Studio Violi S.r.l.
Organizzazione con sistema di gestione certificato secondo la norma ISO 9001: 2015

2003-2025
anni di consulenza per le imprese

ISO 9001
BUREAU VERITAS
Certification
IT334467

I Partners dello Studio

Giorgio Violi	tel: 3386132605	givioli@gmail.com
Alberto Sant'Unione	tel: 3409125853	santunionea@gmail.com

Qualità Sicurezza Privacy Ambiente Risk Management
Responsabilità Amministrativa 231 Etica Consulenza e Audit per la Direzione

Organizzazione con sistema di gestione certificato secondo la norma ISO 9001: 2015 per Progettazione ed erogazione di servizi di consulenza relativa ai Sistemi di Gestione Aziendale Qualità, Ambiente, Sicurezza, Etica; servizi di consulenza in ambito Privacy, Modelli Organizzativi, Sicurezza sul lavoro, Consulenza di Direzione e sostenibilità ESG

2025 Marzo **Il nostro punto di vista su…** *Anno 18 – 1° sem*

Periodico di informazione per i CLIENTI dello STUDIO VIOLI

Indice delle NOTIZIE (N)

SENTENZE DI CASSAZIONE SUL LAVORO

- Sul sito http://www.dottrinalavoro.it/argomento/giurisprudenza-c/corte-di-cassazione-c sono presenti le ultime sentenze di Cassazione relative al lavoro

AFORISMA DEL MESE

"In un paese sottosviluppato, non bere l'acqua; in un paese sviluppato, non respirare l'aria"

(Anonimo)

E-mail: info@studiovioli.com **SDI:** giorgiovioli@pec.it
Web: www.studiovioli.com **Fax:** 059 682304
Studio Violi Srl - Via per Capanna Tassone, 1156 41021 Ospitale - Fanano (MO)
P.I. e C.F. 02836380366 – REA 335410 CCIAA MO – Cap. Soc. € 10.000 I.V.

"Verifica dell'idoneità tecnico professionale"

Notizie

- N1) Sicurezza: Registro telematico infortuni INAIL e novità introdotte

Il "Manuale Registro Infortuni Telematico" prodotto dall'INAIL fa riferimento alla versione 1.0, che è stata rilasciata il 4 marzo 2025. La versione 1.0 segna l'aggiornamento del sistema con una riorganizzazione del "Cruscotto infortuni" che ora assume la denominazione di "Registro Infortuni", introducendo nuove funzionalità e interfacce per gli utenti.

Il manuale utente può essere scaricato dal sito ufficiale dell'INAIL.
Gli utenti devono accedere alla sezione dei servizi online del portale INAIL, dove, dopo il login tramite credenziali SPID, CNS o CIE, è possibile scaricare il manuale nella versione aggiornata.
L'accesso ai contenuti è reso possibile attraverso l'interfaccia web dell'INAIL, che garantisce un facile recupero delle risorse disponibili.

A chi si rivolge e chi può accedervi

Il "Registro Infortuni Telematico" è destinato a una pluralità di utenti, che includono:

- **Ispettori: gli ispettori appartenenti all'INAIL, alle ASL, all'Ispettorato Nazionale del Lavoro (INL)**, agli Ispettorati Territoriali del Lavoro (ITL), ai Carabinieri del Ministero del Lavoro e agli ufficiali di Polizia Giudiziaria, che hanno accesso per la consultazione e il monitoraggio degli infortuni.
- **Datori di Lavoro e Delegati**: i datori di lavoro nei settori industriale, artigianale, dei servizi e delle pubbliche amministrazioni, nonché i loro delegati, possono consultare i dati relativi agli infortuni occorsi all'interno della propria azienda o struttura.
- **Intermediari: i consulenti del lavoro, inclusi commercialisti e professionisti equiparati** dalla Legge 12/1979, che agiscono come intermediari tra i datori di lavoro e l'INAIL.

Modalità di accesso e decorrenza

Per accedere al "Registro Infortuni Telematico", gli utenti devono effettuare il login attraverso il portale ufficiale INAIL, utilizzando uno dei seguenti metodi di autenticazione:

- SPID (Sistema Pubblico di Identità Digitale)
- CNS (Carta Nazionale dei Servizi)
- CIE (Carta di Identità Elettronica)

Provenienza dei dati raccolti

I dati presenti nel Registro Infortuni Telematico provengono dalle Denunce e Comunicazioni di Infortunio che vengono trasmesse all'INAIL dai datori di lavoro, pubbliche amministrazioni e altre strutture organizzative.

Criteri di consultazione

La consultazione del Registro Infortuni Telematico avviene secondo criteri territoriali e settoriali, che variano in base alla tipologia di utente:

- **Ispettori:** possono effettuare ricerche in base alla provincia o regione di competenza. Possono ricercare dati relativi a settori specifici, come le aziende IASPA (tutte quelle cioè che fanno riferimento alla gestione assicurativa presso l'INAIL che riguarda i settori industriale, artigianale, dei servizi e delle pubbliche amministrazioni e che hanno una posizione assicurativa territoriale presso l'INAIL.) e il settore agricolo.
- **Datori di Lavoro:** possono consultare solo gli infortuni che riguardano la propria azienda o la struttura di pubblica amministrazione di loro competenza.
- **Intermediari:** possono visualizzare solo i dati relativi alle aziende per le quali hanno delega.

Dati estraibili

I dati che possono essere estratti dal "Registro Infortuni Telematico" comprendono:

- Informazioni generali: codice fiscale e nome del lavoratore, data e luogo dell'incidente.
- **Tipologia dell'adempimento**: se il dato riguarda una denuncia o una comunicazione di infortunio.
- **Dettagli specifici dell'incidente**: come la natura e sede della lesione, la prognosi, l'inabilità temporanea o permanente, la durata dell'inabilità, la data di ripresa del lavoro, e i dati relativi alla morte (se presente).
- Informazioni sulla gestione assicurativa: codice dell'azienda, posizione assicurativa territoriale e dettagli dell'unità produttiva.

Tutti questi dati possono essere esportati in formato PDF o XLS.

Vantaggi dell'accesso

L'accesso al "Registro Infortuni Telematico" offre numerosi vantaggi, tra cui:

- Monitoraggio e gestione sicura: consente un monitoraggio preciso degli infortuni sul lavoro in tempo reale, facilitando la gestione delle pratiche burocratiche e degli adempimenti previsti dalla legge.
- Ottimizzazione del flusso informativo: centralizza i dati relativi agli infortuni, rendendo più facile l'accesso e la gestione da parte degli utenti autorizzati, riducendo il carico amministrativo.
- Conformità legale: aiuta le aziende a garantire la conformità con le normative in materia di salute e sicurezza sul lavoro, facilitando la consultazione delle denunce e comunicazioni di infortunio, nonché la gestione delle relative pratiche.
- Estrazione dati per analisi: gli utenti possono estrarre i dati per fare analisi statistiche, migliorando così la pianificazione delle misure preventive per ridurre gli infortuni.

- N2) Sicurezza: Sull'intelligenza artificiale, i poteri datoriali e la sicurezza sul lavoro

Un saggio propone uno sguardo oltre la siepe per parlare di intelligenza artificiale e sicurezza sul lavoro. Focus sulle implicazioni derivanti dall'esercizio del potere direttivo a mezzo algoritmico e l'emersione di nuovi rischi per la sicurezza.

Come più volte sottolineato nella campagna europea "Lavoro sano e sicuro nell'era digitale", promossa dall'Agenzia europea per la sicurezza e la salute sul lavoro (EU-OSHA), la rivoluzione digitale sta portando ad un crescente ed inevitabile impiego dell'intelligenza artificiale anche nella gestione dei rapporti di lavoro.

Ed infatti sempre più frequentemente "i poteri datoriali di organizzazione, decisione e controllo vengono esercitati mediante il ricorso a processi decisionali automatizzati basati sull'utilizzo di strumenti algoritmici". E

questo passaggio, in relazione alla "natura ambivalente delle tecnologie che si basano sull'intelligenza artificiale", pone di fronte ad importanti quesiti, anche di "ordine giuridico e ontologico".

In "Intelligenza artificiale e sicurezza sul lavoro: uno sguardo oltre la siepe" l'autore vuole indagare i rischi e le opportunità che sorgono dall'impiego dell'intelligenza artificiale nella gestione dei rapporti di lavoro, con particolare attenzione all'ambito della tutela della salute e della sicurezza dei lavoratori.

L'autore presenta "le implicazioni derivanti dall'esercizio del potere direttivo a mezzo algoritmico e l'emersione di nuovi rischi per la sicurezza".

A questo proposito si segnala, come indicato in premessa, che "sempre maggiore è la tendenza alla sostituzione dei 'tradizionali' poteri datoriali di decisione e controllo con processi decisionali affidati all'automazione algoritmica". **E, in questo senso, l'impiego di strumenti algoritmici sembra orientato "ad estendere a dismisura i poteri datoriali, determinando importanti implicazioni non solo sul versante del trattamento dei dati personali del lavoratore e su quello del monitoraggio e del giudizio sugli stessi, ma anche su quello della garanzia dell'integrità psico-fisica dei lavoratori, che si fonda anche e soprattutto su un efficace esercizio del potere di vigilanza e di controllo".**

Viene sottolineato il problema della c.d. "opacità algoritmica", ossia della "scarsa trasparenza intrinseca che contraddistingue i processi decisionali automatizzati, potendo accentuare lo stato di soggezione del lavoratore ovvero creare ulteriori e inediti squilibri nel rapporto di lavoro o, ancora, avallare pratiche discriminatorie". Ed infatti la Commissione dell'Unione europea (UE) in una Comunicazione del 5 marzo 2020 (Un'Unione dell'uguaglianza: la strategia per la parità di genere 2020-2025) ha evidenziato come gli algoritmi, "laddove non siano sufficientemente trasparenti, rischino di riprodurre, amplificare o contribuire a far sorgere pregiudizi, di cui i programmatori possono non essere a conoscenza o che sono il risultato di una specifica selezione di dati".

Sempre in un'ottica di contrasto della opacità algoritmica la Direttiva sul lavoro mediante piattaforme digitali adottata dal Parlamento europeo il 24 aprile 2024 fornisce "alcuni interessanti strumenti volti a favorire la trasparenza informativa delle decisioni assunte con procedure automatizzate gestite da algoritmi attraverso il monitoraggio ed il riesame umano delle decisioni stesse".

In particolare, si ricorda che l'articolo 6 prevede che le "piattaforme digitali debbano fornire ai lavoratori informazioni in merito ai sistemi di monitoraggio utilizzati e ai sistemi decisionali, prevedendo, in particolare, che essi abbiano diritto di ottenere le informazioni relative ai principali parametri utilizzati dai sistemi decisionali automatizzati, nonché ai motivi sottesi alle decisioni da essi assunte, richiedendo espressamente che le informazioni siano comunicate «in forma concisa, trasparente, intellegibile e facilmente accessibile". E l'articolo 8 "contempla il diritto del lavoratore a ottenere una spiegazione per qualsiasi decisione presa o sostenuta dal sistema decisionale automatizzato, con la possibilità di rivolgersi a tal proposito a una persona di contatto, designata dalla piattaforma per discutere e chiarire i fatti, le circostanze e i motivi della decisione".

Intelligenza artificiale e sicurezza sul lavoro: valutazione dei rischi e probabilità

L'avvento dei sistemi di intelligenza artificiale deve "innervare l'adempimento dell'obbligo prevenzionistico sotto un duplice profilo".

Ad esempio "come possibile fattore di rischio per la salute fisica e mentale dei lavoratori (anche sotto forma di rischi da stress lavoro correlato o rischi di natura psico sociale), cui porre rimedio". Ma senza trascurare come tali sistemi possano "integrare misure di sicurezza idonee per migliorare il livello di tutela e che, come tali,

possano divenire immediatamente obbligatorie in base ai principi di massima sicurezza tecnologica sopra evocati".

Se però per rischio - ai sensi dell'art. 2, comma 1, lett. s), del d.lgs. n. 81/2008 - si intende la «probabilità di raggiungimento del livello potenziale di danno nelle condizioni di impiego o di esposizione ad un determinato fattore o agente oppure alla loro combinazione», il grado di probabilità in questione "potrebbe mancare (o non essere calcolabile) nel caso di utilizzo di algoritmi non deterministici o auto apprendenti", e ciò rende la valutazione del rischio "pressoché impossibile, se non in termini generali proprio per l'imprevedibilità che caratterizza il risultato".

- N3) Privacy: NIS2 e GDPR: due normative differenti che richiedono sinergia tra esperti IT e consulenti legali

Il GDPR disciplina il trattamento dei dati personali imponendo misure di sicurezza a tutela dei diritti degli interessati. La NIS2, invece, amplia il perimetro di protezione includendo la resilienza operativa delle infrastrutture critiche e delle aziende strategiche.

Uno degli aspetti chiave in cui le due normative si sovrappongono riguarda la gestione degli incidenti di sicurezza. Il GDPR impone la notifica di una violazione dei dati personali all'Autorità Garante entro 72 ore, mentre la NIS2 prevede un processo più articolato, con una prima comunicazione entro 24 ore, una segnalazione dettagliata entro 72 ore e una relazione finale entro un mese.

Questi requisiti impongono alle imprese l'adozione di un sistema di incident response coordinato, evitando il rischio di gestire le due normative come compartimenti separati potendo quindi incorrere facilmente in problemi dovuti all'assenza o all'errata comunicazione fra reparti.

L'integrazione tra NIS2 e GDPR non è solo una questione di compliance, ma una sfida organizzativa che richiede la sinergia tra esperti IT e consulenti legali. I tecnici sono responsabili dell'implementazione delle misure di cybersecurity e della gestione delle vulnerabilità, mentre i legali devono garantire la conformità normativa, la redazione di policy interne adeguate e la gestione del rischio legale in caso di violazioni e il controllo su tutta la documentazione necessaria ad iniziare dalle lettere di incarico e le clausole contrattuali.

La cooperazione tra queste due categorie di operatori è essenziale per evitare esposizioni a contenziosi e sanzioni, oltre che per garantire la protezione effettiva delle informazioni aziendali; forse oggi il più importante asset patrimoniale di molte imprese che sembra non se ne rendano conto. Un modello di governance efficace deve pertanto integrare i requisiti di entrambe le normative in una strategia aziendale coerente, in cui le misure di sicurezza adottate per la NIS2 siano compatibili con i principi di privacy by design e by default previsti dal GDPR.

Un aspetto critico che emerge in questo ambito è la gestione dei contratti con fornitori e partner. La NIS2 introduce obblighi specifici sulla sicurezza della supply chain, mentre il GDPR disciplina la protezione dei dati nei rapporti con terze parti. Le aziende dovranno quindi rivedere i contratti e includere clausole che garantiscano la conformità a entrambe le normative, definendo con precisione le responsabilità in caso di incidenti di sicurezza e prevedendo obblighi di cooperazione tra le parti. Il rischio di scarico di responsabilità è altissimo.

L'integrazione tra NIS2 e GDPR non può poi prescindere dalla formazione continua del personale aziendale, ma impone anche accertamenti su come partner e fornitori gestiscano la loro filiera della privacy.

La sensibilizzazione su aspetti normativi e operativi, come il riconoscimento dei tentativi di phishing o l'uso sicuro delle credenziali di accesso, è essenziale per ridurre i rischi di violazioni e migliorare la resilienza aziendale.
In estrema sintesi NIS2 e GDPR devono essere considerati due ingranaggi essenziali dello stesso meccanismo, complementari nella costruzione di un ambiente digitale sicuro e conforme ma anche strumenti allineati all'interno di un'organizzazione aziendale che non può permettersi sbavature.
Le imprese che sapranno integrare efficacemente cybersecurity e protezione dei dati potranno pertanto non solo affrontare con maggiore sicurezza le sfide del panorama digitale europeo, ma anche rafforzare la propria competitività, allineandosi ai modelli organizzativi richiesti dal legislatore nel richiamato art. 2086.
Le aziende devono infatti strutturarsi con un assetto organizzativo, amministrativo e contabile adeguato alla loro natura e dimensione, garantendo un monitoraggio tempestivo della continuità aziendale e predisponendo misure idonee per prevenire e gestire eventuali crisi, in conformità con gli strumenti normativi previsti.
La cybersecurity e la protezione dei dati non sono solo obblighi di legge, ma il fondamento stesso di un'impresa che vuole restare in piedi.
E l'esperienza ci dice che, spesso, non è facile rimanerci.

-N4) Privacy: Azienda di autotrasporti sanzionata per violazione della privacy dei dipendenti tracciati illecitamente tramite sistema Gps installato sui veicoli

Il Garante privacy ha sanzionato un'azienda di autotrasporti per aver controllato in modo illecito circa 50 dipendenti, durante la loro attività lavorativa, utilizzando un sistema Gps installato sui veicoli aziendali

Diverse le violazioni riscontrate dall'Autorità, intervenuta a seguito della ricezione di un reclamo da parte di un ex dipendente dell'azienda.
Dalle ispezioni, effettuate in collaborazione con il Nucleo tutela privacy della Guardia di Finanza, è emerso che il sistema Gps tracciava in modo continuativo i dati di localizzazione, velocità, chilometraggio e stato dei veicoli (ed es. quando erano spenti o accesi), senza rispettare la normativa privacy e in modo difforme da quanto previsto dal provvedimento autorizzatorio rilasciato dall'Ispettorato territoriale del lavoro.
In particolare, sono state rilevate gravi carenze nell'informativa fornita ai lavoratori, tra cui la mancata indicazione delle specifiche modalità con cui il trattamento veniva realizzato e la informazione relativa alla diretta identificabilità dei conducenti dei veicoli geolocalizzati.
Tali trattamenti sono risultati contrari anche alle specifiche misure di garanzia indicate dall'Ispettorato del lavoro nel provvedimento di autorizzazione che era stato rilasciato all'azienda, che infatti prevedeva l'anonimizzazione dei dati raccolti e l'adozione di soluzioni tecnologiche in grado di limitare la raccolta di dati personali non necessari o eccedenti rispetto alle finalità di sicurezza e organizzazione aziendale. Inoltre, **i dati raccolti venivano conservati per oltre 5 mesi, in violazione dei principi di minimizzazione e limitazione della conservazione dei dati stabiliti dal GDPR.**
Il Garante, in considerazione delle numerose e gravi violazioni riscontrate, oltre al pagamento **di una sanzione di 50mila euro,** ha ordinato all'azienda di fornire un'idonea informativa ai dipendenti e di adeguare i trattamenti effettuati attraverso il sistema Gps alle garanzie prescritte nel provvedimento autorizzatorio rilasciato, a suo tempo, dall'Ispettorato territoriale del lavoro all'azienda.

- N5) Privacy: Allarme intelligenza artificiale nelle aziende: l'89% di app e tool usati dai dipendenti è fuori controllo; Uso indiscriminato di AI in azienda: la formazione dei dipendenti gioca un ruolo chiave per la compliance privacy; Attenzione alla truffa telefonica del curriculum che vi sottrae soldi e dati personali

Allarme intelligenza artificiale nelle aziende: l'89% di app e tool usati dai dipendenti è fuori controllo. L'89% di app e tool di intelligenza artificiale generativa utilizzate dai dipendenti è fuori dal controllo delle aziende.

Infatti, circa il 20% degli utenti aziendali ha installato di propria iniziativa almeno un'estensione di AI nel proprio browser, ma il 58% delle estensioni di AI ha permessi di accesso classificati come a rischio alto o critico, che consentono di monitorare le attività di navigazione, leggere contenuti delle pagine web e accedere a cookie e altri dati dell'utente, mentre il 5,6% delle estensioni di intelligenza artificiale è addirittura potenzialmente dannoso, in quanto ha la capacità di sottrarre informazioni sensibili. E come se non bastasse, il 18% degli utenti incolla incautamente i dati negli strumenti GenAI, e di questi circa il 50% sono informazioni aziendali.

A evidenziare queste allarmanti criticità è il rapporto "Enterprise GenAI Security Report 2025", pubblicato da LayerX Security, leader nelle estensioni del browser per la sicurezza aziendale.

Il report, basato sui dati di telemetria della vita reale dei clienti aziendali, rileva delle serie lacune di sicurezza e compliance e ha l'obiettivo di fare un quadro di come gli utenti aziendali interagiscono con gli strumenti di intelligenza artificiale generativa ed i relativi rischi sulla sicurezza dei dati. Il 71% delle connessioni agli strumenti di GenAI usati dai dipendenti avviene utilizzando l'account privato del dipendente, che così facendo bypassa gli strumenti aziendali.

Le principali cause di tali criticità sono riconducibili al fatto che account personali e i tool non monitorati espongono dati sensibili a rischi nascosti che non sono presidiati dall'azienda, la mancanza di consapevolezza e adeguata formazione del personale che agisce in buona fede ma imprudentemente, la mancanza di strumenti GenAI che siano ufficialmente riconosciuti dalla direzione aziendale come utilizzabili per finalità lavorative, e l'assenza di policy e regolamenti interni che ne disciplinano l'uso, fattore da cui deriva quindi un pericoloso "fai da te" che sfugge al controllo del management.

I risultati del rapporto evidenziano quindi la necessità di un approccio proattivo basato sul rischio per garantire le minacce nascoste dell'adozione di applicazioni di GenAI all'interno delle organizzazioni.

I CISO (Chief Information Security Officer) e i security manager dovrebbero pertanto implementare un framework completo per mitigare i rischi legati all'uso di strumenti di intelligenza artificiale. Questo richiede una oculata mappatura dell'utilizzo di applicazioni di GenAI nell'organizzazione per comprendere il profilo di rischio aziendale e costruire una strategia di bonifica efficace.

Le organizzazioni dovrebbero inoltre applicare anche strategie e procedure di auditing dell'IA a livello di endpoint per ottenere la piena visibilità dell'attività delle applicazioni di intelligenza artificiale utilizzate dei dipendenti ed essere così in grado di rilevare potenziali perdite di dati. Inoltre, è necessario limitare gli account personali e far rispettare SSO garantisce che i dipendenti utilizzino gli account GenAI aziendali con misure di sicurezza integrate.

Uso indiscriminato di AI in azienda: la formazione dei dipendenti gioca un ruolo chiave per la compliance privacy. L'uso indiscriminato di applicazioni e tool di intelligenza artificiale (AI) da parte dei dipendenti sta emergendo come una delle principali criticità nella gestione della sicurezza aziendale. L'intelligenza artificiale, nel suo potenziale dirompente, offre strumenti potenti per aumentare la produttività, migliorare i processi decisionali e automatizzare attività ripetitive.

Tuttavia, l'adozione incontrollata e non regolamentata di queste tecnologie da parte dei dipendenti può rappresentare una grave minaccia per la sicurezza dei dati, la privacy e l'integrità delle organizzazioni. In particolare, il tema dell'istruzione e della formazione riveste un ruolo cruciale per affrontare questo problema e mitigare i rischi associati.

L'adozione indiscriminata e spesso non regolata dell'AI generativa sta creando un terreno fertile per vulnerabilità critiche. È imperativo che le organizzazioni adottino misure rigorose per garantire la sicurezza dei propri sistemi, monitorare l'uso delle tecnologie da parte dei dipendenti e prevenire l'esposizione a rischi che potrebbero avere conseguenze devastanti. La sfida per il futuro non sarà soltanto quella di sfruttare al meglio le potenzialità dell'intelligenza artificiale, ma anche di gestirne i pericoli in modo proattivo e responsabile.

La diffusione incontrollata di strumenti basati sull'IA all'interno delle aziende solleva questioni cruciali in materia di privacy e sicurezza. Le informazioni sensibili, sia personali che aziendali, possono finire nelle mani sbagliate, con conseguenze devastanti. Questo scenario richiede un approccio proattivo e rigoroso per la gestione dei rischi. È fondamentale che le aziende adottino politiche chiare e rigorose sull'uso dell'IA, stabilendo regole precise per l'installazione e l'utilizzo di software e strumenti tecnologici. Inoltre, è necessario sviluppare framework di governance capaci di garantire che i sistemi di intelligenza artificiale siano progettati e utilizzati in modo responsabile.

La formazione dei dipendenti gioca un ruolo chiave in questo contesto. Promuovere una cultura della consapevolezza tecnologica è essenziale per ridurre i rischi associati all'uso improprio dell'AI. I lavoratori devono essere informati e sensibilizzati sui potenziali pericoli legati all'adozione di strumenti non autorizzati, comprendendo l'importanza della protezione dei dati personali e aziendali.

Questo utilizzo imprudente non solo mette a rischio i dati aziendali, ma può anche compromettere la reputazione delle imprese e portare a gravi conseguenze legali. Nel contesto di normative sempre più stringenti, come il GDPR in Europa, la violazione della privacy e la mancanza di protezione dei dati personali possono tradursi in gravi lacune sulla compliance con sanzioni significative e danni reputazionali irreparabili. Alla luce di questi rischi, diventa evidente che la formazione e l'istruzione dei dipendenti sull'uso corretto e responsabile dell'intelligenza artificiale non sono più un'opzione, ma una necessità. Uno dei principali problemi è la mancanza di consapevolezza tra i dipendenti riguardo ai rischi associati all'uso di applicazioni AI non autorizzate. Spesso, per comodità o per ignoranza, i lavoratori scaricano e utilizzano tool che promettono di semplificare il lavoro quotidiano, senza considerare le implicazioni per la sicurezza. Questo comportamento, se non affrontato, può trasformarsi in una vulnerabilità sistemica per l'intera organizzazione.
È qui che entra in gioco l'importanza di un'adeguata istruzione. Le aziende devono investire in programmi di formazione strutturati per educare i dipendenti sui pericoli dell'uso incontrollato dell'IA e sulle migliori pratiche per proteggere i dati aziendali. Questi programmi dovrebbero includere informazioni chiare sui rischi associati all'installazione di software non autorizzati, sulle normative relative alla protezione dei dati e sulle politiche aziendali in materia di sicurezza informatica. Inoltre, è fondamentale sensibilizzare i dipendenti sull'importanza della trasparenza e della conformità, spiegando come un uso consapevole dell'IA possa tradursi in un vantaggio competitivo per l'azienda. La formazione non dovrebbe limitarsi a semplici lezioni teoriche, ma dovrebbe includere anche simulazioni pratiche e scenari realistici che mostrino le conseguenze di comportamenti scorretti. Ad esempio, creare esercitazioni che simulano attacchi informatici o violazioni dei dati può aiutare i dipendenti a comprendere meglio l'importanza della sicurezza e a sviluppare un atteggiamento più responsabile nei confronti dell'uso delle tecnologie. L'intelligenza artificiale rappresenta senza dubbio una delle tecnologie più rivoluzionarie del nostro tempo, ma senza un'adeguata formazione e consapevolezza da parte dei dipendenti rischierebbe di compromettere la privacy e mettere a repentaglio la sicurezza globale.

Attenzione alla truffa telefonica del curriculum che vi sottrae soldi e dati personali. "***Abbiamo ricevuto il tuo curriculum, aggiungimi su WhatsApp per parlare di lavoro***", in questi giorni molti stanno ricevendo una telefonata con una voce registrata che pronuncia queste parole apparentemente allettanti, ma si tratta di una nuova truffa mirata a diffondere virus e sottrarre soldi e dati personali.
Occorre fare molta attenzione, perché la telefonata arriva un numero di provenienza italiano, facendola credere più attendibile, ma in realtà ha lo scopo di diffondere malware, rubare dati sensibili o soldi con finti investimenti.
La "truffa telefonica del curriculum" si sta diffondendo in Italia già da qualche settimana e se ne sta parlando molto sui social media. Questo stratagemma è particolarmente insidioso perché i criminali sfruttano l'aspettativa di chi sta effettivamente cercando lavoro e di chi, pur non avendo inviato alcun curriculum, potrebbe essere attirato da una qualche opportunità di guadagno.
Se si acconsente a proseguire la conversazione su WhatsApp si corre però il rischio di perdere soldi e/o i propri dati personali tramite la compilazione di moduli online che, a detta del sedicente recruiter, farebbero parte della procedura necessaria per procedere con l'assunzione. Per difendersi, bisogna tenere gli occhi aperti e terminare la chiamata truffaldina.
Comprendere meglio come funziona la truffa del curriculum è essenziale per non cadere in questa frode, che rientra nella categoria delle cosiddette "Online Recruitment Scam", ossia truffe basate su false opportunità di lavoro. Questa frode sfrutta un meccanismo semplice quanto efficace. Il primo contatto avviene innanzitutto con una chiamata con prefisso italiano +39, a differenza di altre truffe che utilizzano prefissi stranieri, spesso più facilmente riconoscibili come sospetti. Il messaggio iniziale, che informa del presunto curriculum ricevuto da una fantomatica azienda, ha lo scopo di incuriosire la vittima e spingerla a proseguire l'interazione. Se la persona sta cercando lavoro, potrebbe pensare che si tratti di una risposta a un curriculum inviato più o meno recentemente ed è per questo che il destinatario della chiamata potrebbe accettare di proseguire la conversazione su WhatsApp, come richiesto dalla voce registrata.
A questo punto, il raggiro entra nella fase più pericolosa. La chat su WhatsApp serve a instaurare un clima di fiducia, facendo credere alla vittima di avere tra le mani un'opportunità di lavoro concreta. La presunta azienda propone attività semplici, promettendo compensi in cambio di interazioni sui social network ad esempio. Il vero obiettivo, però, è spingere la persona a effettuare investimenti su piattaforme online. In alcuni casi, viene inviato un link su cui cliccare, magari con la scusa di compilare moduli necessari per procedere con l'assunzione, e che in realtà può contenere malware che verranno usati per rubare informazioni personali oppure dati finanziari. In ogni caso, a prescindere dalla specifica proposta fatta dai truffatori, in questa fase il loro obiettivo è quello di convincere la potenziale vittima che si tratta di una reale opportunità di guadagno e che, per questo motivo, sarebbe un peccato perdersela. Dopo aver convinto la vittima della bontà dell'offerta iniziale, i truffatori potrebbero anche suggerire di investire somme di denaro su piattaforme di trading. Queste piattaforme sono spesso fittizie o strutturate in modo da rendere impossibile il recupero dei fondi una volta versati. L'inganno si perfezione nel momento in cui la vittima tenta di ritirare il denaro e si accorge che l'azienda non risponde più: a quel punto, i truffatori avranno già chiuso ogni canale di comunicazione e saranno svaniti nel nulla. Cosa ancora peggiore, questo tipo di frode non si limita alla perdita economica immediata. Oltre ai soldi, i criminali possono ottenere informazioni personali sensibili, come indirizzi, numeri di telefono e, in alcuni casi, dati bancari. Con queste informazioni, potrebbero tentare ulteriori attacchi, come il furto d'identità o l'accesso a conti online. Nel caso vi accorgeste troppo tardi della trappola quando ormai siete già caduti vittima della truffa del curriculum, non resta altro che fare una segnalazione alla Polizia Postale di quanto accaduto.

- N6) Ambiente: MUD 2025 - la scadenza è il 28 giugno 2025

È stato pubblicato in Gazzetta Ufficiale (Serie Generale) del 28 febbraio 2025, il Decreto del Presidente del Consiglio dei ministri recante l'approvazione del Modello Unico di Dichiarazione ambientale (MUD) per l'anno 2025, che sarà utilizzato per le dichiarazioni riferite all'anno 2024.

Il Ministero dell'ambiente e della sicurezza energetica comunica che, in base all'articolo 6 della Legge 25 gennaio 1994 n. 70, il termine per la presentazione del MUD è fissato in centoventi giorni a decorrere dalla data di pubblicazione e, pertanto, **la presentazione del MUD dovrà avvenire entro il 28 giugno 2025**.

La pubblicazione degli allegati al DPCM recante l'approvazione del MUD per l'anno 2025 è demandata al Ministero dell'ambiente e della sicurezza energetica che, a tal fine, ha pubblicato sul proprio sito web le istruzioni per la compilazione del Modello unico di dichiarazione, il modello per la comunicazione rifiuti semplificata, i modelli raccolta dati e le istruzioni per la presentazione telematica.

Unioncamere ha iniziato a pubblicare progressivamente i prodotti informatici e i portali per la compilazione e presentazione del MUD 2025,

Inoltre Unioncamere mette a disposizione:

- il prodotto informatico per la compilazione delle Comunicazioni Rifiuti, Imballaggi, Veicoli fuori uso, Rifiuti da apparecchiature elettriche ed elettroniche, che sarà reso disponibile tramite la sezione MUD del portale EcoCamere e tramite il sito del MUD Telematico;
- il prodotto informatico per il controllo formale delle dichiarazioni trasmesse dai soggetti che utilizzano prodotti software diversi da quello predisposto da Unioncamere.

Voglia gradire i nostri più cordiali saluti *ing. Giorgio Violi* *ing. Alberto Sant'Unione*