PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5892 di Mercoledì 16 luglio 2025

Digitalizzazione e cyberviolenza: i nuovi rischi per i lavoratori

Un articolo di OSHwiki evidenzia come intelligenza artificiale, social media e lavoro da remoto favoriscano nuove forme di violenza digitale da parte di terzi (clienti, pazienti, ecc.), aumentando i rischi di molestie verso i lavoratori.

La digitalizzazione sta trasformando il mondo del lavoro e richiede soluzioni nuove e aggiornate in materia di salute e sicurezza sul lavoro. Sviluppi recenti come l' intelligenza artificiale, i social media, i nuovi strumenti di comunicazione e un aumento significativo del lavoro da remoto si traducono in nuove opportunità per lavoratori e datori di lavoro, ma anche in nuove sfide e rischi per la sicurezza e la salute dei lavoratori. Una di queste sfide è rappresentata dal fatto che le nuove tecnologie offrono a terzi (pazienti, clienti, consumatori, genitori o altri membri del pubblico) nuovi modi per perpetrare violenza e molestie nei confronti dei lavoratori. Inoltre, offrono nuovi mezzi per la violenza e le molestie commesse dai colleghi di lavoro, il che esula dall'ambito del presente articolo.

Violenza sul lavoro e digitalizzazione del lavoro

La violenza sul lavoro da parte di terzi può essere definita come qualsiasi episodio in cui una persona subisce abusi, minacce o aggressioni in circostanze relative al proprio lavoro da parte di soggetti esterni all'organizzazione. Include aggressioni fisiche, abusi verbali o minacce perpetrate di persona, online o al telefono.

Il panorama digitale in continua evoluzione può aumentare il rischio di violenza e molestie sul lavoro in molti modi. Ad esempio, la digitalizzazione dei servizi può aumentare le aspettative dei clienti in termini di velocità ed efficienza. I clienti potrebbero anche provare frustrazione per sistemi mal progettati, aumentando ulteriormente il rischio di comportamenti violenti e di ricerca di capri espiatori. Questi rischi sono ulteriormente aggravati dall'introduzione di chatbot o altri sistemi automatizzati per l'assistenza clienti, poiché le richieste e i casi più semplici vengono gestiti da algoritmi, mentre ai lavoratori vengono affidati quelli più complessi. I social media e le app di messaggistica, d'altro canto, rendono molto più facile organizzare e intensificare le molestie pre-esistenti nei confronti dei lavoratori o di altri rappresentanti dell'azienda. Nell'era delle app di messaggistica, delle email e dei social media, la tecnologia ha fornito agli aggressori nuovi mezzi per minacciare o abusare delle persone, anche nel contesto lavorativo. Inoltre, le molestie sul lavoro possono estendersi agli account social privati dei lavoratori, estendendone l'impatto anche al di fuori dell'orario di lavoro.

Cosa sono la violenza informatica e le molestie sul lavoro?

La violenza informatica comprende un'ampia gamma di comportamenti dannosi che spesso sfruttano l'anonimato e la portata degli spazi online [1] [2] . Esempi di tali comportamenti includono l'antagonizzazione di qualcuno pubblicando commenti offensivi o provocatori su Internet (trolling), l'invio di messaggi, fotografie o video sessualmente espliciti per via elettronica (sexting), la ricerca e la pubblicazione di informazioni private o identificative (doxing), la predazione di qualcuno online molestando, spaventando o minacciando di danni fisici (cyberstalking), ottenendo l'accesso non autorizzato ai dati o al dispositivo di qualcuno (hacking) o pubblicando commenti offensivi sul lavoro o sui social media di una persona [3] . Le giovani lavoratrici possono essere colpite in modo sproporzionato da forme digitali di molestie sessuali, minacce e abusi.

Non del tutto nuova nel mondo del lavoro, la violenza informatica dovrebbe piuttosto essere inquadrata come l'estensione di un rischio preesistente, ovvero la violenza correlata al lavoro. Ad esempio, l'Health and Safety Executive del Regno Unito definisce

la violenza correlata al lavoro come: "Qualsiasi incidente in cui una persona subisce abusi, minacce o aggressioni in circostanze relative al proprio lavoro [...] ciò può includere abusi o minacce verbali, inclusi attacchi fisici faccia a faccia , *online* e via telefono" [4] .

I lavoratori possono essere presi di mira sui social media non solo da clienti risentiti con cui hanno avuto contatti, ma anche dal pubblico in generale. La facilità e la velocità con cui tali attacchi possono essere perpetrati è la vera differenza rispetto a telefonate o lettere offensive. L'anonimato rafforza inoltre l'autore del reato, creando una distanza tra lui e la vittima, proteggendolo al contempo dalle conseguenze delle sue azioni. Consentendo una rapida condivisione delle informazioni, le tecnologie digitali consentono anche una rapida escalation degli attacchi contro la vittima, a volte provenienti da più autori. Esempi tipici di violenza informatica da parte del pubblico in generale includono il trolling ai danni di giornalisti , gli attacchi online ai lavoratori delle telecomunicazioni correlati alla disinformazione online sulle reti 5G e sulle antenne di telefonia mobile e le molestie online agli operatori sanitari da parte di individui e gruppi contrari alle vaccinazioni.

Pubblicità

Conseguenze della violenza informatica sul lavoro

Secondo Work Safe Australia "comportamenti come violenza, aggressività, bullismo e molestie sessuali possono avere impatti significativi a breve e lungo termine sulla salute fisica e psicologica di una persona, anche quando svolti online o tramite tecnologie digitali" [5] . Gli impatti sulla salute mentale possono includere bassa autostima, ideazione suicida, rabbia e frustrazione [6] , nonché disturbo da stress post-traumatico [7] . Gli impatti negativi del cyberbullismo sul posto di lavoro si intensificano con il tempo e la vittima rischia di sopportare stress estremo, ansia e cattiva salute mentale. Inoltre, la violenza informatica correlata al lavoro può intensificarsi fino a compromettere la sicurezza fisica di una persona [8] . Sebbene la ricerca sull'impatto organizzativo della violenza informatica sia scarsa, gli effetti noti della violenza di terze parti includono aumento dell'assenteismo, diminuzione della motivazione dei lavoratori, riduzione della produttività e dei costi di reclutamento se i lavoratori interessati decidono di andarsene [9] [10] .

Quanto è diffusa la violenza informatica?

Uno studio prospettico dell'EU-OSHA del 2018 [11] ha rilevato che il cyberbullismo era già diffuso in molti luoghi di lavoro in numerosi settori ed era in aumento. Gli autori hanno suggerito che una maggiore dipendenza da Internet e dai social media per scopi lavorativi potrebbe aumentare il cyberbullismo da parte di concorrenti, colleghi, stakeholder o cybertroll. Il rapporto ha anche suggerito che il passaggio dalla comunicazione faccia a faccia a quella virtuale potrebbe comportare una perdita di capacità comunicative, che a sua volta potrebbe favorire un tono di comunicazione negativo e un linguaggio ostile.

Secondo l'indagine ESENER dell'EU-OSHA sulle imprese [12] , nel 2019 quasi il 60% delle imprese ha segnalato la violenza come fattore di rischio presente nella propria attività, rispetto al 54% del 2014. Non si sa in che misura la digitalizzazione o la violenza informatica in particolare possano aver contribuito a questo aumento.

Nel 2022, l'indagine OSH Pulse dell'EU-OSHA [13] su 27.000 lavoratori ha suggerito che l'uso di alcuni tipi di tecnologie digitali aumenta l'esposizione a violenza e molestie. Nello specifico, gli intervistati che hanno segnalato violenza e molestie legate al lavoro avevano maggiori probabilità di utilizzare computer desktop rispetto a coloro che non li utilizzavano (64% rispetto al 59%). Anche in questo caso, non è noto in che misura questa maggiore esposizione sia correlata alla violenza informatica o al bullismo.

Uno studio europeo [14] che ha coinvolto le parti sociali nei settori della sanità, dell'istruzione, della pubblica amministrazione locale e regionale, del commercio e della sicurezza privata ha indagato l'entità della violenza informatica sul lavoro. Lo studio includeva un'indagine rivolta alle organizzazioni delle parti sociali per sapere quali fossero le principali forme di violenza e molestie legate al lavoro a cui erano sottoposti i lavoratori del loro settore. Le molestie informatiche sono state segnalate come la principale forma di violenza legata al lavoro dall'11% degli intervistati, come per le molestie sessuali ma dietro le molestie verbali (15%), le molestie psicologiche e la violenza fisica (13%). Solo il 45% degli intervistati ha segnalato politiche o accordi che affrontano la violenza legata al lavoro da una prospettiva di genere, sebbene i risultati suggerissero che le donne siano colpite in modo sproporzionato dalla violenza legata al lavoro. Infine, una revisione della letteratura evidenzia che la violenza informatica ha colpito il 14% - 20% dei dipendenti universitari (Regno Unito), il 22% degli insegnanti (Repubblica Ceca), il 22% dei giornalisti (Svezia) e il 72% dei dipendenti pubblici (Australia).

Le donne sono colpite in modo sproporzionato

Alcuni dati suggeriscono che le donne siano colpite in modo sproporzionato [15] . Secondo uno studio globale della UN Generation Equality Action Coalition on Technology and Innovation (2021), il 38% delle donne ha riferito esperienze personali di violenza online [16] . Le giovani lavoratrici sono particolarmente colpite da forme digitali di molestie sessuali, minacce e abusi. Ad esempio, secondo uno studio del 2021, le molestie e gli abusi online nei confronti delle giornaliste sono particolarmente diffusi quando il reportage riguarda politica, diritto, economia, sport, diritti delle donne e femminismo, tendono a essere più gravi di quelli subiti dagli uomini ed è probabile che includano minacce di stupro o immagini sessualmente grafiche e offensive, e minacce contro i membri della famiglia [17] .

Le molestie informatiche nel metaverso

Il metaverso è uno spazio virtuale tridimensionale in cui gli utenti possono interagire con oggetti e altri utenti tramite un avatar digitale. Sebbene le applicazioni pratiche nel lavoro rimangano limitate, è stato suggerito che questi ambienti immersivi potrebbero plasmare il futuro del lavoro a distanza.

Nel 2024, l'Istituto Sindacale Europeo (ETUI) ha condotto una breve revisione [18] [19] che ha identificato possibili rischi fisici, ergonomici, di sicurezza, biologici e psicosociali derivanti da questi ambienti immersivi. Tra i problemi psicosociali, la revisione evidenzia segnalazioni di utenti che hanno subito molestie informatiche e persino "aggressioni informatiche" sessuali nel metaverso. Oltre alle molestie e al trolling, il cyberbullismo nel metaverso può manifestarsi sotto forma di aggressione fisica con lo sviluppo di tecnologie di rilevamento. La tecnologia tattile crea la sensazione fisica di "toccare" oggetti e, quindi, il senso di contatto fisico tra due avatar. La revisione evidenzia anche che gli utenti tendono a comportarsi in un modo che corrisponde all'aspetto del loro avatar. Noto come effetto "Proteo", si suggerisce che questo amplifica il cyberbullismo negli ambienti immersivi, dove ogni interazione è mediata da un avatar. Potrebbe avere implicazioni per la violenza di terze parti, poiché questi ambienti immersivi potrebbero essere utilizzati dalle aziende per presentare i propri prodotti e interagire con i clienti. L'autore conclude sottolineando che le tecnologie immersive devono essere progettate per essere sicure. Se si vuole considerarne l'utilizzo in ambito lavorativo, è necessaria una valutazione del rischio per determinarne l'appropriatezza e attuare opportune misure preventive.

Prevenzione e gestione della violenza informatica sul lavoro da parte di terzi

La prevenzione della violenza informatica e delle molestie da parte di terzi sul lavoro dovrebbe essere affrontata con la stessa sistematicità delle altre forme di violenza sul lavoro , basandosi sulla valutazione del rischio e con il coinvolgimento dei lavoratori . È necessaria una risposta organizzativa. Politiche, procedure e protocolli sulla violenza sul lavoro devono includere la violenza informatica.

Come per tutte le forme di violenza sul lavoro, gli obiettivi sono:

1. Prevenire gli atti di violenza informatica e molestie

2. Arrestare l'escalation e limitare le conseguenze
3. Sostenere la vittima

Safework Australia [20] suggerisce i seguenti **10 passaggi per affrontare gli abusi online sul posto di lavoro** :

- Crea un ambiente di lavoro online sicuro e protetto, ad esempio utilizza le impostazioni di sicurezza e gli strumenti sui servizi online per bloccare, disattivare l'audio o rimuovere contenuti offensivi
- Cambiare il modo in cui si lavora per ridurre al minimo i rischi attraverso sistemi, politiche e procedure, ad esempio identificare e gestire le cause dei problemi che generano abusi; progettare il lavoro per impedire al personale di interagire con materiale offensivo e disporre di procedure chiare affinché i lavoratori possano proteggersi e rispondere agli abusi online.
- Moderare i contenuti sulle piattaforme online dell'organizzazione, ad esempio attraverso linee guida per i contenuti accettabili.
- Segnala contenuti offensivi. Contatta la polizia nei casi più gravi.
- Implementare politiche sul posto di lavoro, ad esempio definire policy per l'uso appropriato di piattaforme online, telefoni e altre tecnologie, e delineare come verranno prevenuti gli incidenti e come verrà affrontata la questione.
- Fornire informazioni e formazione, ad esempio su come gestire le persone difficili e sulla sicurezza online. Parlare con i lavoratori su dove, quando e come potrebbero verificarsi abusi online legati al lavoro e su cosa si sta facendo per prevenirli.
- Creare un ambiente di lavoro positivo e rispettoso.
- Contrastare gli abusi online sul posto di lavoro.
- Incoraggiare i lavoratori a segnalare gli abusi online e supportarli quando sollevano preoccupazioni
- Parla con i lavoratori: per aiutarli a identificare dove, quando e perché potrebbero verificarsi abusi online e ottenere idee su come prevenirli.

La Guida eSafety australiana [21] fornisce informazioni su piattaforme e app professionali diffuse (come LinkedIn e Zoom) su come proteggere le informazioni e segnalare contenuti inappropriati. Altre pagine del sito web eSafety forniscono informazioni su come proteggere la propria identità [22] e segnalare abusi [23] . Sebbene la segnalazione sia collegata alla legge australiana, le informazioni sulla raccolta delle prove sono generalmente applicabili.

Un'indagine può essere utile per scoprire l'entità dei casi di violenza informatica sul lavoro, includendo dove e quando si sono verificati gli incidenti, come e da chi. Sono necessari un sistema di segnalazione e un meccanismo di feedback per individuare gli incidenti, fornire supporto alle vittime e adottare misure di follow-up, ad esempio con la polizia e/o le aziende tecnologiche o di social media. Gli episodi dovrebbero essere indagati adottando una cultura no-blame, concentrandosi sulle lezioni da imparare e aggiornando protocolli e procedure se necessario. In ogni caso, il lavoratore non dovrebbe mai essere lasciato solo ad affrontare gli incidenti.

La formazione può includere, ad esempio, buone pratiche su come proteggersi online, come verificare e migliorare la sicurezza delle password, come verificare se si è presi di mira online (una caratteristica particolare di alcune forme di violenza informatica, come lo stalking o il trolling online, è che il lavoratore potrebbe non essere consapevole di essere preso di mira). Le informazioni e la formazione dovrebbero includere supervisori e manager e il loro ruolo.

Le politiche dovrebbero essere sviluppate e riviste regolarmente con il coinvolgimento dei lavoratori. Rivedere e aggiornare le procedure in materia di violenza informatica è fondamentale, considerando la rapidità con cui l'ambiente digitale cambia.

Per quanto riguarda i rischi, le misure preventive devono essere adattate al tipo di lavoro e alle circostanze lavorative. Le sezioni seguenti forniscono due brevi esempi di professioni particolarmente soggette a violenza informatica sul lavoro, evidenziando le tipologie di misure che possono essere adottate in questi contesti.

personale docente

Nelle scuole e nei college, gli abusi nei confronti del personale possono provenire da alunni e studenti, ma anche da genitori o dal pubblico in generale. Per proteggere il personale docente, le scuole devono disporre di regole e procedure chiare che coprano: l'accesso al numero di telefono, all'indirizzo email o agli account sui social media degli insegnanti; la protezione delle password e di altre informazioni sensibili; l'adozione di misure in caso di pubblicazione di contenuti su un sito web o una

piattaforma di social media; l'uso del telefono a scuola e durante le lezioni; le procedure da seguire in caso di incidenti, anche al di fuori dell'orario scolastico; e la definizione di una politica comportamentale scolastica con regole sia per gli alunni che per i genitori.

È importante assicurarsi che studenti, personale e genitori siano informati sui codici e sulle misure comportamentali, poiché gli abusi possono provenire anche dai genitori.

Il Comitato sindacale europeo per l'istruzione (ETUCE) ha affrontato per la prima volta il problema della violenza informatica nei confronti degli insegnanti nel 2010 [24] .

giornalisti

Per la maggior parte dei giornalisti , avere una presenza online è essenziale per sviluppare, pubblicare e promuovere il proprio lavoro. È noto che le giornaliste sono tra le più vittime di abusi, con ricerche che mostrano collegamenti tra violenza online e attacchi offline, spesso nel contesto dello stalking [25] [26] .

Pen America [27] ha sviluppato un manuale di buone pratiche per i datori di lavoro del settore dei media, al fine di proteggere e supportare i lavoratori che subiscono abusi online. Il manuale sottolinea l'importanza di adottare un approccio organizzativo alla violenza informatica e di creare una cultura di supporto, con un'adeguata valutazione del rischio e un forte coinvolgimento dei lavoratori. Le raccomandazioni pratiche includono: il coinvolgimento dei familiari nella valutazione del rischio; l'impostazione di una politica di scrittura per garantire che i titoli non siano deliberatamente provocatori; una politica di moderazione dei contenuti che impedisca ai lettori di pubblicare commenti per determinati tipi di articoli, ad esempio se l'argomento è controverso; la formazione sulla sicurezza digitale e sull'"autodifesa" contro gli abusi online; il follow-up degli incidenti con le aziende di social media; l'emissione di una dichiarazione pubblica di supporto per il dipendente; l'offerta di una tregua temporanea, in cui qualcun altro monitora l'account della persona presa di mira, segnalando, bloccando o silenziando i trasgressori.

violenza domestica

La violenza domestica può essere un problema sul posto di lavoro se l'autore minaccia di usare violenza o intimidisce un partner o un familiare sul posto di lavoro, anche tramite e-mail o telefonate [28] . Se l'autore lavora nello stesso posto di lavoro della vittima, può utilizzare sistemi di messaggistica interna per molestare la collega vittima [29] . La Convenzione OIL 190 considera la violenza domestica un problema legato al lavoro.

La violenza domestica dovrebbe essere inclusa nelle politiche e nelle misure sul posto di lavoro per affrontare la violenza [30] [31] , in particolare per quanto riguarda gli aspetti relativi alla comunicazione digitale e alle molestie informatiche. Inoltre, la violenza domestica nei confronti dei telelavoratori dovrebbe essere trattata nelle politiche sul telelavoro.

Esistono semplici misure che i datori di lavoro possono adottare per proteggere i telelavoratori che subiscono o potrebbero subire abusi domestici [32] [33] . Ad esempio, è comune che i partner violenti monitorino la comunicazione della vittima. In questo contesto, fornire telefoni e laptop aziendali può contribuire a garantire maggiore autonomia e sicurezza digitale alla vittima.

Conclusioni

La violenza informatica rappresenta una nuova forma di un rischio preesistente ben noto, ovvero la violenza sul lavoro. In quanto tale, pone nuove sfide alla prevenzione e alla gestione della violenza sul lavoro. La velocità di escalation e l'anonimato degli autori la rendono intrinsecamente più difficile da affrontare, mentre legislazione, policy e conformità sono in ritardo rispetto a un panorama digitale in continua evoluzione.

Ciononostante, è dovere dei datori di lavoro affrontare questa forma di violenza sul lavoro e attuare misure per proteggere i propri lavoratori. L'attuale approccio di prevenzione alla violenza sul lavoro può essere adattato e aggiornato per affrontare

esplicitamente la violenza informatica sul lavoro, prestando particolare attenzione alle specificità settoriali e del luogo di lavoro. È necessario un approccio olistico, sistemico e sistematico, con politiche coerenti e integrate che affrontino la sicurezza dei dati, il telelavoro, la parità di genere e la SSL, e con approcci di valutazione del rischio aggiornati che affrontino esplicitamente tali questioni. Infine, la cooperazione tra Ispettorati del Lavoro, forze dell'ordine, organizzazioni di social media e altri soggetti, a seconda dei casi, è importante per un approccio integrato.

Riferimenti

[1] Parlamento europeo (2018) Cyberviolenza e incitamento all'odio online contro le donne. Bruxelles, Parlamento europeo. Disponibile all'indirizzo

[2] Parlamento europeo (2021) Combattere la violenza di genere: violenza informatica. Valutazione del valore aggiunto europeo. Bruxelles, Parlamento

[3] Work Safe Australia, Abuso online sul posto di lavoro - Informazioni per i datori di lavoro.

[4] Health and Safety Executive (HSE) Violenza e aggressione sul lavoro.

[5] Work Safe Australia, Abuso online sul posto di lavoro - Informazioni per i datori di lavoro.

[6] Hinduja, S., & Patchin, JW (2019). Collegare il suicidio adolescenziale alla gravità del bullismo e del cyberbullismo. Journal of School Violence, 18(3), 333?346

[7] Posetti, Shabbir, Maynard, Bontcheva, Aboulez, 2021, The Chilling: Global Trends in Online Violence Against Women Journalists.

[8] Farley, S., Coyne, I., Sprigg, C., Axtell, C., & Subramanian, G. (2015). Esplorazione dell'impatto del cyberbullismo sul posto di lavoro sui medici tirocinanti. Medical Education, 49(4), 436?443.

[9] OSHwiki, 2015, Violenza sul posto di lavoro, EU-OSHA.

[10] EU-OSHA, 2022, Violenza sul lavoro. Scheda informativa 24.

[11] EU-OSHA, 2018, Studio prospettico ? digitalizzazione e rischi nuovi ed emergenti.

[12] EU-OSHA, 2022, Terza indagine europea tra le imprese sui rischi nuovi ed emergenti (ESENER 2019): Rapporto di sintesi su come i luoghi di lavoro europei gestiscono la sicurezza e la salute.

[13] EU-OSHA, 2022, OSH Pulse - Sicurezza e salute sul lavoro nei luoghi di lavoro post-pandemici.

[14] Pillinger, J, 2023, Non fa parte del lavoro.

[15] Pillinger, J, 2023, Non fa parte del lavoro.

[16] The Economist Development Unit/Jigsaw, 2021, Misurare la prevalenza della violenza online contro le donne.

[17] Posetti, Shabbir, Maynard, Bontcheva, Aboulez, 2021, The Chilling: Global Trends in Online Violence Against Women Journalists.

[18] ETUI, 2024, Lavorare nel metaverso: quali sono i rischi? Una rapida revisione della letteratura.

[19] Bérastégui, P., 2023, Il metaverso potrebbe essere il futuro del lavoro a distanza?, HesaMag n. 28. ETUI.

[20] Work Safe Australia, Abuso online sul posto di lavoro - Informazioni per i datori di lavoro.

[21] Governo australiano, Guida alla sicurezza elettronica

[22] Furto di identità

[23] Segnalare abusi informatici da parte di adulti

[24] Progetto sulle molestie informatiche (2009-2010).

[25] Posetti J., Shabbir N. (a cura di). The Chilling: uno studio globale sulla violenza online contro le giornaliste, International Center for Journalists.

[26] UNESCO, 2020, Violenza online contro le giornaliste: un'istantanea globale dell'incidenza e degli impatti.

[27] Pen America, Manuale sulle molestie online.

[28] Work Safe Australia, Abuso online sul posto di lavoro - Informazioni per i datori di lavoro.

[29] EU-OSHA, 2023, Costruire spazi sicuri: violenza domestica e luogo di lavoro.

[30] EU-OSHA, 2023, Costruire spazi sicuri: violenza domestica e luogo di lavoro.

[31] OSHwiki, Violenza domestica e luogo di lavoro.

[32] Servizio di sicurezza e prevenzione sul posto di lavoro, 2021, Adotta misure ora per proteggere i tuoi telelavoratori dalla violenza domestica.

[33] Safe Work Australia. Violenza familiare e domestica sul posto di lavoro.

Fonte: OshWiki

Licenza Creative Commons

www.puntosicuro.it