Istituto Comprensivo "De Amicis - Giovanni XXIII"
Piazza Di Vagno, 18 - 70021 Acquaviva delle Fonti (BA) - Tel. 080.761314 - 080.761013 - Fax 080.3051357
www.icdeamicisgiovanni23.edu.it
baic89400e@istruzione.it
baic89400e@pec.istruzione.it
C.F. 91121590722
Codice Meccanografico BAIC89400E

- A tutto il personale Docente
- E per loro tramite alle famiglie degli alunni
  I.C.De Amicis - Giovanni XXIII
- Al DSGA
  LORO SEDI

COMUNICATO N.212

inviato a mezzo mail

OGGETTO: **Vigilanza per un uso consapevole delle piattaforme per le attività sincrone (zoom, meet, skype, …)**

La maggior parte delle attività sincrone si svolge con l'uso di piattaforme che potrebbero consentire comunque **l'intrusione di hacker**. Questo potrebbe avvenire anche con ***Zoom Cloud Meetings*** che, al momento, è la piattaforma più diffusa fra i docenti di questo istituto.
Si consiglia pertanto di vigilare e di INFORMARE alunni e famiglie sull'eventualità di tale rischio.
Di seguito vi forniamo alcune accortezze da seguire per prevenire spiacevoli inconvenienti.

1. **Proteggete il vostro account**

Un account Zoom è come un qualsiasi altro account e, quando lo configurate, dovreste applicare le regole base che ne garantiscano la protezione. Usate una password robusta e unica, e proteggete il vostro account con l'autenticazione a due fattori, che rende il vostro account più difficile da hackerare e maggiormente protetto, anche nel caso in cui i dati del vostro account dovessero trapelare (sebbene fino ad ora non sia mai successo). C'è bisogno di almeno un altro dettaglio da considerare di Zoom: dopo la registrazione, oltre al login e alla password si ottiene un Meeting ID Personale. Evitate di renderlo pubblico. Poiché Zoom offre la possibilità di creare riunioni pubbliche con il vostro Meeting ID Personale (PMI, dalla sigla in inglese), è abbastanza facile che questo codice venga condiviso senza pensarci troppo. Se lo fate, chiunque conosca il vostro PMI, può partecipare a qualsiasi riunione che organizzate (e probabilmente non vorrete che persone a caso possano intrufolarsi), quindi **condividete queste informazioni con prudenza.**

2. **Non utilizzate i social network per condividere i link delle conferenze**

A volte vorreste creare un evento pubblico, e in questi giorni spesso gli eventi online sono gli unici disponibili, quindi Zoom sta attirando sempre più persone. Ma anche se il vostro evento è veramente aperto a tutti, dovreste evitare di condividere il link sui social network.

Se sapevate qualcosa di Zoom prima di leggere questo post, avrete probabilmente sentito parlare del cosiddetto Zoombombing. È un termine coniato dal giornalista di Techcrunch Josh Constine per descrivere i troll che disturbano le riunioni di Zoom pubblicando contenuti offensivi. In questo momento, potrebbero essere attive diverse chat su Discord o thread su 4Chan (piattaforme entrambi popolari tra i troll) dove si parla di quali saranno i prossimi obiettivi dei loro raid.

Ma i troll da dove prendono le informazioni sui prossimi eventi in programma? Ebbene sì, le trovano sui social network. Per questo motivo, evitate di postare pubblicamente i link alle riunioni di Zoom. Se per qualche motivo desiderate ancora farlo, assicuratevi di non attivare l'opzione Use Personal Meeting ID (Usa il Meeting ID Personale).

3. **Proteggete ogni riunione con una password**

Impostare una password rimane il miglior mezzo per garantire che solo le persone da voi scelte possano partecipare alla riunione. Recentemente Zoom ha attivato la protezione della password di default, una buona mossa effettivamente. Detto questo, non confondete la password della riunione con la password del vostro account Zoom. Esattamente come i link delle riunioni, le password dei meeting non dovrebbero mai apparire sui social network o su altri canali pubblici, o i vostri sforzi per proteggere la vostra chiamata dai troll saranno inutili.

4. **Attivate la Waiting Room**

Un'altra impostazione che consente un maggiore controllo sulla riunione, è la Waiting Room: recentemente abilitata di default, fa attendere i partecipanti in una "sala d'attesa" fino all'approvazione di ognuno da parte dell'organizzatore. Questo vi dà la possibilità di controllare chi sono i partecipanti alla riunione, nel caso in cui una persona non autorizzata sia riuscita a ottenere la password. Questa opzione consente anche di escludere una persona indesiderata dalla riunione, facendola ritornare nella sala d'attesa. Si consiglia di lasciare questa casella spuntata.

5. **Prestate attenzione alle funzioni di condivisione dello schermo**

Qualsiasi app per videoconferenze offre la condivisione dello schermo, ovvero la possibilità per un partecipante di mostrare il proprio schermo agli altri, e Zoom non fa eccezione. Alcune impostazioni che vale la pena di tenere sott'occhio:

Possibilità di condivisione dello schermo all'organizzatore o di estenderla a tutti i partecipanti alla chiamata. Se non avete bisogno che altre persone mostrino i loro schermi, sapete quale opzione scegliere;

Possibilità per più partecipanti di condividere simultaneamente il proprio schermo. Se non riuscite a capire subito perché le vostre riunioni avrebbero bisogno di questa funzionalità, probabilmente non ne avrete mai bisogno; tuttavia, tenetelo presente nel caso in cui vi risulti necessario abilitare questa opzione.

6. **Utilizzate il client web, quando possibile**

I vari clienti di Zoom hanno rilevato una serie di difetti. Alcune versioni consentono ai cybercriminali di accedere alla fotocamera e al microfono del dispositivo; altre permettono ai siti web di aggiungere utenti alle chiamate senza il loro consenso. Zoom ha risolto rapidamente questi i problemi (così come altri simili) e ha smesso di condividere i dati degli utenti con Facebook e LinkedIn. Tuttavia, data l'assenza di un'adeguata valutazione della sicurezza, è probabile che gli utenti Zoom rimangano vulnerabili, e potrebbero ancora accadere pratiche poco trasparenti come la condivisione di dati con terze parti.

Ecco perché consigliamo di utilizzare l'interfaccia web di Zoom e di non installare l'app sul dispositivo, se possibile. La versione web si trova in una sandbox nel browser e non ha le autorizzazioni di cui dispone un'applicazione installata, limitando così la quantità di danni che può potenzialmente causare.

In alcuni casi, tuttavia, anche se si vuole usare l'interfaccia web, potreste notare che Zoom ha proseguito il download del programma di installazione, e non c'è altra opzione per connettersi al meeting se non quella di installare il client. In questo caso, potete almeno limitare l'installazione di Zoom su un solo dispositivo. Che sia il vostro smartphone secondario o, ad esempio, un portatile di riserva. Scegliete un dispositivo che non contenga quasi nessuna informazione personale.

7. **Non credete alla cifratura end-to-end pubblicizzata da Zoom**

Zoom ha guadagnato la sua quota di mercato non solo per i suoi prezzi e le sue caratteristiche, ma anche perché ha pubblicizzato la cifratura end-to-end del prodotto. Grazie a essa, tutte le comunicazioni tra voi e le persone che state chiamando sono cifrate in modo che solo voi e le persone in chiamata possano decifrarle. Tutte gli altri, compresi i fornitori dei servizi, non possono.

Sembrerebbe bello, ma è quasi impossibile, come hanno sottolineato i ricercatori di sicurezza. Zoom ha dovuto riconoscere che, nel suo caso, l'altro end si riferisce al server Zoom, il che significa che il video è cifrato ma i dipendenti di Zoom, e potenzialmente le forze dell'ordine, vi hanno accesso. Il testo nelle chat, però, sembra essere davvero cifrato con metodo end-to-end. Questa puntualizzazione non è necessariamente un motivo per abbandonare definitivamente Zoom, anche altri popolari servizi di videoconferenza non dispongono di un sistema di cifratura end-to-end. In ogni caso, ne dovreste tenere conto, e non discutere di segreti personali o commerciali su Zoom.

8. **Pensate a ciò che la gente può vedere o sentire**

Questo vale per ogni servizio di videoconferenza, non solo per Zoom. Prima di avviare la chiamata, prendetevi un momento per considerare ciò che gli altri vedranno o sentiranno quando vi unirete alla chiamata. Anche se siete a casa da soli, potrebbero aspettarsi che siate completamente vestiti. È sempre una buona idea mantenere un certo decoro.

Lo stesso vale per il vostro schermo, se avete intenzione di condividerlo. Chiudete tutte le finestre che preferite che gli altri non vedano.

IL DIRIGENTE SCOLASTICO
Prof.ssa Valeria BRUNETTI
(firma autografa sostituita a mezzo stampa ai sensi
e per gli effetti dell'art. 3, co. 2, D.Lgs. n. 39/93)

Acquaviva delle Fonti, 24 aprile 2020

Il responsabile del procedimento (L 241/90)
Anna BIFERNO