Associazione Protezione Diritti e Libertà Privacy

CONSULENZE PACI PRIVACY

La sicurezza nell'e_learning
Seminario formativo
sulla protezione dei dati personali
16 aprile 2020

Luciano Delli Veneri

La sicurezza nell'e_learning

Documenti di riferimento:

1) **"Didattica a distanza: prime indicazioni ", Provvedimento del 26 marzo 2020 - Garante privacy**
2) **«Emergenza sanitaria da nuovo Coronavirus. Prime indicazioni operative per le attività didattiche a distanza», Ministero dell'Istruzione, 17 marzo 2020**
3) **"Orientações para utilização de tecnologias de suporte ao ensino à distância", Comissão Nacional de Proteção de Dados Portugues –8 aprile 2020**
4) **«RESOLUTION ON E-LEARNING PLATFORMS», International Conference of Data Protection and Privacy Commissioners –Bruxelles, ottobre 2018**
5) **"Working Paper on E-Learning Platforms", International Working Group on Data Protection in Telecommunications (ICDPPC), 24-25 aprile 2017**

La sicurezza nell'e_learning

Secondo l' International Working Group on Data Protection in Telecommunications (ICDPPC):

«Le aule sono diventate ambienti sempre più collegati in rete che possono mettere a rischio la privacy degli studenti.

In particolare, queste aule collegate possono presentare problemi di trasparenza, in considerazione del fatto che pratiche di elaborazione dei dati delle piattaforme di e-learning non abbiano tenuto nella debita considerazione la privacy.

Potrebbero, inoltre, essere impiegati un processo decisionale automatizzato opaco o un uso improprio dell'analisi dei dati di apprendimento che rischiano di compromettere la protezione dei dati e i diritti alla privacy.

Nel caso di bambini e giovani, ciò può avere conseguenze sociali, economiche e professionali a lungo termine e non riuscire a tenere conto della loro curva di apprendimento in evoluzione»

La sicurezza nell’e_learning

L’ ICDPPC invita tutte le parti interessate nel campo dell'e-learning, in particolare:

- Fornitori e produttori di piattaforme di e-learning, compresi i fornitori di servizi di trasmissione dati rivolti agli studenti; e
- Autorità educative, compresi ministeri dell'istruzione, consigli scolastici, scuola, amministratori ed educatori.

a rispettare pienamente i diritti degli studenti, dei genitori e degli educatori («interessati") alla protezione dei loro dati personali e privacy e a garantire che i dati raccolti vengano utilizzati esclusivamente a fini educativi e per finalità conformi alla legge sulla protezione dei dati

La sicurezza nell'e_learning

L'ICDPPC ritiene che:

Autorità che governano l'istruzione debbano:

1. Garantire che dispongano di autorità e competenza per selezionare i servizi delle piattaforme di e-learning;
2. Sviluppare politiche e procedure per valutare, approvare e supportare l'uso di piattaforme di e-learning e, ove possibile o richiesto, condurre la valutazione di impatto sulla privacy (DPIA);
3. Somministrare adeguata formazione e fornire supporto continuo agli educatori;
4. Collaborare con altre autorità educative e, in collaborazione con le autorità locali per la protezione dei dati, concordare standard comuni per l'utilizzo delle piattaforme di e-learning;
5. Ove richiesto o appropriato, chiedere il consenso valido, informato e significativo da parte degli interessati;
6. Coerentemente con la normativa nazionale, attuare una politica per le persone che accedono alla piattaforma di apprendimento con i loro dispositivi elettronici personali.

La sicurezza nell'e_learning

L'ICDPPC ritiene che:

Autorità educative, fornitori e produttori di piattaforme di e-learning, congiuntamente o indipendentemente secondo la legge nazionale sulla protezione dei dati, debbano:

1. Garantire che le piattaforme di e-learning proteggano adeguatamente i dati personali degli utenti e adottino gli standard di protezione dei dati appropriati;
2. Assicurare che le finalità per cui i dati personali vengono raccolti, elaborati e utilizzati siano legittimi, adeguati al contesto e autorizzati dalla legge;
3. Ridurre al minimo la quantità di dati personali trattati;
4. Informare le persone sui dati personali che devono essere raccolti ed elaborati dalla piattaforma di e-learning e sui motivi del trattamento (Informativa privacy);
5. Se possibile, consentire alle persone di utilizzare la piattaforma di e-learning senza l'impiego di dati personali (non identificativi/pseudoanonimizzati);
6. Evitare, ove possibile, l'uso dei dati personali e in particolare dei dati comportamento di apprendimento, a fini predittivi, profilazione o processo decisionale automatizzato;
7. Definire e rispettare i periodi di conservazione per le diverse categorie di dati personali.

La sicurezza nell'e_learning

L'ICDPPC ritiene che:

Fornitori e produttori di piattaforme di e-learning, debbano:

1. Essere trasparenti sulle loro pratiche di trattamento dei dati sia con le autorità educative che con le persone che utilizzano le piattaforme di e-learning;
2. Limitare gli scopi della raccolta dei dati personali in base al contesto e descrivere nei «termini di servizio» se e quando i dati personali possono essere divulgati;
3. Adottare le Privacy Enhancing Technologies (PET) e applicare i principi di Privacy by Design e per impostazione predefinita allo sviluppo delle piattaforme e del sw;
4. Garantire che i dati personali siano archiviati in conformità con la legislazione locale sulla protezione dei dati e nel rispetto dei tempi di conservazione fissati.

La sicurezza nell'e_learning

L'ICDPPC ritiene che:

Coerentemente con il diritto nazionale sia necessario attuare una politica per le persone che accedono alla piattaforma di e-learning con i propri dispositivi elettronici personali, e che le Autorità educative, i Produttori e Fornitori di piattaforme e-learning debbano:

1. Valutare con attenzione i rischi connessi all'utilizzo di dispositivi elettronici personali da parte degli utenti delle piattaforme definendo opportune azioni di mitigazione;
2. Ridurre, e se possibile evitare, di raccogliere dati personali presenti nei dispositivi elettronici personali utilizzati dagli utenti per collegarsi alle piattaforme, che non siano quelli strettamente necessari per il corretto funzionamento dei servizi;
3. Fornire adeguate istruzioni sulle modalità da adottare per garantire i necessari livelli di sicurezza di tali dispositivi elettronici personali anche indicando indicazioni circa l'esigenza di mantenere aggiornati le patch di sicurezza e gli antivirus.

La sicurezza nell'e_learning

dovrebbe, quindi, essere possibile:

1. Consentire alle persone di utilizzare la piattaforma di e-learning senza registrarsi per un account personale. Laddove è necessario un identificativo o un account studente, è necessario creare pseudonimi che non rivelino nomi o altri dati identificativi personali;
2. Laddove i dati personali debbano essere raccolti dalla piattaforma di e-learning, deidentificare o aggregare i dati il prima possibile;
3. Evitare l'uso degli account dei social media per l'accesso alla piattaforma in quanto può comportare una raccolta e una divulgazione eccessive del profilo dettagliato e altre informazioni identificabili tra il sito di social network e la piattaforma di e-learning e può limitare la capacità degli studenti di impedire il monitoraggio delle loro attività online sul Web.

In sintesi:

I fornitori di piattaforme di e-learning dovrebbero consigliare agli educatori di ridurre al minimo le informazioni personali utilizzate per creare un profilo assegnando pseudonimi agli studenti. Gli studenti dovrebbero poter accedere ai loro profili inserendo un codice di accesso univoco fornito loro. In questo modo, gli studenti non devono fornire le loro informazioni personali e possono utilizzare il servizio in modo pseudoanonimizzato.

La sicurezza nell'e_learning

Nel provvedimento del 26 marzo 2020, "**Didattica a distanza: prime indicazioni** ", l'Autorità per la protezione dei dati personali Garante richiama l'attenzione dei Fornitori e Utilizzatori della didattica a distanza sui seguenti aspetti:

1. **Base giuridica del trattamento dei dati personali**, ossia l'esigenza che il trattamento dei dati personali abbia una base giuridica chiara ed inequivoca che renda lecito e legittimo l'impiego della formazione a distanza;
2. **Privacy by design e by default**: scelta e configurazione degli strumenti da utilizzare che garantiscano che la raccolta ed il trattamento dei dati personali sia rispettosa fin dall'origine e che siano trattati solo il set di dati personali indispensabili al perseguimento delle finalità eventualmente effettuando la DPIA nel caso di rischi elevati per i diritti e le libertà degli Interessati;
3. **Il ruolo dei fornitori dei servizi on line e delle piattaforme**, che devono essere selezionati accuratamente tra quelli che garantiscono il pieno rispetto delle prescrizioni della normativa sulla protezione dei dati personali in particolare che i dati trattati per loro conto siano utilizzati solo per la didattica a distanza e che siano rispettate le specifiche istruzioni sulla conservazione dei dati, sulla cancellazione - al temine del progetto didattico - di quelli non più necessari, nonché sulle procedure di gestione di eventuali violazioni di dati personali;
4. **Limitazione delle finalità del trattamento**, evitando utilizzi ulteriori e non previsti dei dati personali;
5. **Liceità, correttezza e trasparenza del trattamento**, dovendo le istituzioni scolastiche e universitarie assicurare la trasparenza del trattamento informando gli interessati (alunni, studenti, genitori e docenti), compreso, per i docenti, gli aspetti relativi al possibile «controllo a distanza dei lavoratori» (l. 300/70).

La sicurezza nell'e_learning

Nel provvedimento del 26 marzo 2020, "**Orientações para utilização de tecnologias de suporte ao ensino à distância**", l'Autorità per la protezione dei dati personali portoghese richiama l'attenzione delle Autorità educative, dei Fornitori e degli Utilizzatori della didattica a distanza sui seguenti aspetti:

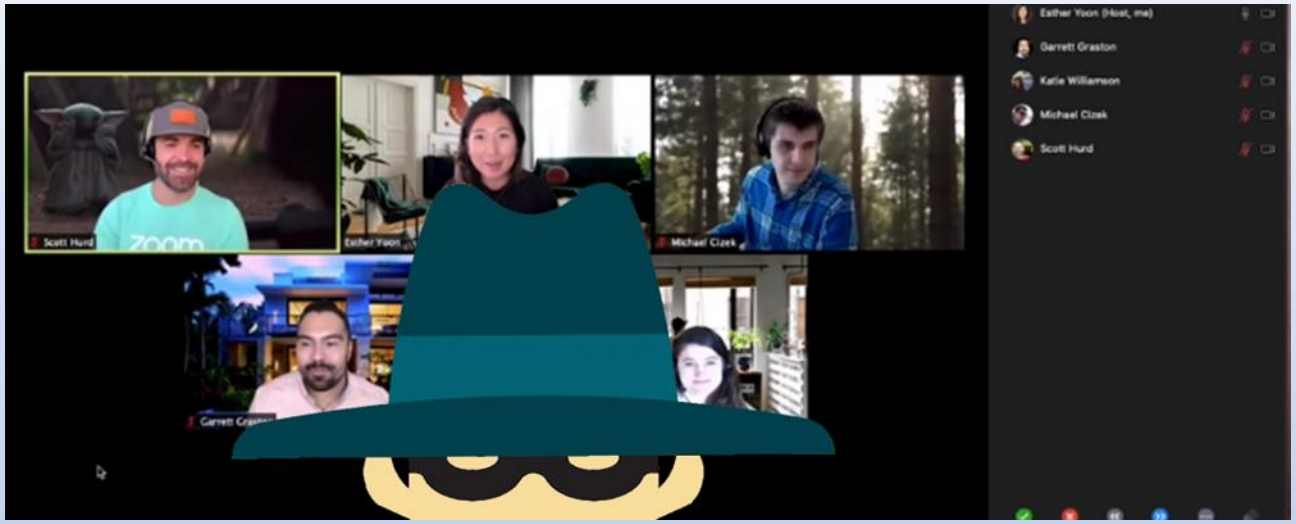
1. Il **numero di accessi alla piattaforma, le ore di accesso alla piattaforma, livello di partecipazione alle attività**, da cui sono deducibili dati personali degli utenti di queste piattaforme (ad es. interesse per le attività, problemi) e che, nel suo insieme, consentono la definizione di profili utente personalizzati. In effetti, questi contesti promuovono la raccolta automatizzata di informazioni e le successive analisi e previsione di aspetti legati, in particolare, alle capacità intellettuali, caratteristiche professionali, tratti di personalità, prestazioni professionali e anche con la salute di utenti. E questo è particolarmente evidente su piattaforme dal cui utilizzo possono discendere decisioni automatizzate basato su sistemi di intelligenza artificiale che analizzano il comportamento e rendimento degli studenti (apprendimento analitico).
2. La **profilazione**, relativa a informazioni particolarmente rilevanti (alcune delle quali per quanto riguarda i dati appositamente protetti dalla legislazione sulla protezione dei dati), come nel caso di attitudini intellettuali e dati sanitari che, se usati in altri contesti, possono stigmatizzare bambini e giovani, compromettendo la loro integrazione nella società e nel mondo del lavoro;
3. L'insegnamento mediante piattaforme di e-learning che, in modo automatizzato, **analizzano il comportamento e le prestazioni degli studenti,** presenta il rischio di errori di valutazione che, anche in considerazione di un utilizzo prolungato di questo tipo di tecnologia, può condizionare l'accesso degli stessi studenti a determinati contenuti pedagogici e, quindi, limitarne l'apprendimento a livelli di conoscenza più elementari o meno approfonditi.

La sicurezza nell'e_learning

Inoltre, l'Autorità per la protezione dei dati personali portoghese richiama l'attenzione dei Fornitori e Utilizzatori della didattica a distanza sui seguenti aspetti:

1. **la realtà del bullismo non è scomparsa** e potrebbe anche essere potenziato dalla quarantena e dall'uso massiccio di queste tecnologie; quindi il rischio di riutilizzo dei dati con condivisione dei dati, senza legittimità a tale scopo, come il pubblicare immagini e suoni su social network o altre piattaforme, nonché come l'accesso improprio ai dati e il loro utilizzo per scopi non legittimi, dovrebbe meritare attenzione speciale;
2. **Dati personali che possono essere registrati durante l'utilizzo delle piattaforme** e che rivelano aspetti della vita privata degli utilizzatori: immagini dei partecipanti e dei loro dintorni (ad es. immagini della casa); dichiarazioni vocali e verbali dei partecipanti; dichiarazioni dei partecipanti alle conversazioni di messaggistica e forum; immagine, suono e dichiarazioni di altre persone che si trovano nello stesso spazio dei partecipanti; documenti condivisi dai partecipanti attraverso le piattaforme (ad es. foto, test e relativa valutazione);
3. **Rischio di uso improprio dei dati trasferiti attraverso le piattaforme** dai responsabili dei trattamenti o dai subappaltatori che forniscono servizi su tali piattaforme (ad esempio, sistemi basati sul cloud computing);
4. **L'uso di piattaforme di comunicazione che non garantiscono la sicurezza delle comunicazioni** o la cui configurazione errata comporta la divulgazione o l'accesso non autorizzati può mettere a rischio la riservatezza dei dati.

La sicurezza nell'e_learning



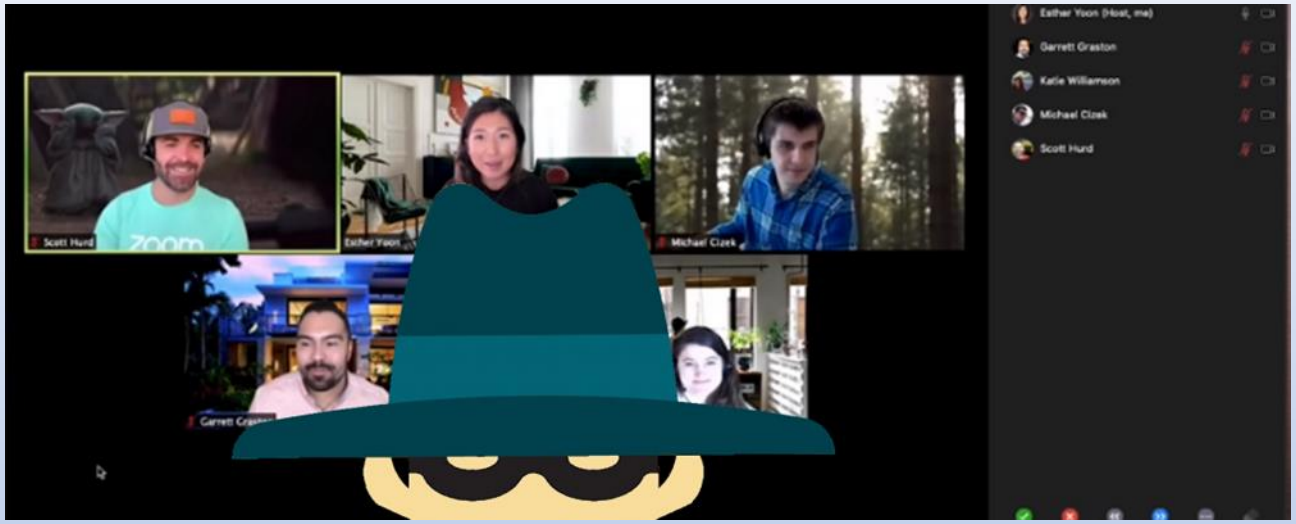
Zoombombing: come difendere le videoconferenze Zoom

Zoombombing è il nuovo fenomeno che affligge le videoconferenze Zoom di questi giorni, vediamo come difenderci e renderle sicure.

Il massiccio utilizzo dello smart working e la didattica a distanza di questo periodo hanno incrementato esponenzialmente l'utilizzo di piattaforme per le videoconferenze, tra queste **Zoom** è stata quella che nell'ultimo mese ha avuto un **aumento del 553%** del traffico giornaliero verso la sua pagina di download e la sua app per iPhone è la più scaricata da settimane. Questo aumento di popolarità Zoom unito ad alcuni bug strutturali e di sicurezza hanno creato il fenomeno dello **Zoombombing**

Credits to: punto-informatico.it

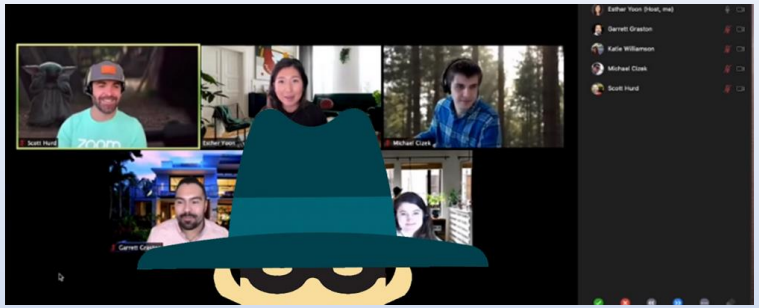
La sicurezza nell'e_learning



Gli sviluppatori di Zoom stanno cercando di risolvere i problemi, ma al momento sono riusciti solo a nascondere il numero ID e la password dalla descrizione della videochiamata, nella speranza di migliorare la situazione sul lato della privacy.
Prima della modifica compariva proprio l'ID del meeting e la relativa parola chiave, condividendo lo schermo ogni partecipante poteva vederlo e collegarsi alla riunione.
Rimangono comunque diverse lacune di sicurezza, come la mancanza della crittografia end-to-end, che Zoom ha inizialmente pubblicizzato come esistente nella sua app

Credits to: punto-informatico.it

La sicurezza nell'e_learning



Come mantenere sicure le chiamate Zoom

Il primo passo è cambiare le impostazioni della riunione Zoom in modo tale che i partecipanti casuali non possano **condividere le loro schermate**. Per fare ciò, selezionare *Condividi schermo* > *Impostazioni avanzate> Chi può condividere? > Ospita solo nella parte inferiore della riunione Zoom*.

Impostare questa preferenza prima di avviare la chiamata Zoom tramite *Impostazioni> Condivisione schermo*

Oltre a rendere private le stanze Zoom , gli amministratori possono anche richiedere ai partecipanti di **inserire una password** per poter partecipare. Per le impostazioni della password vai a *Impostazioni> Riunioni> Pianifica riunioni> Richiedi password per pianificare nuove riunioni.*

Da considerare la possibilità di **disabilitare i trasferimenti di file** durante le riunioni o di limitare i tipi di file che possono essere trasferiti così come può essere utile **creare una sala d'attesa** per la riunione, il che significa che i partecipanti devono essere aggiunti manualmente prima di poter partecipare alla riunione.

Se l'amministratore, se si accorge che è in atto un'azione di zoombombing, può cliccare su Rimuovi accanto al suo nome nel menu Partecipanti e disabilitare un successivo tentativo di accesso.

Credits to: punto-informatico.it

La sicurezza nell'e_learning

Zoom, l'app per videoconferenze condivide i dati con Facebook

Credits: Zoom/Apple Store

University of Toronto-based internet watchdog **Citizen** Lab said it found "**significant weaknesses**" in the encryption protecting the confidentiality of Zoom meetings as well as evidence that encryption keys - key bits of code whose possession could enable a hostile power to eavesdrop on conversations - were sometimes being sent to servers in China, even when the meeting's participants were in North America.

La sicurezza nell'e_learning

Zoom, l'app permette ai siti web di controllare la webcam del Mac

Una falla nella sicurezza del servizio per videoconferenze consente di attivare la webcam dei computer Apple all'insaputa dell'utente. L'esperto: "Rimuovete l'applicazione o disabilitate la cam"

Account di Zoom Hakerati

Gli account di Zoom hackerati sono diventati prodotti venduti in massa sul dark web e sui forum di hacker. Secondo **BleepingComputer,** che ha contattato la società di cybersecurity **Cyble**, attualmente ci sono oltre 500.000 utenze di account Zoom hackerate. Gli esperti di Cyble hanno notato l'afflusso di account Zoom in vendita il 1 aprile e sono stati in grado di acquistarne 530.000 a un prezzo all'ingrosso di $ 0,002 ognuno.

Le credenziali includono l'**indirizzo e-mail** dell'utente, la **password**, l'URL della riunione e la chiave dell'host di Zoom, un **pin** di sei cifre collegato all'account Zoom del proprietario, che viene utilizzato per i controlli dell'host per ogni meeting

La sicurezza nell'e_learning

A 3D printed Zoom logo is placed on the keyboard in this illustration taken April 12, 2020. REUTERS/Dado Ruvic/Illustration

Standard Chartered Plc (STAN.L) is the first major global bank to tell employees not to use Zoom Video Communications Inc (ZM.O) during the coronavirus pandemic due to cybersecurity concerns, according to a memo seen by Reuters.

The message, sent by Chief Executive Officer Bill Winters to managers last week, also warned against using Alphabet Inc's (GOOGL.O) Google Hangouts platform for virtual gatherings.

Neither service offers the level of encryption of conversations that rivals like Cisco System Inc's (CSCO.O) Webex, Microsoft Corp's (MSFT.O) Teams or Blue Jeans Network Inc do, industry experts said.