CENSIS

DEEPCYBER
a Maggioli Group company

Advanced Intelligence, Protection, Antifraud.

RAPPORTO CENSIS - DEEPCYBER

IL VALORE DELLA CYBERSECURITY

Perché serve la sicurezza informatica per la buona rivoluzione digitale

Roma, 22 aprile 2022

ASSOCOMUNICATORI
ASSOCIAZIONE NAZIONALE COMUNICATORI D'IMPRESA

ital communications
A STRATEGIC COMMUNICATION AGENCY

Indice

1. L'ESSENZIALE *CYBERSECURITY*

1.1. Il digitale sicuro per tutti

L'apprezzata *digital life*, ormai al centro delle nostre vite, coincide con il massimo dell'insicurezza informatica: da virus e attacchi informatici di tipo distruttivo, a furti d'identità, passando per truffe con finalità di riscatto e frodi, è ormai ampia la gamma dei rischi che minaccia la vita di famiglie, aziende e istituzioni nel quotidiano.

In un mondo ad alta competizione, dove la minaccia informatica è arma per fini illeciti e strumento per colpire gli altri, la *cybersecurity* diventa decisiva per difendere e promuovere benessere e libertà.

Quanto ne sono consapevoli gli italiani? Quali comportamenti di prevenzione e difesa dalle tante e diverse minacce adottano? E ancora: qual è il contributo possibile della *cybersecurity* per la tutela dell'integrità di dati, documenti e degli stessi sistemi digitali e, in generale, per ridurre le *cyber-paure* che rischiano di amplificare il clima di incertezza sociale del Paese?

Sono i principali temi del *Primo Rapporto Censis-DeepCyber sul valore della cybersecurity*: l'esito è il racconto di un settore ormai irrinunciabile, perché solo una protezione efficace e condivisa dai rischi informatici potrà restituire la serenità necessaria per vivere bene tutti nella *digital life*.

1.2. I principali risultati

1.2.1. La trama

Phishing, *ransomware*, *trojan*, *malware*: sono termini ormai diffusi che richiamano alcune delle minacce informatiche con cui gli italiani fanno quotidianamente i conti, a cui si aggiungono gli attacchi informatici in grande stile verso istituzioni o aziende maggiori. Esempi sono quelli contro l'Inps nella fase iniziale dell'emergenza sanitaria, o quelli contro istituzioni sanitarie ed i sistemi di prenotazioni vaccinali o, più di recente, quelli che hanno bloccato i sistemi di bigliettazione nelle stazioni ferroviarie.

Fatti che hanno causato problematiche rilevanti, paralizzando le regolari attività di istituzioni e aziende finite sotto attacco, con costi rilevanti per le persone coinvolte.

D'altronde, sono significative le quote di italiani che hanno fatto esperienza diretta di alcuni rischi informatici: dal ritrovarsi il proprio pc infettato da un virus, al ricevere email con mittente falso, fino al ritrovarsi pagamenti online fatti a proprio nome tramite carte di credito clonate, passando per i furti o le violazioni di dati sensibili tramite i social fino agli incontri sul web con malintenzionati. Nel lavoro, poi, in molti hanno sperimentato attacchi informatici contro la propria azienda.

Entrati di corsa nella *digital life*, diventati intensi produttori e fruitori di dati a distanza per lavoro, studio, *entertainment* e relazioni, gli italiani non hanno ancora una compiuta consapevolezza dell'importanza di culture, strategie, tecnologie, competenze e sistemi di protezione informatica per il proprio benessere: ad oggi oltre un terzo degli italiani semplicemente non fa nulla per la sicurezza dei propri dispositivi informatici e solo 1 su 4 ha un'idea precisa di cosa sia la *cybersecurity*.

Invece, anche i recenti eventi rilanciano il ruolo decisivo della *cybersecurity*, che non può più essere considerata un costo o un ambito per soli esperti e iniziati. Si tratta sempre più di un investimento sociale di interesse collettivo, perché significa rendere cittadini, aziende, istituzioni meno esposti ad attacchi malevoli, e ridurre i conseguenti costi sociali ed economici potenzialmente elevatissimi e massimizzando così i benefici e le opportunità della *digital life.*

1.2.2. I numeri in pillole

Chi si difende dai cyber-attacchi e chi no. Il 61,6% degli italiani è preoccupato per la sua sicurezza informatica e adotta precauzioni per difendersi: di questi, l'82% ricorre a software e app di tutela ed il 18% si rivolge ad un esperto. Il 28,1%, pur dichiarandosi preoccupato, non fa nulla di concreto per difendersi, mentre il 10,3% non ha alcuna preoccupazione sulla sicurezza informatica. In generale, quindi, quasi 4 italiani su 10 sono indifferenti o non si tutelano contro gli attacchi informatici.

La cybersecurity da far conoscere. Il 24,3% degli italiani conosce precisamente cosa si intende per *cybersecurity*, il 58,6% per grandi linee,

mentre il 17,1% non sa cosa sia. Ad averne una conoscenza precisa sono soprattutto giovani (35,5%), laureati (33,4%), imprenditori (35,4%) e dirigenti (27,7%). Il 39,7% degli occupati dichiara di aver avuto in azienda una qualche formazione specifica sulla *cybersecurity*, quota che raggiunge il 56,8% per le posizioni apicali. Ampia è la disponibilità dei lavoratori a partecipare ad iniziative formative in azienda o altrove sulla *cybersecurity*: il 65,9% dei lavoratori vorrebbe parteciparvi.

Scene di insicurezza informatica. Al 64,6% dei cittadini (75,6% tra i giovani, 83,8% tra dirigenti) è capitato di essere bersaglio di email ingannevoli il cui intento era estorcere informazioni personali sensibili, presentandosi come provenienti dalla banca di riferimento o da aziende di cui la persona era cliente. Il 44,9% (53,3% tra i giovani, 56,2% tra gli occupati) ha avuto il proprio pc/laptop infettato da un virus. L'insicurezza informatica viaggia anche tramite i pagamenti online: al 14,3% dei cittadini è capitato di avere la carta di credito o il bancomat clonato, al 17,2% di scoprire acquisti online fatti a suo nome e a suo carico. Il 13,8% ha subìto violazioni della *privacy*, con furti di dati personali da un *device* oppure con la condivisione non autorizzata di foto o video. Al 10,7% è capitato di scoprire sui social account *fake* con il proprio nome, identità o foto, al 20,8% di ricevere richieste di denaro da persone conosciute sul web, al 17,1% di intrattenere relazioni online con persone propostesi con falsa identità. Diffuso anche il cyberbullismo: il 28,2% degli studenti dichiara di aver ricevuto nel corso della propria carriera scolastica offese, prese in giro, aggressioni tramite social, WhatsApp o la condivisione non autorizzata di video.

I cyber-rischi per aziende e lavoratori. Il 19,5% degli occupati ha sperimentato attacchi informatici con danni agli account social o al sito web della propria azienda, il 14,7% attacchi che hanno causato la perdita di dati e informazioni aziendali. Anche il lavoro da casa genera rischi per la sicurezza informatica. Al 52,8% degli occupati capita di svolgere attività lavorative da casa, *in remote*: di questi, il 20,1% utilizza *device* aziendali, ma senza separarli dai *device* personali per le proprie attività private. C'è molta confusione sulle modalità di salvataggio del lavoro fatto da o in casa: infatti, l'82,1% salva gli output del proprio lavoro su singoli *device*.

Cyber-paure avanzano. L'81,7% degli italiani teme di finire vittima di furti e violazioni dei propri dati personali sul web. Una paura diffusa, trasversale al corpo sociale. Tra le attività, che gli italiani percepiscono come a più alto

rischio per il furto d'identità, ci sono la navigazione web con consultazione di siti (57,8%), l'utilizzo di account social, da Facebook ad Instagram (54,6%), gli acquisti di prodotti online (53,7%), le operazioni di home banking, come effettuare bonifici, verificare il proprio conto corrente, ecc. (46,6%), le prenotazioni di viaggi e hotel (41,5%), l'utilizzo di app per incontri, relazioni, come ad esempio Tinder (41%), quello di programmi di messaggistica istantanea, come WhatsApp (40,2%), il pagamento online di bollettini (38,4%), la partecipazione a webinar o incontri online (38,3%), l'accesso a servizi digitali della pubblica amministrazione, ad esempio, tramite Spid (30,8%). *Cyber-paure* che condizionano il rapporto con il digitale e che rischiano di sovrapporsi alle paure fisiche, materiali, amplificando all'estremo l'incertezza sociale.

2. LO SCENARIO

2.1. Vite digitali

2.1.1. Nuova priorità

A lungo la *cybersecurity* è rimasta oggetto oscuro per la gran parte degli italiani, evocando in principio scenari fantascientifici come nei romanzi di Isaac Asimov o in film cult come Matrix.

In seguito, si è diffusa una letteratura popolare che ha via via identificato la *cybersecurity* con le sfide di singoli *hacker*, divenuti nell'immaginario collettivo sognatori anarcoidi in lotta con i nuovi poteri digitali.

Più recentemente il proliferare delle *cyber-minacce,* molto presenti anche nell'aggressione russa all'Ucraina e la connessa evidenza dei loro costi economici e sociali hanno reso urgente l'importanza di costruire solide barriere di protezione.

In tale contesto occorre rivedere il significato sociale della *cybersecurity*, che sempre più emerge come la sola efficace risposta al nuovo bisogno individuale e collettivo di sicurezza informatica: in poche parole, è diventata un'esigenza fondamentale, stringente, quotidiana.

D'altro canto, gli avversari della *cybersecurity* non sono più lunatici *hacker* solitari, ma potenti e strutturate organizzazioni, capaci di mixare raffinate competenze con le più avanzate soluzioni tecnologiche, dall'intelligenza artificiale al *machine learning*.

Per questo, la *cybersecurity* deve diventare strategia intenzionale, organizzata, di soggetti e processi per proteggere le risorse digitali da attacchi ostili esterni. Operativamente, essa va implementata con l'opportuno ricorso a tecnologie, strumenti, processi e attività per rispondere all'obiettivo esplicito di tutelare sistemi, dispositivi e dati.

Ogni soggetto che dispone di tecnologie digitali è chiamato ad effettuare una valutazione dei rischi relativi a riservatezza, integrità e disponibilità dei dati: infatti, è da questo che dipende il grado di sicurezza.

Bastano questi pochi riferimenti per capire che la *cybersecurity* è un'attività essenziale per il benessere economico, la sicurezza del Paese e anche delle

nostre vite e dei tanti ambiti in cui si svolgono: infatti, se insicurezza e vulnerabilità informatica conducono a danni gravi, occorrono processi articolati di gestione del rischio tecnologico e digitale per prevenire o sventare attacchi o, eventualmente, mitigarne le conseguenze.

2.1.2. Capirne la complessità, per difendersi meglio

Le minacce informatiche e le relative risposte sono materia non facile, densa, perché richiedono elevate competenze tecniche e voglia di misurarsi con un universo cangiante, che impone continuo studio e adattamento.

Infatti, la *cybersecurity* è impegnata in una perenne corsa in avanti, dalla velocità crescente, perché ogni strumento di tutela, per quanto sofisticato, rischia di essere obsoleto in poco tempo a seguito di minacce informatiche nuove, diverse, sfuggenti, pervasive, e sempre più difficili da individuare e sconfiggere.

In tale quadro ad alta complessità, è importante creare una grammatica comune, che consenta di distinguere le aggressioni a partire dalle motivazioni di chi attacca evitando di mettere negli stessi grandi contenitori cose che in realtà sono tra loro molto diverse. Pertanto, ci sono attacchi:

- motivati dalla volontà di monetizzare, come ad esempio le frodi informatiche o le richieste di riscatti per *ransomware*;
- di *cyber-spionaggio*, o chiaramente promossi e sponsorizzati da Stati, perpetrati da mercenari che vendono i propri servizi.

Gli attacchi, poi, hanno un livello di sofisticatezza e complessità via via maggiore, che li rende al contempo efficaci e pervasivi: per questo nessuno può dirsi al riparo, ed è ingenuo pensare che sia sufficiente tutelarsi da attacchi semplici, *basic*.

Oltre a garantire sempre e ovunque le tutele basiche, è fondamentale una nuova fase di investimenti in efficienti ed efficaci sistemi di sicurezza informatica, capaci di reagire in tempi stretti alle emergenze ricorrenti.

Dare centralità alla *cybersecurity*, in parallelo con la crescita della digitalizzazione, significa creare i contesti per cercare di prevedere nelle singole realtà e nella società in generale i pericoli futuri.

Per questo occorre un salto di qualità negli strumenti di tutela e protezione cibernetica all'altezza delle minacce globali, che spesso non hanno un centro immediatamente riconoscibile e che operano tramite filiazioni invisibili, puntando a destabilizzare aziende o addirittura interi Paesi.

Il periodo pandemico prima e l'aggressione all'Ucraina hanno reso evidente che la digitalizzazione impone investimenti in sistemi di protezione adeguati, perché il salto nella *digital life* amplia la gamma di pericoli e situazioni in cui gli avversari possono inserirsi.

In estrema sintesi si può dire che: più digitale, senza adeguata protezione informatica, significa più insicurezza e maggiore vulnerabilità.

2.1.3. È un problema di tutti

La tecnicità dei temi e del lessico rende la *cybersecurity* ostica, rischiando di relegarla quasi naturalmente ad un ambito per soli iniziati. Invece, i rischi informatici sono diffusi e puntuali e possono colpire imprese di ogni dimensione e ogni persona che dispone di *device* digitali.

Al contempo, la moltiplicazione delle attività *in remote* tra lavoro, studio e *entertainment* diffonde all'estremo le richieste di accesso veloce e simultaneo a banche dati più o meno liberamente accessibili per una moltitudine di persone, amplificando di conseguenza anche i rischi di attacchi.

Pertanto, la *cybersecurity* è questione collettiva, che riguarda tutti e, se non viene affrontata con una mobilitazione adeguata di risorse, espone la società ad attacchi dagli effetti devastanti persino sulla quotidianità minuta.

È un tema su cui è prioritario accrescere sia l'*awareness* della *public opinion* sia l'attenzione dei decisori: infatti, essere vulnerabili ed esposti ai *cyber-attacchi* significa esporsi al rischio di una regressione della qualità della vita e delle libertà.

Il digitale è strumento che cambia in meglio le nostre vite se è adeguatamente tutelato e messo nelle condizioni di funzionare: attualmente si stima che ciascun individuo crei in media ogni secondo 1,7 *megabytes* di dati, che poi affluiscono nelle aziende, chiamate a loro volta a garantirne la conservazione nel rispetto della privacy e dell'uso consentito dalla legge.

L’esito è la creazione di valanghe di dati che vanno archiviati e tutelati, il cui accesso va reso disponibile in simultanea ad una molteplicità di soggetti: sfide straordinarie di per sé, che tuttavia devono anche misurarsi con le intenzioni avverse di chi, operando sempre più con organizzazioni strutturate, a volte di diretta emanazione di Stati, vede in tali dati persino un’arma per colpire un altro Paese, attaccandone istituzioni vitali.

È un contesto che rende la *cybersecurity* una grande questione collettiva, priorità per le agende di cittadini, imprese e istituzioni.

2.2. I *cyber-pericoli* percepiti e reali

2.2.1. L’incertezza da combattere

Nel tempo un’incertezza esistenziale, che è arrivata a toccare ambiti molto intimi, ha pervaso progressivamente le vite, condizionando i comportamenti individuali e collettivi.

In tale scenario, tutelarsi dai rischi significa ridurre la paura che, se notoriamente è un sentimento fondamentale per la sopravvivenza, tuttavia può pesantemente condizionare e limitare l’azione dei singoli e lo sviluppo della società.

Il digitale, innestando nelle nostre vite nuove dimensioni e modificando il modo di praticarne altre più tradizionali, ha anche ridefinito l’incertezza e l’insicurezza: infatti, alle paure legate all’insicurezza fisica ed alla vita ordinaria di relazioni, ha aggiunto e giustapposto quelle legate al mondo del web e dell’informatica, con il rischio di essere vittima dei sempre più diffusi e articolati reati informatici.

In tale quadro, la *cybersecurity* non è solo un insieme di tecniche, tecnologie e competenze praticate da soggetti professionali e aziende del settore, ma è lo strumento attraverso cui la società può riportare sotto controllo un’area di insicurezza delle persone, quella informatica, riducendo così il tasso complessivo di paura.

Ecco perché la *cybersecurity* non ha solo un valore economico, non è solo necessaria per evitare che le aziende e le persone siano colpite nei loro interessi e nella privacy, ma assolve ad una funzione sociale fondamentale:

far sentire le persone con le spalle protette quando si muovono nel web per lavoro, studio, diletto o voglia di relazionarsi con gli altri.

La *cybersecurity* partecipa di quella fondamentale rassicurazione sociale, indispensabile per il benessere soggettivo e della collettività.

2.2.2. Difesi e indifesi

Oltre due terzi degli italiani è convinto che nel prossimo futuro occorrerà abituarsi al reiterarsi di emergenze con impatti sulle vite quotidiane simili a quelli del Covid-19. Un dato che certifica come la maggioranza della popolazione percepisca il pericolo estremo, non più eccezionale, ma in grado in qualsiasi momento di trasformarsi in realtà, facendo deragliare le vite quotidiane.

È una percezione completamente nuova e diversa del rapporto tra la vita quotidiana e le minacce che incombono su di essa, laddove queste ultime sono potenti e pervasive, capaci di cambiare d'improvviso il corso delle esistenze.

Se a lungo vite individuali e dibattito pubblico sono stati monopolizzati dalle paure legate all'insicurezza quotidiana, indotte dal timore di essere vittima di reati, ora prevale una insicurezza diversa, che rinvia al nesso tra grandi eventi globali, vita quotidiana ed alla nuova centralità della *digital life*.

Il 61,6% degli italiani si preoccupa della propria sicurezza informatica, adottando anche precauzioni sui propri *device*, con valori che arrivano al 69,1% tra i laureati (tab. 1). Alto è il livello di attenzione anche tra imprenditori (73%) e dirigenti (72,6%). Si tratta di tipologie professionali in cui sono più presenti nomadi digitali, cioè persone che lavorano di solito con propri *device in remote*, interagendo con una molteplicità di clienti e che hanno un assoluto bisogno di buoni livelli di prevenzione e sicurezza.

Il 28,1%, invece, seppur preoccupato per la propria sicurezza informatica, non adotta alcuna precauzione. Il 10,3% non ha alcuna preoccupazione per a riguardo. Dichiarano di non essere preoccupati della sicurezza informatica anziani (26,8%), bassi titoli di studio (25,4%), donne (13,8%), bassi redditi (11,4%). Gruppi sociali che, presumibilmente, sono anche quelli maggiormente esposti ai rischi del web.

Ma quali precauzioni sono concretamente adottate? Dai dati emerge che (fig. 1):

- l'82% prova ad applicare regole di sicurezza, ricorrendo a software e app di tutela, e a farlo di più sono adulti (86,7%), laureati (83,9%) e occupati (88,6%);
- il 18% ricorre ad un esperto per avere supporto, e a farlo di più sono anziani (36,4%), persone con un basso titolo di studio (23,9%), donne (21,5%).

In definitiva, attualmente ci sono quasi 4 persone su 10 che non sono preoccupate per la sicurezza informatica o che, pur preoccupate, non fanno nulla per tutelarsi. Un ventre molle pericoloso, fatto di bersagli facili, potenziali *gate* di ingresso per *cyber-criminali* in evidente crescita di potenza, astuzia e capacità operativa.

Come rilevato, la sicurezza informatica è da intendersi come un'attività collettiva, poiché l'integrazione tra *device* e persone tramite le reti trasforma ciascun soggetto in una potenziale porta d'ingresso degli attaccanti.

Per questo, oltre alla tecnicità competente degli esperti della *cybersecurity*, occorre una responsabilizzazione individuale, tramite l'adozione di comportamenti conformi di autotutela: infatti, senza una *compliance* consapevole di tutti gli attori variamente coinvolti lungo tutta la filiera, tecnicità e competenza degli esperti di *cybersecurity,* seppure elevate*,* non potranno certo bastare.

2.2.3. Conoscere per difendersi, tutti insieme

Solo il 24,3% degli italiani dichiara di sapere precisamente cosa si intende per *cybersecurity*, mentre il 58,6% la conosce a grandi linee ed il 17,1% non sa cosa sia. Più preparati sul tema, perché dichiarano di avere una conoscenza precisa, sono gli uomini (31,8%), i giovani (35,5%), i laureati (33,4%), gli imprenditori (35,4%) (tab. 2).

Il 39,7% degli occupati dichiara di aver ricevuto una formazione specifica sulla *cybersecurity* (tab. 3). Se la *cybersecurity* è sempre più strategica e se le *défaillances* nelle modalità di protezione generano costi economici e sociali eccezionali per le aziende, i dati indicano come sia ancora lunga la strada che dovrà percorrere il sistema delle imprese italiano.

In tal senso, è certamente fondamentale affidarsi ad esperti, anche internalizzando figure professionali in grado di dialogare con le aziende del settore, ma al contempo è necessario mettersi al riparo da comportamenti non conformi dei singoli dipendenti.

Senza la condivisione di appropriati criteri di sicurezza e dei relativi comportamenti di tutela dagli attacchi informatici, anche i più sofisticati sistemi rischiano di saltare, con la complicità involontaria di chi non è stato reso consapevole dei rischi.

Tra gli occupati che non hanno mai ricevuto formazione sulla sicurezza informatica è alta la quota di chi si dichiara pronto a ricevere una formazione specifica: infatti, ben il 65,9% dei lavoratori vorrebbe partecipare ad attività formative che gli consentano di capire come evitare di diventare vittima ed eventualmente complice involontario degli attaccanti (fig. 2).

3. ESPERIENZE DI INSICUREZZA E ILLEGALITÀ INFORMATICA

3.1. Virus, truffe tentate e pagamenti rischiosi

La mancanza di informazione e formazione su prevenzione e sicurezza informatica rende le persone altamente vulnerabili alle minacce. Le esperienze di insicurezza informatica sono piuttosto diffuse, troppo spesso le persone le reputano accadimenti fatalisticamente inevitabili, più o meno come l'arrivo di virus o di eventi atmosferici avversi.

Eppure, come rilevato, è alta la quota di persone che ha avuto esperienza di attacchi informatici. Infatti (tab. 4):

- il 64,6% dei cittadini dichiara di essere stato bersaglio di email ingannevoli il cui intento era di estorcere informazioni personali sensibili, utilizzando come finto mittente la banca di riferimento o aziende di cui la persona era cliente, con valori che arrivano al 72,5% tra i laureati, al 75,6% tra i giovani.
- Il 44,9% degli italiani ha avuto il proprio pc/laptop infettato da un virus, esperienza diffusa soprattutto tra i maggiori utilizzatori, vale a dire giovani (53,3%) e laureati (52%).

Altra dimensione in cui le persone hanno sperimentato la pericolosità degli attacchi informatici è quella dei pagamenti online, perché:

- il 14,3% ha avuto la carta di credito o il bancomat clonati, ed è il 15,4% tra i laureati, il 18,8% tra i giovani;
- il 17,2% ha scoperto acquisti online fatti a suo nome ed a suo carico, ed è il 26,1% tra i giovani, il 25,2% tra gli imprenditori.

Sono esperienze diffuse di violazione di sfere personali essenziali, che toccano anche il portafoglio delle persone e che, in generale, tendono a minare la fiducia nelle reti informatiche, alimentando un clima di incertezza.

3.2. Identità violate

Il 13,8% degli italiani dichiara di aver subìto violazioni della *privacy* con furti di dati personali, oppure con la condivisione non autorizzata di foto o video. Al 10,7% è capitato di vivere la traumatica esperienza di scoprire sui social account *fake* con il proprio nome, identità o foto (fig. 3).

Sono dimensioni particolarmente drammatiche dal punto di vista individuale, perché la scoperta che altri stanno utilizzando la propria identità oppure che sono stati immessi nel web e, quindi, condivisi contro la propria volontà, foto, video, messaggi, materiali personali, tocca la sfera della *privacy,* violando l'intimità più segreta delle persone.

Si tratta di una vera e propria violenza alla persona che, in molti casi, genera conseguenze psicologiche e sociali durature, ed è la dimensione che più rende evidente alle persone l'urgenza di mettere in atto una difesa efficace per non ritrovarsi esposti nella pubblica piazza per fatti non commessi o che si voleva restassero riservati.

3.3. Altre disavventure informatiche

Il 20,8% degli italiani ha ricevuto richieste di denaro da persone conosciute sul web, mentre il 17,1% ha avuto conversazioni e frequentazioni con persone presentatesi con una falsa identità (fig. 4).

Il web diventa, quindi, luogo in cui gli aspiranti criminali si mimetizzano per agganciare le persone, approfittando della loro vulnerabilità per estorcere denaro. E il motivo è presto detto: il web accelera il passaggio verso modalità più intime di relazione perché, dopo una diffidenza iniziale, la distanza fisica garantita dal *remote* tranquillizza le persone e le porta ad abbassare le difese.

È una dimensione della sicurezza non tanto tecnica quanto psicologica, che richiederebbe una preparazione specifica degli internauti al mondo virtuale, perché se è vero che lo schermo tiene lontane le minacce fisiche dirette e immediate, proprio la distanza fa abbassare la guardia esponendo gli utenti a pericolose manipolazioni e strumentalizzazioni.

Le cronache sono piene di vulnerabilità schernite e strumentalizzate, di cui spesso le vittime si vergognano e che, pertanto, diventano anche a basso rischio e basso costo per i malfattori.

Tra chi è studente ben il 28,2% dichiara che nella sua carriera scolastica ha subìto un qualche episodio di *cyber-bullismo,* essendo vittima di offese, prese in giro, aggressioni su social, *WhatsApp* o tramite condivisione di video.

Sono dati che confermano una percezione diffusa: tra le giovani generazioni sta diventando significativa la quota di ragazzi in età scolare colpiti da tali degenerazioni.

È un processo per certi versi inevitabile, visto l'elevato tasso di digitalizzazione dei più giovani, le cui vite si svolgono per una parte rilevante sul web su cui si sono trasferite forme di bullismo che un tempo si svolgevano nel mondo reale.

È un terreno da presidiare subito e bene, perché è la nuova frontiera su cui si generano elevati costi psicologici e sociali per i più vulnerabili ed è una palestra sin troppo facile per aspiranti prepotenti o criminali.

Nato come luogo della libertà estrema, con inesistenti barriere d'accesso, dove chiunque poteva esprimere la propria personalità, magari vincendo inibizioni e timidezze, oggi il web rischia di trasformarsi nel suo contrario: un luogo dove vince l'aggressività e la violenza verbale, e le vulnerabilità sono apertamente schernite e violentate, con una ferocia che beneficia della relativa impunità.

Un mondo di libertà è virtuoso, un mondo totalmente sregolato è il regno del più forte: ecco l'insegnamento primo di questi anni di web.

4. BERSAGLIO AZIENDE

4.1. I luoghi decisivi della sfida

La spinta alla digitalizzazione del biennio del Covid-19 ha reso evidente che non ci sarà una buona rivoluzione digitale, capace di semplificare e migliorare la vita di cittadini e imprese, senza un adeguato livello di protezione dalle sempre più complesse e pericolose minacce informatiche.

Del resto, sono ormai evidenti i tanti e diversi fattori che amplificano i rischi per la sicurezza informatica di cittadini, imprese, Pubblica Amministrazione, quali ad esempio:

- la proliferazione delle minacce informatiche a livello internazionale, componente rilevante delle tensioni e conflittualità tra Paesi;
- la ridotta cultura digitale e la ancora più ridotta attenzione agli aspetti di *cybersecurity*;
- il *digital divide,* che rende altamente vulnerabili interi gruppi sociali, più facilmente preda di comportamenti digitali ad alto rischio.

È evidente che la situazione di aziende e occupati, così come quella dei professionisti che, come lavoratori autonomi sono in relazione professionale con le aziende, è decisiva perché si possa fare della *cybersecurity* uno dei tratti costitutivi della rivoluzione digitale in corso.

Peraltro, le aziende oggi sono fortemente sollecitate dalle regolazioni in materia di *privacy*, tutela dei dati e altri aspetti che chiamano in causa la loro concreta responsabilità.

Rispondere a queste sfide, richiede un salto di qualità nella *cyber-cultura* delle aziende, con un deciso *upgrading* del *digital risk management* e significativi investimenti per non restare indietro nella perenne corsa con i *cyber* avversari malintenzionati.

Al contempo, è indispensabile che il settore della *cybersecurity* sia messo nelle condizioni di espandersi e potenziarsi per star dietro alla domanda di sicurezza informatica, risolvendo lo *shortage* di competenze e risorse con cui sinora è stato costretto a fare i conti.

4.2. La difesa di filiera

Al 19,5% degli occupati è capitato che gli account social o il sito web della propria azienda subissero attacchi informatici con danni, mentre al 14,7% che la propria azienda perdesse dati, informazioni a causa di un attacco informatico (fig. 5).

L'esperienza degli occupati segnala come gli attacchi informatici colpiscano diffusamente le aziende, con danni economici rilevanti. Ci sono casi in cui gli attacchi rinviano anche a comportamenti inappropriati da parte di dipendenti, esito di una scarsa consapevolezza riguardo ai rischi informatici e della già citata mancanza di formazione specifica.

Ci sono i rischi di fughe di notizie interne, ad esempio a causa della rivelazione involontaria di password di accesso o della mancata verifica di interlocutori a cui si finisce per passare informazioni sensibili.

Le modalità di attacco sono in continua evoluzione: pertanto, richiedono l'adattamento sistematico dei sistemi di tutela.

Peraltro, nessuno può chiamarsi fuori o pensare di non essere bersaglio.

La sicurezza aziendale diventa sempre più un tema di filiera, che chiama alla responsabilità in primo luogo le aziende maggiori. Queste dovrebbero consapevolmente guidare i processi di adeguamento della sicurezza informatica anche negli operatori di dimensioni inferiori che, in qualità di fornitori, possono rappresentare una porta di accesso per raggiungere bersagli più ambìti.

Occorre pensare alla sostenibilità di filiera non solo come sostenibilità ambientale, economica e sociale, ma anche nella sua dimensione di sicurezza informatica, in quanto il costo della mancata protezione dei sistemi può minare nel profondo la stessa sostenibilità economica delle aziende variamente coinvolte.

4.3 I rischi dello *smart working*

Il lavoro a distanza è stato a lungo visto con sospetto, come fosse un'opportunità non consueta da riservare a pochi.

Obbligando in casa i lavoratori, la pandemia ha consentito di scoprire i benefici del lavoro a distanza, a cominciare dalla possibilità stessa di continuare a svolgere la propria attività anche nel pieno di una drammatica emergenza.

La riorganizzazione improvvisa del lavoro è stata possibile grazie alle tecnologie digitali ed allo straordinario adattamento degli italiani alle nuove attività da svolgersi a casa.

I primissimi giorni del *lockdown* sono entrati nella memoria collettiva come una fase eroica in cui gli impegni individuali hanno contribuito a trovare un'incredibile, straordinaria, "quadra" sociale e lavorativa di fronte all'inedito inatteso della pandemia.

Lo spirito di squadra di tante comunità aziendali ha consentito di dare risposta alle notevoli difficoltà di spostare il lavoro dalla compresenza fisica al *remote,* anche grazie a soluzioni improvvisate frutto dell'inventiva e della disponibilità di ciascuno.

Nella gran parte dei casi le soluzioni hanno ben funzionato, fino al punto da far scoprire alle aziende che lo *smart working* non è il luogo di tutte le pigrizie, ma una delle modalità con cui si può lavorare, anche con buone *performance*.

La pressione dell'emergenza con le sue priorità non poteva non lasciare in secondo piano gli aspetti della sicurezza informatica che, invece, man mano che si torna alla normalità, assumono un'importanza maggiore.

Infatti, trasformare le case in uffici o utilizzare indifferentemente *device* personali e di lavoro fragilizza le reti aziendali, rendendole vulnerabili alle cattive intenzioni di chi vuole impossessarsi di informazioni riservate o semplicemente bloccarle per ricatto o in ogni caso danneggiarle.

Al 52,8% degli occupati capita di lavorare da casa in *smart working* o semplicemente di svolgere alcune attività *in remote* per l'azienda o per committenti (fig. 6).

Di questi, il 59,6% utilizza *device* aziendali, mentre il 20,1% non tiene separati i *device* per lavoro dai *device* personali per attività non lavorative, private. Un comportamento che è spia di un buco evidente nella rete di protezione che può aprire varchi molto pericolosi per i malintenzionati (25,5%).

Altra area di rischio riguarda le abitudini di salvataggio del proprio lavoro quotidiano da casa: infatti, all'82,1% capita di salvare gli output del proprio lavoro su singoli *device.*

I numeri disegnano un quadro piuttosto confuso della modalità di lavoro in *remote* che di certo non aiuta la sicurezza, perché la commistione tra reti aziendali e reti personali, attuale costitutivo del quotidiano, è di per sé stesso una minaccia.

È una situazione che andrà progressivamente adeguata agli standard di sicurezza più alta, altrimenti gli sforzi delle aziende nel tutelare *device* e reti rischiano di essere vanificati dalla moltiplicazione di *end-point* in reti non altrettanto protette.

5. PAURA PER DATI PERSONALI E IDENTITÀ

5.1. Le minacce concrete

Alto è il timore tra gli italiani di un'appropriazione indebita dei propri dati da parte di malintenzionati informatici. Infatti, pensando alle varie attività che si svolgono sul web, l'81,7% della popolazione esprime il timore che in almeno una di queste si possa finire vittima di furti della propria identità digitale (fig. 6).

In particolare, le attività digitali che gli italiani percepiscono come più rischiose per l'integrità della privacy o per l'eventuale furto delle identità sono per (fig. 7):

- il 57,8% la navigazione sul web, con la consultazione di siti;
- il 54,6% l'utilizzo degli account social, da Facebook ad Instagram;
- il 53,7% gli acquisti di prodotti online;
- il 46,6% le operazioni di *home banking,* come effettuare bonifici, verificare il proprio conto corrente, ecc;
- il 41,5% le prenotazioni di viaggi e hotel;
- il 41% l'utilizzo di app per incontri, relazioni, come ad esempio Tinder;
- il 40,2% l'utilizzo di programmi di messaggistica istantanea, come *WhatsApp*;
- il 38,4% il pagamento online di bollettini;
- il 38,3% la partecipazione a webinar o incontri online che richiedono l'iscrizione con i propri dati,
- il 30,8% la richiesta e/o accesso a servizi digitali della pubblica amministrazione (ad esempio, tramite Spid).

Un universo ampio e variegato di attività digitali che, per una parte significativa di italiani, è esposto ai rischi di violazione della *privacy* e di indebita appropriazione dei dati personali.

Guardando alla geografia delle paure, emerge come i giovani siano più spaventati, con quote superiori al dato medio per i rischi legati agli utilizzi dei loro account social (64,3%), alle operazioni bancarie online (54,1%), all'utilizzo di app per incontri, relazioni, come ad esempio Tinder (49,6%),

mentre chi possiede una laurea teme di più quel che potrebbe accadere quando fa acquisti online (60,3%) e prenota viaggi e hotel (45,7%).

Sono paure che non possono non condizionare il quotidiano informatico di persone già alle prese con le paure più classiche del quotidiano e con un biennio dagli eventi inattesi.

Attenuare queste paure è urgente: perciò è essenziale promuovere la consapevolezza dell'importanza della *cybersecurity* come fatto sociale e settore economico, con aziende, talenti e servizi specifici senza i quali il rischio informatico potrebbe pesantemente condizionare la vita collettiva.

5.2. Le aspettative sociali sul digitale

Al digitale sono appese rilevanti speranze di ulteriore miglioramento della vita delle persone. L'esempio più eclatante riguarda la sanità, dove gli italiani sono convinti che l'uso intelligente dei dati consentirà un *upgrading* della qualità della medicina e una notevole personalizzazione di cure e assistenza.

Si consideri che oltre 7 italiani su 10 sono favorevoli a cedere i propri dati per ragioni di sperimentazione e ricerca, e che ben il 65% è favorevole alla costituzione di fascicoli sanitari elettronici in cui confluiscano sia dati rilevati in occasione di visite, accertamenti, ricoveri, sia quelli più quotidiani che possono essere generati da app e wearable.

È evidente che sono dati altamente sensibili, che definiscono dimensioni molto personali, di cui le persone sono particolarmente gelose. Eppure, è alta la propensione a renderli disponibili per ragioni sanitarie alle autorità di competenza, nella convinzione che la loro elaborazione intelligente consentirà di migliorare la sanità tramite la ricerca scientifica e di promuovere la personalizzazione di cure e dell'assistenza, che, nella fase attuale, rappresenta l'aspettativa maggiore degli italiani sul futuro della sanità.

Ebbene, questa notevole propensione a cedere dati personali si fonda sulla fiducia che i cittadini hanno nelle istituzioni sanitarie e nella loro capacità di garantire l'utilizzo dei dati nel rispetto della *privacy*.

Tuttavia, affinché fiducia e aspettative siano soddisfatte, è assolutamente indispensabile che i sistemi di protezione dei dati siano a prova di attacchi informatici, e che la *cybersecurity* sia garantita al massimo livello possibile.

Pertanto, nel caso della sanità sono evidenti le ragioni che rendono la *cybersecurity* una priorità di sicurezza nazionale, perché ogni *défaillance* su questo piano non solo produrrebbe un danno grave e tangibile per le singole persone coinvolte, i cui dati personali finirebbero sotto gli occhi di utenti da loro non autorizzati, ma anche perché darebbe un colpo micidiale alla fiducia che i cittadini hanno nelle istituzioni.

La *cybersecurity* ad altissima efficacia è visibilmente una priorità nazionale di tipo istituzionale, che riguarda anche altri ambiti di rapporto tra le persone e la Pubblica Amministrazione, tenuto conto del progressivo passaggio verso la sua digitalizzazione.

Fughe e furti di dati o altre forme di rottura della sicurezza informatica nelle istituzioni pubbliche avrebbero un inaccettabile effetto sulla *social reputation* istituzionale, minando le basi del patto sociale collettivo.

Per tale ragione, occorrono adeguati investimenti e un'agenda precisa e prioritaria per la *cybersicurezza.*

5.3. La tutela urgente

I dati analizzati mostrano che le tecniche di furti dell'identità digitale o dei dati personali, come attacchi *ransomware*, *phishing* (tramite email o messaggi sul cellulare), con comunicazioni ingannevoli per indurre le persone a cliccare su link particolari o a condividere dati sensibili, sono una minaccia rilevante. Essi generano danni alle persone e costi sociali, alimentando un clima di incertezza e sfiducia che intacca il benessere soggettivo e, anche, il pieno dispiegarsi delle potenzialità positive del web.

Come rilevato, è vitale la promozione di una più approfondita conoscenza delle varie modalità con cui la minaccia informatica si palesa, nonché la formazione all'autotutela per evitare che le persone cadano anche nelle trappole più semplici ed evidenti.

Vedere la propria identità utilizzata per fini criminali o ritrovarsi con dati e informazioni personali fuori dai contesti in cui si riteneva dovessero restare,

ha un effetto traumatico, rendendo evidente l'elevata vulnerabilità del digitale e generando una pericolosa paura che porta ad assumere condotte che riducono i vantaggi del web, senza realmente mettere le persone al riparo dei rischi.

La *cybersecurity* ha bisogno di un clima sociale di riconoscimento del suo valore sociale, che sarà tanto più condiviso quanto più sarà reso evidente alle persone che essa rappresenta la chiave che, unitamente alla responsabilizzazione individuale, consentirà di ridurre drasticamente il costo economico e sociale della nuova criminalità informatica.

6. LE SOLUZIONI NECESSARIE

6.1. Gli approcci

È indispensabile nelle singole aziende, ma anche nelle istituzioni e a livello sociale, mettere in campo culture e strumenti adeguati a rispondere in modo efficace alle *cyber minacce*.

Occorre riconoscere la strategicità del settore della *cybersecurity* e, al contempo, condividere l'idea molto pratica che ciascun attore economico e sociale deve sviluppare una propria specifica capacità di prevenzione, individuazione precoce e risposta alle minacce informatiche.

Solo così sarà possibile creare un sistema di protezione efficiente, senza improvvisi buchi in cui - grazie alla sua continua evoluzione - l'intelligenza *cyber-criminale* sarà in grado di infiltrarsi e colpire.

La *cyber-minaccia* è plurale, assume forme e intensità diversificate, rendendo inevitabile per i player dei diversi settori economici e sociali attrezzarsi per individuare non solo le principali minacce ma anche le fonti da cui provengono, costruendo un sistema di protezione che preveda sempre più il supporto di aziende esperte e l'adozione di comportamenti funzionali alla tutela.

È importante sviluppare il concetto di *cyber-protezione*, che significa l'esercizio di un ruolo attivo da parte di ciascun soggetto e non la sola attivazione da parte di professionisti di uno scudo a cui si associa la deresponsabilizzazione degli altri attori.

Inoltre, la *cybersecurity*, anzi la *cyber-protezione*, non si limita alla sola individuazione delle minacce rilevabili da *deep* e *dark web*, ma impone un percorso di accompagnamento degli attori nella gestione delle minacce e nelle modalità di prevenzione e tutela.

Occorrono progettualità specifiche, personalizzate, che facciano riferimento al meglio delle *best practice* internazionali, modulate sulle specificità di ogni singolo soggetto.

Infatti, è difficile affrontare un avversario globale come il *cybercrime* con una logica locale o solo nazionale ed è altrettanto difficile affrontare un

avversario capace di personalizzare l'attacco senza ricorrere a modalità molto specifiche, di *fine tuning* per la protezione.

Inoltre, la *cybersecurity* va considerata come un investimento sociale, al pari delle spese pubbliche o private per altri settori strategici, perché le *défaillances* sul fronte della sicurezza informatica generano tremende conseguenze socio-economiche.

6.2. La *cyber-minaccia* e la nuova geopolitica

Le recenti vicende ucraine hanno reso evidente alla *public opinion* quanto da tempo era già chiaramente visibile agli esperti: esiste la possibilità di portare attacchi informatici con effetti molto dannosi verso agenzie governative ed imprese strategiche produttive e dei servizi. Il caso citato all'origine del conflitto è quello del malware '*HermeticWiper*', in grado di distruggere i dati sui dispositivi e bloccare il funzionamento di un sistema operativo.

È l'esempio di quell'approccio distruttivo che, in scenari di competizione dura o addirittura di guerra, diventa possibile. Sono esperienze concrete che mostrano l'urgenza di infrastrutture digitali in grado di resistere ad attacchi informatici altamente dannosi.

È evidente che si tratta di attacchi subdoli, nel senso che non sono esplicitamente riconducibili ad un nemico ben identificato, che tenta con la sua azione di destabilizzare il digitale, saltando confini e distanze.

Ecco che è indispensabile una strategia globale di cooperazione tra Stati per rispondere alla sfida, garantendo tutela di dati, documenti e sistemi digitali. Per questo la *cybersecurity* deve diventare priorità dell'agenda sociopolitica, componente della cultura sociale collettiva e destinataria di congrui investimenti per sistemi di protezione informatica efficienti, reattivi, flessibili nelle risposte alle cangianti sfide.

Le drammatiche crisi globali più recenti, da quella sanitaria a quella dell'aggressione all'Ucraina, hanno indicato in energie, alimentazione e digitale i riferimenti su cui si deve fondare la reale sovranità, chiamando in causa l'azione almeno al livello dell'Unione europea.

In generale, è essenziale:

- innalzare la media delle competenze informatiche dal basso verso l'alto;
- promuovere lo sviluppo di un settore della *cybersecurity* in grado di misurarsi con le sfide criminali più avanzate.

Del resto, il settore è anche uno straordinario volano di innovazione e sviluppo per l'industria e può diventare un altro rilevante componente del buon *Made in Italy*, tanto apprezzato nel mondo.

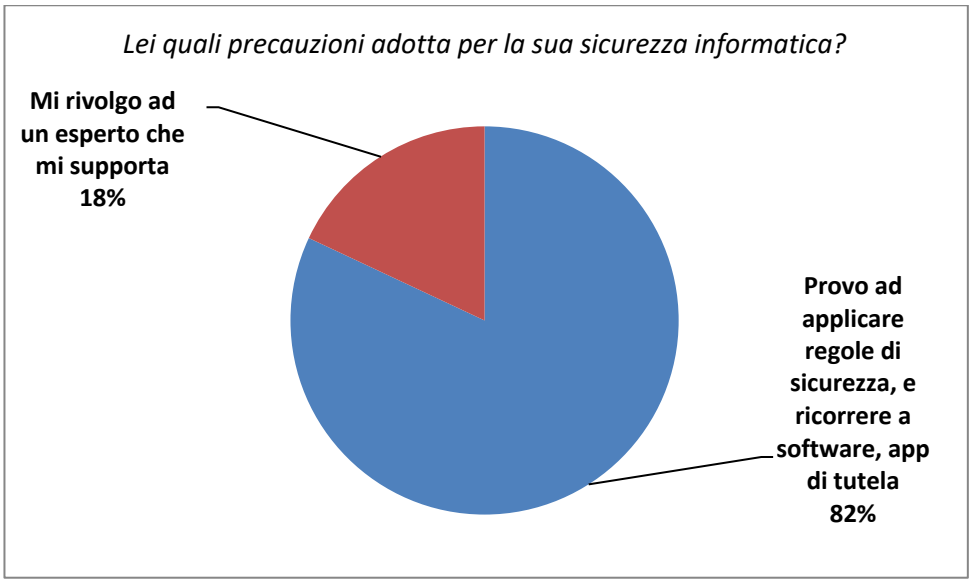
TABELLE E FIGURE

Tab. 1 – Italiani preoccupati della sicurezza informatica, per titolo di studio
(val. %)

Lei si preoccupa della sua sicurezza informatica?	Al più la licenza media	Diploma	Laurea o oltre	**Totale**
Sì, e prendo precauzioni	49,4	60,4	69,1	**61,6**
Sì, ma non faccio niente di concreto	25,2	31,0	25,0	**28,1**
No	25,4	8,6	5,9	**10,3**
Totale	**100,0**	**100,0**	**100,0**	**100,0**

Fonte: indagine Censis, 2022

Fig. 1 – Precauzioni adottate dagli italiani preoccupati della loro sicurezza informatica *(val. %)*



Fonte: indagine Censis, 2022

Tab. 2 – Italiani che dichiarano di sapere cosa si intende per *cybersecurity*, per età *(val. %)*

Lei sa cosa si intende per cybersicurezza?	18-34 anni	35-64 anni	65 anni e oltre	**Totale**
Sì, precisamente	*35,5*	*26,5*	*11,9*	***24,3***
Sì, a grandi linee	*57,6*	*63,7*	*49,8*	***58,6***
No	6,8	9,8	38,3	**17,1**
Totale	**100,0**	**100,0**	**100,0**	**100,0**

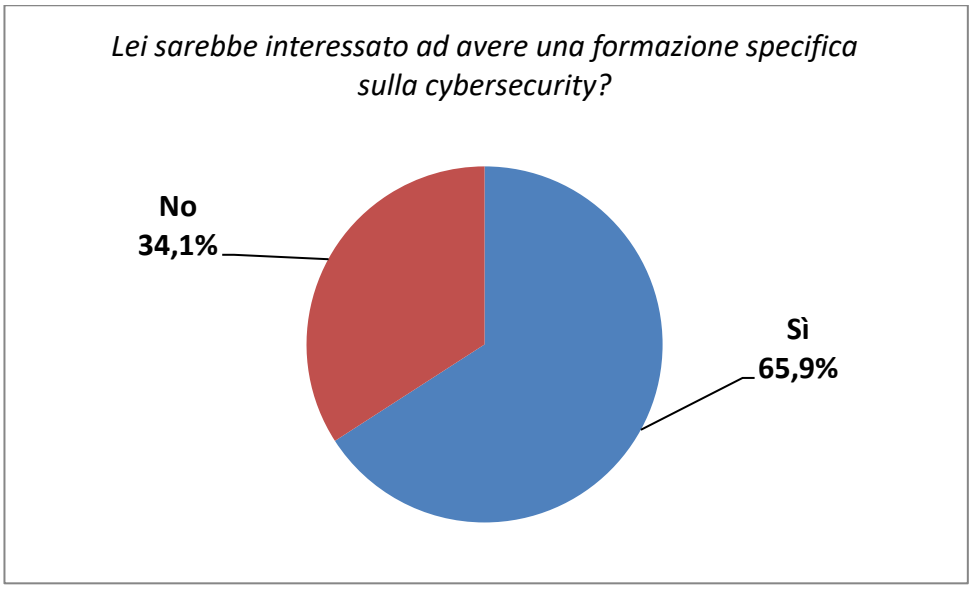
Fonte: indagine Censis, 2022

Tab. 3 – Lavoratori che hanno ricevuto una formazione specifica sulla *cybersecurity*, per ruolo svolto in azienda *(val. %)*

In azienda Lei ha avuto formazione specifica sulla cybersecurity, cioè sulle protezioni contro gli attacchi informatici?	Dirigenti	Impiegati	Operai ed esecutivi	**Totale occupati**
Sì	56,8	47,9	23,5	**39,7**
No	43,2	52,1	76,5	**60,3**
Totale	**100,0**	**100,0**	**100,0**	**100,0**

Fonte: indagine Censis, 2022

Fig. 2 – Lavoratori disponibili a partecipare ad una formazione specifica sulla *cybersecurity* *(val. %)*



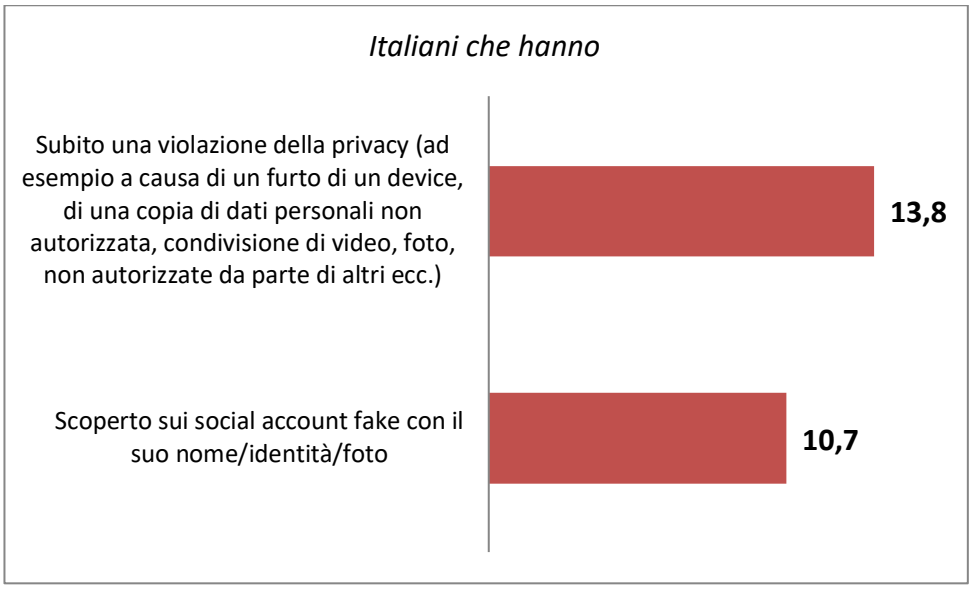
Fonte: indagine Censis, 2022

Tab. 4 – Italiani che hanno subito alcune minacce informatiche, per età *(val. %)*

Le è capitato di:	18-34 anni	35-64 anni	65 anni e più	**Totale**
Essere bersaglio di email ingannevoli per truffarla, convincerla a dare informazioni sensibili che la riguardano (ad esempio con mittente banche e/o aziende di cui lei è cliente)	75,6	74,2	38,9	**64,6**
Avere il pc/laptop infettato da un virus	53,3	52,5	24,7	**44,9**
Scoprire pagamenti di acquisti online fatti a suo nome e a suo carico	26,1	19,2	6,9	**17,2**
Vedersi clonata carta di credito e/o bancomat	18,8	16,9	6,1	**14,3**

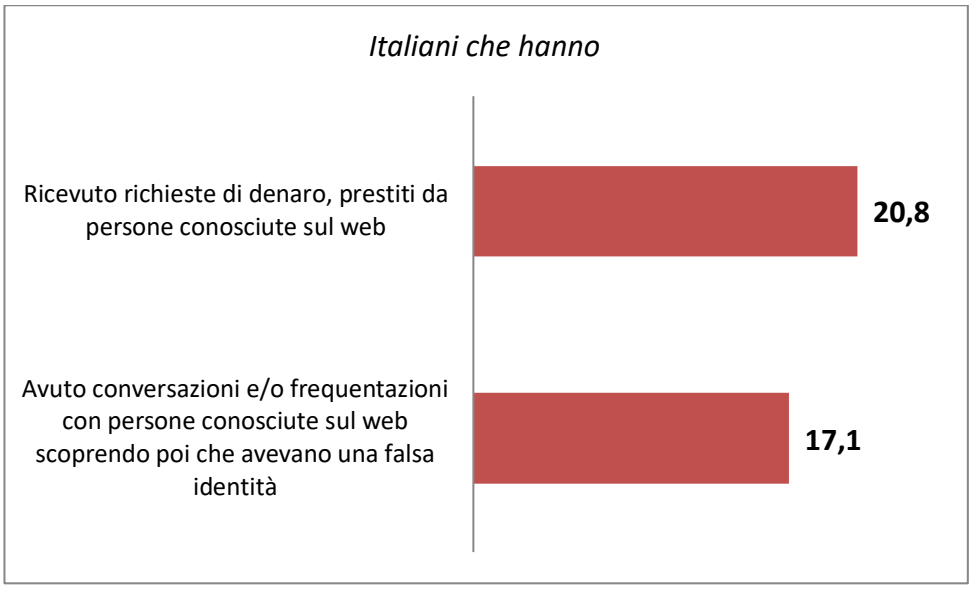
Fonte: indagine Censis, 2022

Fig. 3 – Italiani che hanno subito furti di dati e violazioni degli account social
(val. %)



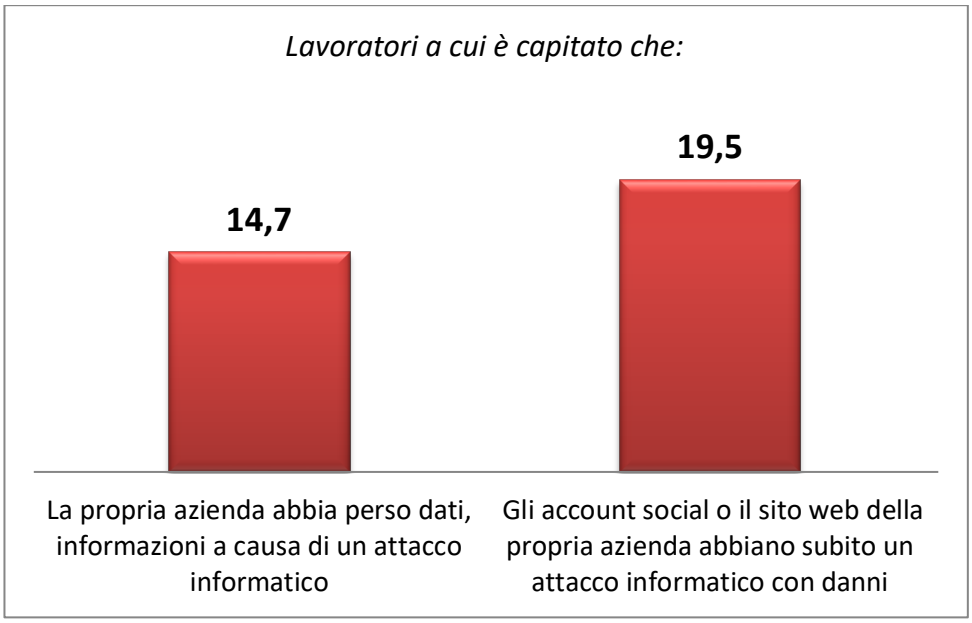
Fonte: indagine Censis, 2022

Fig. 4 – Italiani che hanno ricevuto sul web richieste di denaro e intrattenuto relazioni con persone sotto falsa identità *(val. %)*



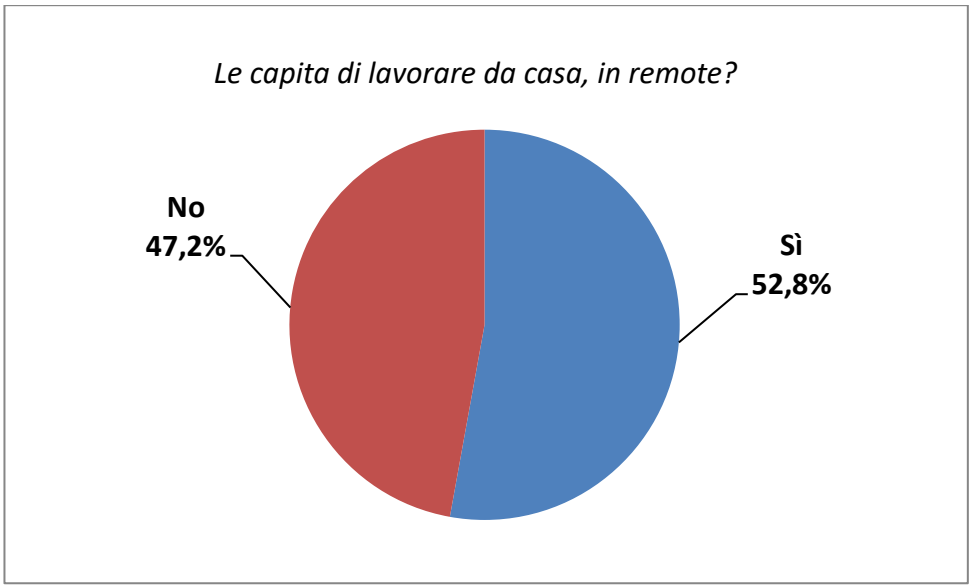
Fonte: indagine Censis, 2022

Fig. 5 - Lavoratori la cui azienda ha subito attacchi informatici *(val. %)*



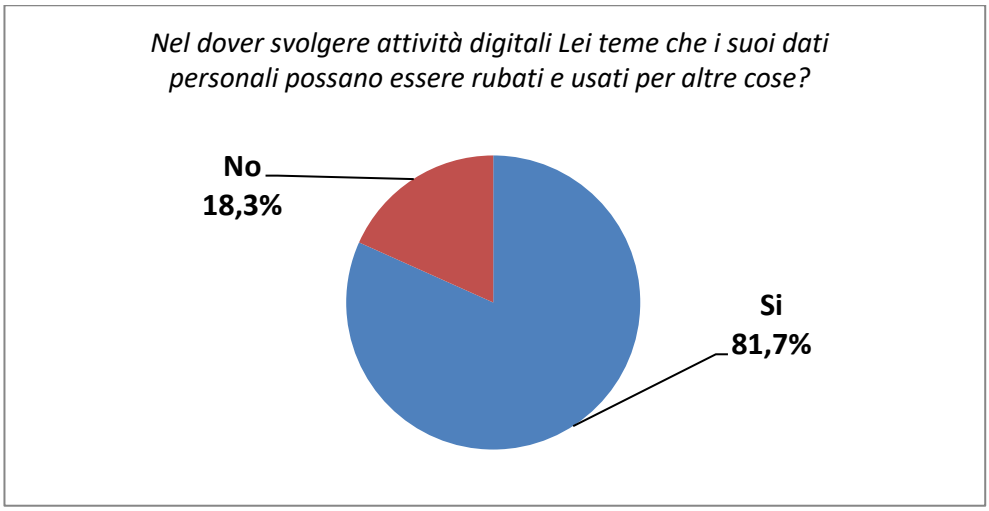
Fonte: indagine Censis, 2022

Fig. 6 – Lavoratori a cui capita di lavorare da casa, *in remote* *(val. %)*



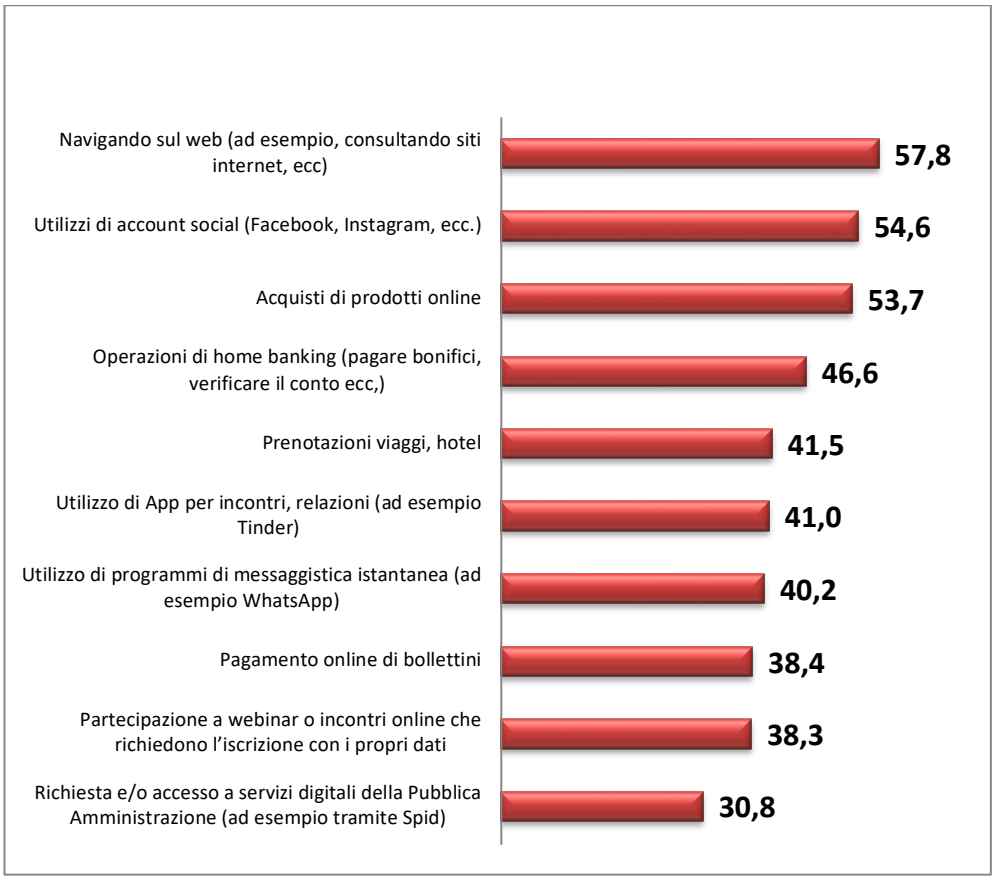
Fonte: indagine Censis, 2022

Fig. 7 – Italiani spaventati dai rischi per la sicurezza dei dati personali durante attività digitali *(val. %)*



Fonte: indagine Censis, 2022

Fig. 8 – Attività digitali in cui gli italiani ritengono più alto il rischio per la sicurezza dei propri dati personali *(val. %)*



Fonte: indagine Censis, 2022