere il termine "autorizzazioni dell'applicazione".</i>
Riferimento Syllabus 6.4.3	<i>Essere consapevoli che le applicazioni mobili possono estrarre informazioni private dal dispositivo mobile, quali dettagli dei contatti, cronologia delle posizioni, immagini.</i>
Riferimento Syllabus 6.4.4	<i>Essere consapevoli delle misure precauzionali e di emergenza da adottare in caso di perdita di un</i>



dispositivo mobile, quali disattivazione remota, cancellazione remota dei contenuti, localizzazione del dispositivo.

Contenuti della lezione

Cifrare e decifrare un messaggio di posta elettronica; La "firma digitale"; Identificare possibili messaggi fraudolenti e indesiderati; Le caratteristiche più comuni del phishing; Essere consapevoli della possibilità di denunciare tentativi di phishing a organizzazioni legittime o alle autorità preposte; Rischio di infettare il computer o il dispositivo con malware attraverso l'apertura di un allegato contenente una macro o un file eseguibile; Importanza di non divulgare informazioni riservate o informazioni personali; Rivedere con regolarità le impostazioni del proprio account; Applicare le impostazioni degli account di reti sociali; I potenziali pericoli connessi all'uso di siti di reti sociali; Possibilità di denunciare usi o comportamenti inappropriati della rete sociale al fornitore del servizio o alle autorità preposte; Le vulnerabilità di sicurezza della messaggistica istantanea e del VoIP; I metodi per assicurare la confidenzialità durante l'uso della messaggistica istantanea e del VoIP; Le possibili implicazioni dell'uso di applicazioni provenienti da "app store" non ufficiali; Comprendere il termine "autorizzazioni dell'applicazione"; Essere consapevoli che le applicazioni mobili possono estrarre informazioni private dal dispositivo mobile; Misure precauzionali e di emergenza da adottare in caso di perdita di un dispositivo mobile.

40

Cifrare e decifrare un messaggio di posta elettronica

I messaggi di posta elettronica sono trasmessi in chiaro e quindi chiunque si trovi sul percorso compiuto dal messaggio può leggerlo senza che il destinatario se ne possa accorgere.

Volendo fare un paragone con la posta tradizionale, si potrebbe affermare che l'invio di un messaggio di posta elettronica può essere paragonato, più che a una lettera in busta chiusa, ad una cartolina postale.

Per rendere la comunicazione per mezzo di e-mail sicura e proteggere la propria privacy è pertanto necessario cifrare il messaggio in modo che solo il legittimo destinatario, in possesso di una chiave di decodifica, sia in grado di leggerlo.

La "firma digitale"

Oltre al problema della riservatezza, la posta elettronica presenta anche il problema dell'identificazione del mittente. E' molto facile creare un messaggio di posta e spedirlo facendolo risultare come se fosse stato spedito da qualcun altro.

La firma digitale sopperisce a questa carenza e permette di garantire l'identificazione del mittente.

Più in generale, si può affermare che la firma digitale si può applicare a qualsiasi documento in formato elettronico con tre benefici:

- o **integrità**. Il destinatario non può alterare un documento né crearne uno facendolo risultare firmato da qualcun altro.
- o **autenticità**. Il destinatario è sicuro dell'identità del mittente del documento.
- o **non ripudiabilità**. Il mittente non può negare di aver inviato il documento da lui firmato.



www.micertificoeCDL.it

© Copyright AICA 2014 – 2019

La firma digitale non è l'inserimento in un messaggio della scansione della propria firma, bensì una procedura di autenticazione capace di garantire che il contenuto di un documento informatico sia esattamente quello voluto dal suo autore e, soprattutto, che tale documento "provenga" proprio da quell'autore.

Con riferimento alla posta elettronica si può pertanto affermare che la firma digitale è un metodo per attestare che il messaggio ricevuto sia stato effettivamente inviato dal mittente e che il suo contenuto non sia stato alterato.



APPROFONDIMENTO

Il funzionamento della firma digitale è tutt'altro che complicato: si basa su una coppia di chiavi asimmetriche, capaci di codificare una firma. Le due chiavi hanno però due fondamentali caratteristiche:

- la coppia di chiavi è inscindibile (ad una chiave **A** corrisponde una e una sola chiave **B** e viceversa);
- se la chiave **A** è utilizzata per codificare, per la decodifica è necessaria la chiave **B** (da qui il termine "asimmetrico").

Delle due chiavi, inoltre, una deve essere resa **pubblica**, ovvero accessibile a chiunque.

Ciò significa che una volta sottoscritto un dato documento e codificato con la chiave **privata**, colui che ne venga in possesso potrà prelevare la chiave "pubblica" del "presunto" autore e con essa provare a decodificarlo, verificando così la reale paternità del documento stesso.

Nella pratica il meccanismo coinvolge l'utilizzo di una funzione di **Hash** per ricavare l'impronta digitale (digest) del documento (cioè una stringa di dimensioni contenute - circa 160 byte - indipendentemente dalla lunghezza del documento) ed è questo a essere cifrato e non il documento stesso. Il risultato di questa codifica è la **firma digitale**.

Si noti che la firma prodotta dipende dall'impronta digitale del documento e, quindi, dal documento stesso, oltre che dalla chiave privata dell'utente.

Per maggiori dettagli sulle **reali** procedure e modalità di firma digitale (e verifica della stessa) si consulti il documento **Linee guida per l'utilizzo della Firma Digitale** emesso dal CNIPA (Centro Nazionale per l'Informatica nella Pubblica Amministrazione) disponibile all'indirizzo https://ca.notariato.it/approfondimenti/LineeGuidaFD_200405181.pdf.

41

Identificare possibili messaggi fraudolenti e indesiderati

La rete internet è sede di un gigantesco scambio di informazioni, che può avvenire anche attraverso l'uso della posta elettronica.

Purtroppo, c'è sempre qualcuno che utilizza gli indirizzi di posta elettronica per inviare e-mail non richieste con il preciso intento di ricavarne un beneficio economico o carpire informazioni riservate.

Viene chiamata **junk-mail** (posta spazzatura) o anche **spam** tutta la posta indesiderata ricevuta indebitamente nella propria casella postale. In genere si tratta di messaggi pubblicitari che hanno lo scopo di indurre il destinatario ad acquistare qualcosa.

Talvolta però si tratta di messaggi fraudolenti che inducono i destinatari a fornire inconsapevolmente a chi li ha inviati dati riservati dei destinatari allo scopo di frodarli.

Quando si ricevono messaggi di questo tipo, la cosa da fare è cancellarli immediatamente, senza aprirli e soprattutto senza rispondere, per non confermare che l'indirizzo email è attivo.




 APPROFONDIMENTO

In genere i client di posta sono dotati di filtri anti spam locali e la posta riconosciuta come tale viene spostata tra la posta indesiderata ma deve essere comunque osservata per verificare che non sia stata spostata a torto. Si può quindi dire che i filtri anti spam non risolvono il problema della ricezione dello spam (al più lo attenuano) ma provvedono a riunire in un'unica cartella tutta la posta di quel tipo in modo che dopo un'analisi possa essere rapidamente cancellata.

Per quanto riguarda i messaggi fraudolenti, la validità o l'attendibilità del mittente può essere controllata (esempi per Gmail) come segue:

- Visualizzare l'intestazione dell'email per verificare la reale provenienza del messaggio selezionando dall'elenco dello strumento  **Rispondi** la voce **Mostra originale**. In un'intestazione tipica, vengono visualizzate diverse righe che iniziano per "Received" simili alla seguente **Received: from sitoweb [xxx.xxx.xxx.xxx]**. Dato che le informazioni sono riportate in ordine cronologico inverso, le informazioni sul mittente sono le ultime. Se le relative informazioni non corrispondono all'indirizzo email del mittente o dell'azienda presente nell'email, solitamente significa che il messaggio non proviene realmente da tale persona o azienda.
- Puntare il mouse sul nome presente nella colonna del mittente per visualizzare la scheda contatto. Comparando il nome presente nella scheda contatto con quello visualizzato, si potrà stabilire se l'email proviene da un dominio riconoscibile legato al nome effettivo del mittente.

In generale, tutti i messaggi fraudolenti contengono uno o più link con un invito a cliccarli per i motivi più vari. Prima di farlo è bene puntarli con il mouse e verificare che indirizzino dove affermano. Infatti, nella barra di stato del browser si può vedere l'URL reale e non quello scritto che può anche essere un semplice commento. Se gli URL non corrispondono o quello effettivo non proviene da un dominio o da un'azienda riconoscibile, è probabile che si tratti di un email fraudolenta.

42

Le caratteristiche più comuni del phishing

Come già appreso il phishing è una truffa on-line nata per sottrarre con l'inganno numeri di carte di credito, password, informazioni personali o di carattere finanziario. Attuata quasi sempre tramite posta elettronica si basa sull'invio da parte del truffatore di e-mail che sembrano provenire da siti web autentici i quali richiedono all'ingenuo utente l'inserimento dei propri dati personali.

Nel messaggio di phishing viene generalmente riportato il link a un sito web fasullo, ma identico nell'aspetto al sito legittimo. Nel tempo infatti, gli sciacalli del web hanno affinato le loro armi: grafica accattivante, loghi ufficiali di aziende e istituzioni, messaggi efficaci e scritti in buon italiano o in altre lingue, cortesia e semplicità possono fare pensare di non essere vittime di un raggio.

Per distinguere il sito fasullo da quello legittimo occorre controllare il dominio presente nella barra dell'indirizzo, che sarà diverso (seppur molto simile) da quello originale, salvo quando viene usata anche la tecnica del pharming.


 APPROFONDIMENTO

Per evitare di cadere nella rete del phisher attenersi alle seguenti linee guida:

- Non rispondere mai alle e-mail che chiedono dati personali; nessuna istituzione chiederà mai la conferma delle credenziali tramite email, in quanto è risaputo che si tratta di un mezzo non sicuro.
- Per accedere al sito dell'istituto di credito nel quale si detiene il conto online non cliccare mai un link ma digitare l'URL direttamente nella barra indirizzo del browser oppure attraverso i "preferiti".
- Verificare che la comunicazione avvenga in modo sicuro attraverso il protocollo HTTPS.



Essere consapevoli della possibilità di denunciare tentativi di phishing a organizzazioni legittime o alle autorità preposte

Nel dubbio di aver lasciato i propri dati personali su un sito contraffatto è sempre possibile contattare il servizio Clienti dell'organizzazione legittima o scrivere un'email agli indirizzi indicati nei loro siti web, specificando nel testo l'indirizzo del sito di Phishing e allegando il testo della mail ricevuta.

È altresì possibile segnalare online alla polizia postale i sospetti usi illeciti delle proprie informazioni personali all'indirizzo <http://www.commissariatodips.it>.

Rischio di infettare il computer o il dispositivo con malware attraverso l'apertura di un allegato contenente una macro o un file eseguibile

43

La maggior parte del malware in circolazione arriva nei computer all'interno degli allegati di posta elettronica.

Prima di aprire un allegato è bene essere certi che il mittente sia fidato, che lo abbia inviato volontariamente e, attraverso una scansione antivirus, che non sia infetto.



APPROFONDIMENTO

Gli allegati che contengono virus sono programmi o file eseguibili (i tipi di file: .com, .exe, .vbs, .zip, .scr, .dll, .pif, .js) o virus macro (i tipi di file: .doc, .docm, .pst, .dot, .xls, .xlt, ...). I file più pericolosi sono in generale i ".doc" perché considerati sicuri. Il modo più sicuro per proteggersi è quello di evitare l'attivazione automatica delle macro.

Importanza di non divulgare informazioni riservate o informazioni personali

Le reti sociali sono strumenti di comunicazione e condivisione molto diffusi sia tra i giovani che tra gli adulti. Spesso però il loro utilizzo è assai superficiale dimenticando che tutto ciò che viene messo su Internet diventa di pubblico dominio e di fatto se ne perde il controllo. Per questa ragione è importante non utilizzare questi strumenti per divulgare informazioni confidenziali, soprattutto di natura economico-finanziaria, o dati personali apparentemente innocui come l'assenza da casa.

Ma questo non è tutto. Anche la pubblicazione di immagini personali, come ad esempio le folle notturne di una festa, andrebbero valutate con attenzione, soprattutto se non si è avuto l'accortezza di limitare correttamente l'accesso a queste informazioni. Analogamente è importante porre attenzione a quello che si scrive evitando la divulgazione di idee e tendenze di carattere politico, religioso o sessuale.

Rivedere con regolarità le impostazioni del proprio account

La partecipazione a una rete sociale spesso fornisce l'impressione di essere all'interno di un circuito protetto e questo può spingere le persone a rivelare molte informazioni, anche private, su se stessi.

Per controllare la condivisione di informazioni tutti i siti web delle reti sociali offrono la possibilità di impostare il livello di privacy desiderato per il proprio profilo.



Sebbene in molti non curino questo aspetto, è importante essere consapevoli che questa possibilità esiste e che se non si interviene, in generale, il proprio profilo rimane di dominio pubblico.

Per un uso responsabile, l'accesso al proprio profilo dovrebbe essere concesso soltanto a persone che si conoscono anche nella vita reale rifuggendo dalle scelte generiche e men che meno da quelle tipo "amici degli amici".

Un altro elemento che ha un importante impatto con la privacy è la geo localizzazione resa possibile dalla presenza del GPS in cellulari e smartphone. Se da un lato la tecnologia mette nelle mani dei navigatori servizi sempre più innovativi online, dall'altro gli utenti non sono coinvolti pienamente nella comprensione di quanto le informazioni provenienti dai propri Gps possano minare la propria riservatezza.

44

Per questi motivi è bene rivedere periodicamente le impostazioni del proprio account e disattivare le funzionalità non più coerenti con il proprio stato corrente.



APPROFONDIMENTO

L'utente accetta la politica di privacy e le condizioni d'uso di una rete al momento della sua iscrizione. In genere, deve solo selezionare l'opzione "accetto" e, spesso, questo avviene senza leggerne le condizioni. Il rischio è quello di prestare il consenso all'utilizzo dei propri dati e dei documenti multimediali che mette sulla rete sociale senza sapere come saranno utilizzati. Per questa ragione è sempre importante leggere attentamente le condizioni d'uso e l'informativa sulla privacy presenti e poi agire di conseguenza.

Interessante a questo proposito è il vademecum rilasciato dal *Garante della privacy* il 23 maggio 2014 e intitolato "Social Privacy- Come tutelarsi nell'era dei social network" con l'obiettivo di aumentare la consapevolezza degli utenti e offrire loro ulteriori spunti di riflessione e strumenti di tutela.

Una ulteriore riflessione va posta nell'uso di social network specificamente orientati all'uso della geo localizzazione che consente ai propri utenti di interagire con gli esercizi commerciali fino ad ottenere omaggi e sconti. Il rovescio della medaglia è la perdita di privacy che si concretizza rendendo pubblica al propria posizione geografica. Se si considera poi che molti degli utenti dei social network ne fanno un utilizzo contemporaneo, non è remoto ipotizzare che si potrebbe veder pubblicata la propria posizione su un altro sito, per esempio su Facebook, e da lì a tutti gli amici e agli amici degli amici.

Applicare le impostazioni degli account di reti sociali

Il controllo delle impostazioni di privacy sulle reti sociali è molto diverso e variegato ma si riduce fondamentalmente a possedere il controllo su chi può vedere i contenuti personali e chi può contattarvi.

In **Facebook**, è possibile decidere chi può diventare nostro "amico" e bloccare le persone indesiderate. Su **Twitter**, chiunque può diventare un "follower" a meno che l'account sia impostato come privato.

Google+ tuttavia combina queste funzioni nelle cosiddette "cerchie": gruppi di persone a cui assegnare permessi.

Molti di questi permessi sono attribuibili nella finestra "**Profilo**" e comprendono anche la gestione delle impostazioni della posizione.

Altre impostazioni sono controllabili e modificabili nella finestra delle impostazioni dell'account, raggiungibili cliccando la propria immagine e selezionando il collegamento "Account".



I potenziali pericoli connessi all'uso di siti di reti sociali

Utilizzando le reti sociali si può diventare vittima di diversi tipi di attacchi quali:

- il **cyberbullismo** che consiste nell'utilizzo di Internet per intimorire, molestare, mettere in imbarazzo, far sentire a disagio o escludere altre persone;
- l'**adescamento** che consiste nel tentativo di acquisire la fiducia di un minore, per scopi sessuali o comportamenti inappropriati;
- la **divulgazione dolosa di informazioni personali** ovvero la possibilità che le informazioni vengano utilizzate a fini diversi da quelli previsti inizialmente e che se divulgate al di fuori del gruppo previsto possano arrecare grave pregiudizio alla persona interessata;
- le **false identità**, o "fake", che consistono nel creare falsi profili sovente a scopo di adescamento o cyberbullismo;
- i **link o messaggi fraudolenti**, meglio conosciuti come "phishing", che hanno lo scopo di carpire informazioni basandosi sull'ingegneria sociale.

45

Possibilità di denunciare usi o comportamenti inappropriati della rete sociale al fornitore del servizio o alle autorità preposte

Ogni rete sociale impone specifiche regole d'uso dei contenuti pubblicabili. Alcuni social dettagliano esattamente quello che è vietato, altri sono molto più generici e tolleranti, ma in generale tutti offrono la possibilità di segnalare contenuti inappropriati che possono portare alla rimozione di quel contenuto, al blocco, o persino alla disabilitazione dell'account nei casi più gravi.

Oltre a questo, e come già visto per il caso del phishing, è sempre e comunque possibile rivolgersi alla polizia postale quando si ritiene di essere vittima di un reato o di abusi di qualsiasi genere.



APPROFONDIMENTO

In generale, ogni membro di una rete sociale ha la possibilità di bloccare o come si dice in gergo "bannare", un utente per una qualsiasi ragione impedendogli di commentare, postare o contattare il membro stesso. Questa possibilità, se sfruttata, contribuisce a mitigare i possibili eccessi e i comportamenti inappropriati di alcuni internauti.

Le vulnerabilità di sicurezza della messaggistica istantanea e del VoIP

Come la posta elettronica, anche la messaggistica istantanea comporta il rischio di ricevere sul proprio computer dei malware che possono comprometterne la sicurezza. Il malware può venire dall'apertura di file allegati ad un messaggio istantaneo o al clic su un link che porta ad un sito infetto.

Alcuni tipi di malware possono essere particolarmente pericolosi per la privacy, installando accessi nascosti al computer e spiando quanto viene digitato.

Inoltre, come tutti i software, anche quelli di messaggistica istantanea possono avere delle vulnerabilità che malintenzionati possono sfruttare per accedere illegalmente al computer. Anche le linee VoIP, in quanto sistemi basati su Internet, sono soggette agli stessi tipi di attacchi delle connessioni Web e, in particolare, alle intercettazioni.

Infatti, dato che la peculiarità del VoIP, è il trasporto della voce sotto forma di dati attraverso il protocollo IP, un'intrusione può avvenire intercettando i pacchetti e trasformandoli in file wav o mp3. Inoltre, all'insaputa degli interessati, un malintenzionato può attivare i microfoni dei telefoni o dei PC connessi alla rete VoIP ed intercettare qualsiasi conversazione avvenga intorno agli apparecchi colpiti.





APPROFONDIMENTO

L'utilizzo delle tecnologie VoIP espone l'utilizzatore alle seguenti potenziali vulnerabilità:

- **Spam.** Il VoIP è soggetto a un tipo specifico di pubblicità non richiesta, nota con l'acronimo **SPIT** (Spam over Internet Telephony).
- **Interruzioni.** Attacchi di rete da parte di worm e virus possono causare interferenze al servizio VoIP o arrivare a disattivarlo.
- **Phishing vocale.** Noto anche come "**vishing**", avviene quando un aggressore ci contatta tramite VoIP e cerca di indurci a divulgare dati personali importanti, come il numero di carta di credito o informazioni sul conto corrente bancario.
- **Perdita della privacy.** La maggior parte del traffico VoIP non è crittografato, per cui è facile che un intruso possa intercettare le conversazioni.
- **Hacking.** Gli hacker possono ottenere accesso alla propria connessione VoIP e usare la linea per effettuare chiamate. In alcuni casi, possono arrivare a vendere le informazioni relative alla connessione sul mercato nero. Una volta introdotti nella rete domestica, gli hacker possono individuare informazioni sensibili memorizzate sul PC.

Oltre alle vulnerabilità citate, non va dimenticato che l'utilizzo del VoIP è dipendente dalla rete e dall'alimentazione elettrica. Se il servizio Internet o l'elettricità subiscono un'interruzione, non è possibile telefonare e questo può rappresentare un pericolo in situazioni di emergenza.

46

I metodi per assicurare la confidenzialità durante l'uso della messaggistica istantanea e del VoIP

Le modalità per assicurare confidenzialità alla posta elettronica sono integralmente applicabili anche per la messaggistica istantanea e al VoIP. L'applicazione di sistemi crittografici alle comunicazioni resta infatti il sistema migliore.

Naturalmente anche i comportamenti utente giocano un ruolo prezioso. La crittografia potrà anche impedire che malintenzionati spiino i nostri messaggi ma non potrà impedire la comunicazione di dati personali o l'invio di file sensibili a persone non affidabili.

E' fondamentale infatti che chi utilizza Internet acquisisca una sensibilità alla protezione dei propri dati e alla non divulgazione delle informazioni personali.

Le possibili implicazioni dell'uso di applicazioni provenienti da "app store" non ufficiali

Si è già detto che i principali sistemi operativi per device mobili consentono di scaricare nuove app solo dal proprio Store a meno di non attuare pratiche quali il Jailbreak nei sistemi Apple e il Rooting per quelli Android.

Benché app non ufficiali potrebbero essere perfettamente sicure, in generale, il loro uso espone l'utilizzatore a rischi potenziali di malware, quale furto di credenziali d'accesso e di dati. Inoltre si possono incontrare applicazioni di bassa qualità che hanno poca attenzione al consumo di risorse e che quindi scaricano più velocemente la batteria.

Un ulteriore pericolo, riportato più volte anche in Commissione europea, è quello dei costi nascosti delle app dichiarate come gratuite ma con contenuti a pagamento. Questi costi chiamati "**in-app**" sono più facilmente presenti nelle app non ufficiali ma sfortunatamente anche in quelle disponibili negli store di Apple e Google.



www.micertificoecdi.it

© Copyright AICA 2014 – 2019

Comprendere il termine “autorizzazioni dell’applicazione”

Ogni app che viene installata, per poter funzionare richiede delle autorizzazioni: una sorta di badge nel quale sono indicate quali risorse del dispositivo potrà utilizzare.

La visualizzazione di queste richieste prima dell’installazione ha lo scopo di impedire la diffusione di app dannose in quanto le app necessitano di queste autorizzazioni per poter eseguire quello per cui sono state create.



APPROFONDIMENTO

Per semplificare e velocizzare la decisione dell’utente in merito alle autorizzazioni richieste da ogni app, **Google Play** (lo Store per i sistemi Android) ha introdotto il concetto dei “gruppi di autorizzazioni” visibili ancor prima di scaricare l’app. L’elenco dei gruppi di autorizzazioni previsto da Google Play (al momento della redazione di questo documento) è il seguente:

- Acquisti in-app
- Impostazioni dati cellulare
- Identità
- Contatti
- Posizione
- SMS
- Telefono
- Foto/elementi multimediali/file
- Fotocamera/microfono
- Informazioni sulla connessione Wi-Fi
- Informazioni sulla connessione Bluetooth
- Dati attività e sensori indossabili
- ID dispositivo e informazioni sulle chiamate
- Altro

Nello Store, è altresì possibile vedere tutte le singole autorizzazioni richieste esaminando la pagina dei dettagli dell’app.

Dopo l’installazione su un dispositivo Android è possibile verificare le autorizzazioni di cui dispone un’app aprendo **Impostazioni > Gestione applicazioni > app**.

47

Essere consapevoli che le applicazioni mobili possono estrarre informazioni private dal dispositivo mobile

L’elenco delle autorizzazioni richieste dalle app è molto variegato e comprende termini di non chiara e immediata comprensione. Ad esempio, l’autorizzazione “*Lettura dello stato e dell’identità del telefono*” può essere assolutamente normale. L’app chiede di controllare lo stato per interrompersi in caso di chiamata in arrivo. Peccato però che questa stessa autorizzazione fornisca l’accesso agli ID univoci del telefono (codici IMEI e IMSI) che molti sviluppatori usano per proteggere le proprie app dalla pirateria, ma che potrebbero essere utilizzati da un malintenzionato per tracciare o localizzare lo smartphone.

In buona sostanza è bene sapere che le app possono accedere a molte informazioni di carattere personale quali: contatti, cronologia di navigazione, segnalibri, localizzazione GPS, foto e video.

È quindi opportuno verificare se l’applicazione che si sta utilizzando utilizza autorizzazioni coerenti con il proprio scopo, oppure no, e quindi regolarsi di conseguenza.




APPROFONDIMENTO

Cosa sono i codici IMEI ed IMSI?

IMEI (acronimo di International Mobile Equipment Identity) è un codice numerico che identifica univocamente il terminale mobile ed è salvato nella memoria non volatile del cellulare (NVRAM).

IMSI è la sigla di International Mobile Subscriber Identity cioè rappresenta l'identità internazionale di utente di telefonia mobile. Si tratta di un numero univoco memorizzato nella SIM che identifica una coppia SIM-operatore telefonico, ossia la SIM all'interno di una rete GSM di un certo operatore.

Quali sono le autorizzazioni a cui prestare maggiore attenzione?

TIPO	DESCRIZIONE
Chiamata diretta numero telefonico	Necessaria con Skype, Facebook Messenger e similari, ma sospetta in altre applicazioni che possono utilizzare questa autorizzazione per comporre numeri a pagamento (solitamente ad alto costo) all'insaputa dell'utilizzatore.
Invio SMS	Un utilizzo fraudolento potrebbe attivare un abbonamento indesiderato.
Modifica/eliminazione dei contenuti dell'archivio USB/SD	Questa è una autorizzazione molto chiara. L'accesso alla scheda di memoria implica la possibilità di accedere anche alle immagini che possono essere così catturate e trasferite via Internet.
Lettura/Scrittura dati di contatto	Con questa autorizzazione un'app può sfogliare e modificare i contatti. Per le applicazioni di messaggistica e i social network questa app è necessaria, ma è bene prestare attenzione qualora questa autorizzazione venga richiesta da app di natura diversa.
Lettura stato e identità del telefono	Di questa autorizzazione si è già parlato più sopra ma si può ancora aggiungere che consente anche di determinare il numero del telefono e il numero a cui è collegata la chiamata in corso.
Acquisizione di foto e video	Un'app con questa autorizzazione potrebbe scattare foto autonomamente ma per trasmetterla su Internet avrebbe bisogno di altri permessi come elencato più sopra.

Misure precauzionali e di emergenza da adottare in caso di perdita di un dispositivo mobile

Gli smartphone per molte persone sono diventati i compagni indispensabili della propria vita; e non solo lavorativa, ma anche privata!

Per quanto riguarda la possibile perdita o furto del dispositivo è doveroso conoscere quali precauzioni adottare. Innanzi tutto è bene segnarsi, e conservare in un luogo sicuro, le informazioni fondamentali del telefono, quali: numero telefonico, marca e modello, colore, codice di sicurezza/pin e soprattutto l'IMEI. Queste informazioni saranno utili sia per la denuncia di furto o smarrimento, sia per le attività con l'operatore di rete. In secondo luogo è bene attivare sul dispositivo un software con funzione di antifurto in modo da potersi collegare in remoto per localizzarlo, bloccarlo e cancellarne i contenuti.



Adottando queste precauzioni minime, in caso di furto o smarrimento, si disporrà dei dati per sporgere denuncia alle autorità di Polizia e si potrà contattare il proprio operatore telefonico per procedere al blocco delle chiamate. Si rammenta che tale blocco è possibile solo mediante il codice IMEI che l'operatore inserirà in una black list comune a tutti gli operatori nazionali.

Per quanto attiene alla gestione remota questo varia in funzione del sistema operativo e in alcuni casi anche del modello.



Capitolo 7 – Gestione sicura dei dati

Riferimento Syllabus 7.1.1	<i>Riconoscere i modi per assicurare la sicurezza fisica di computer e dispositivi mobili, quali non lasciarli incustoditi, registrare la collocazione e i dettagli degli apparati, usare cavi antifurto, controllare gli accessi alle sale dei computer.</i>
Riferimento Syllabus 7.1.2	<i>Riconoscere l'importanza di avere una procedura di copie di sicurezza per ovviare alla perdita di dati da computer e da dispositivi mobili.</i>
Riferimento Syllabus 7.1.3	<i>Identificare le caratteristiche di una procedura di copie di sicurezza, quali regolarità/frequenza, pianificazione, collocazione del supporto dei dati salvati, compressione dei dati.</i>
Riferimento Syllabus 7.1.4	<i>Effettuare la copia di sicurezza di dati su un supporto quale: unità disco/dispositivo locale, unità esterna, servizio su cloud.</i>
Riferimento Syllabus 7.1.5	<i>Ripristinare i dati da una copia di sicurezza su unità disco/dispositivo locale, unità esterna, servizio su cloud.</i>
Riferimento Syllabus 7.2.1	<i>Distinguere tra cancellare i dati ed eliminarli in modo permanente.</i>
Riferimento Syllabus 7.2.2	<i>Comprendere i motivi per eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi mobili.</i>
Riferimento Syllabus 7.2.3	<i>Essere consapevoli che l'eliminazione del contenuto dai servizi potrebbe non essere permanente, come nel caso dei siti di reti sociali, blog, forum su internet, servizi su cloud.</i>
Riferimento Syllabus 7.2.4	<i>Identificare i metodi più comuni per distruggere i dati in modo permanente, quali uso di trita documenti, distruzione di memorie di massa/dispositivi, smagnetizzazione, uso di software per la cancellazione definitiva dei dati.</i>
Contenuti della lezione	I più comuni modi per assicurare la sicurezza fisica di computer e dispositivi mobili; Effettuare copie di sicurezza per ovviare alla perdita di dati da computer e dispositivi mobili; Le caratteristiche di una procedura di copie di sicurezza; Effettuare la copia di sicurezza di dati su un supporto quale unità disco/dispositivo locale, unità esterna, servizio su cloud; Ripristinare i dati da una copia di sicurezza su unità disco/dispositivo locale, unità esterna, servizio su cloud; Distinguere tra cancellare i dati ed eliminarli in modo permanente; Comprendere i motivi per eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi mobili; Essere consapevoli che l'eliminazione del contenuto dai servizi potrebbe non essere permanente; Identificare i metodi più comuni per distruggere i dati in modo permanente.

51

I più comuni modi per assicurare la sicurezza fisica di computer e dispositivi mobili

Nella gestione della sicurezza informatica non c'è solo la crittografia dei dati e le password di accesso. Anche la sicurezza fisica gioca un ruolo importante. Avere accesso fisico ad un dispositivo rende più facile per un malintenzionato estrarre o corrompere le informazioni.



Utilizzare un **controllo accessi elettronico** permette la gestione di molti utenti e consente di rilevare orari e punti di accesso del personale che lo utilizza in modo da poter più facilmente risalire all'autore di eventuali furti.

È però evidente che il controllo accessi non è che una delle prime linee di difesa. Per prevenire i furti è necessario che i singoli apparati siano messi in sicurezza, specialmente se questi sono facili da trasportare come notebook o tablet.

Un metodo di protezione molto diffuso, soprattutto nei luoghi aperti al pubblico, è dato dall'utilizzo dei **cavi di sicurezza** (Kensington o similari) che fissano il dispositivo alla scrivania con cavo e lucchetto.

52

Come ulteriore misura è opportuno **catalogare i dispositivi** registrandone dettagli e collocazione in modo da poter verificare in modo preciso eventuali mancanze.

Effettuare copie di sicurezza per ovviare alla perdita di dati da computer e dispositivi mobili

A nessuno piacerebbe che le proprie fotografie accumulate negli anni, i documenti, le pubblicazioni o i propri dati finanziari, si perdano nel nulla a causa di problemi tecnici o di un computer che si rompe. Non va poi dimenticata la possibilità per i dispositivi portatili come smartphone o tablet di essere smarriti o rubati.

Per tutte queste ragioni è importante fare delle copie di sicurezza dei file più importanti o anche dell'intero sistema in modo da poter ricostruire i propri archivi nel caso vadano persi..



APPROFONDIMENTO

Le copie di sicurezza dei dati sono spesso chiamate con il termine inglese "**backup**". Questo termine è anche utilizzato per definire sia le procedure che lo realizzano sia gli speciali programmi che lo implementano. La procedura opposta al backup è detta "**Restore**".

La copia dell'intero sistema invece è chiamata "**immagine del sistema**" e va registrata in altra partizione del disco, o meglio ancora, in un hard disk esterno.

Le caratteristiche di una procedura di copie di sicurezza

Appare evidente a tutti che fare una copia di sicurezza dei dati "una tantum" non è di grande utilità. Una backup è davvero utile se è recente.

È quindi fondamentale impostare la procedura di copia in modo che questa avvenga automaticamente a scadenze regolari e possibilmente in un momento in cui il computer rimane acceso ma non utilizzato, per evitare che la copia dei dati rallenti il lavoro.

La frequenza delle backup è un altro parametro importante. In base alla quantità di dati movimentati ogni giorno si può stabilire se eseguire l'attività su base giornaliera, settimanale o mensile.

Da ultimo è opportuno riflettere sulla collocazione delle copie di sicurezza. Conservarle assieme al dispositivo le espone agli stessi rischi, specie nel caso di eventi quali fuoco o acqua. Perciò è bene riporle in un luogo diverso, magari sfruttando le possibilità offerte oggi dal cloud.





APPROFONDIMENTO

Benché la discesa del costo delle memorie di massa, unito al contestuale incremento di capacità, abbia messo in secondo piano l'esigenza di ridurre i volumi delle backup, una caratteristica comune a tutti i prodotti che la realizzano è la compressione dei dati. Questa caratteristica si dimostra di particolare utilità nella riduzione del traffico di dati necessario a trasferire i dati da preservare, specialmente se attuata sul cloud.

Non meno importante, come ulteriore tecnica per ridurre il volume dei dati e contestualmente aumentare la velocità della backup, è quella di attuare una selezione degli elementi da copiare; non in termini di dischi, cartelle o file, ma scegliendo una delle seguenti tipologie di backup:

- **Backup Incrementale** - backup che contiene tutti i file aggiunti o cambiati dall'ultimo backup (completo o incrementale). È più rapido di quello differenziale ma richiede tempi di Restore più lunghi poiché è necessario partire dall'ultimo backup completo e poi aggiungere in sequenza tutti i backup incrementali.
- **Backup Differenziale** - backup cumulativo di tutti i cambiamenti effettuati a partire dall'ultimo backup completo. È meno veloce rispetto all'incrementale ma impiega meno tempo per il ripristino dei dati, poiché basterà utilizzare l'ultimo backup completo più il differenziale.

53

Effettuare la copia di sicurezza di dati su un supporto quale unità disco/dispositivo locale, unità esterna, servizio su cloud

In Windows 7 per eseguire delle copie di sicurezza, sia manualmente che sulla base di una pianificazione, si può utilizzare l'utilità **Backup e ripristino** del *Pannello di controllo*.

Al primo utilizzo è necessario configurare il backup selezionando il percorso in cui si desidera salvare la copia. Tale percorso può essere in un disco esterno, in una rete o anche su un supporto removibile. Scegliendo ad esempio un percorso di rete si dovrà scegliere la cartella di destinazione e le credenziali d'accesso.

A seguire la procedura di configurazione chiederà di specificare gli elementi che si desiderano salvare, con un default che comprende l'immagine dell'intero sistema.

Specificando una selezione manuale si potrà accedere alla finestra di selezione degli elementi desiderati. Avanzando nella procedura, si potrà accettare la pianificazione dell'attività suggerita da Windows, cioè ogni domenica alle ore 19, o modificarla a piacere.

A questo punto, si prosegue salvando le impostazioni e avviando il backup. Durante l'attività è mostrata una barra che si incrementa fino a completamento.



APPROFONDIMENTO

Dopo la configurazione iniziale verrà eseguito un backup dei dati selezionati con la frequenza impostata, ma sarà sempre possibile aprire **Backup e ripristino** ed eseguire una backup manuale premendo il pulsante **Esegui Backup**.

Per modificare qualsiasi impostazione del backup selezionare invece il link **Cambia impostazioni** e ripercorrere la procedura di configurazione cambiando gli elementi desiderati.

Per salvare su cloud i propri dati la soluzione Microsoft si chiama **OneDrive**. Si tratta di uno spazio di archiviazione (gratis i primi 15 GB) che può essere sincronizzato automaticamente con i contenuti desiderati del PC. Il sistema in realtà non è pensato per le sole procedure di backup così come sono state esposte ma per avere una copia online unica o sincronizzata di cartelle e file. Installando il servizio "OneDrive" in Windows 7 si potrà visualizzare l'omonima cartella in Esplora risorse e quindi si potrà salvare sul cloud qualsiasi file semplicemente trascinandolo in questa cartella. Naturalmente OneDrive risulta visibile anche come percorso di salvataggio della procedura *Backup e ripristino* e pertanto il file di backup potrà essere salvato anche su cloud.



Ripristinare i dati da una copia di sicurezza su unità disco/dispositivo locale, unità esterna, servizio su cloud

In caso di perdita, danneggiamento o modifica accidentale di file importanti sottoposti a backup è possibile ripristinare uno o più file dalla copia più recente disponibile. Anche questa attività viene svolta dall'utilità **Backup e ripristino**.

Si parte premendo il pulsante **Ripristina file personali** oppure attivando il link **Ripristina i file di tutti gli utenti** a seconda che il backup sia stato fatto per la propria user o per un'altra.

Si prosegue cercando il file o la cartella da ripristinare. Ad esempio, volendo ripristinare un file eliminato per errore, si seleziona **Cerca file** e quindi si digita tutto o parte del suo nome.

Premendo **Cerca** Windows scorrerà l'ultimo backup e individuerà uno o più file. A questo punto basta selezionare quello desiderato e premere **OK** per tornare alla prima finestra ma questa volta con il nome del file nel riquadro di ripristino.

Premendo **Avanti** sarà possibile specificare il punto di ripristino con un default previsto nella sua posizione originale.

La premuta del pulsante **Ripristina** conclude la procedura anche se poi sarà necessario premere **Fine** per chiudere l'ultima finestra di dialogo.

Distinguere tra cancellare i dati ed eliminarli in modo permanente

Forse non tutti sanno che quando si cancella un file sul computer nella maniera standard, ossia usando il **Cestino** del desktop, Windows non lo distrugge in modo permanente ma segnala al file system che lo spazio occupato da quel file è disponibile per essere scritto da qualcos'altro.

Praticamente esso sparisce visivamente dal computer, ma rimane presente nel disco fino a che i dati che lo formano non vengono sostituiti da quelli di un altro file nuovo.

Per un certo periodo di tempo, quindi, è possibile recuperare i dati cancellati usando un programma di recupero file.

Per rendere irrecuperabile un dato e cancellarlo completamente, bisogna sovrascriverlo più volte prima della sua eliminazione utilizzando un programma specifico.



APPROFONDIMENTO

Nemmeno formattando il pc si cancellano i file perché tale operazione serve solo a rendere invisibili i file al sistema, a meno di non formattare il disco a basso livello con apposite utility fornite dal produttore del disco stesso.

Comprendere i motivi per eliminare in modo permanente i dati dalle memorie di massa o dai dispositivi mobili

Sui dischi del proprio computer e sui dispositivi di memorizzazione esterna viene salvato di tutto: foto, documenti lavorativi, file personali, ecc.

Quando si decide di cancellare file "sensibili" per motivi di sicurezza o di privacy, si desidera avere la certezza che il loro contenuto non possa essere recuperato.



A maggior ragione quando si presta, si cede o si vende un computer è importante sapere che i propri dati privati non siano in alcun modo ripristinabili.



APPROFONDIMENTO

Per conservare la propria sicurezza e privacy è opportuno che vengano cancellati in modo sicuro i propri dati anche quando si rottama il computer o il dispositivo di memorizzazione. In questi casi, non essendoci il problema del loro riutilizzo, si può anche pensare di distruggerli fisicamente.

Essere consapevoli che l'eliminazione del contenuto dai servizi potrebbe non essere permanente

55

Si è visto in precedenza come la cancellazione dei dati eseguita nei sistemi operativi locali non sia mai definitiva se non adottando speciali procedure.

A maggior ragione questo è vero negli ambienti cloud dove non si possiede il controllo diretto degli stessi e dove la cancellazione in linea, anche se attuata, non esclude la permanenza su copie di backup al di fuori del proprio controllo.

Ancora peggio, nei siti di reti sociali, laddove si siano condivisi dati con altri utenti.

La cancellazione dei dati dal proprio profilo non esclude che ne persistano copie negli archivi di questi utenti.

Discorso del tutto analogo si applica ai siti di blog e forum.

Identificare i metodi più comuni per distruggere i dati in modo permanente

Per distruggere i dati in modo permanente si possono utilizzare diverse tecniche:

- Per i documenti cartacei e per le memorie ottiche è opportuno utilizzare dei trita documenti, che tagliano a striscioline non solo la carta ma anche i CD/DVD.
- Per le memorie magnetiche si possono utilizzare speciali apparecchi conosciuti come “degausser” in grado di smagnetizzare completamente il disco in soli 4 secondi.

Per cancellare in modo permanente i dati senza distruggere il disco bisogna invece utilizzare appositi programmi che riscrivono le aree del file più volte utilizzando dati variabili e poi rilasciano il file che a questo punto contiene solo bit senza significato. Alcuni di questi programmi consentono anche di cancellare in modo sicuro lo spazio disco considerato libero.



