La sicurezza informatica dei PC domestici

Parte 1 - Quali sono i rischi

Note e avvertenze

Lo scopo di questa documento è quello di presentare a un pubblico di non specialisti i problemi della sicurezza informatica dei computer di casa e i possibili modi per affrontarli e risolverli. In questa prima parte del documento viene esaminata la problematica relativa all'analisi dei rischi.

Dove possibile sono stati indicati ulteriori riferimenti (in rosso) per gli approfondimenti, con collegamenti diretto a documenti presenti su Internet e cercando di sceglierli di preferenza in lingua italiana.

L'ACSI non si assume nessuna responsabilità per eventuali danni derivanti da prodotti o da indicazioni citati nella sezione.

Realizzazione

Testo a cura di Silvano Marioni,

Prima pubblicazione sul sito ACSI: Ottobre 2004
Revisione e adattamento in formato Acrobat/pdf: settembre 2009

I rischi dell'informatica domestica

Perché proteggersi dai pericoli del mondo virtuale?

Nella vita quotidiana ci è chiaro come proteggere i nostri beni: sappiamo quali sono le cose che ci appartengono, quale è il loro valore e di conseguenza chiudiamo porte e finestre quando usciamo di casa e teniamo sotto chiave i nostri beni più preziosi.

Non si può dire la stessa cosa per i beni informatici. Ci rendiamo conto del costo del computer e dei programmi per il prezzo che abbiamo pagato, ma difficilmente siamo in grado di dare un valore alle informazioni che abbiamo memorizzate e al lavoro che abbiamo svolto per raccoglierle o per istallare e configurare i programmi.

Ci è chiaro che cosa sia la sicurezza nel modo reale ma non abbiamo la giusta percezione della sicurezza nel mondo virtuale dell'informatica.

Questo documento vuole informare sui pericoli a cui va incontro il nostro computer di casa e sulle possibili soluzioni per proteggersi. Tutto questo per evitare di essere coinvolti in un Denial of Service distribuito o essere vittime del Social Engineering, del phishing, ma anche per capire che il Cybercrime non esiste solo nei film e la password non è unicamente una fastidiosa parola da ricordare.

Gli obiettivi di questo documento possono essere riassunti nei seguenti punti:

- Identificare i beni informatici da proteggere evidenziando il loro valore.
- Descrivere le possibili minacce di tipo tecnico che potrebbero danneggiare i nostri dati e le situazioni che potrebbero nascondere delle attività fraudolente.
- Presentare i comportamenti più adatti per evitare di cadere in truffe o raggiri e gli strumenti tecnici per proteggerci dai possibili attacchi.
- Far capire che i rischi nel mondo virtuale dell'informatica e di Internet possono essere evitati e che tutti sono in grado di proteggersi usando un minimo di precauzioni.

Sicurezza informatica a casa nostra

Perché dobbiamo preoccuparci della sicurezza informatica?

Così come le precauzioni quotidiane di sicurezza ci proteggono nel mondo reale, la sicurezza informatica ci deve garantire la disponibilità, il controllo e la proprietà esclusiva dei nostri beni e delle nostre risorse informatiche, siano esse apparecchiature, programmi o informazioni.

Questo non vale solo nel caso di attacchi da parte di hackers nei collegamenti a Internet, ma anche in tutti gli altri casi dove guasti, negligenze (anche da parte nostra) o danni causati dalla natura possono minacciare l'integrità dei nostri beni informatici.

I requisiti fondamentali per una corretta sicurezza informatica sono:

- La possibilità di accedere alle risorse informatiche quando è necessario e solo per le persone autorizzate. Nessuna persona o situazione deve impedirci di usare i nostri programmi e di consultare i dati a cui abbiamo diritto di accesso nel momento in cui ne abbiamo bisogno.
- La garanzia che i nostri computer, programmi, e informazioni non siano soggetti a cambiamenti non autorizzati, siano essi intenzionali o accidentali. Dobbiamo avere sempre la certezza che quello che stiamo facendo è veramente quello che pensiamo di fare.
- Il diritto di avere le proprie informazioni protette dalla consultazione da parte di persone non autorizzate. Questo è importante non solo per evitare di essere coinvolto

in truffe e malversazioni a nostro danno ma anche per esercitare il diritto che ogni individuo ha sulla riservatezza dei propri dati personali.

Questi requisiti sono alla base di qualsiasi progetto di sicurezza informatico sia che si tratti di proteggere una rete informatica di un azienda o il computer di casa. Attraverso le considerazioni e le soluzioni che esamineremo di seguito cercheremo di capire perché e come è possibile mettersi al sicuro dai rischi informatici.

Responsabilità pubbliche e private

Verso una cultura della sicurezza

Sono finiti i tempi in cui il computer era utilizzato poco più che come un giocattolo. Oggi con i PC facciamo attività importanti che possono andare dagli acquisti tramite commercio elettronico alle transazioni bancarie, dalla dichiarazione dei redditi all'interazione con le amministrazioni pubbliche e tra non molto potremmo dare il nostro voto al politico preferito con un semplice clic.

Il tema della sicurezza informatica sta diventando sempre più importante non solo per i problemi che possiamo avere personalmente quando il nostro computer è attaccato da un virus ma soprattutto perché oggi la società dipende sempre di più dai sistemi informatici. Internet è oggi il supporto per strutture vitali quali l'energia, i trasporti, le attività finanziarie, l'e-government, la salute e le terapie, i servizi ai cittadini, ecc. con nuove problematiche che vanno oltre il semplice funzionamento di tutti questi sistemi e che includono argomenti fondamentali che vanno dalla protezione della nostra sfera privata fino alla garanzia di un funzionamento corretto dei processi democratici.

Per questa ragione i governi si stanno preoccupando dei rischi delle nuove tecnologie informatiche nell'economia, nelle pubbliche amministrazioni ma anche nelle famiglie, con particolare attenzione alla sicurezza informatica. Perfino l'OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico) ha emanato delle Linee guida sulla sicurezza dei sistemi e delle reti di informazione auspicando "una cultura della sicurezza".

Anche la protezione dei consumatori, di conseguenza, non può tralasciare gli aspetti di sicurezza delle tecnologie informatiche ed è per questo che l'ACSI mette a disposizione dei consumatori questo documento per accrescere la capacità di destreggiarsi tra le insidie della "rete".

Riferimenti:

Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti d'informazione
http://www.oecd.org/dataoecd/16/23/15582268.pdf

MELANI - La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione della Confederazione Svizzera
http://www.melani.admin.ch/index.html?lang=it

Incaricato Federale alla Protezione dei Dati - Protezione del proprio computer
http://www.edoeb.admin.ch/themen/00794/00928/00930/index.html?lang=it

Perché mai dovrebbe succedere a me?

Quali sono i rischi della "rete"

Diversamente dai computer delle aziende, i computer domestici non sono generalmente molto sicuri e sono perciò più vulnerabili alle aggressioni di un intruso. In particolare i collegamenti permanentemente ad Internet (ADSL o cable modem) danno ad un intruso tutto il tempo per scoprire i punti deboli del computer che, se viene compromesso, può essere controllato e utilizzato all'insaputa del proprietario, rivelando tra l'altro tutti i dati memorizzati.

Se una volta i virus erano creati per farsi notare (famoso quello che faceva cadere le lettere dello schermo) oggi il loro scopo è cambiato e i programmi più subdoli agiscono in silenzio catturando informazioni o preparando ulteriori raffinati attacchi.

Purtroppo se un malintenzionato fosse in grado di istallare sul nostro computer un virus o un programma di spyware a nostra insaputa, potrebbe utilizzare tutto quello che è presente nel nostro computer, con tutti i rischi che potrebbero derivare.

A questo punto l'intruso può accedere, consultare o danneggiare le informazioni presenti sul computer compromesso, e addirittura può sfruttarlo per ulteriori attacchi verso altri siti. In questo modo il proprietario del computer controllato dall'intruso fa da paravento impedendo agli investigatori di scoprire chi è all'origine dell'aggressione e diventando a sua insaputa complice nelle successive attività criminali che l'intruso intende fare.

Proteggere il proprio computer non è quindi solo una necessità per proteggere i propri dati ma anche una responsabilità di tutti per impedire la diffusione di attività criminali e garantire il corretto funzionamento di Internet.

Noi non siamo collegati ad Internet

...è Internet che è collegato a noi

Fino all'avvento di Internet i nostri beni informatici sono stati protetti all'interno delle mura domestiche. Se escludiamo il rischio dei virus, che riguardava però solo chi scambiava dischetti con amici e colleghi, un'eventuale minaccia al nostro computer poteva venire solo da chi scassinava la porta di casa.

Internet ci ha proiettato in una nuova realtà, dove tutto è a portata di mano e dove il mondo ci entra letteralmente in casa.

Contrariamente ad altri collegamenti, quali la linea telefonica o la rete elettrica, Internet non ci fornisce solo passivamente i servizi richiesti ma, essendo una piazza virtuale, ci mette spesso alla mercé di personaggi di cui faremmo volentieri a meno. Oggi i venditori che propongono le loro ambigue offerte o i malfattori che tentano di consultare o danneggiare i dati e i programmi sui nostri computer possono trovarsi in qualsiasi parte del mondo, ma ci importunano come se fossero fuori dalla porta di casa.

Non siamo noi collegati a Internet; è Internet che è collegato a noi, con tutte le sue informazioni, le sue potenzialità, i suoi fastidi e i suoi rischi.

Non è solo un problema tecnico

Come sono a rischio le nostre informazioni personali

Quando utilizziamo Internet alcune nostre informazioni quali il browser utilizzato, la risoluzione dello schermo, l'indirizzo IP ed altri dati di tipo tecnico sono rese disponibili al sito con cui ci colleghiamo.

Questo non significa che da Internet possano carpirci informazioni critiche su di noi senza che ce ne rendiamo conto. Fortunatamente, se escludiamo le informazioni tecniche indicate sopra, quando ci colleghiamo ai siti Internet o usiamo la posta elettronica la responsabilità di fornire i nostri dati è ancora in mano nostra. Come nella vita reale sta quindi al nostro buon senso valutare con chi comunicare e che cosa fare conoscere delle nostre informazioni.

Spesso se i beni informatici non sono protetti come i beni reali è soprattutto per la mancanza di consapevolezza dei rischi che corriamo oggi utilizzando le apparecchiature informatiche. I motivi possono essere diversi:

- Non ci rendiamo conto dei nostri beni informatici e del loro valore perché non li possiamo avere visivamente di fronte a noi come i beni reali.
- Utilizziamo i computer così come ce li consegna il fornitore senza nessuna preoccupazione per la sicurezza, (spesso configurati di fabbrica in modo da lasciare la porta aperta ai malintenzionati).
- Ci comportiamo in modo imprudente in situazioni in cui si fa leva sulla nostra curiosità, sulla nostra ingenuità e sulla nostra incompetenza informatica senza mettere in campo la diffidenza che quotidianamente esercitiamo nel modo reale.
- Di fronte ai continui cambiamenti, caratteristici del mondo dell'informatica, facciamo fatica a comprendere quali sono i comportamenti corretti perché le minacce cambiano continuamente così come i mezzi per proteggersi.

Per questo chi vuole attaccare i nostri computer ha spesso più successo sfruttando i nostri comportamenti che utilizzando gli strumenti tecnici più sofisticati.

Il fattore umano: l'anello più debole

La convincente disciplina del "social engineering"

Il "social engineering" o ingegneria sociale è un termine poco conosciuto al di fuori della comunità informatica. Il termine definisce un vero e proprio modo di intrusione di tipo non tecnico, finalizzato ad ingannare le persone, per carpire le informazioni necessarie a superare le barriere di sicurezza.

Un esempio classico che si sta dimostrando particolarmente pericoloso, è la tecnica chiamata "phishing" (storpiatura della parola inglese fishing, pescare).

È possibile infatti pescare le informazioni finanziarie di una persona tramite l'invio di un messaggio di posta elettronica falso, a nome di società finanziarie o siti di acquisti a livello locale o internazionale.

Questi messaggi invitano ad accedere al sito per una verifica della password oppure si presentano come un avviso di addebito anomalo che per essere visto in dettaglio richiede l'inserimento – sembrerebbe logico - del nome utente e della password.

Il problema è che si è accede a un sito fasullo che si presenta esattamente come quello originale e che permette ai malfattori di catturare tutti i dati necessari per accedere al vero conto del malcapitato.

In altri casi facendo leva sulla nostra curiosità si può essere indotti ad accedere a siti o ad aprire documenti o immagini che hanno il solo scopo di istallare del software malefico sul nostro PC e permettono quindi ad un estraneo di accedere e controllare il nostro computer.

Bibliografia

Per rendersi conto della genialità dei metodi e dell'efficacia dei risultati a cui si può arrivare con l'ingegneria sociale basta leggere il libro di Kevin D. Mitnik, considerato tra i più abili hackers del mondo, che descrive le tecniche usate nei suoi attacchi.
Senza nessuna strumentazione tecnica, semplicemente ingannando le persone, è riuscito a farsi rivelare informazioni sensibili che gli permettevano poi di scavalcare i sistemi di sicurezza delle aziende.

Kevin D. Mitnik
L'arte dell'inganno
Feltrinelli, 2003

I rischi della socializzazione

Quando siamo noi a mettere a rischio le nostre informazioni

I siti di social network (Facebook, MySpace, LinkedIn, ecc.) sono oggi di grande attualità perché permettono di stare in contatto con gli amici, pubblicando foto, scambiando messaggi e utilizzando applicazioni sviluppate da altri utenti.

Spesso chi si iscrive a queste reti sociali fornisce le sue informazioni, anche di tipo personale e privato, senza rendersi conto che da quel momento i dati sono memorizzati per sempre su Internet e potranno in futuro essere visti magari da qualcuno a cui non vorremmo mostrarli.

Un altro problema e che spesso non ci si rende conto che i dati vanno protetti e quindi chiunque è in grado di vedere informazioni che non pensiamo siano riservati.
Tutto questo potrebbe portare ad un vero e proprio furto di identità con tutti i problemi che possono derivare

C'è il rischio che le persone con cui si è in contatto potrebbero essere degli impostori o peggio dei truffatori che a poco a poco, con tecniche di social engineering, possono coinvolgerci in situazioni spiacevoli

Da ultimo è stato dimostrato che possono esistere dei rischi anche con le applicazioni, in genere giochi, che si possono utilizzare su questi siti. Chi sviluppa l'applicazione potrebbe inserire dei codici malefici che possono infettare il computer e renderlo in questo modo accessibile da terze persone.

Quanto è sicuro Facebook?

In un momento in cui tutti sono affascinati da Facebook vale la pena di leggere alcuni articoli che analizzano il fenomeno in modo critico.

Fuga da Facebook – La Repubblica
http://www.repubblica.it/2008/03/sezioni/scienza_e_tecnologia/social-networking/facebook-fuga/facebook-fuga.html

Come difendersi da Facebook – Corriere della Sera
http://www.corriere.it/scienze_e_tecnologie/08_novembre_11/magazine_facebook_075505ba-b009-11dd-981c-00144f02aabc.shtml#

Generazione Facebook, adolescenti a rischio – Italia chiama Italia
http://www.italiachiamaitalia.net/news/132/ARTICLE/11638/2008-10-28.html

La criminalità su Internet

Non solo truffe on-line

I crimini su Internet stanno diventando sempre più frequenti. Si manifestano come varianti dei crimini già presenti nella vita reale quali la pedofilia, la pornografia dura, l'incitamento al razzismo, le truffe, le frodi, l'abuso delle carte di credito o la violazione dei diritti d'autore.

Esistono poi crimini tipici dell'ambiente informatico quali l'accesso illecito a sistemi di computer, il cybercrime, il danneggiamento dei dati informatici, il danneggiamento o il blocco dei siti Internet, la diffusione di virus informatici, il sabotaggio delle infrastrutture critiche. Ma quali sono le tipologie di criminali su Internet?.

Ci sono nuove categorie di criminali che come fa notare il criminologo Marco Strano, "..sono soggetti tendenzialmente non violenti che, nella solitudine di un computer, commettono azioni delittuose che non riuscirebbero mai a compiere al di fuori del cyberspazio". Quindi persone che non avrebbero il coraggio di mostrare le loro tendenze pedofile, dipendenti scontenti che non farebbero mai azioni fisiche di sabotaggio alla propria azienda; ladri di informazione che non avrebbero il coraggio di introdursi fisicamente in un ufficio per sottrarre informazioni; teppisti che avrebbero paura di tirare sassi ad una vetrina per strada e così via.

Lo schermo del PC per questi nuovi criminali diventa una sorta di protezione che influenza anche alcuni meccanismi del pensiero quali per esempio la percezione dell'illegalità del comportamento, la stima dei rischi di essere scoperto, la percezione del danno procurato alla vittima.

Ma esistono anche altri tipi di criminali. Vere e proprie organizzazioni attive nel mondo reale che hanno individuato le possibilità di guadagno della rete e che si muovono ormai a livello planetario con decisione, professionalità e disponibilità di mezzi. Attività apparentemente innocue come lo spamming e la diffusione di virus, usate come mezzo per portare successivi truffe, ma anche frodi, ricatti e attacchi nei confronti di siti Internet con la minaccia di farli cadere fino ai possibili attentati alle infrastrutture critiche.

Per impedire al crimine organizzato di invadere il cyberspazio sono importanti due cose

- Mostrare che le attività criminali su Internet non sono tollerate e che saranno sempre più sanzionate dalle legislazioni nazionali ed internazionali e perseguite con l'attività delle forze di polizia
- Diffondere l'informazione sui tipi di crimine e sulle possibili vittime per fare in modo che la conoscenza dei rischi informatici cominci a far parte della consapevolezza che abbiamo dei rischi quotidiani.

Il nostro senso di responsabilità e il nostro ruolo attivo nell'informare le autorità nel caso di minacce ai minori o di pedofilia o nel diffondere informazioni in caso di truffe o altri crimini, può contribuire ad evitare un danno ad altri e a rendere la vita un po' più complicata ai criminali.

Gli attacchi in grande stile

Delinquenti a nostra insaputa

La tecnica di attacco chiamata Denial of Service distribuito serve per colpire un server internet e provocarne il vero e proprio blocco come si è visto più di una volta nel caso di importanti siti commerciali oppure siti di enti governativi. Ci si potrebbe chiedere che cosa centra in tutto ciò con il nostro umile computer domestico?

Per far funzionare questo tipo di attacco è necessario inviare, in contemporanea, un numero elevato di richieste al server in modo da saturarlo e non renderlo in grado di rispondere. E la cosa più utile per poter fare questo tipo di attacco è quello di poter avere sotto controllo migliaia o decine di migliaia di computer che possono essere usati come i soldati di un'armata. Ed è qui che può entrare in gioco il nostro umile computer domestico.

Questo tipo di attacco viene fatto utilizzando computer di persone ignare del fatto di partecipare all'attacco. Questi computer sono infettati, prima di fare l'attacco, con dei virus o worm che mantengono aperti dei canali per poterli controllare. Quando si vuole fare l'attacco basta attivare contemporaneamente tutti i computer infetti e bombardare il server bersaglio di richieste ostili. In questo modo il vero attaccante riesce a restare anonimo.

La maggior parte dei recenti virus in circolazione è stata progettata proprio per trasformare i computer infettati in zombi e permettere di utilizzarli in quelli che sono chiamate le botnet, gruppi di computer compromessi, che possono agire su comando di un padrone.

Queste botnet sono generalmente affittate dai loro creatori a organizzazioni criminali che li utilizzano per attacchi di Denial of Service distribuito ma anche per fare spamming, per truffe nella pubblicità on-line e per altre attività criminali.

L'avvento dei collegamenti ADSL ha contribuito ad incrementare il fenomeno delle Botnets, sfruttando i numerosi computer dotati di una connessione permanente e con scarse misure di protezione.

Scopriamo il valore ai nostri beni

Quali sono i rischi, cosa proteggere e perché

Se analizziamo i possibili danni che riguardano i nostri dati e le nostre apparecchiature informatiche, possiamo identificare tre importanti categorie di rischi:

- I rischi di indisponibilità delle risorse, che potrebbero metterci nella condizione di non poter utilizzare i nostri sistemi o i nostri dati.
- I rischi concernenti l'integrità delle risorse, che potrebbero creare alterazioni o cancellazioni accidentali o non autorizzate dei nostri dati.
- I rischi concernenti la riservatezza delle risorse, che potrebbero esporre pubblicamente i nostri dati o renderli visibili alle persone non autorizzate.

Oggi siamo portati a pensare che i rischi provengono principalmente dall'esterno, come ad esempio il caso di uso improprio del nostro computer da parte di un intruso proveniente da Internet.

Questo non è del tutto vero perché dobbiamo considerare anche i rischi che possono derivare da incidenti, ad esempio un malfunzionamento delle apparecchiature – tipico è la rottura di un disco –, la caduta di corrente o i danni della natura (incendio, alluvione, ecc.), oppure i nostri errori e le nostre negligenze.

Non possiamo proteggerci completamente da tutti i rischi ma con delle semplici precauzioni potremmo essere in grado di ridurre il rischio ad un livello accettabile. Spesso sono precauzioni veramente semplici ma dai risultati molto importanti.

Quando si parla di sicurezza, la prima cosa da fare è identificare i beni da tutelare e il loro valore. Senza una chiara visione di questo concetto potremmo correre il rischio non sapere cosa proteggere e di reagire con contromisure inadeguate oppure eccessive.
Secondariamente non dobbiamo limitarci a considerare solamente i beni che potrebbero essere danneggiati o distrutti ma dovremmo considerare tutti gli aspetti collaterali che potrebbero derivare dopo aver subito un danno.
Per questo è utile valutare le tipologie di danno suddividendoli in due gruppi:

- Danni evidenti
  Possiamo considerare in questa categoria i danni all'hardware, ai programmi e alle informazioni (lettere, foto, posta elettronica, informazioni private, musica, film, documenti contabili, ecc.). Il valore dell'hardware e dei programmi può essere generalmente considerato uguale al loro valore di acquisto mentre il valore delle informazioni, soprattutto quando queste non possono essere più ricostruite, è spesso difficile da quantificare.
- Danni nascosti
  Appartengono a questa categoria le attività necessarie alla ricostruzione dei dati o alla

riconfigurazione del computer, che a dipendenza della situazione possono essere anche di una certa complessità. Un danno informatico può avere dei costi collaterali che nei casi più fortunati possono limitarsi alla semplice pulizia da un virus ma che in casi estremi possono richiedere la completa ricostruzione del computer.

Se vogliamo stabilire il valore di un bene informatico dobbiamo quindi tener conto dei possibili danni diretti e indiretti e in questo modo stilare una classifica dei beni da proteggere secondo la loro criticità. Solo a questo punto saremmo pronti per decidere che tipi di protezioni applicare.

Cosa dobbiamo proteggere

Facciamo l'inventario dei nostri beni critici

I beni e le risorse informatiche che dobbiamo proteggere sono di diverso tipo ma le possiamo raggruppare nelle seguenti categorie:

Le apparecchiature hardware
Il nostro computer di casa, il PC portatile, la stampante, lo scanner sono vulnerabili ai danni fisici (urti, umidità, cadute), ai furti o ai danni provocati da interruzioni elettriche. Dobbiamo quindi proteggerlo con le opportune misure di protezione fisica o elettrica - ad esempio un gruppo di continuità – oppure prestando la dovuta attenzione ad esempio che non ci vengano rubati.

Il software
Il sistema operativo e tutti i programmi istallati sul nostro computer possono essere danneggiati o per attacchi dall'esterno o per malfunzionamenti del computer. In questo caso è possibile istallarli nuovamente e per questo dobbiamo avere a disposizione i dischi e i CD di istallazione di tutti i programmi. Dobbiamo preoccuparci di fare una copia su CD anche dei programmi che abbiamo scaricato da Internet per evitare che vadano persi in caso di rottura del disco.

I dati informatici
Sul nostro computer sono memorizzati tutti i nostri dati personali - lettere, documenti contabili, posta elettronica, informazioni private, filmati, fotografie, musica, ecc. - e in caso di danni o di perdita difficilmente potrebbero essere ricostruiti. Inoltre desideriamo che questi dati siano mantenuti riservati e protetti dalla visione di persone non autorizzate.

Le nostre informazioni personali
Informazioni private sulla nostra persona e sui nostri comportamenti che vogliamo mantenere riservate ma che potrebbero per motivi diversi essere memorizzate sul nostro computer

I dati critici
Questi dati non sono necessariamente memorizzati sul computer ma sono fondamentali per il suo funzionamento o per il funzionamento di applicazioni o servizi finanziari. Se venissero scoperti da un malintenzionato, potrebbero essere usati per svolgere attività illecite e truffaldine nei nostri confronti. Questi dati devono essere quindi considerati strettamente personali.

Tra i dati critici, che non dobbiamo comunicare a nessuno, possiamo citare:

- Le Password
  sia quella del nostro computer che dei vari servizi finanziari o bancari che utilizziamo
- Il PIN
  il numero usato generalmente per le carte bancarie
- Le liste di stralcio
  i numeri usati a complemento delle password nei servizi finanziari e bancari
- I numeri di Carta di credito
- Il Credit Card validation code
  il numero timbrato sul retro della carta di credito che viene sempre più richiesto nelle transazioni di commercio elettronico

- I nostri dati anagrafici
- I nostri dati finanziari
- I nostri indirizzi di posta elettronica

Quali sono le minacce

Conoscere per difendersi

Le minacce possono essere suddivise in due grandi categorie:

- Minacce da parte di altri finalizzate ad accedere e utilizzare il nostro computer e i nostri dati in modo improprio.
- Minacce derivanti da incidenti o da negligenza.

Tra le minacce da parte di altri e finalizzate ad accedere e utilizzare il nostro computer e i nostri dati in modo improprio troviamo:

- **Messaggi di posta elettronica con virus o worm**
  I messaggi di posta elettronica possono contenere virus e gli altri codici malefici inviati come allegati. Non aprite allegati se non siete sicuri della loro autenticità e diffidate delle situazioni sospette. Ad esempio ignorate messaggi relativi ad acquisti che non avete mai fatto o le vincite a lotterie a cui non avete mai partecipato.
- **Cavalli di troia (Trojan horse)**
  Programmi che permettono ad un intruso di prendere possesso del computer controllandolo tramite canali nascosti (backdoors). Possono essere istallati con tecniche di “social engineering” o tramite virus.
- **Falsi messaggio di posta elettronica (email spoofing)**
  I messaggi di posta elettronica possono essere falsificati e alterati sia nell’intestazione che nel testo. Non fidatevi quindi dei messaggi se vi fanno richiesta di informazioni particolari quali password o dati personali anche se provengono da indirizzi che conoscete. Fate una veloce verifica telefonica per chiedere direttamente se il messaggio è autentico.
- **Files con estensioni nascoste**
  Nell’istallazione standard di Windows è abilitata la funzione "Nascondi le estensioni dei files conosciuti". Questo impedisce di capire se il tipo di file può essere eseguibile e creare danni. L’opzione deve essere disabilitata.
  Possono essere a rischio anche gli allegati con solo testo o grafica perché possono nascondere file eseguibili.
- **Istallazione di programmi malefici a nostra insaputa**
  Sono programmi che in genere istalliamo noi stessi, senza renderci conto della pericolosità. Possono essere istallati come programmi spyware associati a programmi gratuiti oppure sono programmi che istalliamo, convinti della loro utilità, dopo essere stati imbrogliati con tecniche di “social engineering”.
- **Directory condivise non protette**
  Le directory condivise non protette permettono ad un intruso di vederne il contenuto e di scaricare programmi che potrebbero essere usati per fare successivi attacchi
- **Pagine Web con contenuti attivi (mobile code)**
  Le pagine web possono contenere programmi scritti in linguaggi, quali ad esempio Java Script o controlli ActiveX, che sono eseguiti sul nostro computer per aggiungere funzionalità o per migliorare la presentazione grafica. Nel caso un malintenzionato sostituisse questi programmi con codici malefici, come ad esempio un dialer, potrebbe crearci dei danni. Anche i programmi di posta elettronica, se hanno abilitato l’uso del codice HTML, possono avere gli stessi problemi.

- **Furto della password**
  La password può essere indovinata, scoperta con particolari programmi di ricerca, oppure fornita inconsapevolmente dall'utente.
- **Ricerca dati nei rifiuti**
  La mancata distruzione dei dati sui dischi e sui supporti magnetici dei computer dismessi permette ad un malintenzionato di ottenere le vostre informazioni. Preoccupatevi di cancellare tutti i vostri dati sui dischi del PC prima di buttarlo.
- **Programmi Peer to Peer, Internet Relay Chat e di Instant Messaging**
  L'aumento dell'uso di questi programmi e la loro scarsa sicurezza li rende un veicolo di trasmissione di codici malefici.
- **Monitoraggio della rete (packet sniffing)**
  Uno sniffer è un programma con cui si possono catturare le informazioni dei pacchetti di dati che transitano sulla rete. Questo permette di conoscere nomi, password e altre informazioni personali, se queste non sono trasmesse in modo cifrato.
- **Phishing**
  Invitare ad accedere, con un falso pretesto, ad un sito fasullo con l'intenzione di rubare il nome utente e la password

Tra le minacce che derivano da incidenti o negligenze troviamo:

- **Rottura del disco**
  Nel caso della rottura del disco viene compromesso il funzionamento del PC e nei casi più gravi la possibilità di ricuperare i dati.
- **Errori operativi e cancellazione di dati**
  Senza renderci conto possiamo fare delle operazioni che possono creare dei danni irreversibili.
- **Interruzione di corrente**
  La caduta improvvisa di corrente oltre impedire il funzionamento del computer può creare dei danni al disco.
- **Furto**
  Il furto del computer non crea solo problemi di mancata disponibilità ma anche delle minacce per la riservatezza dei dati. Nel caso di computer portatili, più soggetti a furti, basta utilizzare delle semplici precauzioni.

Sul sito MELANI vengono pubblicati regolarmente gli avvisi dei principali pericoli.