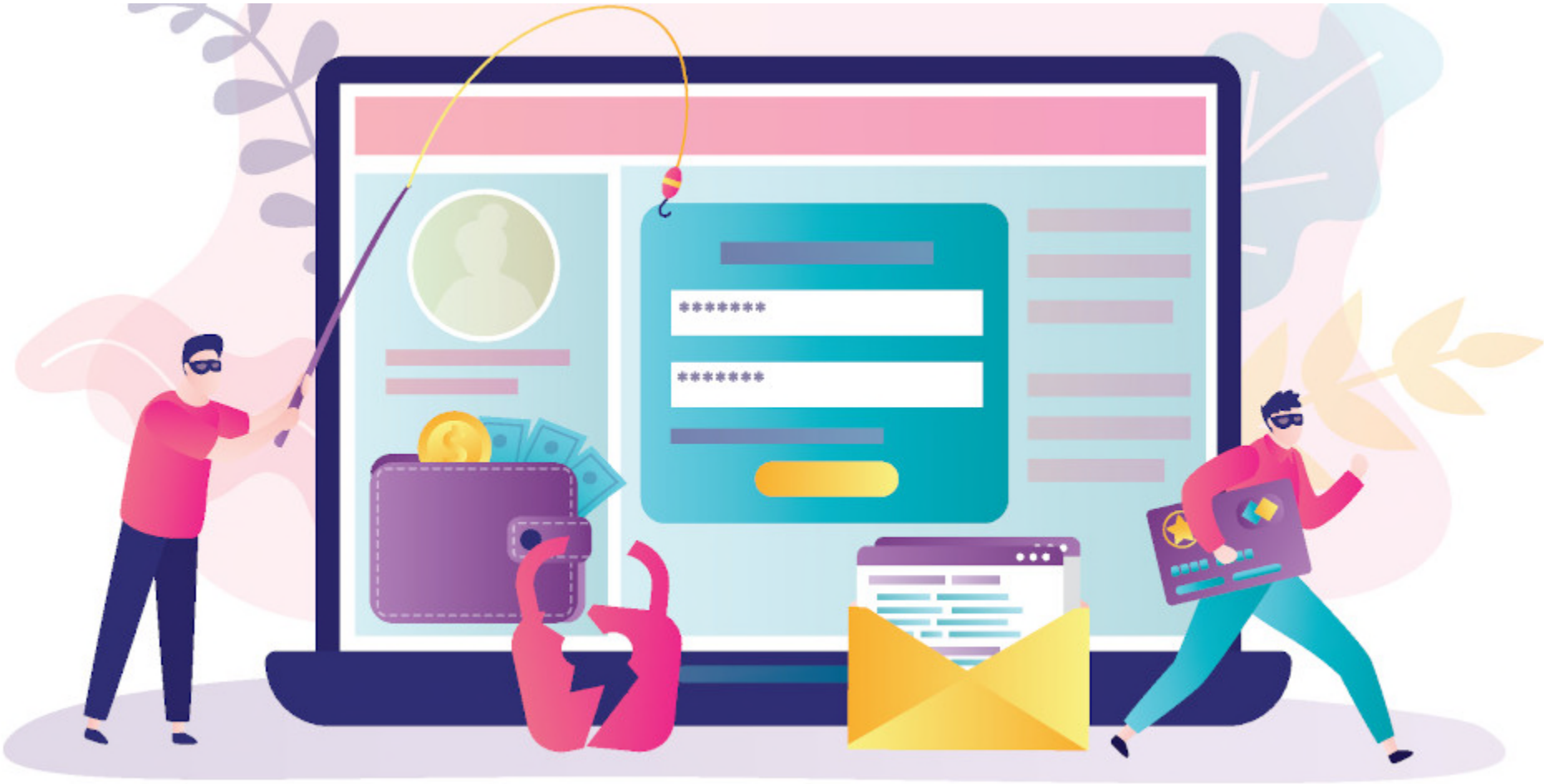
METODOLOGIA DI ATTACCO E TECNICHE DI DIFESA



METODOLOGIA DI ATTACCO E TECNICHE DI DIFESA

«C’è una **rivoluzione** planetaria in corso, non cruenta, ma non per questo meno dirompente sulla vita di ciascuno»

QUALCHE SEGNALE DELLA RIVOLUZIONE

- **Facebook**, nata nel 2006, ha più di 1 miliardo di utenti
- Le aziende informatiche riescono (legalmente) a pagare un terzo in meno di tasse rispetto alle aziende non tecnologiche
- **Ogni minuto** su Internet: 60 ore di video caricate su **Youtube**, 800.000 ricerche su **Google**, 15.000 app scaricate dal sito **Apple**, 190 milioni di mail inviate
- Il conto economico della criminalità informatica (guadagno + danni) è secondo solo al mercato della droga (guadagno)
- Fanno più tendenza i BLOGGER che i giornalisti
- Si diventa star tramite i social (youtube, facebook)

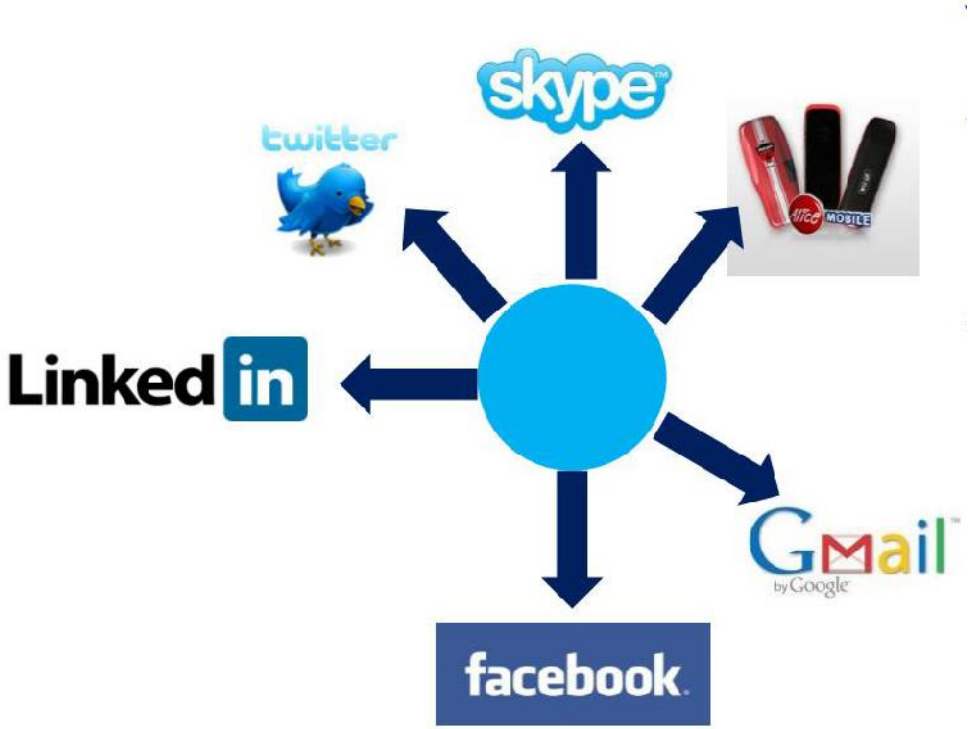
L'informazione assume sempre più valore

- Oggi l'informazione è in stragrande maggioranza in "forma digitale" (=sequenza di digit, ovvero di 0 e 1)
- Un'informazione in formato digitale è più economica, facile e veloce da:
  - Trasmettere - Ma anche da intercettare
  - Copiare - Anche se protetta da copyright
  - Modificare - Ma anche da Alterare
  - Eliminare - Ma anche da cancellare prove
- Cambia il concetto di proprietà e di furto del bene digitale
- Si superano le barriere spazio-temporali del mondo fisico
- Cambiano modalità di accesso e fruibilità dell'informazione
- Si stravolgono i modelli economici tradizionali

Chi vale di più ?

Il **valore** non dipende più dal costo dell'hardware, ma da quali **dati** sono memorizzati al suo interno

NUOVE MODALITÀ



Personal computer, Internet, WWW, telefonia mobile sono state innovazioni **dirompenti…**

… che hanno decuplicato le occasioni di **contatti** e di **apertura** al mondo veramente diventato globale (ma di cui non conosciamo bene le regole, le opportunità e i rischi)

NUOVI RISCHI

- Ogni antenna Wi-Fi
- Ogni numero di telefono
- Ogni smartphone
- Ogni computer collegato alla rete
- Ogni casella di posta elettronica
- Ogni sito di commercio elettronico
- Ogni profilo di social network (Facebook, Twitter, Linkedin)
- Ogni servizio di rete dotato di login+password

costituisce un punto di uscita, ma anche una porta di ingresso verso di noi, le nostre informazioni e la nostra identità digitale

GLI ATTACCHI INFORMATICI OGGI

CHI SONO GLI ATTACCANTI

Professionisti

Cyber-Criminali

Mercenari

Patologici opportunisti

Predatori
Conoscenti
Ex di qualcosa

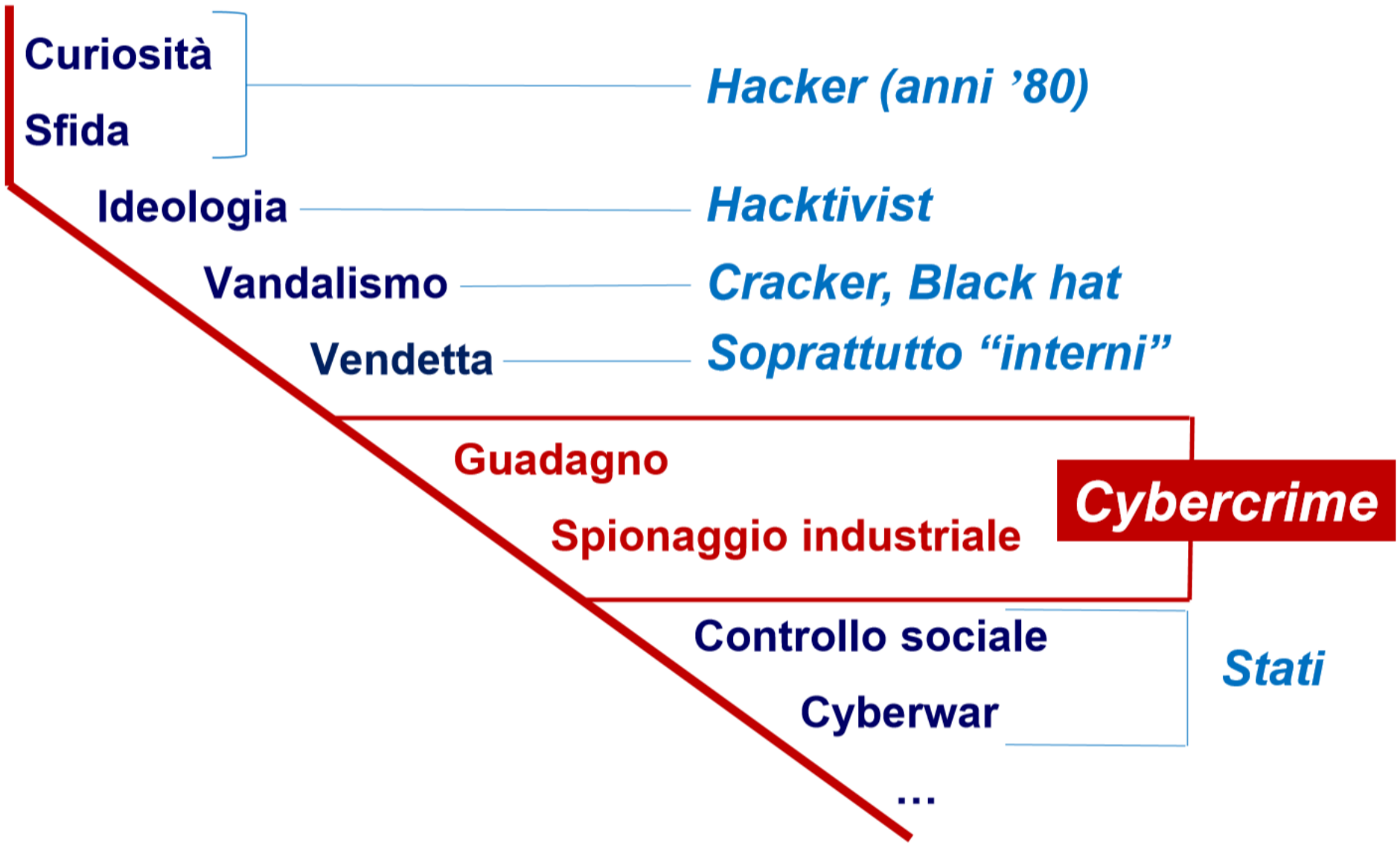
Ideologisti

Hacktivist

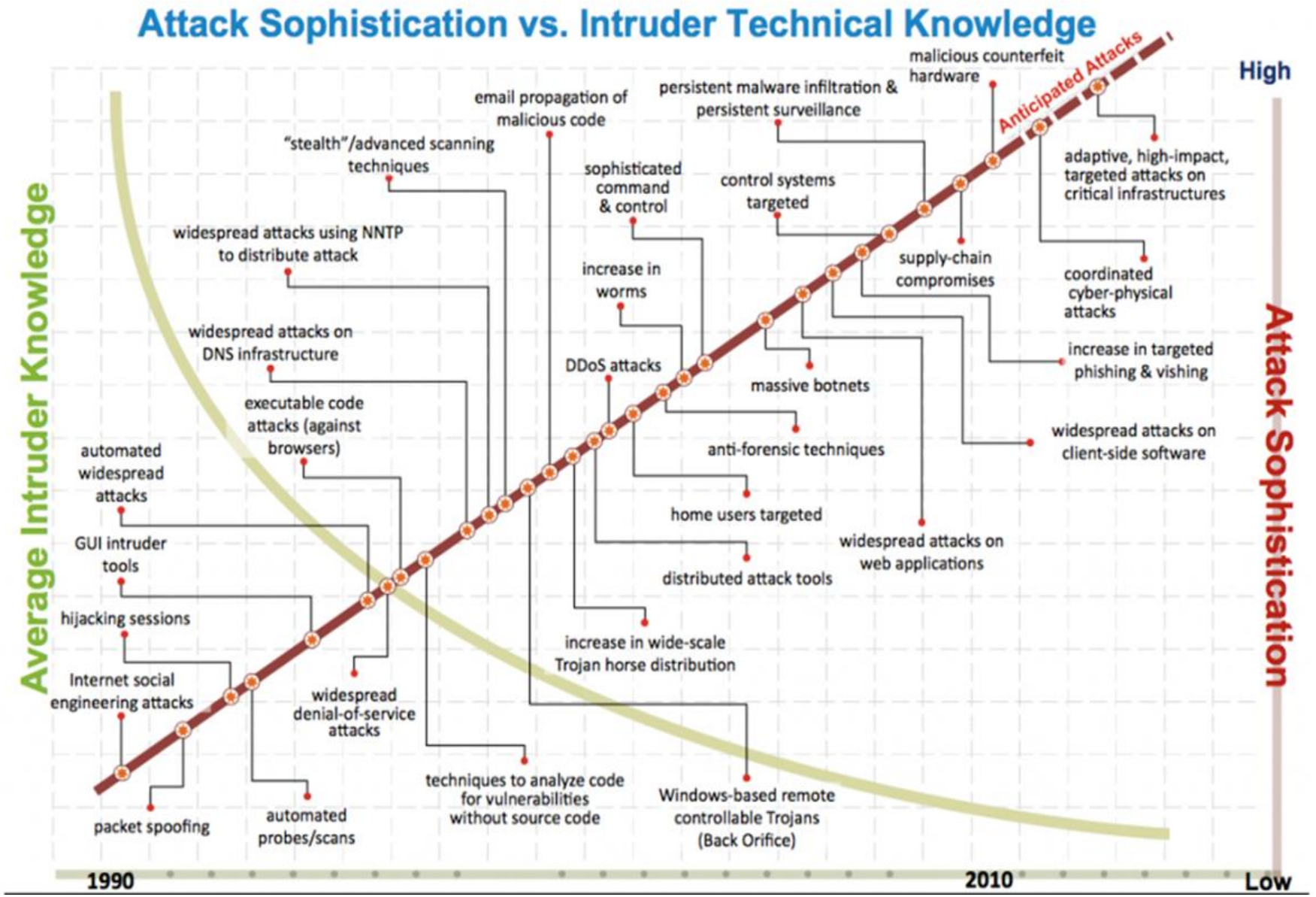
NOI

Noi stessi

EVOLUZIONE DEGLI ATTACCHI - SEMPLIFICATO



EVOLUZIONE DEGLI ATTACCHI - REALE



EVOLUZIONE DEL CRIMINE INFORMATICO

- “**La cosa che più è cambiata in questi anni è il nemico che abbiamo di fronte:**
  - siamo passati dai teenager, che vogliono solo divertirsi a superare le barriere o sfidare il mondo, a professionisti che vogliono i vostri soldi o le vostre informazioni da trasformare in denaro”

- E questi professionisti possono essere ovunque (in Europa, in uno slum brasiliano o in qualche zona rurale della Cina). Non come il ladro della vostra auto che probabilmente abita in prossimità della vostra città o, in ogni caso, deve arrivare sotto casa vostra

TIPI DI OBIEZIONE

- “Io non sono un obiettivo interessante”
- “Non penso di meritare un attacco”
- “Io non ho neanche un conto corrente on-line”
- “Io non uso la carta di credito su Internet”
- “Io non ho informazioni con un valore economico”
- “Nessuno può seriamente vedermi come un obiettivo”
- ……

VALORE DELL'INFORMAZIONE

- Ogni nostro account (login+password) ha un valore economico
- Ogni nostro computer (inteso anche come spazio disco e come possibilità di connessione)
- Il nostro profilo: chi siamo, cosa facciamo, cosa ci piace, quali sono le nostre relazioni, quali siti visitiamo, la nostra rubrica, ecc.

ESEMPI

- Un nostro **account** (login+password) ha un valore economico perché consente a un criminale di compiere azioni mascherando la propria identità
- Un nostro **computer** ha un valore economico per:
  - Spazio disco (e occultamento materiale compromettente)
  - Mascheramento dell'origine delle azioni criminali
  - Perdita del controllo (reti di computer zombie botnet)
- Il nostro **profilo** ha un valore economico per:
  - Motivi pubblicitari e commerciali
  - Truffe mirate
  - In alcuni casi, ricatto

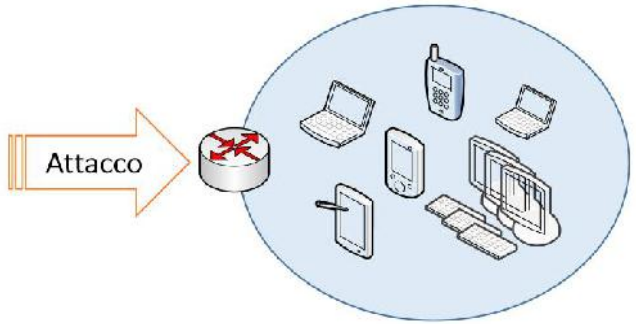
ALCUNI HANNO VALORI ECONOMICI PIÙ ELEVATI

- Personali
  - Conti correnti on-line
  - Carte di credito
  - PIN e Password memorizzate in chiaro – …
- Lavorative
  - Accreditamento per accesso a servizi ristretti: posta elettronica aziendale, servizi finanziari, gestione esami, …
  - Informazioni su ricerche, concorsi, appalti, strategie, …
  - Informazioni e rapporti con colleghi, aziende, clienti, pazienti, …

SICUREZZA INFORMATICA

Con il termine sicurezza informatica si intende quel ramo dell'informatica che si occupa dell'analisi delle vulnerabilità, del rischio, delle minacce o attacchi e della successiva protezione dell'integrità fisica (hardware) e logico-funzionale (software) di un sistema informatico e dei dati in esso contenuti o scambiati in una comunicazione con un utente. Tale protezione è ottenuta attraverso misure di carattere tecnico-organizzativo e funzionali tese ad assicurarne:

- l'accesso fisico e/o logico solo ad utenti autorizzati (autenticazione);
- la fruizione di tutti e soli i servizi previsti per quell'utente nei tempi e nelle modalità previste dal sistema (disponibilità);
- la correttezza dei dati (integrità);
- l'oscuramento dei dati (cifratura);
- la protezione del sistema da attacchi di software malevoli per garantire i precedenti requisiti



CHI È UN HACKER

Un **hacker** è una persona che si impegna per aggirare o superare creativamente le limitazioni che gli vengono imposte in tutti gli aspetti della sua vita.

Esiste un luogo comune, usato soprattutto dai mass media (a partire dagli anni ottanta), per cui il termine hacker viene associato ai criminali informatici, la cui definizione corretta è, invece, "**cracker**".

METODOLOGIA DI ATTACCO
E
TECNICHE DI DIFESA

COS'È UN VIRUS

Un virus informatico è una serie di istruzioni scritte da un programmatore ed eseguibili da un computer, il quale ha le seguenti caratteristiche:

È stato scritto per "inglobarsi" e cioè confondersi alle istruzioni di altri programmi modificandoli.

Chi l'ha scritto ha previsto la possibilità che il virus sia in grado di copiare le istruzioni che lo compongono in altri programmi .

Dopo un tempo prestabilito il virus comincia a compiere l'azione per cui è stato creato (per esempio distruggere dati e/o programmi presenti su di un supporto magnetico).

TIPOLOGIE DI VIRUS

Uno **spyware** è un software che raccoglie informazioni riguardanti l'attività online di un utente senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le .....utilizzerà per trarne profitto.

I **macro virus** sono generalmente script incorporati all'interno di particolari documenti (come ad esempio SMS Word,Excel…).

Un **worm** (letteralmente "verme") è una particolare categoria di malware in grado di autoreplicarsi. È simile ad un virus, ma a differenza di questo non necessita di legarsi ad altri file eseguibili per diffondersi.

I T**rojan** sono dei virus che non fanno alcun danno ma permettono, al loro creatore di accedere al computer e di prenderne il pieno possesso.

DIFENDERSI - ANTIVIRUS - PROTEZIONE DEGLI ENDPOINT

- Un antivirus è un programma che blocca l'esecuzione o la memorizzazione nel sistema del malware.
- L'antivirus viene immediatamente avviato dal sistema operativo e viene invocato prima che un programma venga eseguito e primache un file venga memorizzato nel sistema (download da Internet, copia da chiavetta, ecc.).
- L'antivirus verifica se il programma in procinto di essere eseguito o il file in corso di memorizzazione è presente nel catalogo delle definizioni del malware. Se è così l'antivirus blocca l'esecuzione del programma o la memorizzazione del file.
- Il catalogo delle definizioni è continuamente aggiornato dalla casa produttrice dell'antivirus. Il catalogo delle definizioni presente nel computer che si intende proteggere deve essere allineato con frequenza(via internet) con il catalogo aggiornato dalla casa produttrice, in caso contrario l'antivirus perde di efficacia. L'allineamento del catalogo delle definizioni viene, di norma, eseguito automaticamente dall'antivirus all'avvio del computer.

Il catalogo delle definizioni è aggiornato dalla casa produttrice dell'antivirus DOPO che il malware è stato rilasciato. Per questo nessun antivirus può assicurare una protezione sicura al 100%

LE BACKDOOR

Le backdoor (“porta sul retro”) sono una specie di entrata di servizio nascosta agli occhi di tutti tranne a quelli del cracker.

Una volta installata, essa permette all’intruso di divenire utente amministratore del sistema in questione, e a nulla serve la modifica delle password in entrata o la soppressione di qualche account!!

COME DIFENDERSI

Una tecnica di difesa consiste nell'utilizzare **i file di log** che registrano i passaggi nel sistema e le modifiche da questo subito e che rappresentano il maggior pericolo per gli intrusi. Dopo aver installato la propria backdoor, un cracker sa che deve cancellare le tracce che ha inevitabilmente lasciato per poter attuare il suo piano!

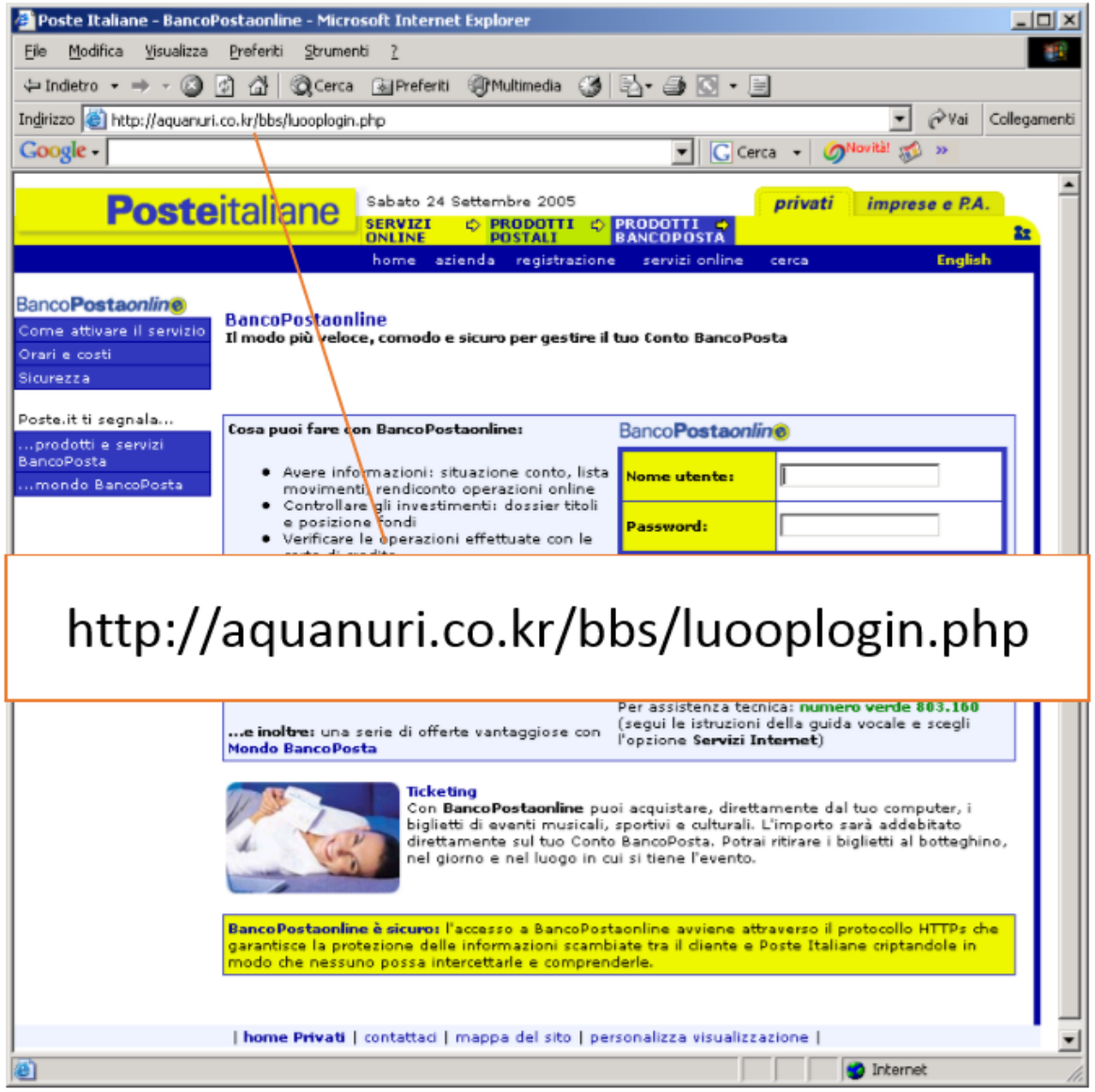
PHISHING

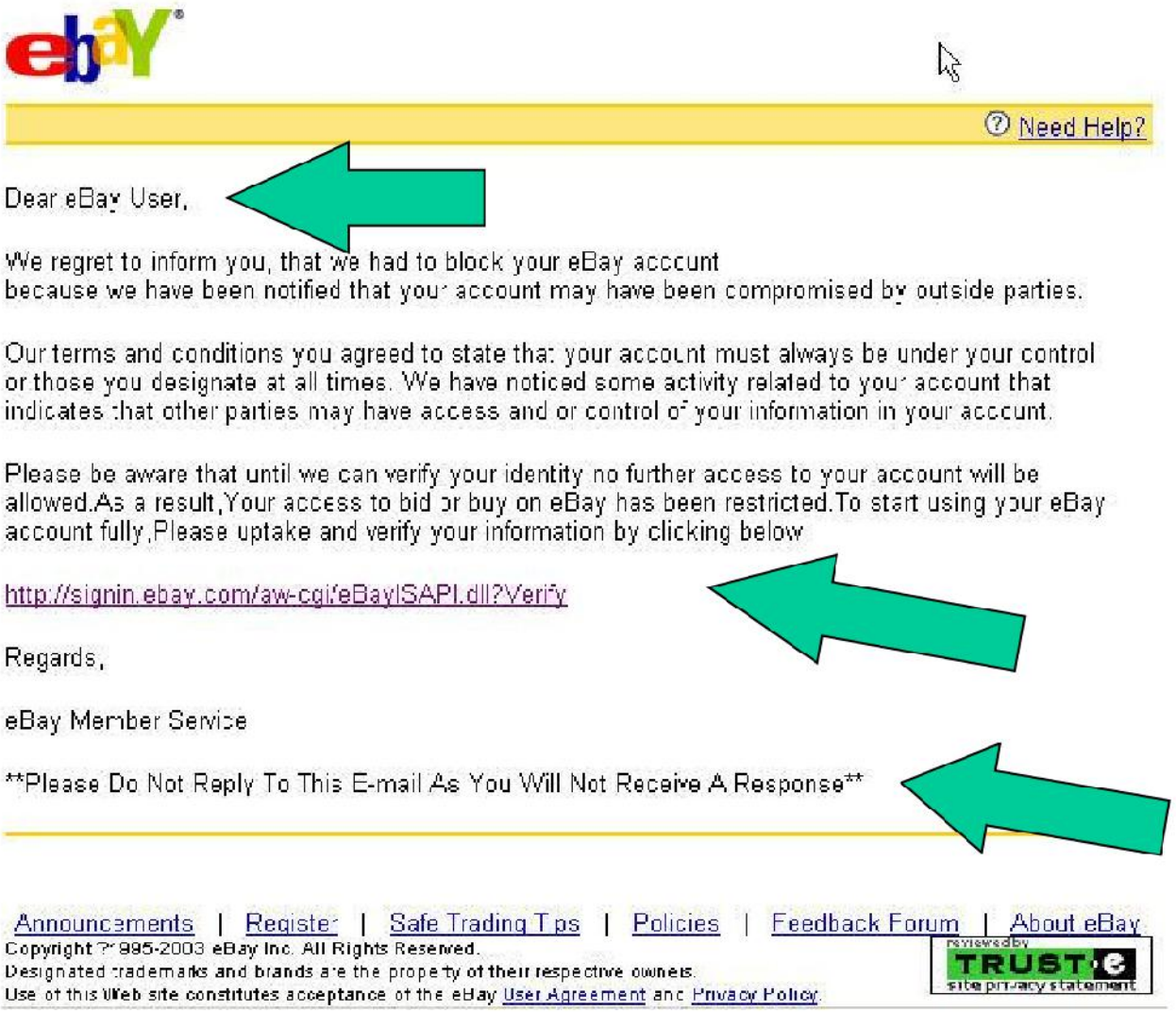
Falsi messaggi che sembrano arrivare da un sito affidabile e frequentato abitualmente
che arrivano nella casella di posta elettronica per ottenere i dati personali.

I truffatori acquistano la fiducia dell'utente attraverso messaggi di posta elettronica da siti che frequentiamo di solito, informandoli che a causa di problemi tecnici è necessario comunicare nuovamente i dati personali.

A quel punto il malcapitato utente viene mandato su una pagina web che sembra essere proprio quella della compagnia in questione ed è invitato a compilare un questionario dove, insieme ai dati anagrafici, vengono richiesti anche la password e il codice della carta di credito.

ESEMPI DI PHISHING





QUALCHE ESCA

- In allegato la notifica di vincita della UK lottery. Si prega di aprire l'allegato.
- Avete bisogno di un prestito? Offriamo i seguenti tipi di prestiti * Prestiti Personali * Business Prestiti * Prestito di consolidamento Prestito minimo è di €5,000. Contattaci subito per la tua forma del prestito
- Buongiorno, Si prega di notare che hai una fattura non pagata. Dettagli: *http://www.organoeorchestra.it/adviser/Confermata.zip*
- I am a dying woman from Switzerland who has decided to donate what I have to charity through you.
- Gentile utente, Monte dei Paschi. Il tuo ordine id:69979 viene elaborato, ma ha problemi. Controlla: *http://www.sulletracce.it/info/Dettagli.zip*

COME DIFENDERSI - DAL PHISHING

• **Eliminate sempre e senza esitazioni le e-mail** che hanno come allegato i file con estensione **.exe**;
Oppure se non si è certi dell'origine o non è presente l'oggetto.

Avast Antivirus, NOD 32, Avira Antivirus, Kaspersky e BitDefender sono degli ottimi antivirus per favorire la sicurezza al vostro dispositivo informatico.

• **Non installate sul proprio computer programmi passati da amici e conoscenti;** loro pur essendo in buona fede potrebbero passarvi virus informatici.

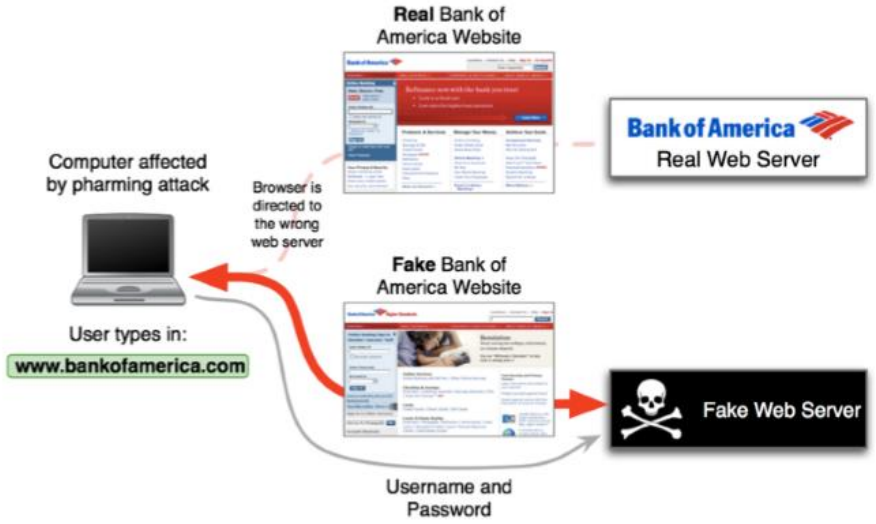
• **Non creare cartelle condivise con i propri dati personali.**

IL PHARMING

E’ una tecnica utilizzata per ottenere l'accesso ad informazioni personali e riservate, con varie finalità. Grazie a questa tecnica, l'utente è ingannato e portato a rivelare inconsapevolmente a sconosciuti i propri dati, come numero di conto corrente, nome utente, password, numero di carta di credito etc.

Esistono varie metodologie di attacco che comunque portano a modificare l’associazione tra l’URL della pagina web desiderata e l’IP del server web.

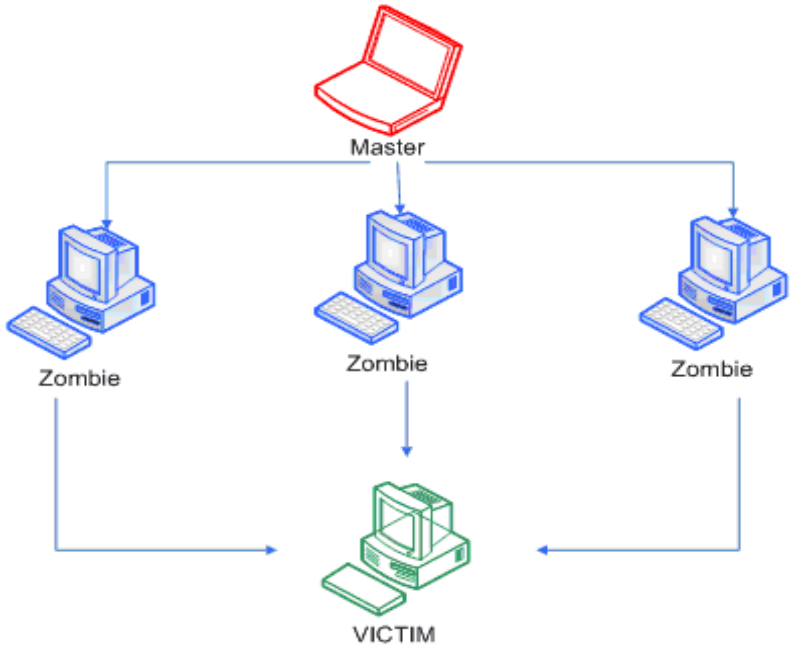
In altre parole l’utente digita nel browser un indirizzo corretto del tipo www.miabanca.it e il sistema DNS, che è stato violato, lo risolve verso il server web dell’organizzazione criminale che nel frattempo ha messo in linea una pagina web identica a quella della banca dell’utente.



DENIAL OF SERVICE

Nella sicurezza informatica **DoS**, è la sigla di **Denial of Service**, letteralmente *negazione del servizio*.

Si tratta di un malfunzionamento dovuto ad un attacco informatico in cui si esauriscono deliberatamente le risorse di un sistema informatico che fornisce un servizio, ad esempio un sito web, fino a renderlo non più in grado di erogare il servizio.



WI-FI

In telecomunicazione il termine **Wi-Fi** indica la tecnica e i relativi dispositivi che consentono a terminali di utenza di collegarsi tra loro attraverso una rete locale in maniera wireless (WLAN).

A sua volta la rete locale così ottenuta può essere allacciata alla rete Internet tramite un router ed usufruire di tutti i servizi di connettività offerti da un ISP(Ad esempio Alice, Fastweb).

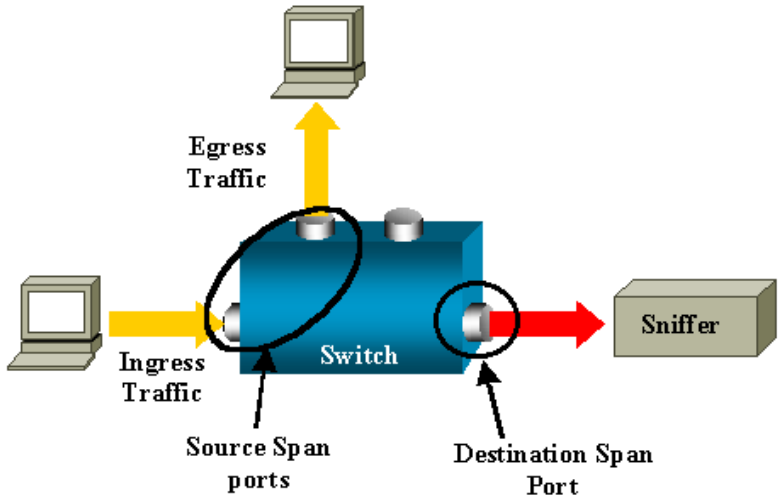
Qualunque dispositivo o terminale di utenza (computer, cellulare, palmare ecc.) può connettersi a reti di questo tipo se integrato con le specifiche tecniche del protocollo Wi-Fi.

SNIFFING

L'attività di intercettazione passiva dei dati che transitano in una rete telematica. Tale attività può essere svolta per scopi illeciti (intercettazione fraudolenta di password o altre informazioni sensibili).

I prodotti software utilizzati per eseguire queste attività vengono detti **sniffer** ed oltre ad intercettare e memorizzare il traffico offrono funzionalità di analisi del traffico stesso.

Gli sniffer intercettano i singoli pacchetti, decodificando le varie intestazioni di livello datalink, rete, trasporto, applicativo.
Inoltre possono offrire strumenti di analisi che analizzano ad esempio tutti i pacchetti di una connessione TCP per valutare il comportamento del protocollo di rete o per ricostruire lo scambio di dati tra le applicazioni.



PROTEZIONE DEI DATI PERSONALI

Informarsi prima di iniziare a navigare in un qualsiasi sito

Non aprire posta inviata da sconosciuti soprattutto se contiene allegati

Non accettare l'amicizia da persone sconosciute

Non memorizzare le password nei pc e cambiarle spesso

Attenzione ai keylogger, in grado di salvare ciò che digitiamo

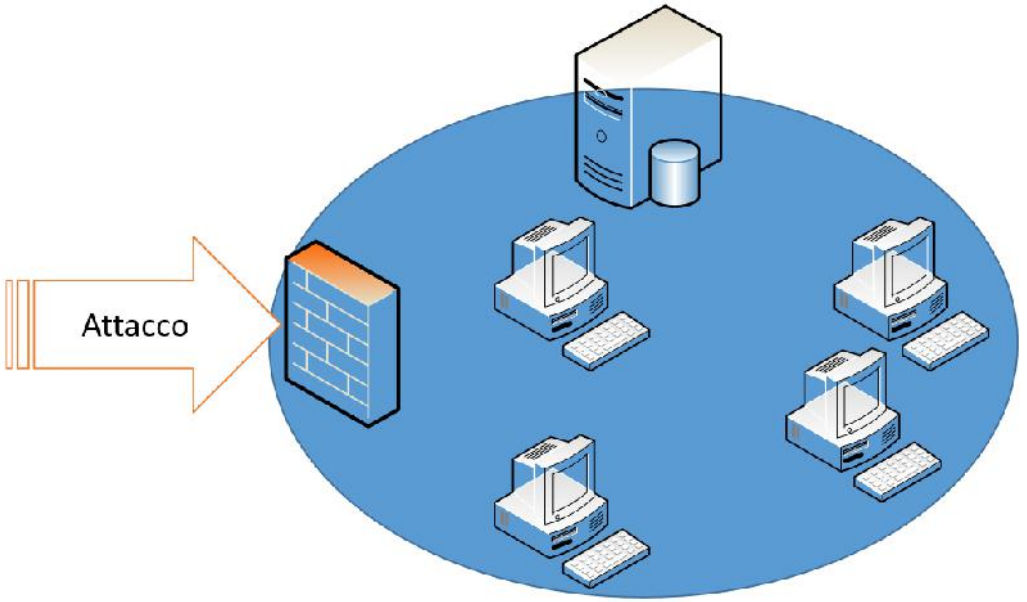
Non inserire i dati personali nei computer pubblici

Controllare periodicamente i processi attivi e in esecuzione sul pc

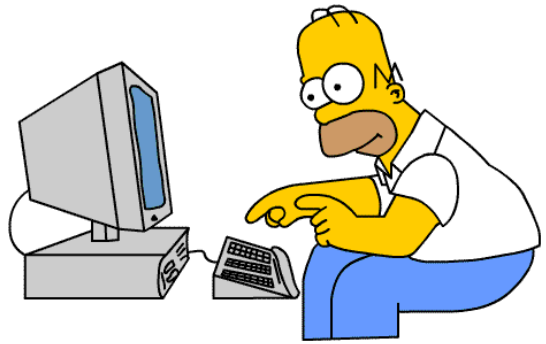
Aggiornare spesso i software

FIREWALL - PROTEZIONE PERIMETRALE

Il firewall è un apparato di rete hardware o un software che filtra i pacchetti entranti ed uscenti, da e verso una rete o un computer, secondo regole prestabilite. Configurando opportunamente le regole è possibile bloccare i pacchetti non desiderati cercando così di proteggere la rete o il singolo computer da attacchi diretti da parte di pirati informatici o da software che cercano di violare il sistema.



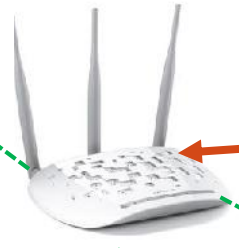
DIFFERENZA FIREWALL IPS



Porta 80 tcp

COME SONO LE INFRASTRUTTURE IT

Server



Access Point

Notebook

Switch

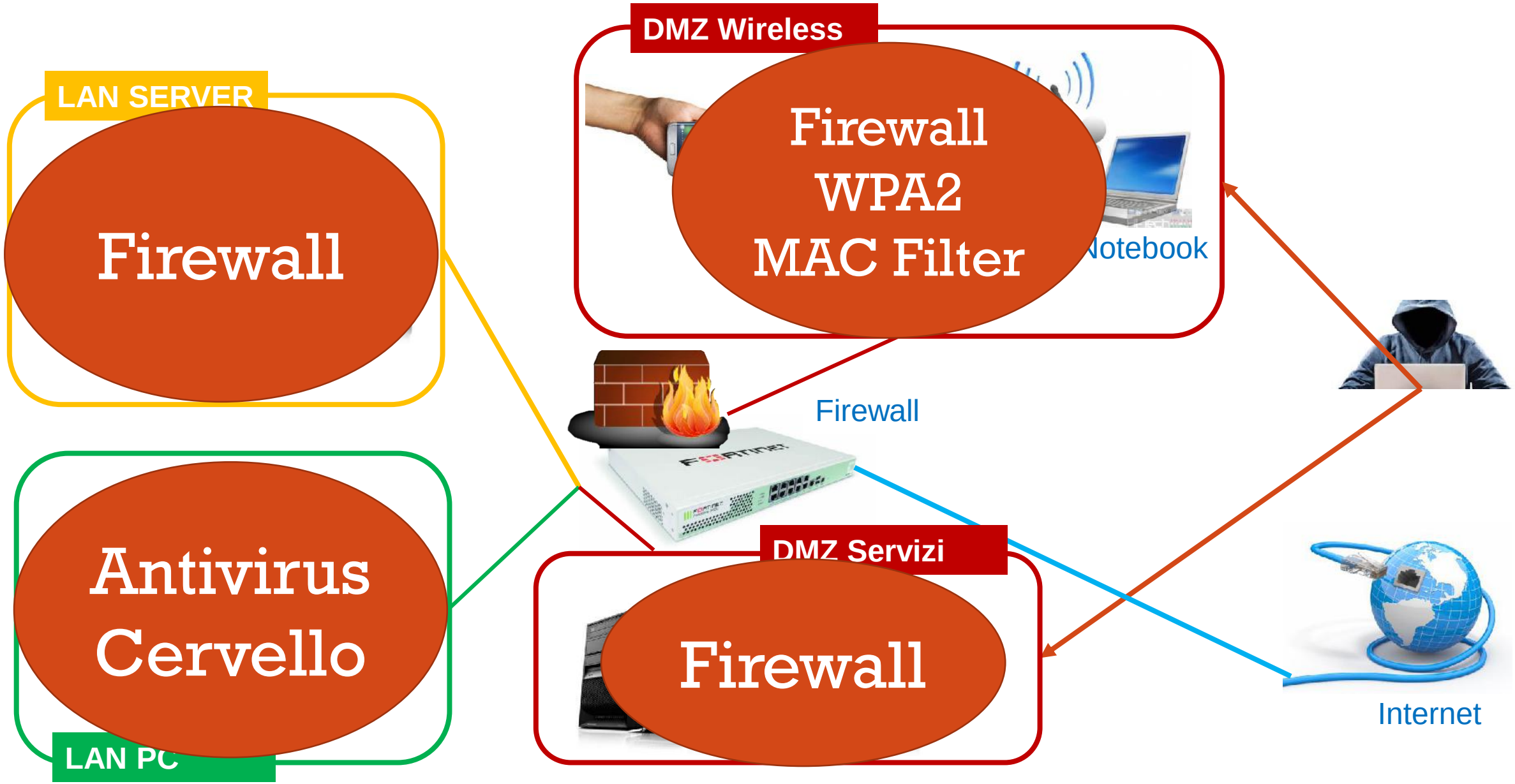
Personal Computer

Firewall

Internet

LAN

COME DOVREBBERO ESSERE LE INFRASTRUTTURE IT



RIEPILOGO

- Usare password sicure
- Installare Antivirus Avanzati
- Utilizzare i Firewall con IPS
- Non aprire email sconosciute o url sconosciuti
- Utilizzare il cervello