DIDATTICA DIGITALE

E-LEARNING NELLA SCUOLA

SCUOLA POLO PER LA FORMAZIONE – AMBITO TERRITORIALE 07

Formazione Docenti – Sicurezza Informatica

dott.ssa Daniela Cotzia - d.cotzia@knowk.it

Know K. è agenzia accreditata dal MIUR per la formazione del personale della scuola Secondo Direttiva Ministeriale n.170/2016 (ex n. 90/2003).

Member of CISQ Federation
CERTIFIED MANAGEMENT SYSTEM
ISO 9001:2015

Know K. è azienda certificata ISO 9001-2015 per la qualità dall'anno 2000, sulla progettazione ed erogazione della formazione.

KnowK®
FORMAZIONE

La Sicurezza Informatica

Argomenti del Corso

- Sicurezza Informatica
- Minacce informatiche
- Malware
- AntivirusRischi nella Navigazione Web
- Attenzione alla posta elettronica
- Come individuare una minaccia informatica
- Alcuni Suggerimenti da Seguire
- Generazioni Connesse
- La privacy
- Web Reputation
- Il Cyberbullismo
- I videogame
- La sessualità in rete
- Link utili

I rischi della rete

- L’accesso alle informazioni in Rete è stato tendenzialmente reso possibile tutti
- Ma un **alto** livello di **accessibilità** corrisponde ad un **basso** livello di **sicurezza** e di **privacy**

Minaccia Informatica

*Una minaccia informatica è una **persona**, **processo** o **evento** con la **capacità** di **causare** danni a **reti** e **dati**.*

Generalmente un programma software, inserito nel computer non necessariamente ad insaputa dell'utilizzatore, che esegue operazioni impreviste o non autorizzate, ma sempre dannose

Tecniche utilizzate dai malintenzionati

- **Produzione di programmi che hanno un comportamento “maligno”**
  (danneggiano il sistema, cancellano dati o li modificano, rendendoli inutilizzabili, rubano informazioni).
- **Sfruttamento della vulnerabilità dei sistemi**
  L'espressione vulnerabilità è da intendere in senso lato per indicare la presenza di errori di programmazione, difetti o anche semplici mancanze da cui possono scaturire una serie di comportamenti inattesi. Una vulnerabilità può avere un impatto in termini di sicurezza perché un malintenzionato può utilizzarla per compiere azioni distruttive.
- **Ingegneria sociale**
  Nel campo della sicurezza delle informazioni per ingegneria sociale (dall'inglese social engineering) si intende lo studio del comportamento individuale di una persona al fine di carpire informazioni di qualsiasi natura oppure al fine di indurlo a compiere azioni che non dovrebbe fare.

Malware -1

Il **malware** (malicious software, programma malvagio, codice maligno) è un qualsiasi software creato con lo scopo di causare danni più o meno gravi al computer su cui viene eseguito. Tra questi:

- **Virus**,
  programma che si diffonde copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da **essere eseguito ogni volta che il file infetto viene aperto**. Si **trasmette da un computer a un altro tramite lo spostamento di file infetti** ad opera degli utenti (da qui il termine “virus”)
- **Worm**,
  programma che modifica il sistema operativo della macchina ospite in modo da **essere eseguito automaticamente** e **tentare di replicarsi sfruttando per lo più Internet**. Per **indurre gli utenti** ad **eseguirlo** utilizza tecniche di **social engineering**, oppure sfrutta dei difetti (**bug**) di alcuni programmi per diffondersi automaticamente

Malware - 2

- **Macro Virus**
  Non attacca i file eseguibili, ma **sono incorporati all'interno di documenti** (come ad esempio un documento Microsoft Word)
- **Trojan horse**
  (Cavallo di Troia), che contiene istruzioni **dannose che vengono eseguite all'insaputa dell'utilizzatore**. **Non** possiede funzioni di **auto-replicazione**, quindi per diffondersi deve essere **consapevolmente inviato alla vittima**.
- **Backdoor**
  Letteralmente "porta sul retro". Si tratta di programmi che consentono un **accesso non autorizzato al sistema** su cui sono in esecuzione.
- **Dialer**
  Si tratta di programmi che si occupano di **gestire la connessione ad Internet** tramite la normale **linea telefonica**. **Alcuni** dialer si comportano come **malware** (**modificano il numero telefonico chiamato** dalla connessione predefinita con uno a tariffazione speciale, allo scopo di trarre profitto all'insaputa dell'utente)

Malware - 3

- **Hijacker (in inglese, “dirottatore”)**
  Si tratta di programmi che si **appropriano di applicazioni di navigazione in rete** (soprattutto browser) e ne **modificano il comportamento** (per esempio l'apertura automatica di pagine Web indesiderate).
- **Rootkit**
  Si tratta di un programma (trojan) o una tecnologia utilizzato per **occultare** la presenza di un **oggetto malevolo** all'utente o all'amministratore del computer. I rootkit non **sono dannosi in sé ma hanno la funzione di nascondere**, sia all'utente che a programmi tipo antivirus, la presenza di particolari file o impostazioni del sistema.
- **Rabbit**
  Programmi che esauriscono le risorse del computer **creando copie di se stessi** (in memoria o su disco) a grande velocità.
- **Spyware**
  Software che vengono usati per **raccogliere informazioni dal sistema su cui sono installati** e per **trasmetterle ad un destinatario interessato** (abitudini di navigazione, password, chiavi di cifratura di un utente)

Malware - 4

- **Adware**

  Si tratta di software che **genera annunci pubblicitari elettronici**, ad esempio popup o collegamenti Web, **senza il consenso dell'utente**. In molti casi l'adware utilizza le informazioni raccolte attraverso lo spyware per visualizzare messaggi mirati in base alle preferenze e alle abitudini dell'utente.

- **Crimeware**

  È un termine generico che descrive il **software utilizzato per il furto finanziario**. Il crimeware può diffondersi attraverso qualsiasi vettore di minaccia (virus/cavalli di Troia/worm, spyware/adware e altri)

“Zombie”

Uno “zombie” è un computer che è stato infettato ed è ed è sotto il controllo di un'altra persona.

Un virus o un Trojan possono infettare un computer e aprire una “back door” che consenta l’accesso ad altri utenti.

I PC vengono utilizzati per eseguire numerose attività dannose, tra cui la distribuzione di spam, il phishing, gli attacchi ad altri computer, la distribuzione di materiale pedopornografico e l’estorsione.

Antivirus

- Un **antivirus** è un software atto a rilevare ed eliminare virus o altro malware (worm, trojan)
- Il successo di questa tecnica di ricerca si basa sul costante aggiornamento degli schemi che l'antivirus è in grado di riconoscere.
- Una volta indentificato il “malware” un antivirus può:
  - ✓ cercare di **riparare il file** che ospita il malware (nel caso di virus o trojan), rimuovendo la parte “infetta”
  - ✓ mettere in “**quarantena**” il file, in modo da renderlo innocuo (ma anche inutilizzabile)
  - ✓ **cancellare** il **file** infetto. In questo caso il “carico distruttivo” del malware ha avuto successo, **si impedisce solo la propagazione**.

Limiti di un Antivirus

- **Elimina solo i virus che riconosce.**

  Questo problema è mitigato dall'uso della tecnologia euristica (nell'analizzare il comportamento dei vari programmi alla ricerca di istruzioni sospette perché tipiche del comportamento dei virus)

- **Il rischio del "falso positivo"**

  Un livello troppo sensibile di "tecnologia euristica" enfatizza questo rischio.

- **Può intervenire solo sui virus già presenti nel computer**

- **Può rallentare il funzionamento del computer**

Rischi nella Navigazione WEB

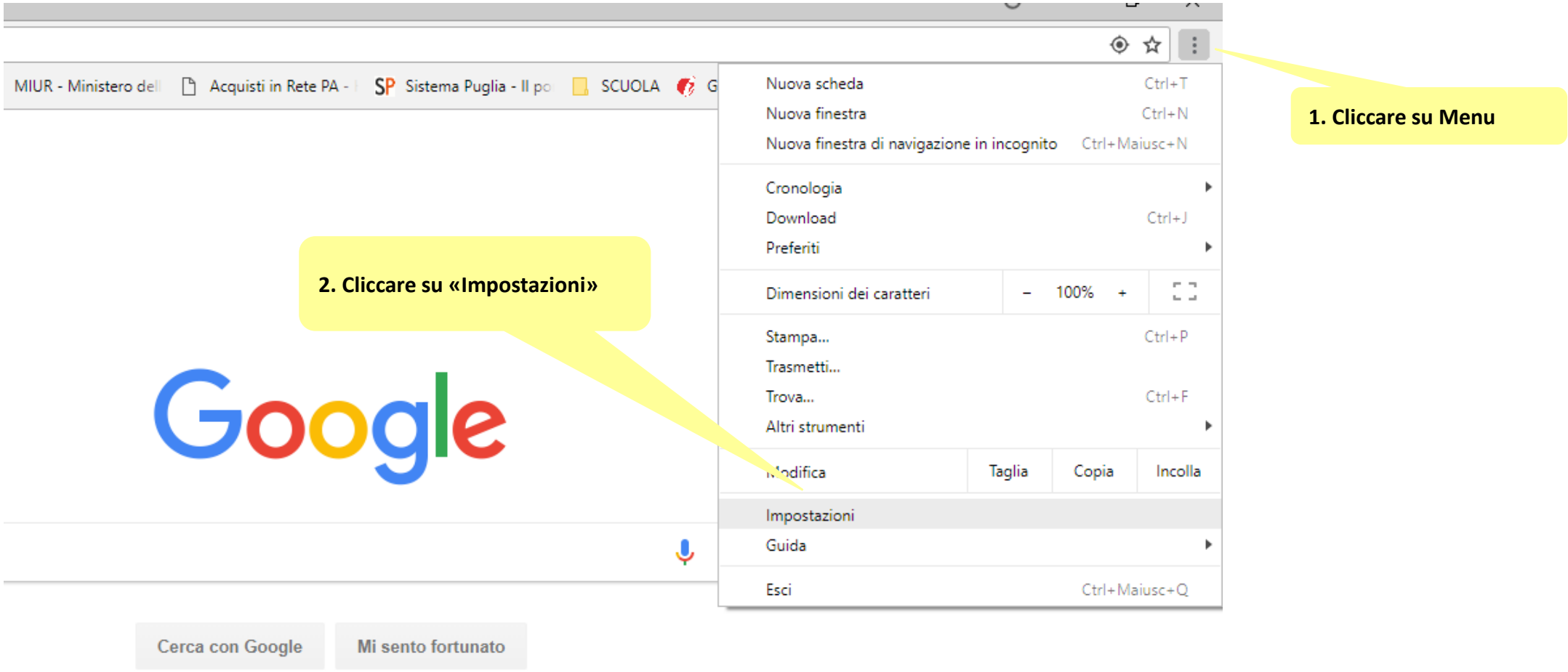
- **WEB come veicolo di codice maligno**

  L'accesso a siti poco raccomandabili diviene un mezzo per l'immissione nella rete di codice maligno: virus, worm, trojan, spyware, adware

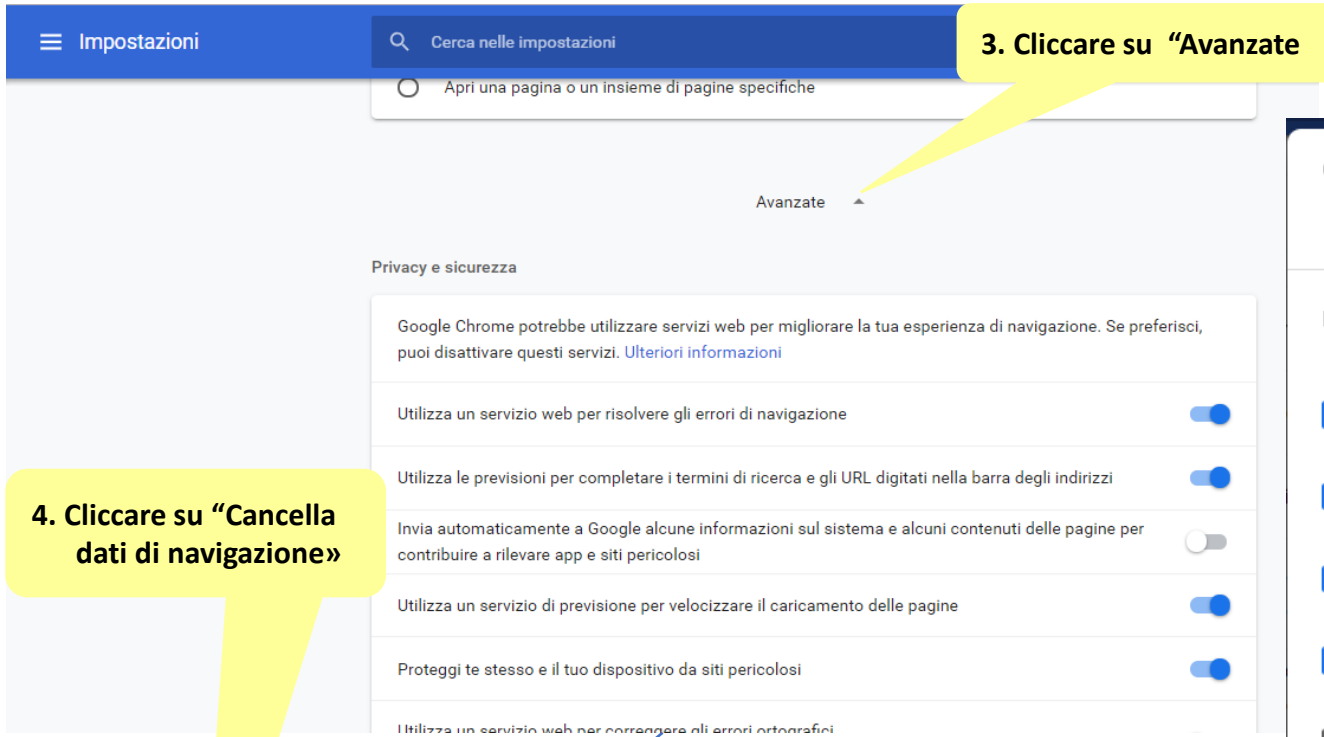
- **Utilizzo fraudolento dei cookie**

  I cookie sono piccole serie di informazioni memorizzate dai browser e comunicate su richiesta ai siti web, come ad esempio il nome dell'utente, l'ultima pagina visitata e altro. In alcuni casi, i cookie sono utilizzati in maniera impropria e possono raccogliere informazioni sui comportamenti e sulle preferenze degli utenti, creando dei profili senza che essi abbiano manifestato il loro consenso, commettendo una violazione della privacy.

Impostazione Avanzata

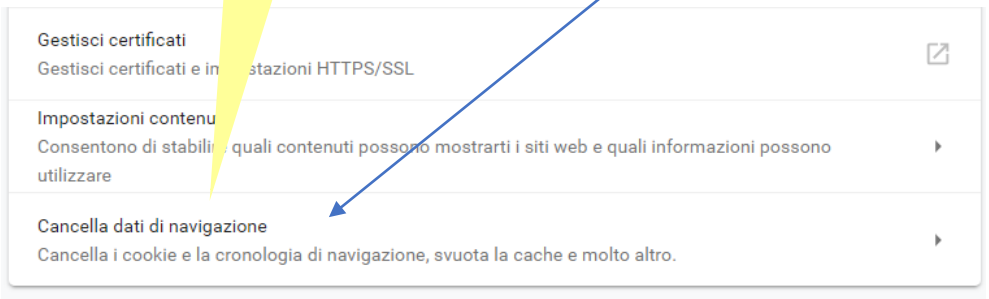


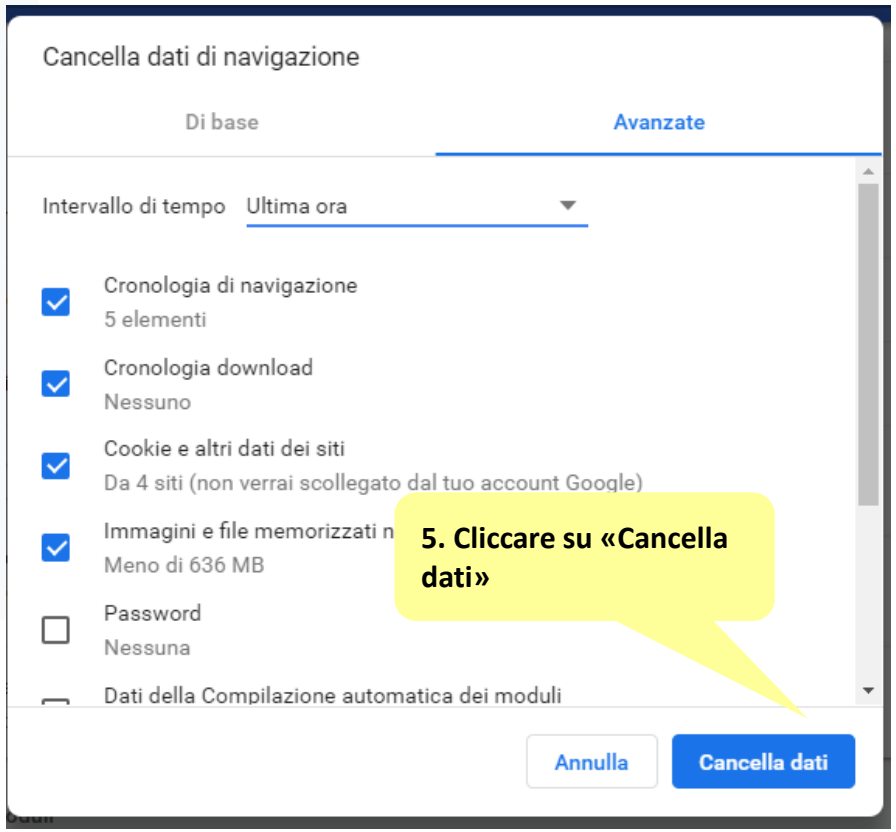
Impostazione Avanzata - 1



3. Cliccare su "Avanzate

4. Cliccare su "Cancella dati di navigazione»





5. Cliccare su «Cancella dati»

Truffe on line - 1

- **Phishing**

  è una attività illegale che sfrutta una tecnica di **ingegneria sociale**, ed è utilizzata per **ottenere l'accesso a informazioni personali o riservate con la finalità del furto di identità** mediante l'utilizzo delle comunicazioni elettroniche, soprattutto **messaggi di posta elettronica fasulli** o messaggi istantanei, ma anche contatti telefonici. Grazie a questi messaggi, l'utente è indirizzato su un falso sito e portato a rivelare dati personali, come numero di conto corrente, numero di carta di credito, codici di identificazione

- **Pharming**

  consiste nel far **comparire sul browser di un utente una pagina web diversa da quella richiesta**. L'utente crede di essere sul sito della propria banca, e invece si trova su un sito civetta che è apparentemente identico al sito originario. Il pharming è difficilmente rilevabile, dal momento che il browser non segnala nessuna anomalia lasciando credere all'utente di navigare in un sito legittimo. Non si basa su metodi da "ingegneria sociale" ma sfrutta debolezze tecniche dei sistemi in uso.

Truffe on line - 2

- **Smishing**

  Con l'**arrivo di un sms** oppure con l'installazione sullo smartphone di un'applicazione software malevola che è in grado di simulare di aver ricevuto un sms.
  I messaggi contengono la **richiesta di cliccare su un link** e, quindi, di **raggiungere una pagina web.** Per ingannare sfruttano meccanismi psicologici, come l'urgenza o la possibilità di ottenere un vantaggio personale. La trappola scatta quando gli utenti, dopo aver cliccato sui link, approdano in **siti online artefatti che chiedono l'inserimento di dati personali**.

Attenzione alla Posta Elettronica - 1

La posta elettronica rappresenta uno dei **principali vettori per la diffusione di diverse tipologie di minacce e di attacchi** (VIRUS, WORM, TROJAN).

- E’ molto **usata anche nell’ambito dell’ingegneria sociale**: SPAM e PISHING trovano un terreno fertile.
- Attacchi tramite gli **allegati di posta elettronica**. Sono ancora i più diffusi.

  Le tecniche che vengono adottate sono molto varie e vanno dall’ingegneria sociale (“ti convinco ad aprire un allegato”), fino all'impiego di pratiche sofisticate che producono come risultato l'esecuzione nascosta del file oppure il suo salvataggio sul disco locale e la successiva esecuzione senza nessun intervento consapevole da parte dell'utente stesso.

Attenzione alla Posta Elettronica - 2

- **Esecuzione di codice arbitrario attraverso i messaggi di posta.** Il codice del **"malware" è normalmente nascosto all'interno di pagine HTML** che la maggior parte dei client di posta elettronica è in grado di gestire.
  Alcuni virus sfruttano le vulnerabilità del sistema operativo o del programma di posta per colpire gli utenti non appena leggono l'e-mail. Si presentano come normali messaggi, ma contengono uno script nascosto che viene eseguito non appena si apre il messaggio di posta o lo si visualizza nel riquadro di anteprima. Questo script può modificare le impostazioni del sistema e inviare il virus ad altri utenti tramite posta elettronica.

- **e-mail spoofing**

  (spoof in inglese significa parodia) **Contraffazione delle intestazioni dei messaggi di posta** elettronica in modo tale che essi sembrano provenire da una sorgente mentre, in realtà, sono originati da altra fonte.

Come individuare una Minaccia Informatica

Una minaccia informatica cerca, ovviamente, di non farsi scoprire; tuttavia si potrebbero rilevare segnali indiretti:

- **Rallentamento delle prestazioni complessive del sistema**
- **File danneggiati o eliminati, che non è più possibile aprire**
- **Mancato funzionamento dei programmi utilizzati comunemente**
- **Riduzione dello spazio di memoria RAM e di spazio su disco rigido**
- **Difficoltà nell'aggiornare il software antivirus**

Alcuni Suggerimenti da Seguire - 1

- **Usare un buon antivirus**
  qualunque computer connesso alla rete Internet deve esserne dotato di antivirus aggiornato
- **Usare un solo antivirus**
- **Non eseguire ingenuamente programmi di ogni tipo**
  È buona regola accertarsi sempre della genuinità di qualsiasi programma prima di eseguirlo. Stessa cosa per tutti i documenti che possono contenere delle macro
- Prestare la massima **attenzione al funzionamento anomalo del sistema operativo**
  È assolutamente opportuno guardare sempre con sospetto ai funzionamenti apparentemente inspiegabili del proprio computer.

Alcuni Suggerimenti da Seguire - 2

- **Usare al minimo il formato HTML per la posta**

  Il testo semplice è molto più sicuro. La posta in formato HTML (quella che consente grassetti, corsivi e altri effetti speciali) può veicolare contenuti pericolosi che possono essere eseguiti automaticamente, senza che sia necessario aprire allegati. La posta HTML è uno degli strumenti preferiti dagli autori di virus.

- **Non fidatevi dei messaggi di allarme diffusi** da stampa generalista, amici e colleghi, e **non diffondeteli**, se non sono documentati.

- **Proteggere e non divulgare le informazioni personali**

  Le password e le altre credenziali devono essere trattate alla stregua di carta di credito o PIN bancomat.

Alcuni Suggerimenti da Seguire - 3

- **Non aprire mail indesiderate o non sollecitate**, non scaricare allegati sospetti.
- **Fidarsi, ma non troppo, dell'antivirus**
- **Non fidarsi di chi vi sta regalando qualcosa**

- **Non cliccare sui popup**

  Se appaiono popup inattesi, come quelli che avvertono della presenza di virus sul computer e che offrono una soluzione, non selezionate il link e non autorizzate nessun download. Potreste scaricare e installare software potenzialmente dannosi

Alcuni Suggerimenti da Seguire - 4

- **Non cliccare sui link presenti all'interno dei messaggi di posta indesiderata**

  Tali collegamenti potrebbero indirizzare l'utente su un sito fittizio, utilizzato per sottrarre informazioni personali, come dettagli bancari e password. Digitare sempre l'indirizzo Internet direttamente nella barra del browser.

- **Utilizzare una password diversa per ogni sito**

  Usate una password diversa per ogni sito sul quale vi registrate. Così, se una password viene scoperta, il pericolo riguarderà un solo account.

Generazioni connesse

La sicurezza dei minori in rete

Generazioni Connesse

- **Progetto SIC** (Safer Internet Center italiano) http://www.generazioniconnesse.it/site/it/home-page/
- Il progetto e coordinato dal MIUR in partenariato con: Autorità Garante per l'Infanzia e l'Adolescenza, Polizia Postale e delle Comunicazioni, Save the Children Italia, Telefono Azzurro, Cooperativa E.D.I. e Movimento difesa del Cittadino ed è volto a rendere **Internet più sicuro per le nuove generazioni**

Nativi digitali

- **Internet** e i cellulari o in generale i "Nuovi Media" rappresentano un aspetto esistenziale **importane nella vita dei ragazzi** contemporanei
- I **Nuovi Media** rappresentano un **nuovo modo di comunicare** con gli altri, ma pongono delle questioni associate alla sicurezza.
- I ragazzi sono **tecnicamente competenti**, ma **non colgono** le **implicazioni del loro comportamento**
- Per tale motivo, la **Commissione Europea finanzia progetti** che hanno l'obiettivo di supportare gli insegnanti nel passaggio al digitale in tutti i suoi aspetti

La privacy

La Privacy è il **diritto alla riservatezza della propria vita privata** ed include:

- **Dati anagrafici**, nome, cognome e indirizzo mail, indirizzo di residenza e/o domicilio, numero di telefono, ecc.
- **Dati finanziari**, codice fiscale, conto corrente, numero carata di credito ecc.
- **Dati sensibili**, informazioni utili a ricavare nazionalità, opinioni politiche, convinzioni religiose, salute, ecc.
- **Dati giudiziari**, processi, denunce ecc.

Gestire la privacy

- Bambini e adolescenti raccontano le loro esperienze in Internet, condividendo foto e informazioni.
  Questi aspetti richiamano problematiche legate alla privacy.
- **Imparare a gestire la privacy è il primo passo per navigare in Internet**

Alcuni suggerimenti – Privacy - 1

E’ importante dare agli studenti alcuni consigli:

- **Evitate di diffondere in rete informazioni** personali, nome, cognome e indirizzo mail, indirizzo di residenza e/o domicilio, numero di telefono, ecc.
- **Proteggere i vostri dati sensibili per evitare spam e truffe**
- **Parlate con i vostri amici di come gestire le foto e ditegli di chiedervi il permesso prima di postare le vostre**

Alcuni suggerimenti - Privacy - 2

- **Create password complesse, contenenti maiuscole, minuscole, numeri e simboli**
- **Non rilevate le vostre password a nessuno**
- **Controllate le impostazioni della privacy nei vostri Social Network, se possibile, rafforzatele**

Web reputation

- La diffusione di massa di Internet e l'utilizzo dei nuovi Device sempre connessi in rete, ha reso necessario **gestire la propria identità non solo nella vita reale, ma anche online**
- **Dati, informazioni e azioni non appartengono più (solo) ai legittimi proprietari poiché lasciano una traccia, spesso indelebile, in Rete.**
  E' molto importante che i gli studenti si rendano conto che ciò che inseriranno in rete lascerà una traccia indelebile e valutino le eventuali future conseguenze.
- **Bisogna far riflettere sui comportamenti online e sulla propria identità pubblica e virtuale fin da giovanissimi**

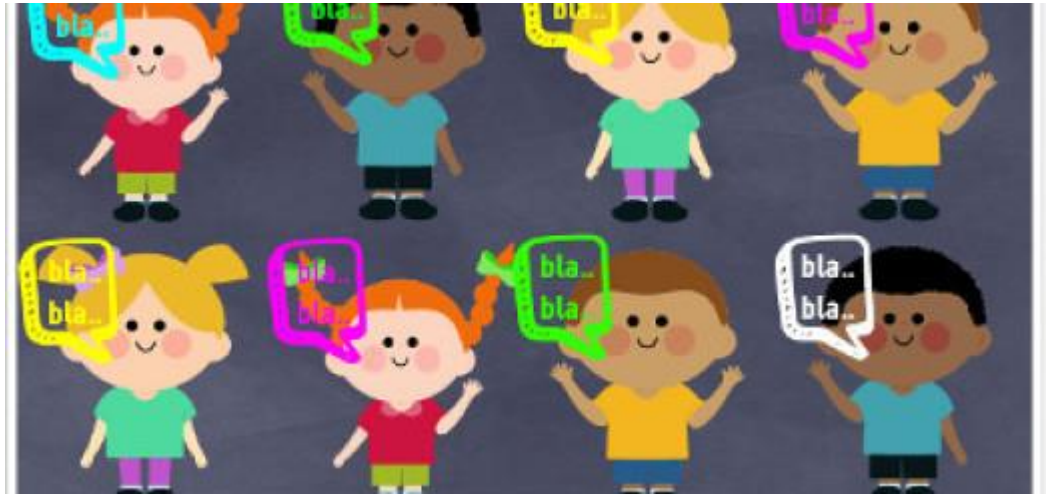
Alcuni suggerimenti - Web reputation - 1

È importante dare agli studenti alcuni consigli:

- **Inserite periodicamente il vostro nome sui principali motori di ricerca e guardate i risultati**, se qualcosa vi infastidisce cercate di eliminarla e, se non siete capaci, parlate con qualcuno di cui vi fidate
- **Limitare l'oversharing ovvero l'abitudine di postare e condividere tutto ciò che capita**

Alcuni suggerimenti - Web Reputation - 2

- **Non postate tutto su internet**, nemmeno nelle chat private
- **Chiudere un account o eliminare un profilo da un social network è una procedura (a volte) complessa ma fattibile**: se non siete capaci chiedete di aiutarvi



Cyberbullismo

Il Cyberbullismo o bullismo elettronico è una forma di prepotenza virtuale attuata attraverso l’uso di nuovi media o da tutto ciò che abbia una connessione a Internet

Cyberbullismo

Differisce dal bullismo tradizionale per:

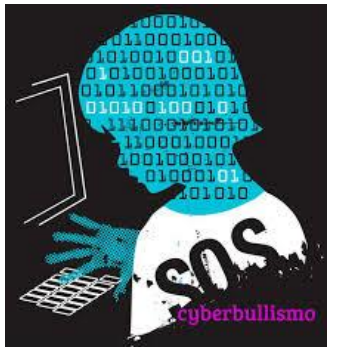
- **L'impatto, la diffusione tramite internet è incontrollabile**, anche a situazione risolta poiché video e immagini posso restare online.
- **L'anonimato**, chi offende online può nascondersi dietro un nickname o false identità (FAKE)
- **L'assenza di confini spaziali**, il fenomeno del cyberbullismo può avvenire ovunque e invadere spazi personali
- **La mancanza di limiti temporali**, per i cyberbulli e per le loro vittima il giorno e la notte hanno lo stesso valore

Come si manifesta il cyberbullismo - 1

Esistono diverse modalità per perpetuare azioni di cyberbullismo:

- **Flaming**
  messaggi online violenti e volgari mirati a suscitare battaglie verbali
- **Harassment**
  spedizione ripetuta di messaggi offensivi mirati a molestare e/o ferire i sentimenti di qualcuno
- **Denigrazione**
  sparlare di qualcuno (via e-mail, SMS, social network, chat ecc) per danneggiare la reputazione di qualcuno
- **Impersonation**
  spacciarsi per un'altra persona per spedire messaggi e/o pubblicare testi reprensibili

Come si manifesta il cyberbullismo - 2



- **Exposure**
  Rilevare informazioni private e/o imbarazzanti su altre persone
- **Trickery**
  Ottenere la fiducia di qualcuno con l'inganno per poi condividere con altri le informazioni
- **Esclusione**
  Discriminare deliberatamente una persona da un gruppo online per provocarle un sentimento di emarginazione
- **Cyberstalking**
  Molestie, persecuzioni e denigrazioni ripetute mirate a intimorire altri utenti

Alcuni suggerimenti - Cyberbullismo- 1

E’ importante dare agli studenti alcuni consigli:

- **Rispettare gli amici virtuali come gli amici reali**
- Se siete **vittime di fenomeni di cyberbullismo**, ricordatevi di **non cancellare le prove in vostro possesso**
- **Bloccate chi vi infastidisce e, se possibile, segnalate il profilo agli amministratori del sito o del social network**
- **Parlare dei vostri problemi con qualcuno di cui vi fidate**, tenersi tutto dentro non risolve le cose
- **Non vendicatevi replicando a tono e mettendovi sullo stesso piano di chi vi attacca**

I Videogame - 1

La diffusione dei giochi online determina stimoli, ma anche insidie legate ad un uso scorretto quali:

- **Uso spesso eccessivo**
- **Rischio di violazione della privacy**
- **Richiesta di contatti e "amicizie", con persone sconosciute nei videogiochi online**
- **Esposizione a contenuti non sempre adatti al target**
- **Esposizione al gioco d’azzardo**

Alcuni suggerimenti - I Videogame - 2

- Parlare ai propri cari non è facile, per questo il **confronto in classe diventa indispensabile**
- **Avviate una discussione sul gioco d'azzardo e le sue conseguenze**, includete tra le opzioni di gioco rischioso anche il gratta & vinci
- **Delineate un confine definito tra gioco e gioco d'azzardo**
- **Limitare il tempi del gioco**
- **Verificare con chi si gioca on line**
- **Fate compilare un mini questionario ai vostri studenti da usare per stimolare la discussione**. Chiedete loro quanto e quando giocano, se scommettono del denaro, se giocano sempre di più, se il gioco li rilassa, li deconcentra, li innervosisce ecc.

La sessualità in rete - 1

Internet è ormai parte integrante di ogni aspetto della vita dei teenagers, sfera sessuale inclusa. I teenagers cercano sempre più spesso risposte sul tema in rete, anche se le risposte sono spesso inadeguate.

Sono da tenere sotto controllo i fenomeni di:

- **Pornografia**
  l'accesso incontrollato a siti pornografici contribuisce in modo a disinformare su un argomento tanto delicato o infastidire alcuni soggetti più sensibili
- **Sexting**
  inviare o postare messaggi di testo o immagini a sfondo sessuale, come foto di nudo o seminudo via cellulare.
  Gli adolescenti diffondo immagini sexy di se stessi o di coetanei. Una volta messi in rete diventano materiale pedopornografico

La sessualità in rete - 2

- **L’espressione "pornografia infantile"** definisce ogni tipo di materiale che rappresenta visivamente un bambino che si dà a un comportamento sessualmente esplicito.
- **Produrre questo materiale e, soprattutto, diffonderlo costituisce un reato penale**.
- **Grooming**, tecnica di manipolazione psicologica che gli adescatori utilizzano online. L’adescamento avviene attraverso alcuni passaggi:
  - ✓ Contatto, l’adescatore crea una situazione che attivi la relazione. Banalmente può essere un commento gentile a una foto del profilo
  - ✓ Fiducia, tentare di conquistare la fiducia e raccogliere informazioni, millantare interesse comuni, affrontare argomenti di natura intima e scambiarsi foto
  - ✓ Esclusività, ottenuta la fiducia inizia le fase dell’esclusività dimostrando l’interesse sentimentale e facendo scivolate i contenuti su aspetti intimi e, in seguito, ricattare il minore

Alcuni suggerimenti - La sessualità in rete - 1

Potete dare i seguenti consigli agli studenti:

- **Evitare di postere immagini personali e intime**, e ricordatevi che si può essere facilmente registrati o fotografati se si usa la webcam in modo inappropriato, un'immagine imbarazzante può essere usata in mille modi
- **Le relazioni sentimentali**, **non giustificano il sexting selvaggio**, se lo fate sappiate che correte il rischio di essere traditi se e quando la vostra relazione finirà

Link utili

Per effettuare segnalazioni e ricevere supporto potete utilizzare:

Help Line

- La linea 1.96.96 e la chat wwww.azzurro.it/chat di Telefono Azzurro forniscono supporto a bambini, adolescenti e altri adulti in merito a esperienze negative e/o problematiche inerenti l'utilizzo dei nuovi media

Segnala contenuti illegali

- Due portali www.stop-it.it di Save the Children e "clicca e segnala " di Telefono Azzurro su www.azzurro.it sono a supporto per segnalare contenuti pedopornografici o dannosi incontrati in rete. Il servizio è collegato direttamente alla Polizia Postale e delle Comunicazioni

Grazie per l'attenzione

dott.ssa Daniela Cotzia

d.cotzia@knowk.it