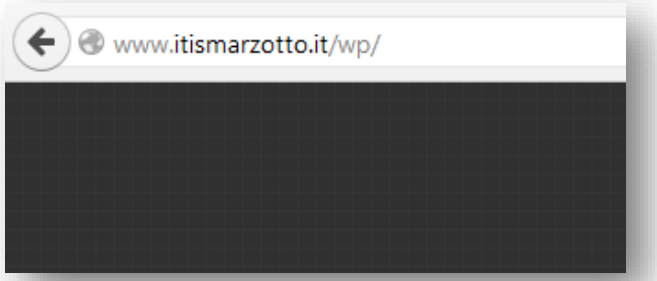
Internet,

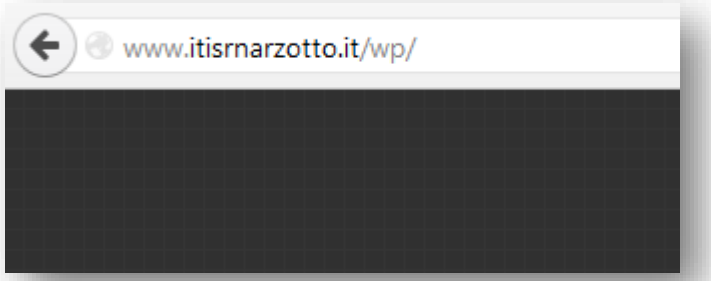
un servizio così utile, ma allo stesso tempo così pericoloso.

Anna Marangon - Davide Ambrosi - Riccardo Simioni - Lazar Milic

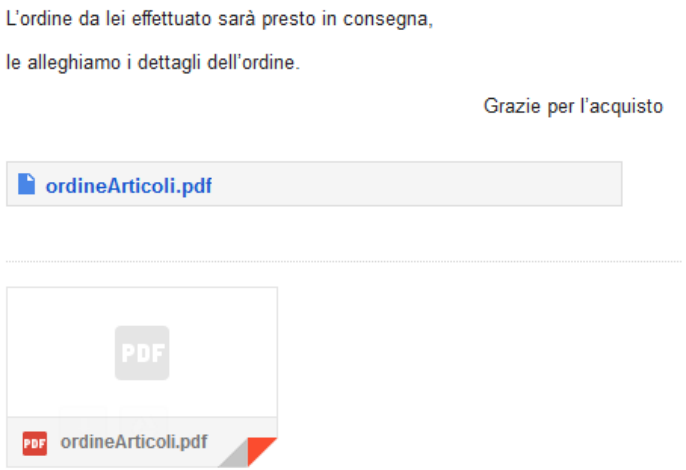
Controlla sempre il dominio

Diffida da e-mail non richieste





Accedendo al sito errato, non posso sapere le intenzioni dei soggetti malevoli. Per esempio possono inserire virus nel pc, ma questi tipi di attacchi hanno un target preciso, ovvero mirano a rubare l'identità degli utenti. L'unico modo di riconoscerli è di controllare il dominio e eventuali errori di ortografia.



E-mail non richieste possono contenere virus, non aprite file allegati o link sterni, a meno che non siate sicuri della provenienza perché potrebbero essere infetti

L'antivirus da una mano anche nel web

L'importanza degli aggiornamenti

Oltre a mantenere il computer pulito, controllando che non si installino virus, i moderni antivirus permettono un controllo sulla navigazione. Con un apposito plugin (ovvero un'estensione ad un programma), gli antivirus controllano tramite dei feedback degli utenti e la reputazione del sito se questo è affidabile.

Mantenere sempre aggiornato il proprio sistema, permette di avere una sicurezza in più. Con gli aggiornamenti gli sviluppatori sistemano i programmi e li rendono più invulnerabili agli attacchi.

La password,

un oggetto sempre più prezioso

Le password al giorno d'oggi sono sottovalutate e scelte senza una critica, offrendo a internet una grande fiducia.

Le password possono permettere di accedere ai servizi più vari, dai più banali ad i più importanti come l'account bancario. Se questo non viene messo in sicurezza in modo adeguato si può incappare nel furto d'identità per i social network o allo svuotamento del conto nel mondo bancario.

Per scegliere una password si deve abbandonare l'uso degli hobbie e fattori personali, preferendo caratteri casuali alternati da numeri.

Ora, il pattern diventa difficile da ricordare anche perchè il numero delle password da gestire diventa man mano sempre più consistente. In nostro aiuto arrivano dei software per la gestione e creazione di password solide, come KeePass 2.

L'ultimo punto consiste nel cambiare spesso la password agli account più sensibili, i quali potrebbero essere oggetto di attacchi malevoli.

Compiere un crimine? …meglio farlo con il tuo nome!

- FURTO D'IDENTITA'

Sostanzialmente il furto d'identità avviene quando il ladro le utilizza le tue informazioni personali per prendere il tuo posto e commettere frodi.

Solitamente è un "crimine d'opportunità", in quanto un utente potrebbe diventare una inconsapevole vittima per il solo motivo che i propri dati personali non sono adeguatamente protetti.

La ricerca e il commercio di dati personali fanno parte di un fenomeno in continua espansione. Per questo si stanno cercando sempre più modi per truffare le persone mezzi sempre più avanzati.

Come potrebbero mettere le mani sulle vostre informazioni?

Man In The Middle

Con questo metodo, l'attaccante è in grado di leggere, inserire o modificare a piacere, messaggi tra due parti comunicanti tra di loro.

Caratteristica è il non permettere che nessuna delle due sia in grado di sapere se il collegamento che li unisce reciprocamente sia stato effettivamente compromesso. L'attaccante così è in grado di osservare, intercettare e replicare verso la destinazione prestabilita il transito dei messaggi tra le due vittime.

Cookie Hijacking

Molti utenti permettono ai siti Web di generare e controllare la loro identità usando un username e password (che può essere cifrata durante il transito) attraverso l'utilizzo dei cookie; questo affinché l'utente non abbia bisogno di re-inserire il proprio username e password in ogni pagina per mantenere la sua sessione.

Una parte delle informazioni sono rilasciate dal server e restituite dal browser dell'utente per confermare la sua identità. Se un attacker è in grado di rubare questo cookie, può fare egli stesso le richieste come se fosse l'utente vero, accedendo alle informazioni e ai dati personali. Se il cookie è persistente, lo scambio d'identità può continuare per un periodo di tempo considerevole.

Il wi-fi è sicuro?

Le reti Wi-Fi casalinghe o meno, sono ormai diffuse ovunque.

Uno dei principali punti deboli di questa tecnologia è il fatto di essere visibile a tutti coloro che si trovano nel campo di un router, questo comporta che chiunque potrebbe accedervi senza che ve ne rendiate conto.

Da uno studio effettuato in Spagna scopriamo infatti che il 12% degli utenti di Internet naviga craccando la rete di qualche vicino.

Come proteggersi?

Migliora le tue difese

- **Cambia la configurazione di default del router:**
  - Nuova password
  - Nuovo SSID
  - Tipo di cifratura (wep/wpa)
- **Controlla la copertura della tua rete Wi-Fi**
- **Non dimenticare il firewall**
- **Disattiva il segnale wi-fi se non lo usi**

..occhio agli honey pot!

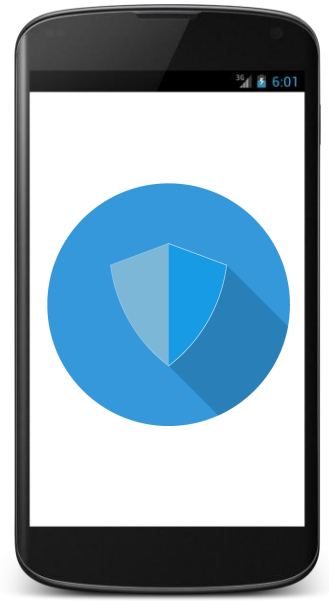
La diffusione del Wi-Fi libero è una gran bella cosa: è comodo avere una rete senza fili a disposizione anche quando usciamo di casa; ma gli utenti tendono a fidarsi un po' troppo, e questo è un problema. Alcune di quelle reti Wi-Fi potrebbero essere una trappola creata ad hoc dai pirati.

Di cosa stiamo parlando? Un malintenzionato potrebbe allestire un hot spot Wi-Fi non protetto da password per invogliare gli utenti a connettersi o per poter intercettare tutta la loro comunicazione

La sicurezza del vostro smartphone non va sottovalutata

Ormai i cellulari vengono usati per un'ampia gamma di attività in continua espansione, dai social network agli acquisti online, alle operazioni bancarie o alla navigazione Web. Di questo fenomeno sono consapevoli anche i malintenzionati che cercano in continuazione nuovi metodi per accedere alle nostre informazioni.

Per questo motivo è molto importante avere in chiaro quali siano i pericoli sul vostro smartphone e sapere come proteggervi.



Attenzione alle autorizzazioni richieste dalle app

Una questione a cui bisogna stare attenti riguarda le autorizzazioni che le app richiedono, esse determinano a quali funzionalità del telefono possono accedere. In molti casi possono essere utili al corretto funzionamento di una app, ma se quest'ultima è fasulla può essere molto pericolosa. Eccone alcune da tenere d'occhio:

- *Chiamata diretta numero di telefono*
- *Invio SMS o MMS*
- *Accesso completo ad Internet*
- *Lettura/Scrittura dati di contatto*
- *Acquisizione di foto/video*

PS: Le autorizzazioni le potrete trovare al percorso:
Impostazioni > Applicazioni > (Nome dell'app) > Autorizzazioni

Alcuni consigli per migliorare la sicurezza del vostro smartphone

- Proteggi il tuo telefono con una password o codice PIN
- Assicurati che le app che installi siano provenienti da una fonte attendibile e consulta sempre le recensioni e i commenti
- Mantieni aggiornato il tuo telefono e le tue app
- Installa un antivirus ed esegui le scansioni regolarmente
- Disattiva Wi-Fi e Bluetooth se non li utilizzi
- Scegli una soluzione antifurto per lo smartphone in caso di furto
- Effettua regolarmente un backup di dati

Che cos'è un malware?

Tutti (o quasi) usiamo comunemente e informalmente il termine virus per indicare un qualsiasi software il cui obiettivo è agire su un qualsiasi dispositivo con lo solo scopo di creare danni e disagi.

In informatica viene definito malware un qualsiasi software creato con lo scopo di recare danni al computer, ai dati degli utenti o in generale a qualsiasi sistema informatico.

Esistono moltissime categorie di malware, qui tratteremo solamente quelle più comunemente conosciute:

- Virus
- Trojans
- Worms
- Spyware
- Dialer
- Rootkit
- Backdoor

Virus, Trojans, Worms, Spyware…

- Un **Virus** è un software che una volta eseguito in grado di infettare file in modo da riprodursi, facendo copie di se stesso. Può causare danni diretti sistema operativo, ma anche l sistema hardware.

- Un **Trojan** è un tipo di malware che deve il suo nome al famoso lo di Troia. Infatti esso si cela all'interno di un programma apparentemente utile che è l'utente stesso ad installare e ad eseguirne il codice.

- I **Worms** (vermi) sono simili ai Virus, ma al contrario di essi non necessitano di legarsi ad altri seguibili per diffondersi, ma si spediscono direttamente tentando di replicarsi tramite Internet. Il mezzo più comune usato per diffondersi è la posta elettronica.

- Lo **Spyware** è un tipo di software che raccoglie informazioni l'attività che compie un utente online così da spedirle a un organizzazione che le utilizzerà per trarne profitto proponendo pubblicità mirata agli interessi dell'utente.

...Dialer, Rootkit e Backdoor.

Un **Dialer** è un software che crea un collegamento tra Internet e un altro dispositivo. Esso viene usato con lo scopo di connettere l'utente a Internet a sua insaputa con una tariffazione speciale truffandolo.

Un **Rootkit** è un programma che assume il controllo sul sistema senza il bisogno di nere un autorizzazione dell'amministratore del dispositivo.

Backdoor (porta sul retro) sono delle porte che consentono di superare completamente o in parte le misure di sicurezza di un sistema informatico. Permettono ad un utente esterno di prendere il controllo remoto della macchina accedendo dati.

Alcuni famosi attacchi informatici

- **1999 Moonlight Maze**

Il Dipartimento della Difesa degli Stati Uniti, insieme a delle università e gruppo di imprenditori di armi si ritrovano i sistemi informatici violati. Fruttò ai malviventi codici navali e informazioni sui sistemi di guida dei missili USA. Si pensa sia opera dell'intelligence Russa, che mirava a mettere le mani sulla tecnoogia degli Stati Uniti.

- **2003 Titan Rain**

Attacco cinese effettuato alla vigilia di Natale che viola contemporaneamente e in poche ore i sistemi di Mc Donald's e Sony, della Nike e della Lockheed Martin, ma anche quelli della Sandia National Laboratories, del Redstone Arsenal e, soprattutto della NASA.