FORMAZIONE DIGITALE ED EDUCAZIONE ALL'USO CONSAPEVOLE DELLA RETE INTERNET

"da Nati a in-Formati Digitali"

il Prof.re Aloe Gino e la Prof.ssa Angela De Carlo incontrano gli alunni del Primo Biennio dell'Istituto

Il Corso di formazione ha l'obiettivo di far conoscere i seguenti concetti sulla sicurezza:

- **Cyberbullismo - Sexting - Adescamento**
- **Sicurezza in rete**
- **Uso sicuro del web**

INTRODUZIONE

Gli strumenti tecnologici sono diventati uno strumento di comunicazione di massa e, spesso, si conoscono nuove persone.

Per questo motivo il nostro Istituto intende far conoscere il concetto di sicurezza nel web che ha l'obiettivo, in questa fase di fornire indicazioni, informazioni utili e strumenti concreti per cercare di prevenire certe situazioni di rischio e a gestirle al meglio nel caso si verifichino.

INTRODUZIONE

Ma cosa sono

CYBERBULLISMO e SEXTING?

Come avviene

l'ADESCAMENTO via internet?

Il cyberbullismo

Il **bullismo** è una forma di comportamento sociale di tipo violento e intenzionale, di natura sia fisica che psicologica, oppressivo e vessatorio, ripetuto nel corso del tempo e attuato nei confronti di persone considerate dal soggetto che perpetra l'atto in questione come bersagli facili e/o incapaci di difendersi.

Il cyberbullismo ("bullismo elettronico" o "bullismo in internet") è una forma di bullismo attuata attraverso l'uso dei Nuovi Media (dai cellulari a tutto ciò che si può connettere a internet).

Come il bullismo tradizionale è una forma di prevaricazione e di oppressione reiterata nel tempo, perpetuata da una persona o da un gruppo di persone più potenti nei confronti di un'altra persona percepita come più debole.

Il cyberbullismo

Le caratteristiche tipiche del bullismo sono:

- l'intenzionalità,
- la persistenza nel tempo,
- l'asimmetria di potere
- la natura sociale del fenomeno (Olweus, 1996),

Il cyberbullismo

Nel cyberbullismo intervengono anche altri elementi, quali:

- L'impatto: la diffusione di materiale tramite internet è incontrollabile e non è possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online.)
- La possibile anonimità: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile
- L'assenza di confini spaziali: il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando
- l'individuo dei suoi spazi-rifugio (la vittima può essere raggiungibile anche a casa.)
- L'assenza di limiti temporali: il cyberbullismo può avvenire a ogni ora del giorno e della notte.

Il cyberbullismo

Come difendersi!

Innanzitutto informare urgentemente i propri docenti, i genitori o persone di fiducia.

Il sexting

Il sexting (dall'inglese, sex e texting) è la pratica di inviare o postare messaggi di testo (sms) e immagini a sfondo sessuale, tra cui foto di nudo o semi-nudo, via cellulare o internet.

È un fenomeno recente ma piuttosto comune tra gli/le adolescenti, quando si trovano nella fase di scoperta della propria identità e, in particolare, della propria sessualità.

Il fenomeno si verifica più frequentemente tra i ragazzi delle superiori e proprio per questo è importante la prevenzione durante gli anni della scuola secondaria di primo grado.

Un post è un messaggio testuale, con funzione di opinione o commento o intervento, inviato in uno spazio comune sul web per essere pubblicato

Il sexting

Dare/diffondere un'immagine "provocante" di se stessi:

- può rappresentare un "regalo" molto intimo o divertente per un fidanzato o una fidanzata;

- può anche rappresentare un modo per dimostrarsi "adulti" o "più maturi" non solo agli occhi degli altri, ma anche verso se stessi;

- può anche essere un modo per gestire, a livello inconsapevole, le tante insicurezze tipiche dell'età adolescenziale.

Il sexting

Tutto sembra facile, la rete permette di sperimentare e "osare" con più libertà e meno pudori.

Occorre sapere innanzitutto che:

- **si perde** il controllo. Quello che si invia tramite cellulare o si posta online è praticamente impossibile da eliminare in forma definitiva: il rischio è di esporsi anche a possibili ricatti. Chi accede a queste immagini/video, le può usare facilmente per danneggiare volutamente chi è ritratto: un ex fidanzato/a che vuole vendicarsi o un cyber bullo possono diffondere questo materiale con estrema facilità e le vittime non avranno mai la possibilità di eliminarlo in modo definitivo.

Il sexting

- **si perde** la reputazione. Immagini troppo spinte o provocanti, possono nuocere alla reputazione di chi è ritratto, creare problemi con nuovi partner, o addirittura influenzare i futuri rapporti di lavoro.

- Si diventa un facile bersaglio di adescamento da parte di adulti potenziali abusanti. Dando una certa immagine di sé online, magari sul profilo di un Social Network, si possono attirare persone sessualmente interessate ai minori e che potrebbero essere incentivate ad accedere ai dati personali dei giovani utenti o a tentarne un adescamento.

Concetti di sicurezza: MINACCE AI DATI

Distinguere tra dati e informazioni.

I dati sono numeri o altro (immagini, testo, ecc...) che rappresentano fatti o eventi non ancora organizzati. Le informazioni sono dati organizzati in modo da essere comprensibili e significativi per l'utente.

Comprendere il termine crimine informatico.

Un crimine informatico è un crimine attuato per mezzo dell'abuso degli strumenti informatici, come computer e internet. Esempi di crimine informatico sono la frode informatica, il furto d'identità o l'accesso non autorizzato a sistemi informatici.

Concetti di sicurezza: MINACCE AI DATI

Comprendere la differenza tra hacking, cracking.

Il termine hacking deriva dal verbo inglese to hack (intaccare) e ha diverse valenze: restringendo il campo al settore dell'informatica, si intende per hacking l'insieme dei metodi, delle tecniche e delle operazioni volte a conoscere, accedere e modificare un sistema hardware o software.
Colui che pratica l'hacking viene identificato come hacker.

Quando lo scopo principale dell'hacker è quello di utilizzare il sistema informatico a cui ha avuto accesso a proprio vantaggio per rubarne i dati o danneggiarlo, si parla di cracking. Colui che pratica il cracking viene identificato come cracker.

Concetti di sicurezza: MINACCE AI DATI

VALORE DELLE INFORMAZIONI

Comprendere i motivi per proteggere le informazioni personali, quali evitare il furto di identità o le frodi.

Dovrebbero essere abbastanza evidenti i motivi per cui è opportuno proteggere le proprie informazioni personali:

se qualcuno entra in possesso di dati riservati, come le credenziali di accesso alla posta elettronica o a una rete sociale, ne può fare un uso illegale facendo ricadere la colpa su di noi;

così, se un malintenzionato entra in possesso del numero di carta di credito o dei dati di accesso a un servizio di internet banking, li può utilizzare a proprio vantaggio.

Concetti di sicurezza: MINACCE AI DATI

Identificare le misure per prevenire accessi non autorizzati ai dati, quali cifratura, password.

Per proteggere i dati riservati, propri o altrui, è essenziale proteggerli con determinate tecniche per mezzo delle quali, anche se finissero nelle mani di malintenzionati (per esempio se immagazzinati su dispositivi mobili che possono più facilmente essere rubati), non potrebbero essere utilizzati.

La prima cosa da fare è proteggere con password robuste i dispositivi che permettono l'accesso ai dati.

La seconda è quella di cifrare, attraverso un opportuno algoritmo crittografico, i dati stessi (crittografia).

Concetti di sicurezza: MINACCE AI DATI

Identificare le misure per prevenire accessi non autorizzati.

Il phishing é una tecnica basata sull'invio di ingannevoli messaggi di posta elettronica.
Il phisher si finge un servizio bancario e, minacciando la chiusura del conto o della carta di credito, chiede di inserire le proprie credenziali per poterle verificare. Ovviamente si tratta di un trucco per entrarne in possesso.
Il shoulder surfing (fare surf sulla spalla) consiste nel carpire le credenziali immesse dall'utente di un servizio spiandolo direttamente, standogli nei pressi, oppure anche da lontano, per mezzo di lenti o telecamere. Ciò può avvenire generalmente in luoghi affollati, come internet cafè o simili.

Concetti di sicurezza: MINACCE AI DATI

Comprendere il termine furto di identità e le sue implicazioni personali, finanziarie, lavorative, legali.

Il furto di identità nel campo informatico consiste nell'appropriazione indebita delle credenziali di accesso a un servizio (accesso a un PC, a una rete locale, a internet, alla posta elettronica, a una rete sociale, a un servizio di internet banking) allo scopo di usarlo a proprio vantaggio, per compiere crimini informatici come frodi o furti.

Concetti di sicurezza: MINACCE AI DATI

Per il furto di identità vengono usati vari metodi, tra cui per esempio frugare negli scarti delle persone tra cui potrebbe nascondersi qualche riferimento ai propri dati sensibili (ad esempio un foglietto su cui e annotata la password di accesso a un servizio).

In alcuni casi ci si finge qualcun altro dotato di diritto ad avere le credenziali, per esempio nel caso del phishing.

Infine in altri casi viene usata la tecnica dello skimming, che consiste nell'acquisire immagini (o filmati) di oggetti su cui sono impressi dei dati sensibili, per esempio la carta di credito o il PIN del bancomat.

Quando si preleva da un bancomat e importante non solo non farsi vedere da qualcuno, ma anche stare attenti che non ci siano webcam posizionate sopra la della tastiera.

Sicurezza in rete

Una rete informatica comprende piu dispositivi, come computer o mobile, in grado di comunicare tra di essi attraverso differenti mezzi.

Una rete può essere limitata nello spazio, per esempio a un locale o a un edificio e prende il nome di **LAN** (Local Area Network).

Se la rete é estesa a un'area cittadina prende il nome di **MAN** (Metropolitan Area Network).

Se la rete e molto estesa come ad esempio Internet, prende il nome di **WAN** (Wide Area Network).

Una **VPN** (Virtual Private Network) è un sistema per avere una rete virtuale privata che pero utilizza una rete pubblica per funzionare.

Normalmente una VPN viene implementata per poter collegare in modo sicuro più computer lontani tra di loro per mezzo di internet.

Un apposito software si occupa di creare un tunnel sicuro attraverso al criptazione dei dati e l'autenticazione della comunicazione.

Sicurezza in rete

Comprendere il ruolo dell'amministratore di rete nella gestione delle operazioni di autenticazione, autorizzazione e assegnazione degli account all'interno di una rete.

Una rete viene gestita da un amministratore (administrator) che si occupa di renderla sicura ed efficiente attraverso l'implementazione di politiche di accesso alle risorse (file, cartelle, stampanti, accesso a internet, ecc...).

Per definire tali politiche e necessario che gli utenti dei dispositivi che fanno parte della rete dispongano di un account attraverso il quale vengano autenticati col proprio nome utente e password.

User Name: _____

Password : _____

Sicurezza in rete

Per autenticazione s'intendono tutte le norme che servono a controllare la corretta identità di un utente (account) di un computer o di un software che chiedono di accedere ai servizi della rete.

L'account è formato da:

Username: che ha il compito di identificare l'utente:

Password: che ha il compito di autenticare lo username precedentemente digitato.

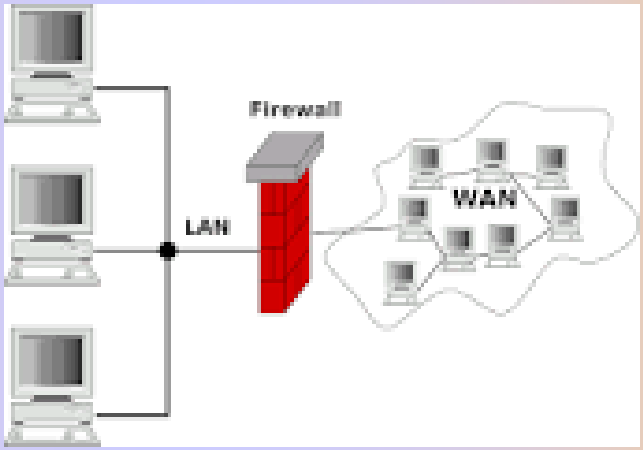
Entrambi permettono l'accesso al servizio.

Sicurezza in rete

Comprendere la funzione e i limiti di un firewall.

Un firewall e un dispositivo hw o un software che monitora e controlla in base a delle regole, definite dall'amministratore, il traffico di rete, generalmente tra la rete locale (LAN) e internet, allo scopo di evitare intrusioni e accessi non autorizzati.

Per funzionare bene il firewall deve essere programmato in modo efficace, dato che si limita a seguire le regole impostate. Se le regole non sono ben organizzate il funzionamento del firewall non sarà efficace.



Sicurezza in rete

Identificare un sito web sicuro, ad esempio associato ad https, simbolo del lucchetto.

In particolare, quando si utilizza il web per trasferimenti di denaro, occorre fare particolare attenzione.

I browser utilizzano normalmente il protocollo http che non é sicuro in quanto trasmette i dati senza alcuna cifratura.

E quindi soggetto ad essere intercettato e utilizzato da malintenzionati.

Esiste pero anche un protocollo sicuro, https (Hyper Text Transfer Protocol Secure) che trasmette i dati dopo averli cifrati con una chiave robusta in modo che il solo sito web che li riceve e li trasmette sia in grado di decodificarli.

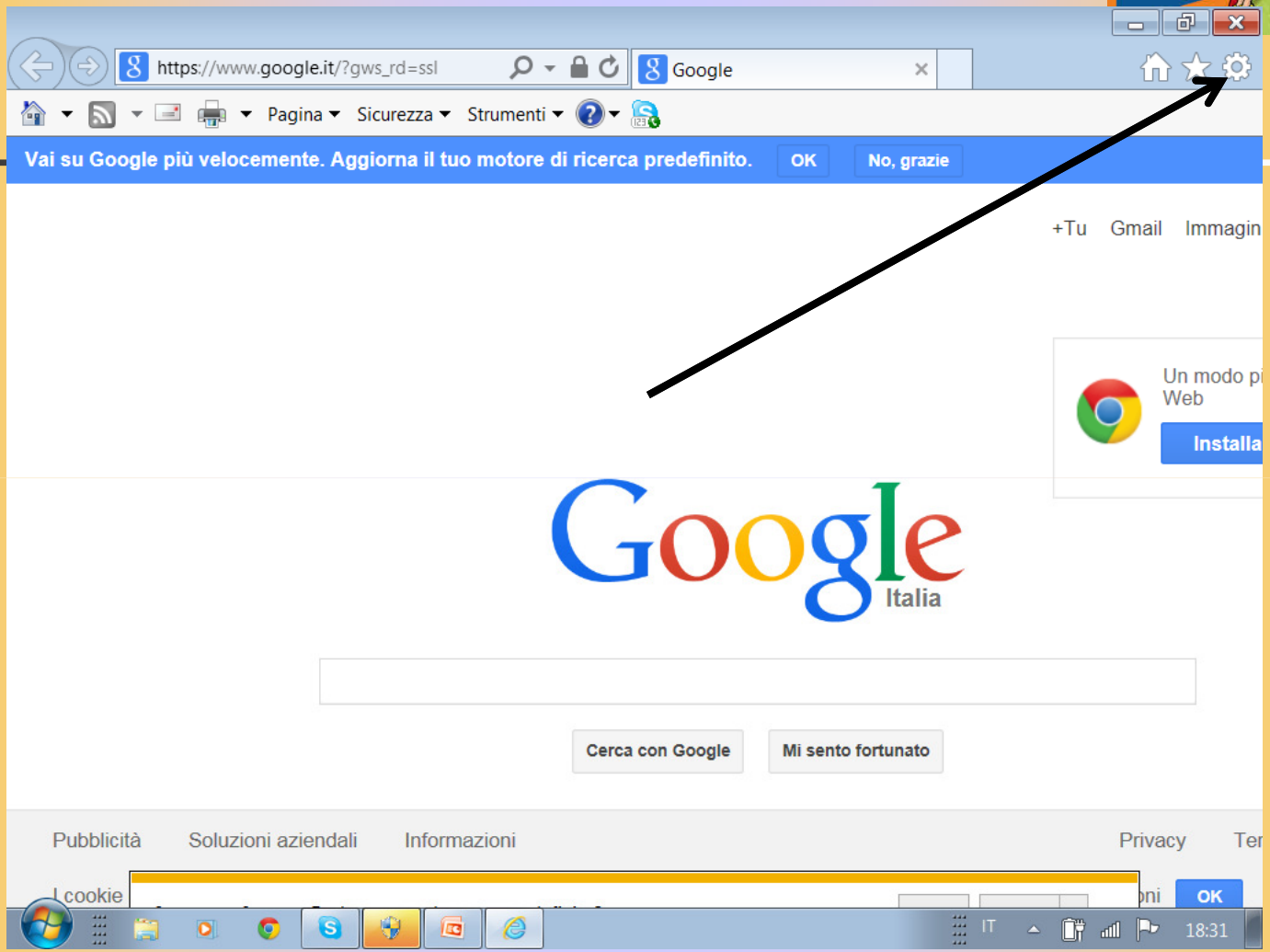
E pertanto essenziale per la sicurezza dei dati trasmessi che quando si utilizza il web per un pagamento, per esempio acquisti online, o transazioni finanziarie per esempio operazioni sul proprio conto corrente bancario, ci si accerti che il browser utilizzi il protocollo https.

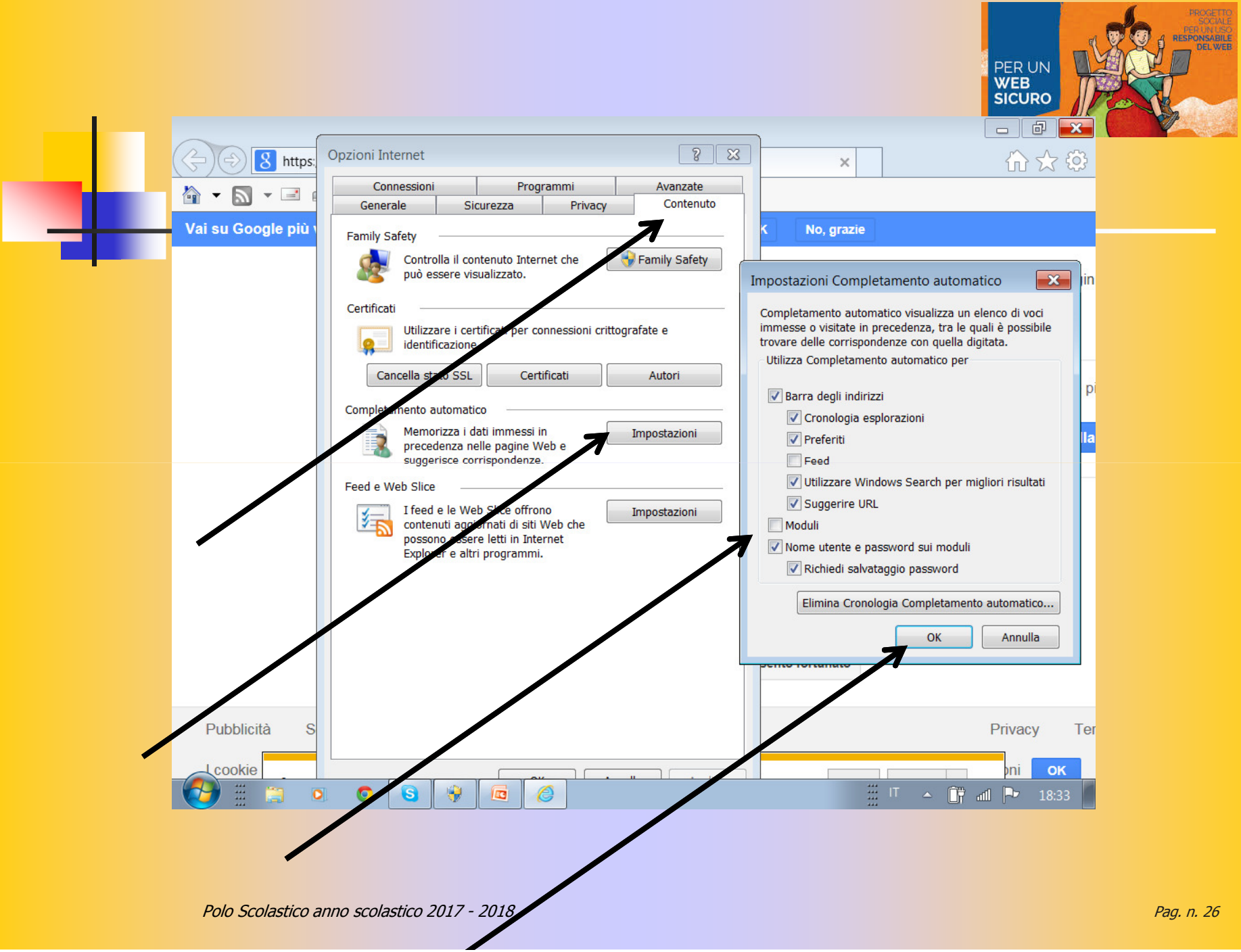
4.1.6 Selezionare impostazioni adeguate per attivare, disattivare il completamento automatico, il salvataggio automatico quando si compila un modulo.

Soprattutto quando il computer é utilizzato da o accessibile a più persone, conviene disabilitare le opzioni di completamento e di salvataggio automatico del browser, per evitare la diffusione dei propri dati personali.

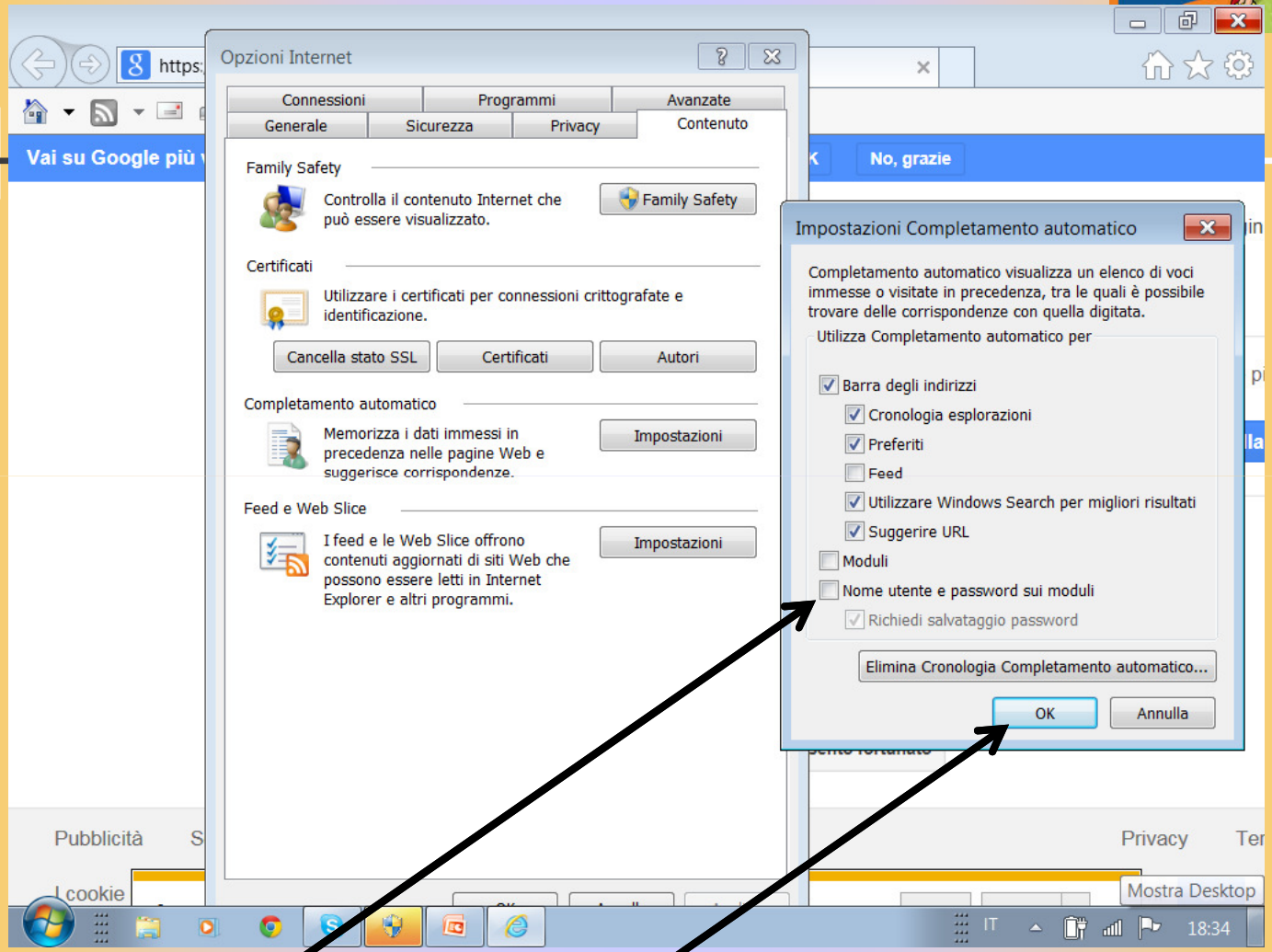
Di seguito sono indicati, con immagini, la procedura per disattivare il completamento automatico.


PROGETTO SOCIALE PER UN USO RESPONSABILE DEL WEB
PER UN WEB SICURO


https://www.google.it/?gws_rd=ssl
Google
Pagina
Sicurezza
Strumenti
Vai su Google più velocemente. Aggiorna il tuo motore di ricerca predefinito.
OK
No, grazie
+Tu
Gmail
Immagin
Un modo p
Web
Installa
Google
Italia
Cerca con Google
Mi sento fortunato
Pubblicità
Soluzioni aziendali
Informazioni
Privacy
Ter
I cookie
OK
IT
18:31


PER UN WEB SICURO
PROGETTO SOCIALE PER UN USO RESPONSABILE DEL WEB
Opzioni Internet
Connessioni
Programmi
Avanzate
Generale
Sicurezza
Privacy
Contenuto
Family Safety
Controlla il contenuto Internet che può essere visualizzato.
Family Safety
Certificati
Utilizzare i certificati per connessioni crittografate e identificazione.
Cancella stato SSL
Certificati
Autori
Completamento automatico
Memorizza i dati immessi in precedenza nelle pagine Web e suggerisce corrispondenze.
Impostazioni
Feed e Web Slice
I feed e le Web Slice offrono contenuti aggiornati di siti Web che possono essere letti in Internet Explorer e altri programmi.
Impostazioni
Impostazioni Completamento automatico
Completamento automatico visualizza un elenco di voci immesse o visitate in precedenza, tra le quali è possibile trovare delle corrispondenze con quella digitata.
Utilizza Completamento automatico per
Barra degli indirizzi
Cronologia esplorazioni
Preferiti
Feed
Utilizzare Windows Search per migliori risultati
Suggerire URL
Moduli
Nome utente e password sui moduli
Richiedi salvataggio password
Elimina Cronologia Completamento automatico...
OK
Annulla
No, grazie
Pubblicità
Privacy
OK
18:33


PROGETTO SOCIALE PER UN USO RESPONSABILE DEL WEB
PER UN WEB SICURO


Opzioni Internet
Connessioni
Programmi
Avanzate
Generale
Sicurezza
Privacy
Contenuto
Family Safety
Controlla il contenuto Internet che può essere visualizzato.
Family Safety
Certificati
Utilizzare i certificati per connessioni crittografate e identificazione.
Cancella stato SSL
Certificati
Autori
Completamento automatico
Memorizza i dati immessi in precedenza nelle pagine Web e suggerisce corrispondenze.
Impostazioni
Feed e Web Slice
I feed e le Web Slice offrono contenuti aggiornati di siti Web che possono essere letti in Internet Explorer e altri programmi.
Impostazioni
Impostazioni Completamento automatico
Completamento automatico visualizza un elenco di voci immesse o visitate in precedenza, tra le quali è possibile trovare delle corrispondenze con quella digitata.
Utilizza Completamento automatico per
Barra degli indirizzi
Cronologia esplorazioni
Preferiti
Feed
Utilizzare Windows Search per migliori risultati
Suggerire URL
Moduli
Nome utente e password sui moduli
Richiedi salvataggio password
Elimina Cronologia Completamento automatico...
OK
Annulla
Vai su Google più
No, grazie
Pubblicità
Privacy
Mostra Desktop
18:34

4.1.7 Comprendere il termine "cookie".

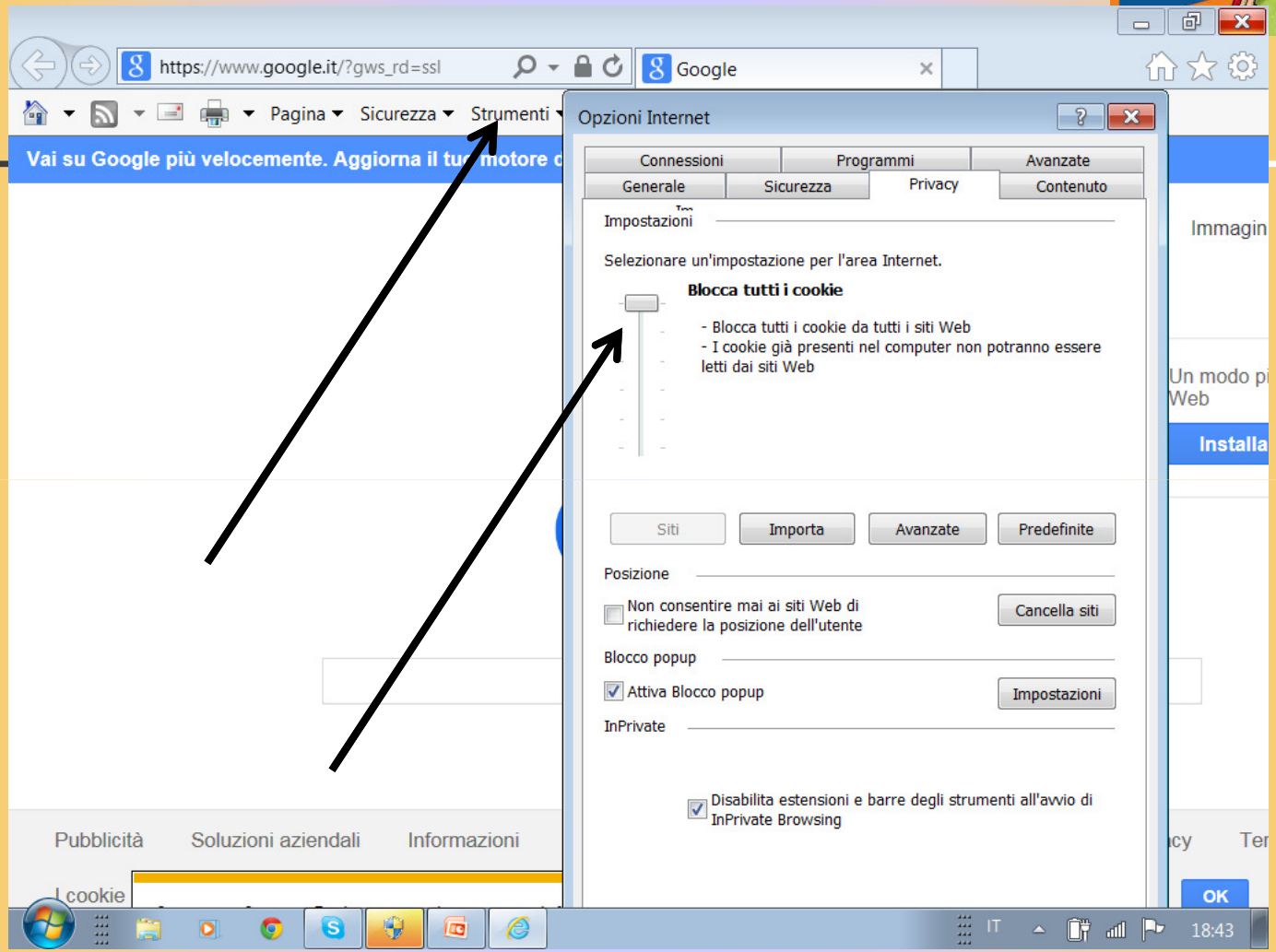
Un cookie (letteralmente biscottino) é una stringa di testo contenente informazioni personali che viene inviata da un server web e memorizzata dal browser, per esempio i dati relativi agli acquisti fatti in un negozio online, il cosiddetto carrello della spesa.

Quando si accede nuovamente allo stesso sito web, il cookie viene inviato dal browser al server per automatizzare la ricostruzione dei propri dati.

Si tratta quindi normalmente di uno strumento utile quando viene utilizzato in modo lecito.

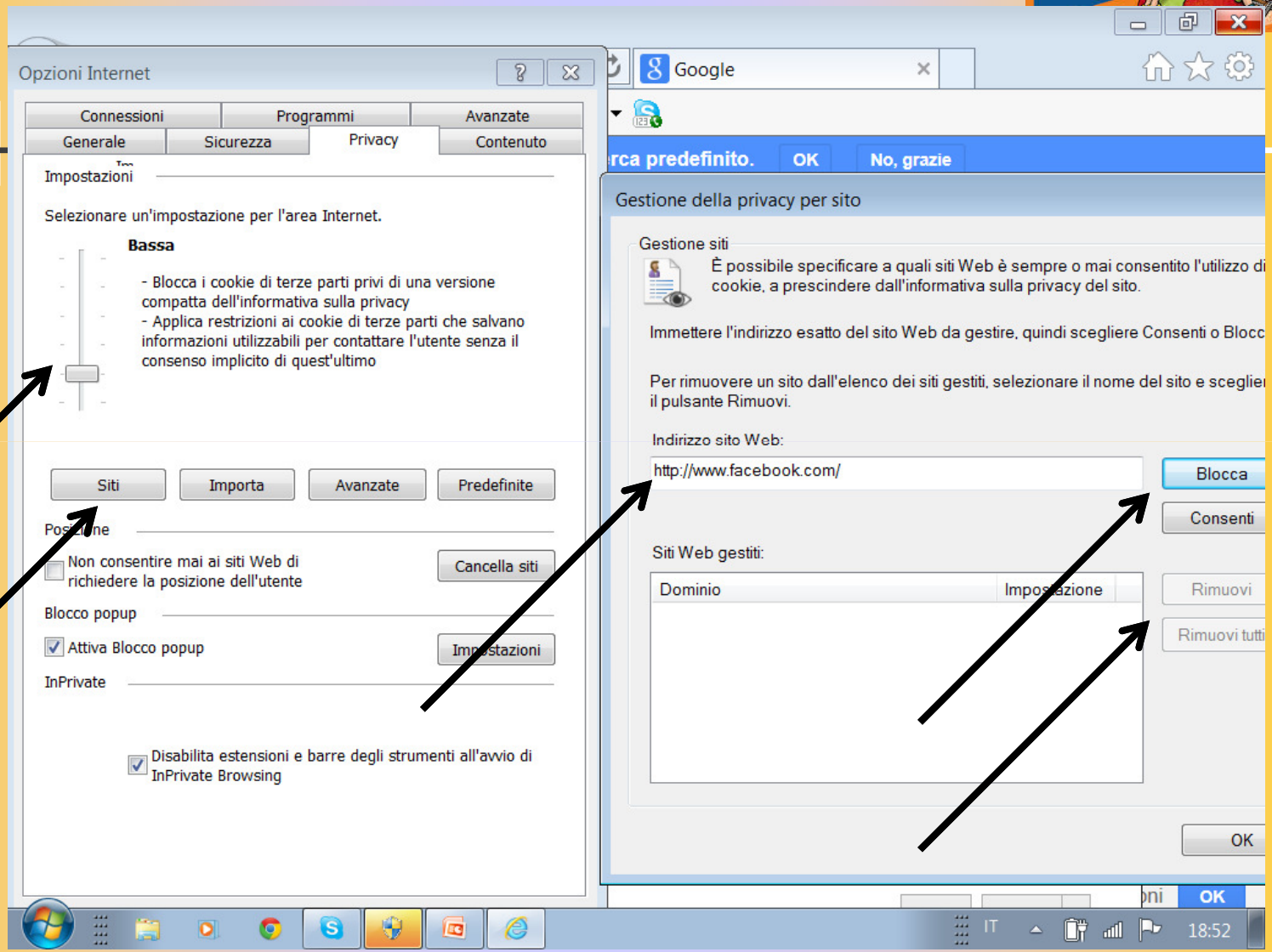
In alcuni casi i cookie sono stati usati in modo illecito per tracciare i comportamenti degli utenti, come uno spyware.

Come si bloccano???


https://www.google.it/?gws_rd=ssl
Google
Pagina
Sicurezza
Strumenti
Vai su Google più velocemente. Aggiorna il tuo motore
Opzioni Internet
Connessioni
Programmi
Avanzate
Generale
Sicurezza
Privacy
Contenuto
Impostazioni
Selezionare un'impostazione per l'area Internet.
Blocca tutti i cookie
- Blocca tutti i cookie da tutti i siti Web
- I cookie già presenti nel computer non potranno essere letti dai siti Web
Siti
Importa
Avanzate
Predefinite
Posizione
Non consentire mai ai siti Web di richiedere la posizione dell'utente
Cancella siti
Blocco popup
Attiva Blocco popup
Impostazioni
InPrivate
Disabilita estensioni e barre degli strumenti all'avvio di InPrivate Browsing
Immagin
Un modo p
Web
Installa
Pubblicità
Soluzioni aziendali
Informazioni
I cookie
OK
IT
18:43

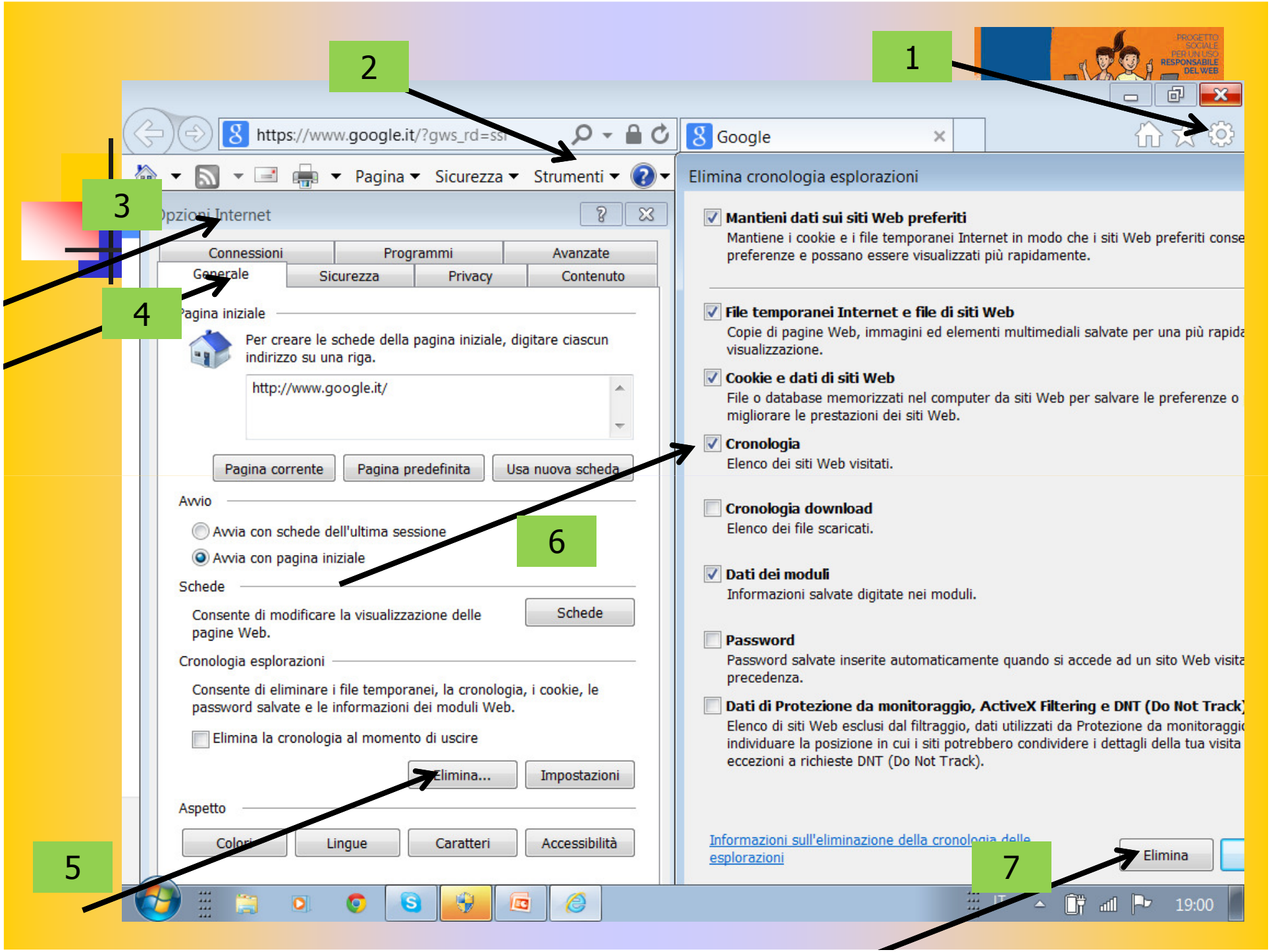
Selezionare impostazioni adeguate per consentire, bloccare i cookie.

Per disattivare completamente i cookie e rendere difficoltosa la navigazione o addirittura impossibile per alcuni siti, é consigliabile eventualmente impostare alcune eccezioni per alcuni siti web.


Opzioni Internet
Connessioni
Programmi
Avanzate
Generale
Sicurezza
Privacy
Contenuto
Impostazioni
Selezionare un'impostazione per l'area Internet.
Bassa
- Blocca i cookie di terze parti privi di una versione compatta dell'informativa sulla privacy
- Applica restrizioni ai cookie di terze parti che salvano informazioni utilizzabili per contattare l'utente senza il consenso implicito di quest'ultimo
Siti
Importa
Avanzate
Predefinite
Posizione
Non consentire mai ai siti Web di richiedere la posizione dell'utente
Cancella siti
Blocco popup
Attiva Blocco popup
Impostazioni
InPrivate
Disabilita estensioni e barre degli strumenti all'avvio di InPrivate Browsing
Google
rca predefinito.
OK
No, grazie
Gestione della privacy per sito
Gestione siti
È possibile specificare a quali siti Web è sempre o mai consentito l'utilizzo di cookie, a prescindere dall'informativa sulla privacy del sito.
Immettere l'indirizzo esatto del sito Web da gestire, quindi scegliere Consenti o Blocc
Per rimuovere un sito dall'elenco dei siti gestiti, selezionare il nome del sito e sceglie il pulsante Rimuovi.
Indirizzo sito Web:
http://www.facebook.com/
Blocca
Consenti
Siti Web gestiti:
Dominio
Impostazione
Rimuovi
Rimuovi tutti
OK
OK
IT
18:52

Eliminare la cronologia.

Per eliminare la cronologia delle pagine web visitate seguire la procedura di seguito indicata:


1
2
3
4
5
6
7
https://www.google.it/?gws_rd=ssl
Google
Pagina
Sicurezza
Strumenti
Opzioni Internet
Connessioni
Programmi
Avanzate
Generale
Sicurezza
Privacy
Contenuto
Pagina iniziale
Per creare le schede della pagina iniziale, digitare ciascun indirizzo su una riga.
http://www.google.it/
Pagina corrente
Pagina predefinita
Usa nuova scheda
Avvio
Avvia con schede dell'ultima sessione
Avvia con pagina iniziale
Schede
Consente di modificare la visualizzazione delle pagine Web.
Schede
Cronologia esplorazioni
Consente di eliminare i file temporanei, la cronologia, i cookie, le password salvate e le informazioni dei moduli Web.
Elimina la cronologia al momento di uscire
Elimina...
Impostazioni
Aspetto
Colori
Lingue
Caratteri
Accessibilità
Elimina cronologia esplorazioni
Mantieni dati sui siti Web preferiti
Mantiene i cookie e i file temporanei Internet in modo che i siti Web preferiti conse
preferenze e possano essere visualizzati più rapidamente.
File temporanei Internet e file di siti Web
Copie di pagine Web, immagini ed elementi multimediali salvate per una più rapida
visualizzazione.
Cookie e dati di siti Web
File o database memorizzati nel computer da siti Web per salvare le preferenze o
migliorare le prestazioni dei siti Web.
Cronologia
Elenco dei siti Web visitati.
Cronologia download
Elenco dei file scaricati.
Dati dei moduli
Informazioni salvate digitate nei moduli.
Password
Password salvate inserite automaticamente quando si accede ad un sito Web visita
precedenza.
Dati di Protezione da monitoraggio, ActiveX Filtering e DNT (Do Not Track)
Elenco di siti Web esclusi dal filtraggio, dati utilizzati da Protezione da monitoraggi
individuare la posizione in cui i siti potrebbero condividere i dettagli della tua visita
eccezioni a richieste DNT (Do Not Track).
Informazioni sull'eliminazione della cronologia delle esplorazioni
Elimina
19:00

Sicurezza in rete

RETI SOCIALI: **Comprendere l'importanza di non divulgare informazioni riservate su siti di reti sociali.**

Le reti sociali (social network: Facebook, Twitter, Google + ..) sono strumenti di comunicazione e gestione delle conoscenze molto diffusi al giorno d'oggi sia tra i giovani che tra gli adulti.

A volte questi strumenti, per certi aspetti così utili, vengono utilizzati in modo poco attento, dimenticando che tutto ciò che viene messo su internet diventa di pubblico dominio e di fatto se ne perde il controllo. Per questo motivo e importante non utilizzare questi strumenti per comunicare dati riservati, come credenziali di accesso a servizi e sistemi informatici, PIN (Personal Identification Number) e qualsiasi altro dato personale e aziendale, soprattutto se di carattere economico e finanziario.

Anche la pubblicazione di immagini private dovrebbe essere considerato con attenzione prima della pubblicazione, cosi come la divulgazione di idee e tendenze di carattere religioso, politico, sessuale.

Sicurezza in rete

Essere consapevoli della necessità di applicare impostazioni adeguate per la privacy del proprio account su una rete sociale.

Utilizzando le reti sociali é possibile impostare la privacy del proprio profilo.

E' importante sapere che esiste questa possibilità ed evitare di lasciare pubblico il proprio profilo.

La cosa migliore è rendere accessibile il proprio profilo solo a persone che si conoscono anche nella vita reale.

BIBLIOGRAFIA

Adattamento, prof. Gino Aloe – Polo Scolastico di Amantea anno scolastico 2017-2018

NB=tutte le immagini utilizzate nella presente dispensa sono state realizzate in proprio (prof. Gino Aloe con informazioni personali o scaricate da Internet