Parte 4
Sicurezza e Privacy

Sicurezza e Privacy

1. Difendere il proprio computer
2. Difendere se stessi
3. Difendere la propria professione

Difendere il proprio computer

Quale fra le seguenti precauzioni garantisce che nessun "computer malevolo" riesca a comunicare con il proprio PC?

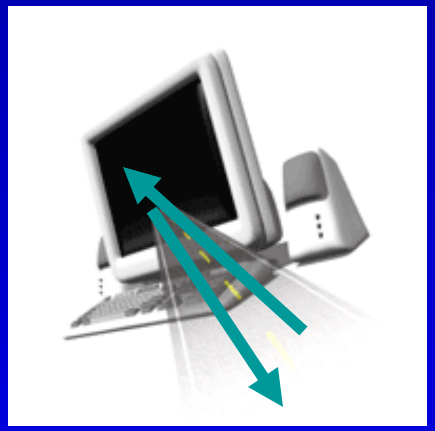
a) Non essere collegati tramite rete wireless
b) Non aprire alcun allegato di posta elettronica
c) Utilizzare un programma antivirus
d) Nessuna della precedenti

Quale, fra i seguenti "fenomeni", è rivelatore del fatto che il proprio computer è stato compromesso?

a) La password, sebbene oscurata, viene mostrata nella procedura di accesso al computer.
b) Se si accede ad un sito protetto, il browser mostra il messaggio "Questo sito ha inviato un certificato non attendibile"
c) Si viene a conoscenza di aver subito un furto di identità.
d) Tutte e tre le risposte

Premessa

- Ci sono più di 2 miliardi di utenti dei servizi Internet
- Tutti, potenzialmente, possono comunicare con il TUO computer, se collegato a Internet



- E, soprattutto, ciascuno di questi utenti può verificare se qualche “porta” del tuo computer è aperta, e entrare senza bussare

Riflessione

- Come cambierebbe il tuo comportamento (nel mondo) se sapessi che il tuo portafoglio, la tua casa e la tua cassetta della posta fossero accessibili a tutti, così come il tuo computer collegato ad Internet?

Possibili conseguenze di un “computer compromesso”

1. **Conseguenze sul tuo computer**
   - Difficoltà operative
   - Controllo/furto/danneggiamento di email e documenti
   - Controllo e possibilità di transazioni finanziarie illecite (a tuo nome)
   - Furto di identità (nuova frontiera negli USA!)

2. **Uso criminale del tuo computer per altri fini (*potrebbe essere rilevante a livello civile e penale*)**

Come te ne accorgi

Sperimenti…

- Ritardi inusuali nell'accensione del computer
- Computer che "va estremamente lento"
- Vi sono (molti) file corrotti, inaccessibili o mancanti
- Non riesci ad accedere ai tuoi dati sul disco o al disco stesso
- Il computer ha improvvisi (e frequenti) messaggi di memoria insufficiente
- Perdi completamente il controllo del tuo computer

- ***Ma potrebbe anche darsi che non sperimenti alcun sintomo e sei del tutto inconsapevole che il tuo computer è stato compromesso***

Quale fra le seguenti precauzioni garantisce che nessun "computer malevolo" riesca a comunicare con il proprio PC?

a) Non essere collegati tramite rete wireless
b) Non aprire alcun allegato di posta elettronica
c) Utilizzare un programma antivirus
d) Nessuna della precedenti

Quale, fra i seguenti "fenomeni", è rivelatore del fatto che il proprio computer è stato compromesso?

a) La password, sebbene oscurata, viene mostrata nella procedura di accesso al computer.
b) Se si accede ad un sito protetto, il browser mostra il messaggio "Questo sito ha inviato un certificato non attendibile"
c) Si viene a conoscenza di aver subito un furto di identità
d) Tutte e tre le risposte

Quale/i fra le seguenti azioni rischia/no di diminuire la sicurezza del proprio computer?

a) Lasciare incustodito il computer acceso
b) Condividere informazioni (password e account)
c) Aggiornare il sistema operativo (patches) e il software antivirus
d) Aprire allegati contenuti in e-mail provenienti da sconosciuti

Quale tra i seguenti è un errore da evitare se si vuol cooperare alla sicurezza del proprio e computer e di quello dei colleghi di lavoro?

a) Non riportare violazioni di sicurezza
b) Non condividere password e account con i colleghi
c) Non condividere password e account con l'amministratore
d) Aggiornare il software

Cosa fare?

- La maggior parte di incidenti può essere prevenuto
- Essere preparati a:
  - Proteggersi (“Protect”)
  - Riconoscere (“Detect”)
  - Reagire (“React”)

Se non tu, chi?

Se non ora, quando?

PROTECT: Evitare errori comuni

- Usare password “banali”
- Lasciare incustodito il computer acceso
- Aprire allegati di e-mail da sconosciuti
- Non usare un software anti-virus
- Perdere (anche temporaneamente) il portatile
- Condividere informazioni (password e account)
- Non riportare violazioni di sicurezza
- Non aggiornare il sistema operativo (*patch*) e il software antivirus

Quale/i fra le seguenti azioni rischia/no di diminuire la sicurezza del proprio computer?

a) Lasciare incustodito il computer acceso

b) Condividere informazioni (password e account)

c) Aggiornare il sistema operativo (patches) e il software antivirus

d) Aprire allegati contenuti in e-mail provenienti da sconosciuti

Quale tra i seguenti è un errore da evitare se si vuol cooperare alla sicurezza del proprio e computer e di quello dei colleghi di lavoro?

a) Non riportare violazioni di sicurezza

b) Non condividere password e account con i colleghi

c) Non condividere password e account con l'amministratore

d) Aggiornare il software

Quale delle seguenti soluzioni ci permette di ottenere la password più sicura?

a) Utilizzare almeno 8 caratteri casuali tra cui lettere maiuscole, minuscole e numeri

b) Scegliere una parola di una lingua straniera

c) Scegliere un nome di persona breve e mnemonico per non doverlo scrivere su un foglio e correre così il rischio di perderlo

d) Utilizzare l'anno di nascita seguito dal nome o dal cognome, ma non da entrambi

Se si dimentica la password di autenticazione presso i sistemi di Ateneo:

a) La si può chiedere per telefono (o comunque mediante un messo diverso dalla posta elettronica) all'amministratore di sistema, che può leggerla direttamente

b) La si può chiedere all'amministratore che, dopo aver rimosso la protezione cifrata, la comunica all'interessato

c) Si può utilizzare un programma per il recupero delle password perdute

d) Si può chiedere all'amministratore di azzerare la password precedente e di ottenerne una nuova

Account e Password: FARE

- **Scegliere una password che non può essere indovinata** (es., un acronimo di una frase con qualche numero inserito a caso)
- **Cambiare la password "con una certa frequenza" e comunque tutte le volte in cui si sospetti che qualcuno l'abbia vista o sentita**
- **Spegnere il computer alla fine della giornata**
- **Usare il *desktop locking* durante il giorno** (es., uno screen saver con password per il ri-accesso)
- (Nel caso in cui si sia dimenticata) chiedere all'amministratore l'azzeramento della password e reimpostarne subito una

Account e Password: NON FARE

- **Diffondere la password (MAI dare la propria password al telefono, neanche a Help Desk o assistenza!)**
- **Consentire a qualcuno di accedere con il tuo account+password**
- **Scrivere la password e attaccarla con Post-It sulla tastiera, mouse-pad, monitor, o portapenne**
- **“Save this Password” nel browser (chi abbia accesso al tuo computer potrebbe “farsi passare per te”)**
- **Cercare informazioni “sensibili” per conto di altri che non ne sarebbero autorizzati e tanto meno farlo per persone al telefono!**
- (Nel caso in cui si sia dimenticata) chiedere all'amministratore di inviarne una nuova via posta elettronica o di comunicarla per telefono

Quale delle seguenti soluzioni ci permette di ottenere la password più sicura?

a) Utilizzare almeno 8 caratteri casuali tra cui lettere maiuscole, minuscole e numeri

b) Scegliere una parola di una lingua straniera

c) Scegliere un nome di persona breve e mnemonico per non doverlo scrivere su un foglio e correre così il rischio di perderlo

d) Utilizzare l'anno di nascita seguito dal nome o dal cognome, ma non da entrambi

Se si dimentica la password di autenticazione presso i sistemi di Ateneo:

a) La si può chiedere per telefono (o comunque mediante un messo diverso dalla posta elettronica) all'amministratore di sistema, che può leggerla direttamente

b) La si può chiedere all'amministratore che, dopo aver rimosso la protezione cifrata, la comunica all'interessato

c) Si può utilizzare un programma per il recupero delle password perdute

d) Si può chiedere all'amministratore di azzerare la password precedente e di impostarne una nuova

Tipicamente un virus si diffonde:

a) Aprendo file allegati ricevuti via e-mail
b) Ricevendo posta da un computer infetto
c) Copiando software non protetto da copyright
d) Inviando posta a un computer infetto

Quali sono gli elementi che caratterizzano email con allegati sospetti?

a) La provenienza, che è sempre (falsamente) da qualcuno che si conosce
b) Il tono, sempre perentorio del messaggio
c) In realtà non ci sono elementi di valutazione
d) Il testo breve e generico

Se siete stati inseriti in una mailing list senza vostra esplicita richiesta, dovete:

a) chiedere di essere rimossi cliccando il link “Remove from this mailing list” che ogni amministratore serio deve prevedere
b) evitare di rispondere ai messaggi fraudolenti
c) in ogni caso non rispondere ad alcuno di tali messaggi
d) eseguire preferibilmente tutte e tre le azioni indicate sopra

Sicurezza nell'e-mail: FARE

- Installare e usare software anti-virus aggiornato
- Assicurarsi dal testo della mail, dallo scopo e dal mittente se è il caso di aprire un allegato (*attachment*)
- Segnalare all'assistenza tecnica tutte le e-mail con contenuti offensivi, osceni e che richiedono informazioni personali (su di te o su altri)
- Cancellare tutte le e-mail di pubblicità non richiesta SENZA RISPONDERE (no reply).

  RICORDARSI che le istruzioni riportate "to remove you from the mailing list" spesso servono per conferma che l'account di e-mail è funzionante

Sicurezza nell'e-mail: NON FARE

- Aprire (*click on*) attachment o link Web inviati in e-mail di cui non si conosce la sorgente
- Considerare le e-mail come se fossero diverse da una "cartolina". La e-mail NON è un messaggio privato, a meno che non sia crittografato
- Inviare identificativi e password in un messaggio di e-mail
- Inviare messaggi offensivi, insultanti, minacciosi, osceni, ecc.
- Inviare dati personali (es., nome, account, indirizzo di casa, foto) a qualcuno non noto personalmente

Aprire o no un allegato?
Cliccare o no su un link?

REGOLA: Se l'allegato è sospetto, non aprirlo!

Se il link è sospetto non cliccarlo!

PROBLEMA: Come rendersene conto?

1. Guardare il mittente della mail
2. Se non lo conosci: non aprire, non cliccare
3. Se lo conosci, chiediti: il testo della mail corrisponde al tono, al modo di rivolgersi di quella persona?
4. No: non aprire, non cliccare
5. Sì: si può assumere il rischio

Attenzione, però, ai testi molto brevi (es., «guarda queste foto», «ho scoperto un sito fantastico», ecc.) che potrebbero impedire un vero controllo del punto 3

Tipicamente un virus si diffonde:

a) Aprendo file allegati ricevuti via e-mail

b) Ricevendo posta da un computer infetto

c) Copiando software non protetto da copyright

d) Inviando posta a un computer infetto

Quali sono gli elementi che caratterizzano email con allegati sospetti?

a) La provenienza, che è sempre (falsamente) da qualcuno che si conosce

b) Il tono, sempre perentorio del messaggio

c) In realtà non ci sono elementi di valutazione

d) Il testo breve e generico

Se siete stati inseriti in una mailing list senza vostra esplicita richiesta, dovete:

a) chiedere di essere rimossi cliccando il link “Remove from this mailing list” che ogni amministratore serio deve prevedere

b) evitare di rispondere ai messaggi fraudolenti

c) in ogni caso non rispondere ad alcuno di tali messaggi

d) eseguire preferibilmente tutte e tre le azioni indicate sopra

È bene che l’antivirus sia aggiornato:

a) Solo quando si aggiungono nuovi programmi
b) Frequentemente, anche una volta al giorno
c) Frequentemente, cioè una o due volte al mese
d) Quando si aggiorna il sistema operativo

Quale, fra i seguenti, non è un tipo di virus informatico:

a) Retrovirus di rete
b) Bomba logica
c) Bufala (Hoax)
d) Cavallo di Troia

Virus

- I **virus informatici** sono dei programmi (tipicamente molto piccoli) realizzati da …… che sono in grado di replicarsi e di diffondersi in modo autonomo da un computer all'altro
- I virus non sono nati o causati da Internet, ma certamente lo sviluppo di Internet ha aggravato il potenziale di diffusione

- I primi sintomi di malfunzionamento o funzionamento diverso dal normale dovrebbe già mettere in allerta
- Come nel caso dei virus non informatici, l'intervento tempestivo è la medicina migliore
- È Importante aggiornare frequentemente il software antivirus, anche giornalmente!

Alcuni tipi di virus

- **Bomba logica: il virus si presenta come una qualsiasi applicazione informatica, ma ha al suo interno una funzione ostile che, tipicamente, si attiva dopo un certo tempo. Può essere molto distruttivo (es., cancellare l'intero contenuto del disco)**
- **Cavallo di Troia: Programma che è collegato ad un altro file innocuo, che viene scaricato o installato dallo stesso utente. Una volta installato sul computer, può avere vari effetti dannosi, come, ad esempio :**

  informare il creatore (o diffusore) quando si attiva una connessione Internet, consentendogli di accedere al computer stesso (in modo manifesto, distruttivo, o anche in modalità nascosta)

HOAX ("bufala")

Chain Letters (In Italia, nota anche come "Catena di Sant'Antonio") – Una mail che richiede al destinatario di inoltrarla al maggior numero di persone che conosce (spesso collegata a opere caritatevoli, promozioni commerciali, …)

Virus Hoax – Un caso particolare del precedente: mail di allerta che avvisa di un nuovo pericolosissimo virus. Richiede all'utente di diffondere l'avviso al maggior numero di persone che conosce

➔ Il virus è la mail stessa! Non perché contiene un virus, ma perché tende ad intasare le mailbox

False Alarms – Un messaggio (volutamente errato) che indica che un certo file risulta infettato da un virus

È bene che l’antivirus sia aggiornato:

a) Solo quando si aggiungono nuovi programmi

b) Frequentemente, anche una volta al giorno

c) Frequentemente, cioè una o due volte al mese

d) Quando si aggiorna il sistema operativo

Quale, fra i seguenti, non è un tipo di virus informatico:

a) Retrovirus di rete

b) Bomba logica

c) Bufala (Hoax)

d) Cavallo di Troia

Lo spyware è:

a) un software che non può essere installato senza il permesso dell'utente

b) un software che spia e registra i dettagli di utilizzo del computer

c) un tempo indicava un software che si collegava periodicamente ad Internet via linea telefonica mediante chiamata addebitata all'utenza domestica.

d) un programma tipicamente utilizzato da agenzie governative di intelligence per spiare nemici e amici.

Quale, fra i seguenti, non è un segnale che indica che il PC è stato infettato da uno spyware?

a) Compaiono pop-up pubblicitari sullo schermo

b) La home page del browser appare modificata

c) Compare una nuova toolbar nel browser che non si riesce ad eliminare

d) Si sperimenta una perdita continua di dati

Spyware

- **Spyware è un termine generale con cui si definisce certo software utilizzato per scopi fraudolenti con diversa rilevanza:**
  - Reperire informazioni personali per scopi pubblicitari
  - Reperire informazioni (personali, password, numero carta di credito, software utilizzato, ecc.)
  - Modificare la configurazione del computer
  - Tracciare tutte le azioni o tracciare solo l'uso di determinati servizi Internet (es., pagine Web visitate)

  Tutto senza chiedere il consenso

Problemi con Spyware

- **Software che raccoglie informazioni su di te e sull'uso del tuo computer**
- **Potrebbe anche essere vista come una cosa positiva.** Es., Ti iscrivi ad un servizio di musica, lo spyware prende nota, e arriva molta più pubblicità di natura musicale
- **La maggior parte, tuttavia, sono molto negativi:**
  - Raccogliere le password, numero di carte di credito, conto corrente, ecc.

ESEMPIO

Programmi Toolbar → una volta installati, possono essere configurati per raccogliere qualsiasi informazione: tasti battuti, siti Web visitati, nomi e password

ANCHE SE VENGONO RIMOSSI, lasciano delle "briciole"

che consentono la re-installazione automatica

Problemi con Spyware

- Tutta l'informazione trasmessa via Web può essere intercettata (a meno di utilizzare connessioni sicure con trasmissioni cifrate)
- Alcuni siti, senza autorizzazione, sono in grado di aggiungersi al desktop, all'elenco dei siti preferiti, o addirittura sostituirsi alla homepage (hijacking)
- Tutta l'attività del browser può essere tracciata e monitorata
- Informazioni personali possono essere trasmesse o vendute a terze parti senza necessità di consenso e in modo del tutto inconsapevole
- Questi componenti malevoli non solo mettono a repentaglio la privacy, ma la stessa integrità del computer, oltre a diminuire l'efficienza (occupano spazio disco, memoria e rallentano le prestazioni)

Come accorgersi di avere uno spyware

- Si vedono pop-up pubblicitari che appaiono sullo schermo, anche quando non si sta navigando
- La home page del browser o altre opzioni sono state modificate senza consenso
- Si nota una nuova toolbar nel browser che non è stata installata esplicitamente e che non si riesce ad eliminare
- Il computer impiega più del necessario ad eseguire alcune operazioni
- Si sperimentano improvvisi crash del computer (es., blocco della tastiera o riavvio inaspettato del computer o di qualche applicazione)

Azioni da compiere

- **L'anti-virus è indispensabile sia per proteggere noi dagli altri sia per proteggere gli altri da noi**

- **Con la diffusione continua di nuovi virus, purtroppo, non si può essere mai sicuri che non si verrà infettati**
- **Tuttavia, si possono ridurre le probabilità di infettarsi**
  - **→Prendendo continuamente nuovi "vaccini"**
- **La frequenza giornaliera nell'aggiornamento non è da "paranoici": è la medicina migliore!**

Difese

- **Bisogna installare un *antivirus* e bisogna tenerlo continuamente aggiornato (anche quotidianamente)**
- **Bisogna installare un *antispyware* e tenerlo aggiornato. Es.,**
  - Spybot Search and Destroy

    http://spybot.eon.net.au/index.php?lang=en&page=start
  - Ad-Aware (da Lavasoft)

    http://www.lavasoftusa.com/software/adaware/
- **E' opportuno installare un *personal firewall***
- **Alternative da considerare: rivolgersi a computer con sistemi operativi meno soggetti a attacchi. Es.,**
  - *Macintosh*
  - *Linux (p.es., Ubuntu è molto semplice da installare)*

Lo spyware è:

a) un software che non può essere installato senza il permesso dell'utente

b) un software che spia e registra i dettagli di utilizzo del computer

c) un tempo indicava un software che si collegava periodicamente ad Internet via linea telefonica mediante chiamata addebitata all'utenza domestica.

d) un programma tipicamente utilizzato da agenzie governative di intelligence per spiare nemici e amici.

Quale, fra i seguenti, non è un segnale che indica che il PC è stato infettato da uno spyware?

a) Compaiono pop-up pubblicitari sullo schermo

b) La home page del browser appare modificata

c) Compare una nuova toolbar nel browser che non si riesce ad eliminare

d) Si sperimenta una perdita continua di dati

Una porta di comunicazione TCP/IP è:

a) un programma che filtra i messaggi in arrivo da Internet sulla base del contenuto

b) lo strumento che permette ad un calcolatore di effettuare più connessioni contemporanee verso altri calcolatori in Internet

c) un'aperrtura fisica nel case del computer per il collegamento di vari dispositivi (es. USB)

d) nessuna delle precedenti

Un firewall è:

a) Un dispositivo hardware installato tra la rete e il computer per esaminare e filtrare i dati in entrata e in uscita

b) Un dispositivo che si interpone tra Internet e il computer (o la LAN) per filtrare i dati in entrata e in uscita secondo regole concordate

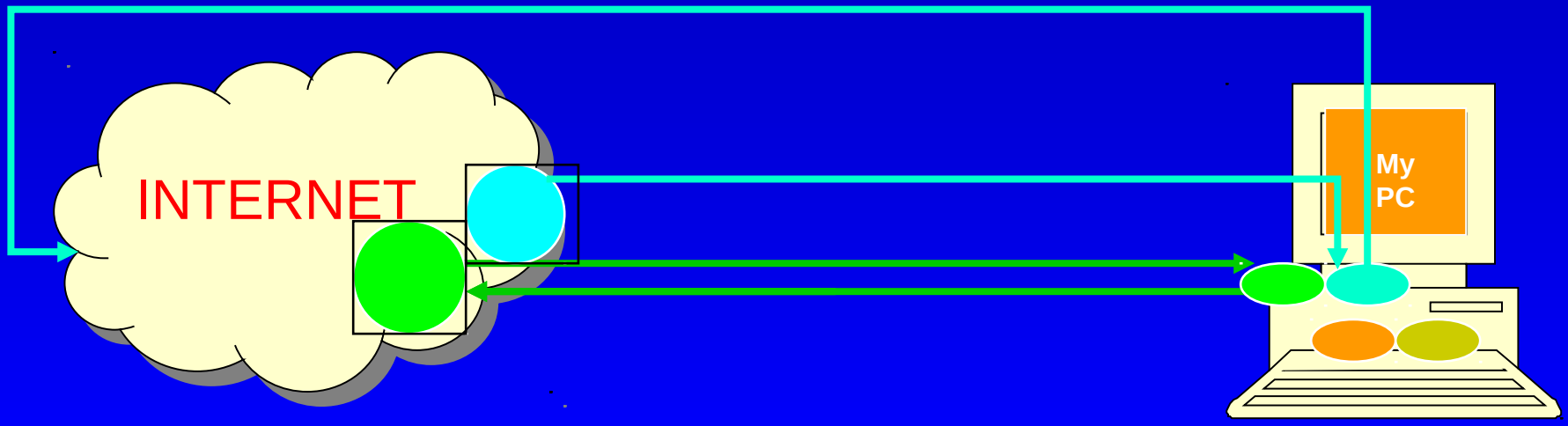
c) Un dispositivo hardware che si installa su una rete locale (LAN) per collegarla a Internet

d) Un software di difesa del computer, sinonimo di antivirus

Comunicazione tra programmi

Ciascuna comunicazione in Internet avviene tra programmi in esecuzione sue due computer. Viene identificata dalla quadrupla:

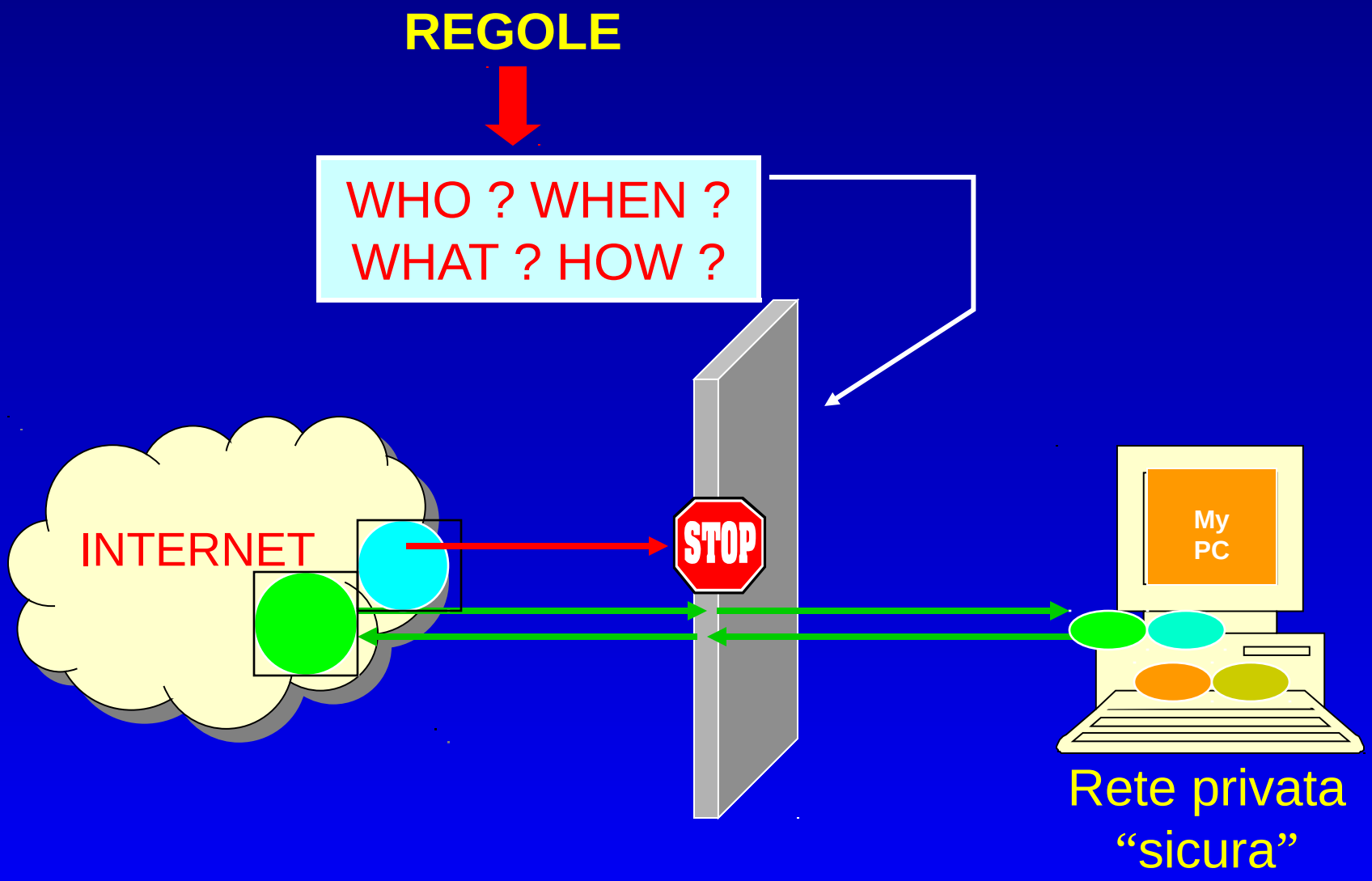
- **indirizzo IP mittente**
- **indirizzo IP destinatario**
- **porta mittente**
- **porta destinatario**



Compiti di un firewall

- Il firewall è un software che ispeziona ciascun pacchetto (“porzioni di messaggio”) non appena arriva alla macchina – PRIMA che il pacchetto venga trasmesso ad altro software che è in esecuzione sul computer
- Il firewall ha potere di veto su tutto ciò che il computer riceve da Internet
- Una “porta” TCP/IP è “aperta” sul computer solo se il primo pacchetto del mittente che chiede una connessione, riceve una risposta dal computer destinatario.
- Se, invece, la “porta è chiusa”, il pacchetto in arrivo viene semplicemente ignorato e scomparirà da Internet. Significa che non è possibile utilizzare quel servizio Internet sul tuo computer

Come funziona



Una porta di comunicazione TCP/IP:

a) un programma che filtra i messaggi in arrivo da Internet sulla base del contenuto

b) lo strumento che permette ad un calcolatore di effettuare più connessioni contemporanee verso altri calcolatori in Internet

c) un'aperrtura fisica nel case del computer per il collegamento di vari dispositivi (es. USB)

d) nessuna delle precedenti

Un firewall è:

a) Un dispositivo hardware installato tra la rete e il computer per esaminare e filtrare i dati in entrata e in uscita

b) Un dispositivo che si interpone tra Internet e il computer (o la LAN) per filtrare i dati in entrata e in uscita secondo regole concordate

c) Un dispositivo hardware che si installa su una rete locale (LAN) per collegarla a Internet

d) Un software di difesa del computer, sinonimo di antivirus

Difendere se stessi

Quale fra i seguenti non rappresenta un rischio che richiede difesa personale?

a) Furto di identità
b) Denial of service
c) Spam
d) Truffa on-line

Perché esiste un problema di tutela della identità personale?

a) perché il furto di identità è il primo atto per perpetrare frodi
b) perché il furto di identità è il primo atto per ottenere informazioni di interesse commerciale
c) perché l'identità è un dato sensibile
d) la domanda è tendenziosa perché non è possibile scambiare identità, almeno non nei contesti che potrebbero interessare i criminali (es. banche)

Rischi

- Furto di identità
- SPAM
- Truffe on-line
- Privacy(?) delle mail
- Adescamento
- Cyber-stalking e cyber-bullismo
- Incancellabilità del materiale “postato” sul Web
- …

Problemi

- **Incompetenza tecnica dei circa 2 miliardi di utente**

- **Inadeguatezza generazionale → per la prima volta nella storia umana, “i genitori ne sanno di meno dei figli” e quindi non sanno dare giusti consigli**

Identità

- L’identità è un bene prezioso, da proteggere con cura
- Dimostrare la propria identità è indispensabile per aprire conti correnti, ottenere carte di credito, prestiti e mutui, acquistare beni e servizi
- Ma impossessarsi dell’identità altrui e usarla a loro danno è più facile di quanto si creda per i delinquenti comuni come per i cybercriminali
- E rubare l’identità è quasi sempre il punto di partenza per perpetrare queste frodi

Identità digitale

Chi siamo nel mondo digitale?

Quasi sempre una login + password

Ma oggi anche:

- Nome/cognome
- Indirizzo
- Data di nascita
- Codice fiscale
- Numero di carta di identità o di patente
- Numero di carta di credito
- PIN del bancomat
- Numero di conto corrente
- …

Le due regole d’oro

- **La testa**

  Non fornire questi dati con leggerezza

- **La tecnologia**

  Verificare che la connessione sia sicura: https e non http evidenziata anche da un lucchetto giallo (in alto su Explorer, in basso a destra Firefox)

Crescita del fenomeno

- **Il fenomeno delle frodi creditizie mediante *furto di identità* è in preoccupante aumento anche in Italia**
  - 2005: oltre 11.000 i tentativi di frode creditizia, per un ammontare di 47 milioni di euro
  - 2006: oltre 24.000, per un importo complessivo di oltre 100 milioni di euro
  - Crescita del 37% nel 2008 rispetto al 2007
  - Più di 30 milioni di persone/dati coinvolti negli Stati Uniti (il 10% della popolazione!)

Scopi

- Controllare i conti finanziari
- Aprire un nuovo conto corrente
- Richiedere un prestito
- Richiedere una nuova carta di credito
- Acquistare beni e servizi sul Web
- Noleggiare auto
- Affittare appartamenti
- Firmare contratti con compagnie telefoniche e di servizi

Quale fra i seguenti non rappresenta un rischio che richiede difesa personale?

a) Furto di identità
b) Denial of service
c) Spam
d) Truffa on-line

Perché esiste un problema di tutela della identità personale?

a) perché il furto di identità è il primo atto per perpetrare frodi
b) perché il furto di identità è il primo atto per ottenere informazioni di interesse commerciale
c) perché l'identità è un dato sensibile
d) la domanda è tendenziosa perché non è possibile scambiare identità, almeno non nei contesti che potrebbero interessare i criminali (es. banche)

Il phishing si verifica quando:

a) Qualcuno mette fuori uso il vostro computer subissandolo di richieste attraverso la rete

b) Qualcuno cerca di ingannarvi per far sì che comunichiate volontariamente vostre informazioni personali

c) Qualcuno cerca di entrare nel vostro computer utilizzando un'applicazione apparentemente innocua

d) Nessuna delle precedenti

Quale fra le seguenti non è una tecnica usata per rubare l'identità digitale?

a) Spamming

b) Spyware

c) Trojan

d) Spoofing

10 metodi per rubare l’identità

- Social engineering
- Phishing
- Pharming
- Trojan
- Spyware
- Keylogging
- Spoofing
- Attacco man-in-the-middle
- Vishing

Phishing

- **Non è un virus, ma delle modalità fraudolente per ottenere informazioni personali**

  → Obiettivo: Furto di credenziali di accesso

- **Può capitare a chiunque…**
- **Vedere http://www.antiphishing.org per una interessante serie di esempi.**

Esempio di phishing

Need Help?

Dear eBay User,

We regret to inform you, that we had to block your eBay account
because we have been notified that your account may have been compromised by outside parties.

Our terms and conditions you agreed to state that your account must always be under your control or those you designate at all times. We have noticed some activity related to your account that indicates that other parties may have access and or control of your information in your account.

Please be aware that until we can verify your identity no further access to your account will be allowed.As a result,Your access to bid or buy on eBay has been restricted.To start using your eBay account fully,Please uptake and verify your information by clicking below

http://signin.ebay.com/aw-cgi/eBayISAPI.dll?Verify

Regards,

eBay Member Service

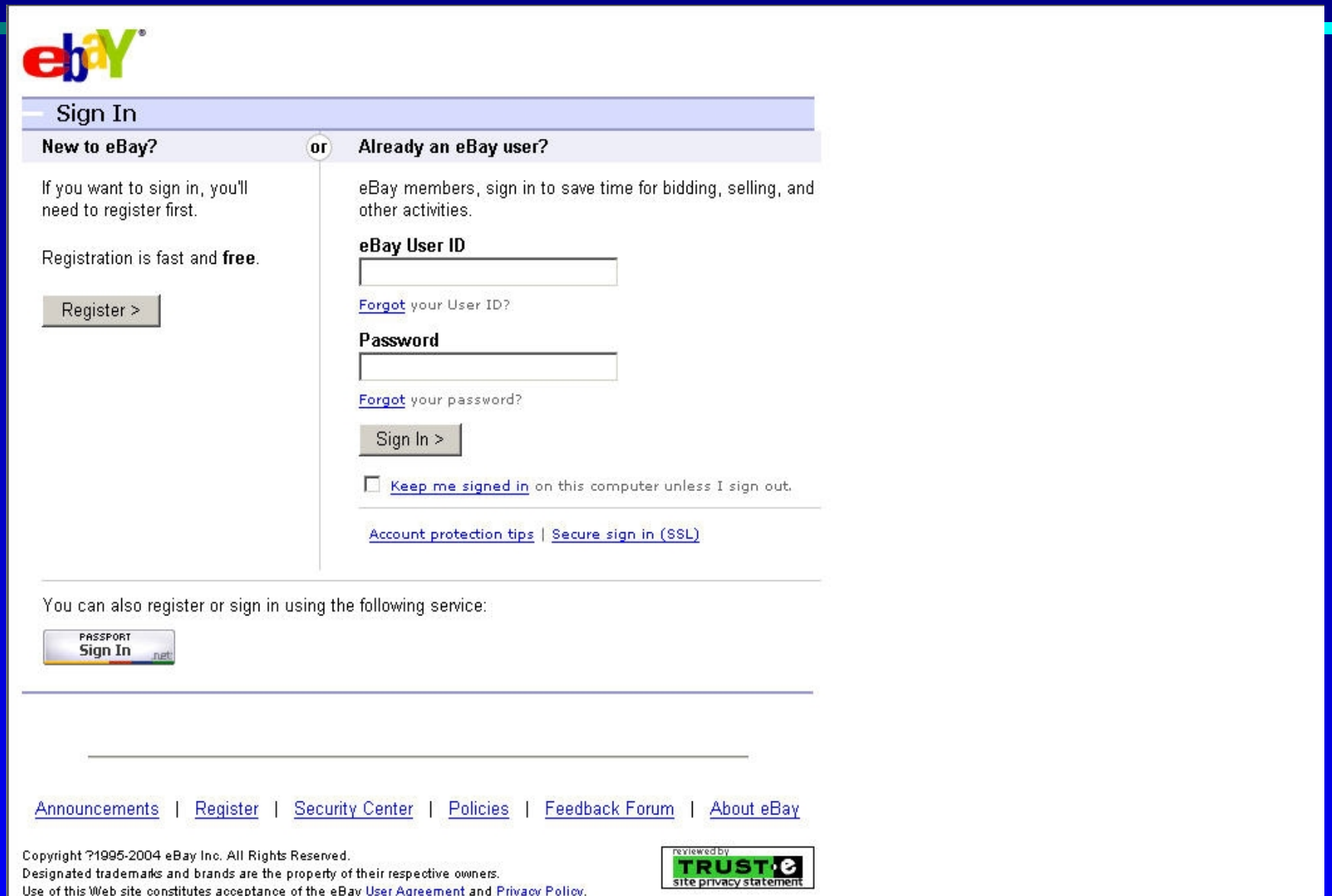
Please Do Not Reply To This E-mail As You Will Not Receive A Response

Announcements | Register | Safe Trading Tips | Policies | Feedback Forum | About eBay

Copyright ?1995-2003 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy.

reviewed by TRUSTe site privacy statement

Esempio di phishing



Sign In

New to eBay? or Already an eBay user?

If you want to sign in, you'll need to register first.

Registration is fast and **free**.

Register >

eBay members, sign in to save time for bidding, selling, and other activities.

eBay User ID

Forgot your User ID?

Password

Forgot your password?

Sign In >

Keep me signed in on this computer unless I sign out.

Account protection tips | Secure sign in (SSL)

You can also register or sign in using the following service:

PASSPORT Sign In .net

Announcements | Register | Security Center | Policies | Feedback Forum | About eBay

Copyright ?1995-2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy.

reviewed by TRUSTe site privacy statement

Il phishing si verifica quando:

a) Qualcuno mette fuori uso il vostro computer subissandolo di richieste attraverso la rete

b) Qualcuno cerca di ingannarvi per far sì che comunichiate volontariamente vostre informazioni personali

c) Qualcuno cerca di entrare nel vostro computer utilizzando un'applicazione apparentemente innocua

d) Nessuna delle precedenti

Quale fra le seguenti non è una tecnica usata per rubare l'identità digitale?

a) Spamming

b) Spyware

c) Trojan

d) Spoofing

Che cosa è lo spamming?

a) L'invio di messaggi email non richiesti o non desiderati
b) Un inutile fatica (per chi la effettua) che comunque mette spesso in crisi le comunicazioni
c) Una tecnica di attacco nota anche col il sinonimo scam
d) Tutte le precedenti

Una buona misura anti-spam consiste nel:

a) utilizzare un solo indirizzo email
b) utilizzare un indirizzo che non include il proprio nome e cognome
c) utilizzare solo webmail
d) utilizzare almeno 3 indirizzi email

Software antispam:

a) interviene bloccando le email indesiderate nel server del mittente
b) non può essere utilizzato se si usa un client di posta (anziché webmail)
c) può essere utilizzato sia da utenti finali sia da amministratori di sistema
d) è comunque inutile se si utilizzano altre precauzioni (non rispondere ai messaggi di spam, non inoltrare spam,...)

SPAM

- Origini da una scenetta del Monty Python Flying Circus (la carne in scatola Spam)

➔ Azione di diffondere in modalità broadcast (cioè, a tutti i possibili utenti di posta elettronica) messaggi pubblicitari via e-mail

In generale, si considera SPAM qualsiasi e-mail non richiesta e non desiderata

- Consuma tempo (per eliminarla) e spazio su disco
- È sempre fastidiosa, spesso offensiva, e talvolta contenente hoax o scam (si vedranno in seguito)
- Costa milioni di dollari ai grandi provider

Perché lo SPAM?

Basta fare un po' di conti …

- Inviare e-mail spam a circa 100 milioni di mailbox
- Se anche solo il 10% legge la mail e clicca sul link ➔ si raggiungono 10 milioni di persone
- Se 1% delle persone che va sul sito, sottoscrive per esempio all'offerta di prova per 3 giorni ➔ (100,000 persone) x ($0.50) = $50,000
- Se l'1% della prova gratuita, si iscrive per 1 anno ➔ (1,000 persone) x ($144/anno) = $144,000/anno

Cosa fare?

- **NON RISPONDERE MAI, NE' CHIEDERE MAI DI ESSERE ELIMINATI DALL'ELENCO**
- **Non rispondere alle e-mail che richiedono dati personali**
- **Non comprare niente che ha origine da una mail spam**
- **Non contribuire a proposte di elemosina provenienti da mail spam**
- **Pensare due volte, meglio tre, prima di aprire un attachment**
- **Non inoltrare messaggi di "catene di e-mail"**
- **Controllare se l'ISP ha in atto provvedimenti o spazi adatti per la gestione dello spam**

➔ USO DI PRODOTTI ANTISPAM

Anti SPAM

- Controllo ortografico
- Liste di siti
- Analisi dei contenuti
- …
- Può essere utilizzato sia da utenti finali (sul proprio client) sia da amministratori del mail server

Proteggere il proprio indirizzo (*se possibile*)

- **Utilizzare almeno due o tre indirizzi:**
  - **Indirizzo privato**
  - **Indirizzo di lavoro**
  - **Indirizzo “commerciale”**
- **Non divulgare il proprio indirizzo privato se non alle persone che si conoscono**
- **Utilizzare un indirizzo di e-mail dedicato esclusivamente alle transazioni/acquisti via Web**
- **Leggere bene le politiche utilizzate (*se utilizzate e dichiarate…*) dai vari siti per la gestione dei dati personali**

Che cosa è lo spamming?

a) L'invio di messaggi email non richiesti o non desiderati

b) Un inutile fatica (per chi la effettua) che comunque mette spesso in crisi le comunicazioni

c) Una tecnica di attacco nota anche col il sinonimo scam

d) Tutte le precedenti

Una buona misura anti-spam consiste nel:

a) utilizzare un solo indirizzo email

b) utilizzare un indirizzo che non include il proprio nome e cognome

c) utilizzare solo webmail

d) utilizzare almeno 3 indirizzi email

Software antispam:

a) interviene bloccando le email indesiderate nel server del mittente

b) non può essere utilizzato se si usa un client di posta (anziché webmail)

c) può essere utilizzato sia da utenti finali sia da amministratori di sistema

d) è comunque inutile se si utilizzano altre precauzioni (non rispondere ai messaggi di spam, non inoltrare spam,...)

Difendere la propria professione

Quale fra le seguenti affermazioni riguardo al Web è falsa:

a) chiunque può pubblicare sul Web ciò che vuole
b) se un nome di dominio è regolarmente registrato non può essere ingannevole
c) se un'organizzazione esiste realmente nel mondo fisico, allora il suo sito è probabilmente affidabile
d) un sito affidabile è normalmente chiaro e ben organizzato

Quale fra le seguenti sono caratteristiche di siti affidabili?

a) certificazione
b) professionalità
c) moderato utilizzo di animazioni
d) uso moderato di risorse di comunicazione

Vari aspetti

- **Usare il Web per il proprio lavoro**
- **Usare le social network per il proprio lavoro**
- **Privacy e attività sanitarie**
  - Cartelle sanitarie elettroniche e online
  - Dati sanitari di milioni di utenti sui server di grandi multinazionali. Es.,
    - Google health
    - Microsoft health

Quanto è affidabile il Web?

- Chiunque può pubblicare sul Web ciò che vuole
- Molta dell'informazione disponibile è falsa, fuorviante, ingannevole, faziosa, diffamatoria o disgustosa
- Come facciamo a sapere se le pagine che troviamo sono affidabili?

- I nomi dei domini registrati possono essere ingannevoli o intenzionalmente truffaldini
- Occorre verificare l'identità della persona o dell'organizzazione che pubblica la pagina Web

Caratteristiche dei siti affidabili

- Esistenza reale nel mondo fisico. Il sito fornisce un indirizzo, numero di telefono e indirizzo di posta elettronica
- Certificazione. Il sito include riferimenti, citazioni o credenziali, nonché collegamenti a siti altrettanto certificati
- Chiarezza. Il sito è ben organizzato, facile da navigare e fornisce servizi come una ricerca interna
- Aggiornamento. Il sito è stato aggiornato di recente
- Professionalità. La grammatica, l'ortografia, la punteggiatura e l'aspetto grafico sono corretti; tutti i link funzionano

➔ **Tuttavia, anche un sito che esibisce tutte queste qualità potrebbe non essere affidabile!**

Quale fra le seguenti affermazioni riguardo al Web è falsa:

a) chiunque può pubblicare sul Web ciò che vuole

b) se un nome di dominio è regolarmente registrato non può essere ingannevole

c) se un'organizzazione esiste realmente nel mondo fisico, allora il suo sito è probabilmente affidabile

d) un sito affidabile è normalmente chiaro e ben organizzato

Quale fra le seguenti sono caratteristiche di siti affidabili?

a) certificazione

b) professionalità

c) moderato utilizzo di animazioni

d) uso moderato di risorse di comunicazione

Quale affermazione è corretta riguardo i cosiddetti “dati sensibili”?

a) Sono sensibili quei dati che possono rivelare lo stato di salute delle persone

b) Sono sensibili i dati che possono rivelare la professione di un operatore sanitario

c) I dati sensibili non possono essere accessibili on-line per ragioni di sicurezza

d) I dati sensibili richiedono un trattamento tecnologico specifico

Privacy

Scopo principale della Legge n. 675/96 è:

- garantire che il trattamento dei dati personali sia effettuato nel rispetto dei diritti, della libertà e della dignità delle persone fisiche, con particolare riguardo alla riservatezza e all'identità personale;
- assicurarsi che tutti coloro che detengono o gestiscono dati personali abbiano l'autorizzazione della persona interessata, proteggano i dati riservati e comunichino il motivo per cui i dati sono stati raccolti

Privacy e sanità

- **Legge n. 675/96**
- **Codice della privacy D.l.196/2003**
- **Prescrizioni del Garante [art. 154, 1 c)] - 09 novembre 2005**

  …
- **Linee guida in tema di referti on-line *(G.U. n. 162 del 15 luglio 2009)***
- **Linee guida in tema di Fascicolo sanitario elettronico *(G.U. n. 178 del 3 agosto 2009)***

Consiglio: consultare regolarmente il sito dell'Authority Privacy:

http://www.garanteprivacy.it

Privacy: concetto di dato sensibile

- **Chiunque ha diritto alla protezione dei dati personali che lo riguardano. I dati personali in grado di rivelare lo stato di salute delle persone sono "*dati sensibili*"**

- **I "dati sensibili" richiedono un trattamento tecnologico specifico per la loro conservazione e trasmissione, nonché delle regole di accesso molto stringenti**

- **Il Codice sulla protezione dei dati personali stabilisce regole per il trattamento dei dati personali in ambito sanitario, per tutelare la privacy e la dignità dei pazienti tenendo conto del ruolo professionale di medici e personale paramedico**

Privacy: dignità dei pazienti

- Il Garante per la protezione dei dati personali il 9 novembre 2005 ha prescritto agli organismi sanitari pubblici e privati una serie di misure da adottare per assicurare il massimo livello di tutela delle persone e della loro dignità

- Al cittadino che entra in contatto con medici e strutture sanitarie per cure, prestazioni mediche, acquisto medicine, operazioni amministrative, deve essere garantita la più assoluta riservatezza ed il rispetto della dignità

Quale affermazione è corretta riguardo i cosiddetti “dati sensibili”?

a) Sono sensibili quei dati che possono rivelare lo stato di salute delle persone

b) Sono sensibili i dati che possono rivelare la professione di un operatore sanitario

c) I dati sensibili non possono essere accessibili on-line per ragioni di sicurezza

d) I dati sensibili richiedono un trattamento tecnologico specifico