A seguito di numerose segnalazioni di presunte violazioni dei profili Instagram dei nostri alunni avvenute tramite Zoom, ci corre l'obbligo di segnalare quanto segue:

1) Zoom ha inviato una email agli utenti, ammettendo di avere avuto dei problemi di gestione della sicurezza in passato e di conseguenza ha annunciato azioni risolutive per garantire la riservatezza dei profili e la sicurezza degli utenti. Tanto è vero che già da alcuni giorni abbiamo potuto verificare differenti modalità di accesso al servizio, più stringenti e quindi anche più complesse, con tempi di accesso più lunghi. Inoltre da poche ore è stato rilasciato un ulteriore aggiornamento dell'applicazione con l'aggiunta di alcuni comandi relativi esclusivamente la sicurezza del collegamento Per questi motivi attualmente il problema appare superato.
2) La segnalazione da parte della stragrande maggioranza degli alunni che hanno riscontrato delle attività anomale sul proprio profilo Instagram, riguardano le indicazioni provenienti dalle "Attività di accesso" indicate all'interno dell'apposito menù all'interno del profilo Instagram. Abbiamo potuto verificare personalmente che questo servizio non è preciso e quindi non può essere questa la dimostrazione di una violazione di un account personale.
3) La violazione di un account Instagram, sebbene tecnicamente possibile ad un malintenzionato dotato di conoscenze informatiche, è comunque una operazione piuttosto laboriosa, perché prevede la necessità del pirata di sostituirsi completamente all'utente, riuscendo ad intercettare una mail od un sms di notifica con una password di ricambio, dopo averne richiesto l'invio a Instagram, fingendosi l'utente reale. L'indirizzo mail può essere un dato ricavabile tramite Zoom, ma il controllo di un terminale quale il cellulare, può avvenire solo o tramite una applicazione che deve venire installata sul cellulare, o tramite la clonazione della sim. Più probabile potrebbe essere la violazione di un indirizzo di posta elettronica, visto che esistono diversi database pieni di indirizzi violati in vendita sul cosiddetto dark web.

In conseguenza di quanto finora esposto, ci pare ragionevole fornire due tipologie di indicazioni: la prima, rivolta a docenti e alunni, sulle condotte elementari di buon senso che si possono utilizzare per mitigare i rischi derivanti dall'utilizzo di una piattaforma elettronica come Zoom. Deve essere chiaro a tutti però, che non esiste una piattaforma esente dagli attacchi dei pirati informatici, e che questi sono particolarmente frequenti nell'ultimo periodo, proprio per il fatto che siamo maggiormente esposti a causa dell'aumento esponenziale dei tempi di collegamento ad Internet. E non si può pensare che Zoom sia meno sicura di altre applicazioni semplicemente perché gratuita. Anche perché in effetti non lo è. È gratuito solo l'utilizzo ridotto (non per i docenti registrati con l'indirizzo di posta istituzionale, ovviamente). Le indicazioni sono raccolte nei due piccoli decaloghi allegati ed indicano un ristretto numero di operazioni a cui fare attenzione per innalzare quanto più possibile il livello di sicurezza degli utenti, di Zoom e di Instagram.

MODALITÁ DI UTILIZZO DELLA PIATTAFORMA ZOOM

I docenti sono invitati a comportarsi come segue:

1) Utilizzare, nell'iscrizione al servizio, esclusivamente la mail istituzionale (nomecognome@istruzione.it), il che permette di avere un profilo senza il limite temporale dei 40 minuti.
2) Verificare preliminarmente l'adesione di tutti i ragazzi al consenso sulla didattica a distanza. Coloro i quali non risultano aver dato l'assenso, non potranno partecipare a questa forma di didattica, per cui i contatti saranno tenuti esclusivamente utilizzando il registro elettronico.
3) Generare un link di accesso al meeting temporaneo (diverso quindi dal link attribuito di default ad ogni iscritto) solo pochi minuti prima della lezione e pubblicarlo solo attraverso il registro elettronico. Evitando cioè di comunicarlo ai ragazzi tramite whatsapp.
4) Verificare, man mano che arrivano le richieste di accesso, l'identità dei richiedenti, senza autorizzare l'ingresso a utenti che si presentano con un nome di fantasia.

Gli alunni sono invitati a comportarsi come segue:

1) Utilizzare dei nomi di accesso chiari e non di fantasia, onde permettere il facile riconoscimento da parte dell'insegnante. Laddove ciò risulti impossibile, perché magari non si è in grado di cambiare il nome di default, che potrebbe riferirsi al device utilizzato per la connessione piuttosto che al nome dell'utente (es. Ipad n°…), può comunicare la sigla che compare quale suo nome, pena la esclusione dal gruppo Zoom.
2) Attivare sempre la cam per permettere all'insegnante di verificarne l'identità e la reale presenza. Laddove ciò non fosse possibile per qualsiasi motivo, ciò deve essere comunicato al docente, che deciderà se tale comportamento è ammissibile in base alla motivazione addotta.
3) Impegnarsi a non pubblicare o rendere pubblico per nessun motivo il link di invito predisposto dal docente e quindi non utilizzare alcun mezzo non autorizzato per comunicare il link in questione a chicchessia.
4) Seguire la lezione in assoluto silenzio, senza arrecare disturbo al gruppo classe.
5) Se si utilizza il servizio Zoom con la sottoscrizione di un account (non obbligatorio), si raccomanda di indicare una mail assolutamente non collegata ad altre iscrizioni quali, ad esempio, social network e simili.
   Il Dirigente scolastico

Il Team dell'Innovazione della S.M.S."G.Scotti"

Il Dirigente Scolastico
Dott.ssa Lucia Monti
(Firmato digitalmente)

OPERAZIONI DA EFFETTUARE NEL CASO SI VOGLIA RAFFORZARE LA SICUREZZA DEL PROFILO PERSONALE SU INSTAGRAM

Nel caso in cui si abbia il sospetto di essere stati oggetto di un attacco al proprio account Instagram, la prima cosa fa fare è cambiare la password. Se non si è in grado di entrare perché l'attacco informatico ha causato la perdita delle credenziali di accesso, utilizzare la procedura prevista da Instagram per il recupero della password smarrita. È consigliabile cambiare la password relativa anche all'indirizzo di posta elettronica legata all'iscrizione dello stesso account. Le password, per essere efficaci, hanno bisogno di una certa complessità (e lunghezza) ma, soprattutto non devono essere sempre le stesse per diversi servizi (non utilizzare ad esempio per l'iscrizione a servizi tipo Zoom la stessa password che viene utilizzata per Instagram o per Facebook, etc. etc.).

In generale, è buona norma massimizzare il livello di sicurezza di un account di Istagram, utilizzando la funzione "Autentificazione a due fattori", opzione che prevede la possibilità di ricezione di codici di backup (necessari nel caso in cui non si riesca più ad accedere al relativo profilo) e di un codice di sicurezza che l'account richiede nel momento in cui vi sia una attività sospetta o inusuale. Questa funzione è raggiungibile cliccando sulla rotellina delle opzioni, andando nel menù sicurezza e poi cliccando sul rigo "Autentificazione a due fattori". È consigliabile conservare i relativi codici in un posto diverso dal proprio cellulare o tablet (o qualsiasi altro device con cui si accede a Instagram), meglio ancora se su supporto cartaceo.

Evitare di cadere in tranelli quali ad esempio il phishing. Se pensate di aver ricevuto una email da Instagram controllatene l'esistenza nell'applicazione. Per eseguire quest'ultima operazione e per approfondire il tema della sicurezza, andare sul link https://www.kaspersky.it/blog/keep-instagram-secure/7240/, che spiega tutte le tecniche di sicurezza possibili su questo Social Network.

Con questo vademecum non si intende affatto incentivare l'uso di un mezzo di comunicazione, Instagram, per il quale la normativa prevede la impossibilità di iscrizione al di sotto dei tredici anni senza il controllo e **l'approvazione da parte dei genitori**. Ma solo un piccolo aiuto per coloro i quali si sono visti violare l'account o presumono che ciò sia accaduto.

A questo proposito, è opportuno ribadire che non è provata la violazione dell'account laddove viene semplicemente segnalata un'attività in un luogo geografico diverso dal proprio, ma, nel dubbio, è sempre possibile innalzare il profilo di sicurezza.

Il Team dell'Innovazione della S.M.S. "G.Scotti"

Il Dirigente Scolastico
Dott.ssa Lucia Monti
(Firmato digitalmente)