

Introduzione alla protezione dei dati

Compito	<ul style="list-style-type: none"> • Confronto delle impostazioni standard dei social network. • Tematizzazione dei problemi relativi alla protezione dei dati (eventualmente anche ricorrendo al dossier informativo e in particolare al cap. 1 «Che cos'è la protezione dei dati?»). • Individuare le difficoltà che potrebbero insorgere in futuro a causa di una gestione imprudente dei dati. • Scheda aggiuntiva: «Ecco cosa rivelo di me!» Gli scolari più veloci possono riflettere, sulla base della scheda, su quali dati condividerebbero e con chi. <p>La successiva discussione può essere svolta a coppie, a gruppi o come discussione plenaria.</p>
Obiettivi	<ul style="list-style-type: none"> • Gli scolari riflettono su cosa desiderano pubblicare sui social network e sul margine di manovra che hanno a disposizione per quanto concerne le impostazioni personali. • Gli scolari sono in grado di valutare i rischi di una trasmissione e di un salvataggio dei dati in formato non criptato.
Riferimenti al programma d'insegnamento	<ul style="list-style-type: none"> • MI.2.3n: «Gli scolari sono in grado di valutare i rischi di una trasmissione e di un salvataggio dei dati in formato non criptato.»
Materiale	<ul style="list-style-type: none"> • Scheda «Discussione – dati degni di particolare protezione» • Screenshot «Impostazioni relative alla privacy» • Scheda «Tabella»
Forma sociale	Lavoro individuale/lavoro a coppie/discussione plenaria
Durata	60 minuti

Informazioni aggiuntive

- Avendo a disposizione gli screenshot, che raffigurano le impostazioni relative alla privacy di diversi social network, gli scolari possono confrontare e valutare diverse varianti delle impostazioni. Ciò è consigliabile in quanto molti giovani si occupano (troppo) poco di questo aspetto e sono pertanto in grado di fornire solo informazioni limitate sulle impostazioni dei propri account. Se le impostazioni di base non vengono modificate dall'utente, i servizi online e le app in genere rivelano più dati rispetto a quelli necessari per il loro funzionamento (ad es. accesso alla rubrica, localizzazione).
- Per spiegare i termini utilizzati (ad es. social network, cloud) è possibile fare ricorso al dossier «Protezione dei dati» che fa parte della lezione.

Introduzione alla protezione dei dati

- **Incaricato federale della protezione dei dati e della trasparenza (IFPDT)**
Informazioni inerenti alle reti sociali
https://www.edoeb.admin.ch/edoeb/it/home/protezione-dei-dati/Internet_und_Computer/servizi-online/media-sociali/informazioni-inerenti-alle-reti-sociali.html.html



Quanto è sicuro il tuo account?



Discussione

Confronta con il tuo compagno di banco/la tua compagna di banco se le impostazioni relative alla sfera privata nei vostri social network sono differenti e in che modo. A tale scopo utilizzate come aiuto gli screenshot che trovate nella pagina successiva.

Esempi: Instagram, google+, Snapchat, Facebook, kik ecc.

- o Constate delle **differenze**?
(sfera privata, sicurezza, richieste di amicizia, notifiche ecc.)
- o Discutete inoltre che cosa cambia se adottate **altre impostazioni per il vostro profilo**.
- o Ci sono impostazioni che devono essere effettuate **assolutamente**?
- o Che cosa invece **non** è possibile **modificare**?

→ Annotate le vostre constatazioni nelle righe seguenti.

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....



Lo sapevi?

I social network in genere sono gratuiti, ma non sono istituzioni di pubblica utilità. In realtà si tratta di un «commercio»: i servizi a favore degli utenti in cambio dei loro dati.

<http://www.giovanimedia.ch/it/home.html>

Avvertenze e consigli interessanti sui social network e le impostazioni di sicurezza consigliate.



Fonte immagini: Wepushbuttons
<https://wepushbuttons.com.au/wp-content/uploads/2013/04/social-media-list.jpg>



Esempio 1: impostazioni relative alla privacy di Facebook (aprile 2018)

Impostazioni sulla privacy e strumenti

Le tue attività	Chi può vedere i tuoi post futuri?	Amici	Modifica
	Controlla tutti i post in cui sei taggata		Usa il Registro attività
	Vuoi limitare il pubblico dei post che hai condiviso con gli amici degli amici o con il pubblico?		Limita i post passati
In che modo le persone ti trovano e ti contattano	Chi può inviarti richieste di amicizia?	Tutti	Modifica
	Chi può vedere la tua lista degli amici?	Tutti	Modifica
	Chi può cercarti usando l'indirizzo e-mail che hai fornito?	Amici	Modifica
	Chi può cercarti usando il numero di telefono che hai fornito?	Tutti	Modifica
	Desideri che i motori di ricerca esterni a Facebook reindirizzino al tuo profilo?	Sì	Modifica

Esempio 2: impostazioni relative alla privacy di Twitter (aprile 2018)

Privacy e sicurezza

Privacy

Privacy dei Tweet **Proteggi i tuoi Tweet**

Se selezionata, solo le persone che autorizzi riceveranno i tuoi Tweet. I Tweet che invierai in futuro non saranno disponibili pubblicamente. I Tweet che hai inviato precedentemente potrebbero essere ancora visibili al pubblico su alcuni siti. [Scopri di più.](#)

Posizione dei Tweet **Twitter con la posizione**

Se selezionato, puoi aggiungere una posizione ai tuoi Tweet, come la tua città o posizione precisa, dal Web e tramite applicazioni di terze parti. Questa impostazione non è valida per l'app Twitter su iOS e Android. [Scopri di più](#)

Elimina l'informazione sulla localizzazione

In questo modo saranno eliminate le informazioni di localizzazione che hai aggiunto ai tuoi Tweet. L'operazione può durare fino a 30 minuti.

Tag nelle foto

- Consenti a chiunque di taggarti nelle foto
- Consenti solo a chi segui di taggarti nelle foto
- Non consentire a nessuno di taggarti nelle foto

Reperibilità

- Consenti reperibilità tramite la tua email
- Consenti reperibilità tramite il tuo numero

Questa impostazione avrà effetto dopo che avrai aggiunto un numero di telefono. [Aggiungilo adesso](#)

[Scopri di più](#) su come questi dati vengono utilizzati per metterti in contatto con le persone.

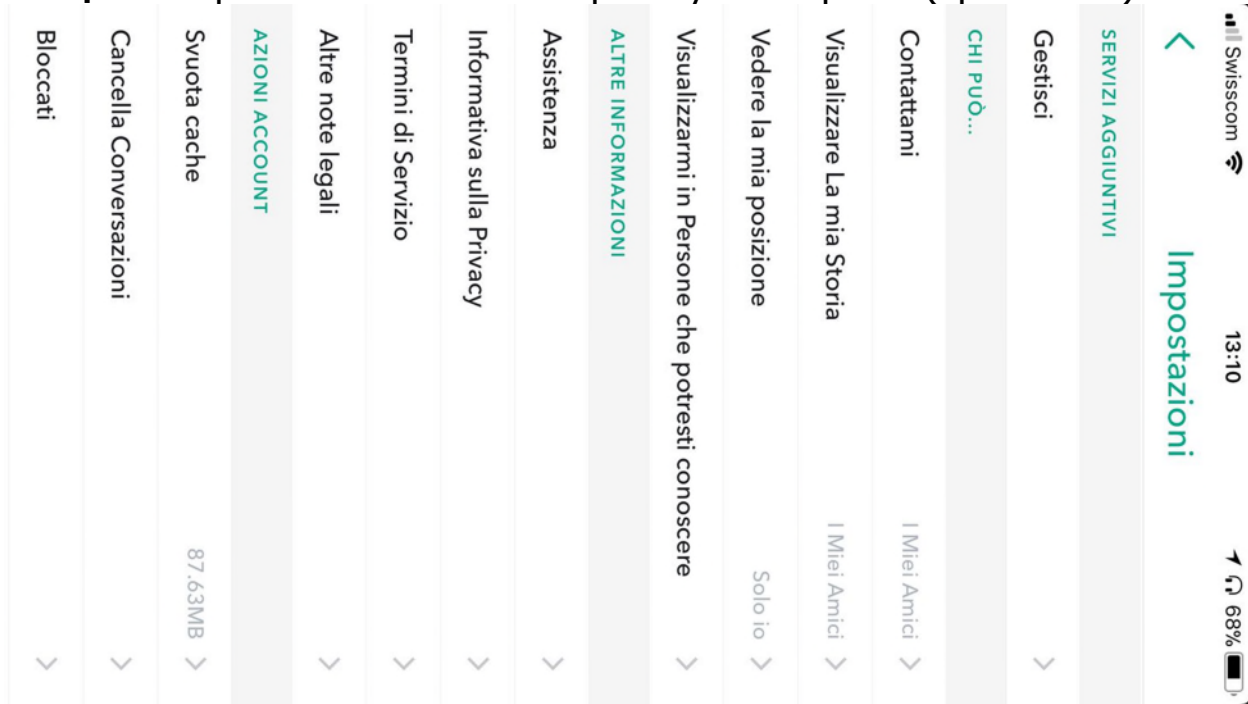
Rubrica

Gestisci i tuoi contatti

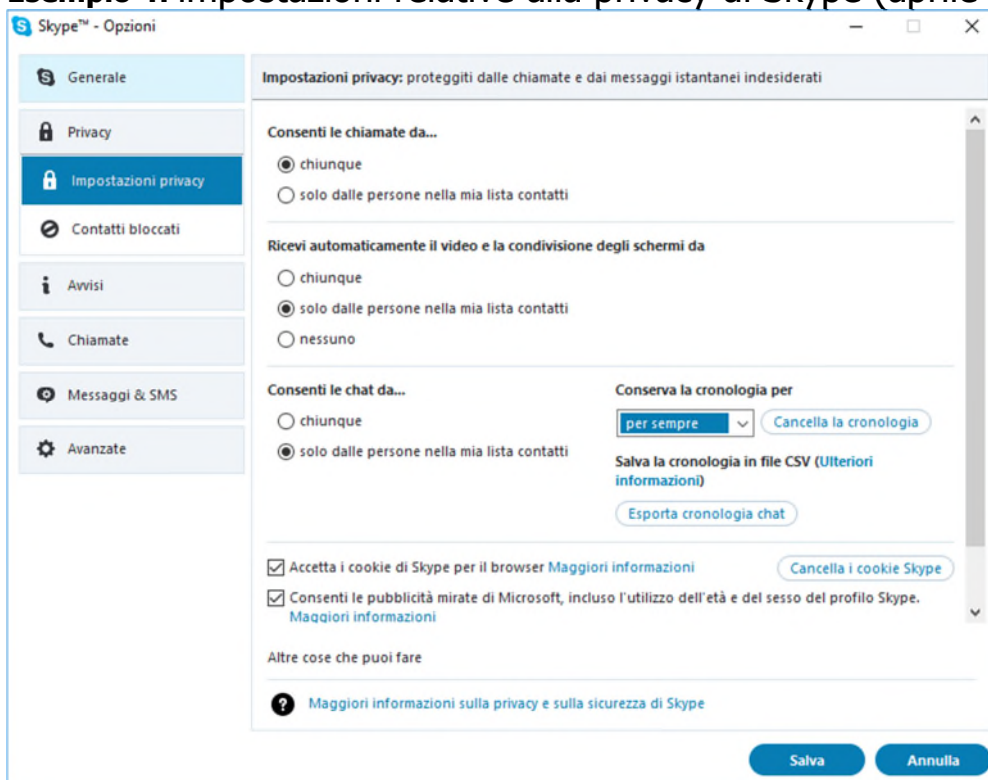
Contatti che hai caricato su Twitter dalla tua rubrica.



Esempio 3: impostazioni relative alla privacy di Snapchat (aprile 2018)



Esempio 4: impostazioni relative alla privacy di Skype (aprile 2018)





Ecco cosa rivelo di me!



Compito

Nella tabella seguente indica con un simbolo quali informazioni comunicheresti ai diversi gruppi di persone.

Indica un (+) per «Sì», un (-) per «No» e un (?), se non sei sicuro/a.

	Famiglia	Amici/amich e	Capo, insegnante	Follower su Instagram	Estranei in strada	Sconosciuti in chat
Età, sesso						
Gruppo sanguigno						
Dati relativi a fratelli/sorelle, membri della famiglia						
Salario, posto di lavoro						
Foto di me e del mio fidanzato/della mia fidanzata						
Contatti di lavoro						
Lista dei contatti del mio cellulare						
Il mio numero di cellulare						
Il mio indirizzo e-mail						
L'indirizzo della mia abitazione						
Il codice PIN del mio cellulare o laptop						
Foto del mio volto						
Foto del mio corpo (con i vestiti)						
Foto del mio corpo nudo						
Il saldo del mio conto						



Proposte di soluzione

Scheda «Quanto è sicuro il tuo account?»

→ Soluzioni individuali degli scolari

Importante è l'avvertenza che, per alcuni social network, le impostazioni relative alla privacy devono essere modificate attivamente. Su Instagram, ad esempio, il profilo è in linea di principio accessibile a tutti. Se si desidera renderlo accessibile solo agli amici (follower), è necessario modificare le impostazioni relative alla privacy.

Vedi anche (in tedesco):

http://praxistipps.chip.de/privatsphaere-fuer-instagram-einstellen-so-klappts_12050

Scheda «Se i dati finiscono in mani sbagliate...»

Possibili continuazioni e spunti di discussione

- Situazione 1** *Dalla chat di gruppo le foto possono essere inviate teoricamente a chiunque e possono addirittura essere pubblicate su Internet. Ciò può causare problemi ad esempio con i genitori, con l'azienda formatrice ecc.*
- Situazione 2** *In base alle impostazioni relative alla privacy, l'immagine del profilo di Stephan può essere visibile anche agli altri utenti. Dato che Stephan ha fotografato un'altra persona senza il suo espresso consenso, pubblicandone la foto, potrebbero derivarne conseguenze non solo a livello civile, ma addirittura a livello penale. Soprattutto per il fatto che l'altra persona è stata fotografata mentre si stava spogliando.*
- Situazione 3** *Dopo la loro separazione, sia Lea che il suo ex ragazzo non hanno alcun controllo su ciò che accade delle foto che si sono scattati reciprocamente. Da un lato le foto possono essere inviate ad altri e pubblicate, il che sicuramente è contrario alla volontà della persona fotografata. Dall'altro lato, inoltrando o pubblicando le foto senza il consenso dell'altra persona, essi violano la legge sulla protezione dei dati e la privacy dell'altra persona, rendendosi eventualmente addirittura penalmente perseguibili.*
- Situazione 4** *Avendo salvato i propri dati su un cloud all'estero, Michael non può essere certo che tali dati siano protetti secondo lo standard vigente in Svizzera. Dato che si tratta di dati riservati e password, l'eventuale accesso abusivo di terzi ai dati potrebbe comportare notevoli danni per Michael.*
- Situazione 5** *Michelle scatta le foto senza il consenso delle persone fotografate e poi le pubblica. Così facendo va incontro a conseguenze a livello civile.*



Situazione 6 *Le richieste di amicizia da parte di sconosciuti non devono essere accettate, perché non si può essere certi che questa persona non abbia cattive intenzioni. Così facendo si rischia di mettere in situazioni spiacevoli o pericolose non solo se stessi, ma anche altre persone. Philipp deve partire dal presupposto che tutti i contenuti che in futuro condividerà con i suoi amici verranno visti anche da questa persona, la quale li potrà utilizzare, elaborare e pubblicare.*

Situazione 7 *Dato che le banche non richiedono mai dati di accesso per SMS o e-mail, bisogna presupporre che una persona non autorizzata stia tentando di ottenere i dati bancari di Corinne con l'inganno. Se Corinne comunica i propri dati bancari, va incontro a un danno finanziario. Per questo non bisogna mai aprire gli allegati di e-mail di questo tipo o cliccare sui link in esse contenuti.*

Situazione 8 *Dato che Francesco non ha protetto il suo cellulare con una password, chi lo trova casualmente ha accesso a tutti i dati, le app e i contenuti presenti sullo smartphone. Ciò può comportare l'accesso abusivo a contenuti sensibili (foto, video, notizie ecc.) oppure un utilizzo degli account di Francesco per filtrare contatti, contattare persone sotto falso nome ecc.*

Per quanto concerne le conseguenze penali nel campo della protezione dei dati vedi «Immagini e diritti di immagine (2.7)», nonché «Rischi concreti e conseguenze giuridiche (2.4)» e «Smartphone (2.5)» nel dossier informativo «Protezione dei dati» relativo a questa serie di lezioni.

Scheda aggiuntiva «Ecco cosa rivelo di me!»

→ *Soluzioni individuali degli scolari.*