Sicur@Mente in rete

Prof. Castellano Roberto

I.I.S. "A. Bafile", a.s. 2015-2016

OBIETTIVI DEL CORSO

Hai reale percezione dei rischi che si “incontrano” in internet?

“Si ho una vaga idea [..], comunque io sono al sicuro [..], a me queste cose non accadono [..], io uso benissimo internet ed i social network!”

PARLEREMO DI:

1. protezione del PC e dei dati personali in rete

2. videodipendenza, cyberbullismo e altri pericoli della rete

PRIMA PARTE DEL CORSO

protezione del PC e dei dati personali in rete

FAKE = falsa identità

Utente di un newsgroup, di un forum, di una chat o di un social network che falsifica la propria identità

WhatsApp

BLOG

Insta

Instagram

ask.fm

I social network più usati….

DATAVEGLIANZA

E’ la possibilità di sorvegliare le persone attraverso i dati che queste lasciano nei vari spazi social.

DATAVEGLIANZA

SI BASA SUL PRINCIPIO DEI DATABASE INCROCIATI

da Twitter si può sapere una parte di noi…da Facebook si può sapere un'altra parte di noi etc....

DATAVEGLIANZA

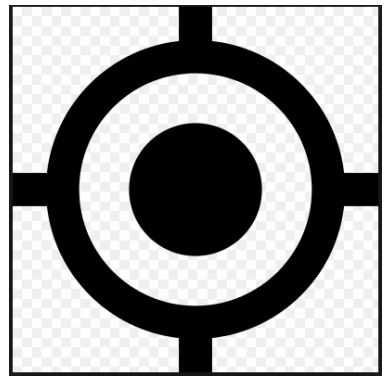
RICORDA

In futuro i datori di lavoro cercheranno di farsi un’idea su voi a partire dal web

GEOLOCALIZZAZIONE

I **motori di ricerca** forniscono risultati alle vostre ricerche che sono **GEOLOCALIZZATI** nelle vicinanze della posizione attuale: questo offre un grande vantaggio rispetto ad avere risultati generici di tutta Italia o addirittura di tutto il mondo.

Oltre alla geolocalizzazione nei motori di ricerca, questo fenomeno si è diffuso grazie all'enorme diffusione di smartphone con GPS.



PROTEZIONE DEL COMPUTER

Proteggere il proprio computer è molto importante per evitare inconvenienti.

Occorre prestare particolare attenzione a:

Un **virus**, in informatica, è un **software** che è in grado, una volta eseguito, di infettare dei file in modo da **riprodursi facendo copie di se stesso**, generalmente senza farsi rilevare dall'utente (da questo punto di vista il nome è in perfetta analogia con i virus in campo biologico).

Virus

1. **sfrutta le vulnerabilitá del nostro PC ed i nostri comportamenti “poco attenti”**
2. **arreca danni al PC**
3. **rallenta e/o rende inutilizzabile il PC infetto**

Tipologie di **VIRUS**

SPYWARE

MACRO VIRUS

WORM

TROJAN

SPYWARE

Uno spyware è un tipo di software che raccoglie informazioni riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete etc) senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, solitamente attraverso l'invio di pubblicità mirata

MACRO VIRUS

I macro virus sono generalmente script incorporati all'interno di file word, excel etc infetti.

Il macro virus è un vero e proprio programma che viene eseguito dal processore e si diffonde appunto attraverso fogli di lavoro di Excel, documenti di Word, e altri applicativi, quindi può essere particolarmente pericoloso e dannoso, rischiando addirittura di compromettere, infettare e cancellare ad esempio file fondamentali per il sistema operativo.

WORM

Un worm (letteralmente "verme") è una particolare categoria di virus in grado di autoreplicarsi.

Un worm si diffonde spedendosi direttamente agli altri computer, ad esempio tramite e-mail o una rete di computer

TROJAN

Deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice *trojan* nascosto.

I Trojan spesso non fanno alcun danno evidente al PC infetto ma permettono al loro creatore di accedere al nostro computer e di prenderne pieno possesso

COME DIFENDERSI?

ANTIVIRUS

COME DIFENDERSI?

L'aggiornamento dell'ANTIVIRUS è fondamentale per proteggere il PC dalle minacce, ma anche il sistema operativo e tutti i programmi devono essere sempre aggiornati.

L'ultima versione di un software garantisce sempre prestazioni migliori anche in ambito sicurezza e maggiore stabilità al tuo computer.

SNIFFING

Attività di intercettazione dei dati che transitano in una rete telematica.

Tale attività e’ svolta per scopi illeciti (intercettazione fraudolenta di password o altre informazioni sensibili).

ATTENZIONE ALLE RETI WIFI

Phishing

Il **phishing** è un tipo di **truffa** effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a **fornire informazioni personali, dati finanziari o codici di accesso**.

Phishing

Si tratta di una attività illegale attraverso la quale il malintenzionato effettua un invio massivo di messaggi di posta elettronica che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi; tali messaggi fraudolenti richiedono di fornire informazioni riservate come, ad esempio, il numero della carta di credito o la password per accedere ad un determinato servizio. Per la maggior parte è una truffa perpetrata usando la posta elettronica, ma non mancano casi simili che sfruttano altri mezzi, quali i messaggi SMS.

UN ESEMPIO DI PHISHING

Come proteggersi

Eliminate sempre le mail che hanno in allegato file con estensione .exe

Evitate di cliccare sui link presenti nelle mail e sms.

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

HACKER

Un **hacker**, in informatica, è un esperto di sistemi informatici in grado di introdursi in reti informatiche protette e in generale di acquisire un'approfondita conoscenza del sistema sul quale interviene, per poi essere in grado di accedervi o adattarlo alle proprie esigenze.

LE BACKDOOR

La backdoor (“porta sul retro”, “porta di servizio”) è una specie di entrata nascosta attraverso la quale l’hacker entra nel nostro PC.

Una volta installata, tale porta 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?

Scaricare e aggiornare periodicamente un ANTIVIRUS e attivare il **firewall**.

Come difendersi?

Non navigare in “siti poco sicuri”

Aggiornare spesso i software

Non memorizzare le password nei PC e cambiarle spesso

Non aprire posta inviata da sconosciuti soprattutto se contiene allegati

Non accettare l’amicizia da persone sconosciute

Consigli per la scelta della password

- **Creare una password di minimo dieci caratteri, contenente almeno una maiuscola, almeno una minuscola, almeno un numero e almeno un carattere speciale tra quelli elencati: ! $? # = * + - . , ; :**
- Includere caratteri dall'apparenza simili in sostituzione di altri caratteri (ad esempio il numero "0" per la lettera "O" o il carattere "$" per la lettera "S").

Evitare:

- **Non utilizzare le stesse password per più account.**
- **Non utilizzare una password contenente dati personali (nome, data di nascita, ecc.)**
- **Non usare sequenze di numeri (1234).**
- **Non creare password di soli numeri, di sole lettere maiuscole o di sole lettere minuscole.**
- **Non usare ripetizioni di caratteri (aa11).**

Suggerimenti per tenere al sicuro la password:

- **Non comunicare a nessuno la password**
- **Non lasciare la password scritta in posti facilmente raggiungibili da altri**
- **Non inviare mai la password per email**
- **Cambiare periodicamente la password**

METTI LO SMARTPHONE AL SICURO

Scaricare un buon antivirus

Controllare l'affidabilità delle APP

Blocco automatico

Reset e cancellazione dei dati prima di disfarsi del vecchio telefono

Modificare il Pin di default

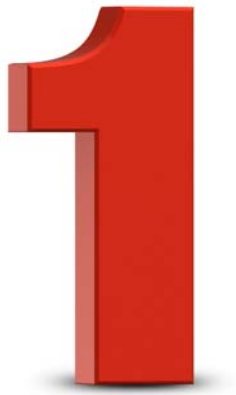
Riassumendo….

- Diffida dei link nelle email.
- Diffida delle pubblicità accattivanti e di chi ti vuole premiare.
- Non scaricare materiale pirata.
- Attento a dove navighi!
- Registrati solo quando è indispensabile
- Non dare dati che possano far risalire alla tua vera identità
- Usa buone password (mai le stesse!) e cambiale spesso!

SECONDA PARTE DEL CORSO

videodipendenza, cyberbullismo e <u>altri</u> pericoli della rete

Posta con la Testa



- Non pubblicate mai foto o filmati vostri o di altri
- Non pubblicate mai informazioni personali vostre o di tuoi amici
- Non offendere e rispettate le opinioni degli altri

Posta con la Testa

- Chiedetevi: pubblicherei questa foto o informazione su un bel cartellone davanti a casa mia?
- Impostate subito la privacy sui tuoi contenuti
- Segnalate gli abusi!

Videodipendenza

Questo termine indica la condizione di chi non può fare a meno di internet, smartphone, tablet e social network.

La dipendenza dai social network preclude la vita sociale.

Videodipendenza

- mal di testa
- stanchezza agli occhi
- depressione
- senso costante di insoddisfazione
- mancanza di concentrazione
- attacchi di panico
- tendenze aggressive e cyberbullismo
- senso di stanchezza continua
- poca attenzione al tempo da dedicare allo studio e alla VITA REALE

SINTOMI

USO INTELLIGENTE DELLE NOTIZIE

Internet non è una fonte di informazioni affidabile

"I social media danno diritto di parola a legioni di imbecilli che prima parlavano solo al bar dopo un bicchiere di vino, senza danneggiare la collettività. Venivano subito messi a tacere, mentre ora hanno lo stesso diritto di parola di un Premio Nobel. È l'invasione degli imbecilli". **(Umberto Eco)**

Chiunque può pubblicare qualsiasi cosa su internet per qualsiasi scopo e renderlo credibile agli occhi di chi legge

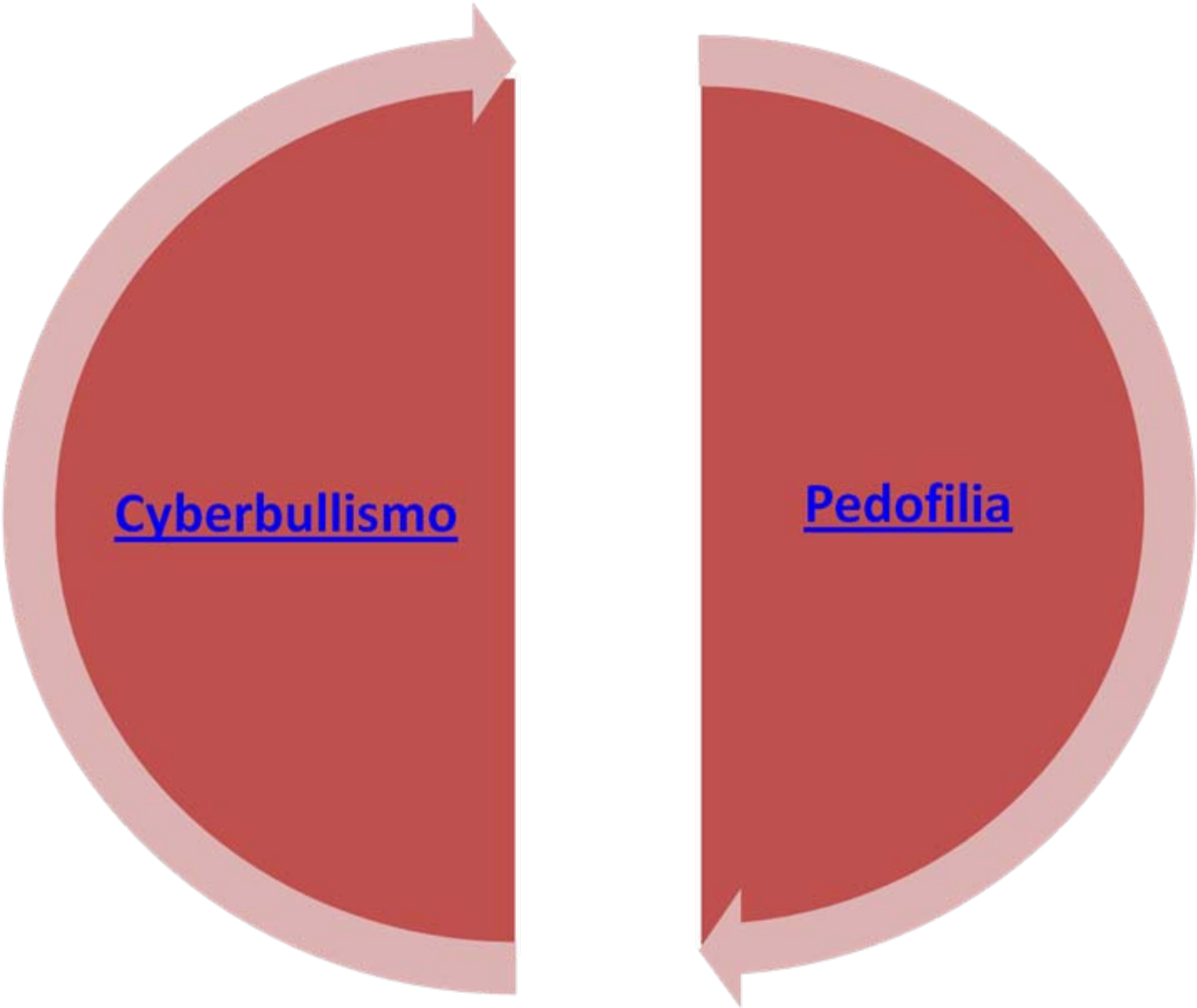
Non esiste alcun controllo su quello che viene pubblicato in rete

Le falsità generalmente non sono rimosse anche se vengono scoperte

Il web è pieno di bufale e di gente che diffonde informazioni false

Internet è il luogo ideale dove molte persone cercano di attirare altra gente allo scopo di **guadagnare soldi e soprattutto notorietà.**

La quasi totalità della gente **non controlla le informazioni che legge**


Cyberbullismo
Pedofilia

Cyberbullismo

Il bullismo in chat viene definito cyberbullismo.

Il cyberbullismo consiste nel:

- Far circolare delle foto spiacevoli
- Inviare mail contenenti materiale offensivo
- Offendere e schernire chi è in difficoltà

Come difendersi dal cyber-bullo

Ignorare le provocazioni e rifiutare ogni ulteriore rapporto

Evitare l'uso di nomi offensivi che possono incoraggiare le reazioni vendicative del soggetto

Non fornire informazioni personali.

I cyber-bulli potrebbero utilizzare il nome, il numero di telefono, l'indirizzo di casa o di posta elettronica delle loro vittime per provocare maggiori danni alla vittima

STATISTICHE

“NEL 2014, IN ITALIA, 1 ADOLESCENTE SU 5 E’ STATO VITTIMA DI BULLISMO E/O CYBERBULLISMO”

Il BULLISMO E' UN REATO PENALE

Le vittime possono (e devono) denunciare i loro aggressori per:

DANNO MORALE

(patire sofferenze fisiche o morali, turbamento dello stato d'animo della vittima, lacrime, dolori);

DANNO BIOLOGICO

(è un danno all'integrità fisica e psichica della persona tutelata dalla Costituzione Italiana all'art. 32);

DANNO ESISTENZIALE

(danno alla persona, alla sua esistenza, alla qualità della vita, alla vita di relazione, alla riservatezza, alla reputazione, all'immagine, all'autodeterminazione sessuale. La tutela del pieno sviluppo della persona nelle formazioni sociali è riconosciuta dall'art. 2 della Costituzione).

NUMERO VERDE ANTI BULLISMO

800 66 96 96

Il numero verde è attivo dal lunedì al venerdì, dalle 10 alle 13 e dalle 14 alle 19, a cui rispondono operatori specializzati

Il numero verde è stato attivato per:

- **segnalare casi;**
- **domandare informazioni generali;**
- **chiedere come comportarsi in situazioni critiche;**
- **ricevere sostegno.**

OVVIAMENTE…..


Su internet nel sito
www.poliziadistato.it


Commissariato di P.S.
online
www.commissariatodips.it

OVVIAMENTE…..

RACCONTA AD UN ADULTO LA SITUAZIONE CHE STAI VIVENDO.

TROLL

I Troll sono persone che interagiscono con altri utenti tramite messaggi provocatori, irritanti o semplicemente senza senso, con l'obiettivo di disturbare la comunicazione e alterare gli animi

Se per caso vi trovate in questa situazione i modi migliori per combatterli sono la segnalazione e l’indifferenza.

STALKING

Insieme di comportamenti persecutori ripetuti e intrusivi, come minacce, pedinamenti, molestie, telefonate o attenzioni indesiderate, tenuti da una persona nei confronti della propria vittima.

Sui social-network è semplice attirare ragazzi e ragazze.

Il metodo più diffuso è quello di creare falsi profili (FAKE) fingendosi minorenni e una volta conquistata la fiducia dei ragazzi viene dato un appuntamento!

COMPORTAMENTO DEL CYBER-PEDOFILO

Inizialmente il pedofilo cerca di

instaurare un rapporto basato sulla fiducia e sull'amicizia, fingendo di essere un coetaneo del bambino o dell'adolescente a cui si rivolge.

COMPORTAMENTO DEL CYBER-PEDOFILO

In seguito, il cyber-pedofilo gradualmente introduce argomenti sessuali, inviando a volte fotografie pedopornografiche.
Tale strategia serve a convincere il minore che tali comportamenti sono normali, anzi sani ed apprezzabili.

COME POTETE DIFENDERVI

1) **Non date confidenza a persone sconosciute.**
2) **Non accettate richieste o incontri da questi individui.**
3) **Comunicate ai genitori o ai professori se qualcuno che non conoscete vi scrive o vi infastidisce sui Social Network**
4) **Non fidatevi delle apparenze.**
5) **State sempre attenti.**

OVVIAMENTE.....

Su internet nel sito

www.poliziadistato.it

Commissariato di P.S.

online

www.commissariatodips.it

GRAZIE PER L'ATTENZIONE