CENSIS

IISFA
ASSOCIAZIONE ITALIANA
DIGITAL FORENSICS

2° RAPPORTO CENSIS - IISFA

IL VALORE DELLA CYBERSECURITY IN ITALIA

LA SICUREZZA INFORMATICA GARANZIA DI BENESSERE E LIBERTÀ

Roma, 19 luglio 2023

ASSOCOMUNICATORI
ASSOCIAZIONE NAZIONALE COMUNICATORI D'IMPRESA

ital communications
A STRATEGIC COMMUNICATION AGENCY

2° RAPPORTO CENSIS - IISFA

IL VALORE DELLA CYBERSECURITY IN ITALIA

LA SICUREZZA INFORMATICA GARANZIA DI BENESSERE E LIBERTÀ

Roma, 19 luglio 2023

Indice

1. LA SICUREZZA INFORMATICA GARANZIA DI BENESSERE E LIBERTÀ

Nel mondo attuale, attraversato dalla transizione digitale e dove l'essere connesso alla rete non è solamente una scelta, ma una necessità per poter contribuire ai processi di creazione del valore ed esercitare i propri diritti di cittadinanza, la dimensione della sicurezza informatica e della salvaguardia dei dati personali ha oramai assunto una sua acclarata e indiscutibile centralità.

Da tempo, infatti, l'Unione Europea ha indicato la cybersicurezza come una priorità della propria agenda digitale, declinando una strategia pluriennale al riguardo. L'Italia da parte sua, in attuazione delle riforme previste dal Piano Nazionale di Ripresa e Resilienza (PNRR), ha istituito dal 2021 l'Agenzia per la Cybersicurezza Nazionale.

Come da più parti sottolineato, la sua costituzione ha segnato l'avvio del processo di istituzionalizzazione della *cybersecurity* a livello nazionale e lo scorso anno, nell'adempimento delle sue funzioni, l'Agenzia ha provveduto a presentare la *Strategia Nazionale di Cybersicurezza 2022-2026*, volta a pianificare, coordinare e attuare misure per rendere il Paese più sicuro e resiliente.

Accanto all'istituzionalizzazione di una *cybersecurity* nazionale, è quantomai opportuna la promozione di una consapevolezza sociale sui rischi collegati all'insicurezza informatica.

Questi rischi, se non contrastati, espandono pericolosamente il perimetro della vulnerabilità sociale ed economica dell'intero "sistema Paese" ai diversi livelli e nei diversi ambiti istituzionali e produttivi, perché in un mondo sempre più interconnesso i danni causati a una parte si ripercuotono inevitabilmente sul resto con effetti a catena.

È sulla spinta di questa avvertita urgenza che il Censis, insieme a IISFA (Associazione Italiana Digital Forensics), ha inteso produrre il presente *Rapporto CENSIS-IISFA sul valore della Cybersecurity*, giunto alla sua seconda edizione. L'intento è quello di continuare la narrazione di una dimensione che, seppure in misura diversa, è divenuta ormai strutturale nell'esistenza di ogni individuo, così da coglierne i mutamenti, anche alla luce dell'intensificarsi degli attacchi offensivi di pirateria informatica contro obiettivi privati e pubblici, e da alimentare così il dibattito pubblico per il consolidamento di una *cyber resilience* nazionale.

1.1. La trama

L'incremento degli attacchi informatici, insieme con il progressivo ampliamento dello spettro del *cyber risk*, sta producendo i suoi effetti sulle condotte di vita degli italiani.

Sentiment e comportamenti ne sono influenzati: aumenta la preoccupazione rispetto all'attuale situazione di crisi, di cui l'alea digitale è elemento ricorrente; si teme per la violazione della propria privacy e per l'integrità dei propri dati personali; in alcuni casi connessioni e transazioni online sono addirittura ridotte in via precauzionale.

Ma al *cyber risk* gli italiani stanno reagendo. Per quanto il concetto di cybersicurezza debba trovare ancora un suo consolidato posizionamento nell'opinione pubblica, tra chi dichiara di conoscerne significato, con la conseguente declinazione fattuale nella società, e chi dichiara di averne una cognizione vaga o, persino, di non averne alcuna, i dati sulle quotidiane misure di sicurezza delineano un certo orientamento rispetto all'adozione di posture difensive.

All'interno del corpo sociale si stanno sviluppando, come risposta dal basso al rischio percepito, anticorpi di protezione, di cui talvolta gli individui non sembrano avere una piena consapevolezza e per questo ancora parzialmente sottotraccia. Più forte è, inoltre, la risposta tra quelli che hanno già avuto diretta esperienza di attacchi malevoli.

È quantomai opportuno, allora, mettere a valore questa reazione sociale e a partire da ciò promuovere una maggiore consapevolezza collettiva al riguardo, che includa anche quei gruppi che per condizione sociale, culturale o anagrafica, oltre a essere più a rischio di *digital divide*, rappresentano le componenti più deboli di tutto l'ecosistema digitale.

1.2. I risultati in pillole

Cresce il *cybercrime*. Nel 2022 gli attacchi informatici a infrastrutture sono più che raddoppiati rispetto all'anno precedente: 138%. Tra il 2012 e il 2021, nell'arco di quasi dieci anni anche i reati informatici denunciati all'Autorità giudiziaria dalle Forze di Polizia sono raddoppiati (+155,2%) in controtendenza con l'andamento totale dei reati (-25,4%). Sono Milano e Roma a guidare la classifica delle prime 10 Province

per numero di reati informatici denunciati (rispettivamente 24.077 e 21.637). È, però, Torino a primeggiare per numero di reati in rapporto alla popolazione con 7,8 reati ogni mille abitanti. Sempre nel 2022, le attività cibernetiche ostili condotte contro assetti informatici rilevanti per la sicurezza nazionale hanno interessato nel 56% dei casi infrastrutture informatiche di soggetti privati (+32% rispetto al 2021) e per il 43% obiettivi pubblici (-26% rispetto al 2021). Tra gli attori ostili prevalgono i gruppi criminali (47%, +33% rispetto al 2021), seguiti da attori statuali o sponsorizzati da Stati (26%, +3%) e, a distanza, dagli *hacktivisti* (8%, -15%).

Digital mismatch. Se in media nel 2022 il 40% delle imprese ha dichiarato di avere difficoltà nella ricerca di lavoratori, nel caso dell'ICT (Information and Communications Technology) tale quota sale al 52%. Accanto al *software developer* o al *data engineer*, il *cybersecurity specialist* è indicato tra le figure emergenti più legate alla transizione digitale nelle previsioni di fabbisogni occupazionali e professionali a medio termine (2023-2027) per il settore dell'informatica e delle telecomunicazioni. Si amplia anche l'offerta universitaria: le lauree specifiche sul tema della *cybersecurity* a gennaio 2022 erano 13, un anno dopo sono 26, mentre sono 234 i corsi universitari in cui è presente l'insegnamento della *cybersecurity*. A giugno 2022, degli 837 corsi erogati dall'Istruzione Tecnica Superiore, quelli dell'area tecnologica denominata Tecnologie dell'Informazione e della Comunicazione erano il 14% del totale e degli oltre 21.300 allievi, quelli aspiranti al titolo di tecnico superiore in campo ICT erano il 14,1%. Dei 13 ITS Academy censiti lo scorso anno e operanti nell'area ICT, 8 hanno almeno un corso sulla *cybersecurity* nella loro offerta formativa.

Cronaca di minacce informatiche quotidiane. Nel corso dell'ultimo anno al 76,9% degli italiani è capitato di imbattersi almeno in una minaccia informatica, quota che raggiunge l'87,3% tra i 18-34enni. Il 63,3%, inoltre, è stato coinvolto in un numero di episodi compreso tra 1 e 3, mentre il 10,4% tra 4 e 6. *Smishing* e *phishing* sono di gran lunga le tecniche prevalentemente introdotte dai *cyber threat actor.* Il 60,9% del totale ha ricevuto un sms o un messaggio su WhatsApp con invito a cliccare su un link sospetto, con valori che arrivano al 70,7% tra i 18-34enni, mentre il 56% è stato bersaglio di e-mail ingannevoli che chiedevano informazioni sensibili, con mittente banche e/o aziende di cui sono clienti (67,2% dei 18-34enni). La richiesta di denaro o di prestiti da persone conosciute sul web è un inconveniente denunciato dal 15,9% degli intervistati e dal 19,7% dei 18-34enni. Una quota pressoché equivalente di individui (15,7%) ha poi avuto il proprio Pc/laptop infettato da un virus. Altre

fattispecie meno ricorrenti, ma non per questo meno pericolose, riguardano i pagamenti online, la violazione della privacy e l'attacco alla sfera emotiva delle potenziali vittime.

L'impatto emotivo del *cyber risk*. Il *cyber risk* ha un impatto sociale pervasivo, che arriva a colpire lo spazio vitale di ogni singolo individuo. Il numero crescente di attacchi informatici a enti e istituzioni dei mesi passati ha condizionato la sfera emotiva e i comportamenti degli italiani. Per il 62,9% di loro sono stati fonte di ulteriore preoccupazione rispetto all'attuale situazione di crisi; un'apprensione aggiuntiva che è maggiore tra le donne (64,4%) rispetto agli uomini (61,4%) e tra i più giovani (67,9% dei 18-34nni). I maggiori attacchi informatici, nel 53,2% della popolazione, hanno ingenerato la paura che i propri dati possano essere rubati e usati per altri scopi, quando ci si collega a Internet per svolgere attività online. Infine, per circa un quarto della stessa popolazione (24,4%), tale paura si traduce, in conseguenza della riduzione dei collegamenti alla Rete in un'autolimitazione precauzionale della propria esistenza digitale (30,8% dei 18-34enni).

Resta fluttuante la conoscenza della *cybersecurity*. Il 28,8% degli italiani dichiara di sapere precisamente cosa si intende per cybersicurezza, una quota cresciuta di 4,5 punti percentuali in confronto al 2022 (quando erano il 24,3%). Più esperti sull'argomento sono gli uomini (35,4%), i laureati (40,5%) e i lavoratori autonomi (45,5%). Diminuiscono coloro i quali affermano di averne una conoscenza a grandi linee: dal 58,6% passano a quota 50,4% (-8,2% punti percentuali rispetto al 2022). Non diminuiscono, anzi crescono in numero, i cittadini che dichiarano, infine, di non conoscere il significato del termine, che dal 17,1% del 2022 salgono al 20,8% del 2023. Più ignari sono gli individui meno scolarizzati (53,9% con al massimo la licenza media) e i più anziani (51,8% con 65 anni e oltre).

Pratiche di sicurezza più ricorrenti. Oltre 7 italiani su dieci utilizzano una password per il wi-fi di casa (75,2%); il 71,5% fa uso di password diverse in funzione dei servizi utilizzati (posta elettronica, home banking, profili social, piattaforme di intrattenimento, ecc.); il 70,8% consente l'aggiornamento periodico del sistema operativo e dei software di produttività del Pc di casa e il 74,6% per il Pc di lavoro; il 70,3% ha un antivirus installato e aggiornato sul Pc di casa e il 75% sul Pc di lavoro. I sistemi di autenticazione più complessi della password (autenticazione biometrica oppure OTP via sms) sono, invece, utilizzati dal 54%. Il backup dei propri file è, invece, una pratica che accomuna il 59,5% degli italiani e che avviene: per il 50,9% dei casi su dispositivi esterni per il 38,9% su cloud e per il 23% in locale. Per la salvaguardia del proprio

cellulare, invece, il 77,1% consente gli aggiornamenti periodici del software di sistema, con valori che arrivano all'82,8% tra i laureati e all'84,5% tra i 18-34enni, mentre il 62,6% utilizza per accedere al proprio cellulare oltre alla password altri fattori (PIN, OTP, impronta digitale o riconoscimento facciale). A fronte del 58,8%, che si dichiara preoccupato della sicurezza dei propri dispositivi informatici e che prende anche delle precauzioni e del 27,1% che, nonostante sia preoccupato e affermi di non fare niente di concreto, i dati nel complesso sembrano evidenziare una realtà che va oltre la percezione che gli italiani hanno delle loro condotte in materia di prevenzione e tutela dal rischio. Su cinque misure di sicurezza con un maggiore gradiente di intenzionalità (regolare esecuzione del backup dei file, password diverse in funzione dei servizi utilizzati, sistemi di autenticazione più complessi della password, password per il wi-fi di casa, installazione e aggiornamento di un antivirus su Pc di casa e cellulare), quasi sei italiani su dieci (il 57,3%) ne adottano tra quattro e cinque, il 32,4% ne adotta cinque.

Comparto aziende. Nel corso dell'ultimo anno il 20,6% degli occupati è stato testimone di almeno 1 problema informatico sul proprio luogo di lavoro e più nello specifico: il 12,8% ha sperimentato un sabotaggio e una sospensione dei servizi aziendali, l'11,7% un attacco informatico agli account social e al sito aziendale con danni conseguenti, il 10,3% una perdita di dati e informazioni a causa di un attacco informatico, infine il 9,1% un furto d'identità e di dati sensibili. Nel 2022 le imprese italiane con 10 e più addetti che hanno avuto un problema di sicurezza ICT sono state il 15,7%, (circa 30.000 unità in valore assoluto). Allo stesso tempo, il 55,4% degli stessi occupati è stato o sarà formato per contrastare o prevenire eventuali attacchi informatici di cui il 27,3% nell'ultimo anno e il 14,6% nei prossimi mesi e il 13,5 oltre un anno fa. A giugno 2022, le imprese antihacker hanno raggiunto la quota di 3.147, registrando un incremento del 5,4% rispetto al mese di settembre dell'anno precedente.

2. LO SCENARIO

2.1. La crescita del *cybercrime*

L'insicurezza informatica può essere considerata a ragione un fattore aggravante dell'attuale condizione di crisi permanente, propria dei tempi che viviamo e caratterizzata dal susseguirsi e sovrapporsi di situazioni d'emergenza. Sono gli eventi stessi che ce lo dicono.

Nel 2022 gli attacchi informatici a infrastrutture critiche, secondo quanto certificato dalle attività di *cyber investigation* della Polizia Postale e delle Telecomunicazioni, sono più che raddoppiati rispetto all'anno precedente (sono stati 12.947 a fronte dei 5.334 nel 2021), incrementandosi del 138%.

Tra il 2012 e il 2021, i reati informatici denunciati all'Autorità giudiziaria dalle Forze di Polizia sono più che raddoppiati, registrando un aumento del 155,2%, in controtendenza con l'andamento decrescente del totale dei reati, che nello stesso periodo di tempo si sono ridotti del 25,4% (**tab.1**).

Sono Milano e Roma a guidare la classifica delle prime 10 Province per numero di reati informatici denunciati (rispettivamente 24.077 e 21.637). È però Torino a primeggiare per numero di reati in rapporto alla popolazione, con 7,8 reati ogni mille abitanti (a fronte di un valore medio nazionale di 5,4 reati informatici ogni mille abitanti), seguita da Milano (7,5), Brescia e Venezia (6,6 in entrambi i casi). Roma, invece, con 5,1 si posiziona dopo Napoli (5,4) e Palermo (5,2) (**tab. 2**)

Le imprese con 10 o più addetti che nel 2022 hanno avuto almeno un problema di sicurezza informatica, con temporanea indisponibilità dei servizi ICT, distruzione o danneggiamento dei dati o divulgazione di dati riservati sono state il 15,7% – quota che sale al 33,1% nel caso di imprese con 250 addetti e più – a fronte del 10,1% nel 2019 (+5,6 punti percentuali). Indisponibilità dei servizi ICT (14,4%) e guasti hardware o software (13%) sono stati i principali problemi riscontrati (**tab. 3**).

La moltiplicazione di azioni criminali a istituzioni, aziende e privati è anche un riflesso dell'attuale scenario di guerra, dove all'azione del *cybercrime* ordinario si sommano attacchi, conseguenti alla messa a terra di strumenti cyber-offensivi da parte di hacker criminali, che fanno della guerra cibernetica una componente del più ampio conflitto tra i due schieramenti geopolitici contrapposti.

Con riferimento alle attività cibernetiche ostili condotte nel 2022 verso assetti informatici rilevanti per la sicurezza nazionale, la *Relazione sulla politica dell'informazione per la sicurezza* – redatta da AISE e AISI, le due agenzie su cui si fonda il sistema di intelligence nazionale – riporta che le azioni di pirateria informatica hanno interessato nel 56% dei casi infrastrutture informatiche di soggetti privati (+32% rispetto al 2021) e sono state prevalentemente orientate verso i settori delle infrastrutture digitali/servizi IT (22%, +16%), dei trasporti (18%, stabile) e bancario (12%, +6%).

Il rimanente 43% delle azioni offensive identificate è stato perpetrato, invece, a danno di obiettivi pubblici (-26% rispetto al 2021), nello specifico amministrazioni centrali dello Stato (62%, +6%) e infrastrutture IT di strutture sanitarie (11%, +1%), Enti locali e Istituti e Agenzie nazionali (9% in entrambi i casi, rispettivamente +1% e +7%).

Tra gli attori ostili prevalgono i gruppi criminali (47%, +33% rispetto al 2021), seguiti da attori statuali o sponsorizzati da Stati (26%, +3%) e, a distanza, dagli *hacktivisti* (8%, -15%) (**fig. 1**).

È, dunque, obbligatorio introdurre strategie articolate a difesa e protezione dagli attacchi a ogni livello: da quello di entità complesse a quello aziendale, fino a quello privato.

2.2. Il valore della *cybersecurity*

Nel 2022 il mercato della *cybersecurity* – secondo le stime *dell'Osservatorio Cybersecurity & Data Protection* del Politecnico di Milano – ha raggiunto il valore di 1,86 miliardi di risorse investite, con un incremento del 18% rispetto all'anno precedente. Il 61% delle imprese sopra i 250 addetti ha aumentato la propria quota di risorse da destinare alla sicurezza informatica.

Forte è dunque la consapevolezza di proteggersi dai crimini informatici, da cui possono derivare non solo costi diretti, ma anche costi indiretti difficili da monetizzare per le diseconomie determinate dall'alterazione del normale processo produttivo e la conseguente perdita di opportunità.

Nonostante la *cybersecurity* stia divenendo una priorità di investimento nel digitale per grandi e piccole e medie imprese, tuttavia nel 2022 il rapporto tra spesa in *cybersecurity* e Pil, seppure in crescita, si attesta allo 0,1%,

collocando il nostro Paese all'ultimo posto tra quelli del G7 (guidano la classifica Stati Uniti e Regno Unito con un rapporto dello 0,31%).

Del resto, non dobbiamo dimenticare che il tessuto produttivo dell'Italia è prevalentemente costituito da piccole e medie imprese interconnesse che, come accade per i processi di innovazione e di transizione digitale, devono essere incentivate e supportate anche nell'avvio di policy interne di sicurezza informatica.

Segnali di crescita si registrano anche sul fronte delle imprese antihacker che – secondo un'analisi di Unioncamere-InfoCamere – a giugno 2022 hanno superato quota 3.147, registrando un incremento del 5,4% rispetto a settembre dell'anno precedente. Di queste, oltre il 50% risulta dislocato in tre Regioni: Lazio, Lombardia e Campania con, rispettivamente, il 22,5%, il 18,5% e il 10,5% delle imprese (**tab. 4**).

2.3. Investire per una cultura *cyber hygiene*

L'alfabetizzazione digitale della popolazione, resa necessaria da un contesto in continua evoluzione, dove l'esercizio attivo della cittadinanza richiede che ogni individuo possieda assieme alle competenze di base anche abilità digitali, non può essere disgiunta da un'educazione alla cybersicurezza, così da garantire un uso responsabile e sicuro delle tecnologie e della rete.

È in particolare tra i nativi digitali, naturalmente inclini all'uso delle tecnologie, ma non altrettanto pronti a ponderare i rischi a esse sottese che è quanto mai opportuno lo sviluppo di una cultura digitale, che faccia proprio quell'insieme di buone pratiche quotidiane, finalizzate a minimizzare i rischi di un uso poco accorto dei dispositivi, e riassumibili nel concetto oramai noto di igiene informatica o *cyber hygiene*.

Se alfabetizzazione digitale e igiene informatica rimandano a interventi formativi che già nelle aule di scuola devono trovare il loro ambito di realizzazione, sotto il profilo della qualificazione del capitale umano disponibile e della progressiva riduzione del *digital mismatch* tra domanda e offerta di lavoratori nel campo digitale e ICT e della sicurezza informatica, in particolare, non può passare sotto silenzio lo sforzo fatto dal sistema universitario per ampliare il numero di corsi in cui l'insegnamento della *cybersecurity* è contemplato.

A tal proposito, vale la pena ricordare che, secondo l'indagine Excelsior 2022, se in media il 40% delle imprese dichiara di avere difficoltà nella ricerca di lavoratori, nel caso dell'ICT tale quota sale al 52%.

Inoltre, tra le figure emergenti più legate alla transizione digitale, le previsioni di fabbisogni occupazionali e professionali a medio termine (2023-2027) per il settore dell'informatica e delle telecomunicazioni indicano *il cyber security specialist*, insieme al *software developer* o del *data engineer*.

A gennaio 2023, sulla base di un censimento I-Com[1], l'insegnamento della *cybesecurity* era presente in 234 corsi universitari, di cui 51 specialistici e divisi tra corsi di laurea, corsi di laurea magistrale, master e dottorati. Le lauree specifiche sul tema della *cybersecurity* che a gennaio 2022 erano 13, un anno dopo sono arrivate a quota 26, di cui 4 lauree triennali e 22 lauree magistrali. Un'offerta formativa concentrata soprattutto nel Lazio (45 corsi) e in Piemonte (32 corsi), seguiti da Campania e Lombardia.

Ancora limitato, ma in fase di espansione è, invece, il contributo dell'Istruzione Tecnica Superiore, recentemente riformata con la legge n. 99/2022 e che, come sancito anche dal PNRR, rappresenta oggi un segmento strategico della formazione terziaria nel nostro Paese, destinato ad affiancare in un regime di complementarità l'offerta universitaria.

A giugno 2022, degli 837 corsi erogati, quelli dell'area tecnologica denominata Tecnologie dell'Informazione e della Comunicazione erano il 14% del totale, mentre degli oltre 21.300 allievi, quelli aspiranti al titolo di tecnico superiore in campo ICT erano il 14,1%.

Infine, dei 13 ITS Academy censiti lo scorso anno e operanti nella già menzionata area tecnologica, di questi, al momento della stesura del presente Rapporto, 8 pubblicizzavano all'interno della loro offerta formativa almeno un corso, attivo o in fase di attivazione, sulla *cybersecurity*.

[1] L'ecosistema italiano della sicurezza informatica tra regolazione, competitività e consapevolezza, rapporto Osservatorio sulla cybersicurezza, I-Com, febbraio 2023.

3. GUAI DIGITALI

3.1. L'incidenza delle minacce informatiche nella vita degli italiani

Nel corso dell'ultimo anno al 76,9% degli italiani è capitato di imbattersi almeno in una minaccia informatica, quota che raggiunge l'87,3% tra i 18-34enni. Il 63,3%, inoltre, è stato coinvolto in un numero di episodi compreso tra 1 e 3, mentre il 10,4% tra 4 e 6 (**fig.2**).

Il 68,3% dei più giovani è stato destinatario da 1 a 3 minacce, a riprova del fatto che alla naturale inclinazione all'uso delle tecnologie delle nuove generazioni non sempre corrisponda una pari ponderazione dei relativi rischi.

Sebbene il possesso di competenze digitali generali e specialistiche è, come avremo modo di vedere anche nel prosieguo del presente Rapporto, funzione del livello di scolarizzazione e nonostante esista una correlazione positiva tra quest'ultimo e l'adozione di prassi di igiene informatica, tuttavia non risulta essere un antidoto assoluto contro il *cyber risk*, giacché – a fronte di un valore medio generale di 76,9% – l'83,5% dei laureati è stato coinvolto nell'ultimo anno in almeno un episodio di minaccia informatica.

È quest'ultima un'esperienza che lascia il segno e può influire sensibilmente sui comportamenti individuali. Se il 58,8% degli italiani è preoccupato della sicurezza dei propri dispositivi informatici e prende precauzioni, ancor di più chi è stato vittima di una minaccia informatica che lo è nel 64,1% dei casi.

3.2. Soprattutto *smishing* e *phishing*…

Smishing e *phishing* sono di gran lunga le tecniche messe in campo dai *cyber threat actor* per ingannare le potenziali vittime e convincerle a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi perlopiù un ente affidabile o conosciuto in una comunicazione digitale.

Ce lo confermano gli italiani che nel corso dell'ultimo anno dichiarano:

- nel 60,9% dei casi di aver ricevuto un sms o un messaggio su WhatsApp con invito a cliccare su un link sospetto, con valori che arrivano al 70,7% tra i 18-34enni;
- nel 56% dei casi di essere stato bersaglio di e-mail ingannevoli che chiedevano il rilascio di informazioni sensibili, avendo come mittente banche e/o aziende di cui sono clienti, esperienza anche questa ricorrente in misura maggiore tra le coorti più giovani della popolazione (67,2% dei 18-34enni).

Si tratta di un tipo di minaccia da cui nessun utente della rete può ritenersi immune. Gli attacchi di *phishing* nelle loro diverse declinazioni possono, infatti, avere una vasta gamma di obiettivi, configurandosi sia come una truffa generica, sia come un attacco più sofisticato, mirato su un obiettivo specifico e, di conseguenza, più difficilmente smascherabile dalla vittima prescelta.

3.3. …ma non solo

L'estorsione o il tentativo di estorsione di dati sensibili, sebbene di gran lunga prevalente, non esaurisce il campionario delle minacce alla sicurezza digitale degli italiani occorse nell'ultimo anno.

La richiesta di denaro o di prestiti da persone conosciute sul web è un inconveniente denunciato dal 15,9 % degli intervistati e da quasi il 20% dei più giovani (19,7% dei 18-34enni).

Una quota pressoché equivalente di individui (15,7%) ha poi avuto il proprio Pc/laptop infettato da un virus.

In questo caso sono più gli uomini (19%) delle donne (12%) a essere incappati in un simile inconveniente, mentre i più giovani, nativi digitali e più assidui utilizzatori delle tecnologie, si confermano ancora una volta come il principale gruppo bersaglio di minacce informatiche, con il 22,4% di 18-34enni il cui Pc è stato attaccato da un virus.

Completano la gamma dei possibili attacchi informatici altre fattispecie meno ricorrenti, ma non per questo meno insidiose e pericolose, che riguardano

tre diverse tipologie di rischio: i pagamenti online, la violazione della privacy e l'attacco alla sfera emotiva delle potenziali vittime.

In quest'ultimo caso si tratta di una minaccia subdola, attraverso la quale il *cyber threat actor* fa leva sulla vulnerabilità psicologica del malcapitato per carpirne la fiducia, soprattutto a scopo estorsivo.

Ciò detto, sulla base delle testimonianze raccolte risulta dunque che:

- l'8,9% degli italiani nell'ultimo anno è stato truffato, facendo acquisti online su siti web fraudolenti o all'interno di piattaforme con annunci legittimi (per esempio Facebook, eBay, Instagram) e che il 6,6% ha scoperto pagamenti di acquisti online fatti a suo nome e con la sua carta, o si è visto, in ultimo, clonare la propria carta;
- l'8,5% ha scoperto sui social account *fake* con il suo nome, la sua identità o sue foto e che l'8,2% ha subito una violazione della privacy in conseguenza del furto di un device o di una copia di dati personali non autorizzati o di una condivisione di un video, ecc.;
- infine, l'8,8% ha avuto conversazioni e/o frequentazioni con persone conosciute sul web, scoprendo poi che avevano una falsa identità (**tab. 5**).

4.LA CYBERSECURITY NEL QUOTIDIANO

4.1. Il peso del *cyber risk* nella vita di tutti i giorni

La comunità internazionale, Italia compresa, da diversi anni a questa parte vive una situazione di *permacrisi*, ovvero di crisi permanente, dove si susseguono e si sovrappongono situazioni d'emergenza: dalla pandemia ai cambiamenti climatici, alla guerra con minaccia nucleare, a una strisciante e mai sopita crisi economica, aggravata, in ultimo, da rischio di razionamento energetico, bollette alle stelle e inflazione.

Ulteriore fattore di aggravamento di uno scenario, che ha oramai cronicizzato al suo interno la variabile crisi, è il *cyber risk* quale nuova frontiera delle sfide della globalizzazione dei processi economici e culturali.

Il *cyber risk,* in conseguenza della naturalizzazione della tecnologia dovuta alla compenetrazione del digitale nelle nostre pratiche quotidiane lavorative e private, ha un impatto pervasivo, che va oltre gli attacchi gravi di dominio pubblico, fino a colpire lo spazio vitale di ogni singolo individuo.

Ne sono ben consapevoli gli italiani, per i quali il numero crescente di attacchi informatici a enti ed istituzioni verificatosi nei mesi passati ha lasciato traccia nei loro vissuti, condizionandone sfera emotiva e comportamenti.

Per il 62,9% di loro i suddetti attacchi sono stati fonte di ulteriore preoccupazione rispetto all'attuale situazione di crisi; un'apprensione aggiuntiva che è maggiore tra le donne (64,4%) rispetto agli uomini (61,4%) e tra i più giovani: il 67,9% dei 18-34nni si dichiara più inquieto a causa del numero crescente di attacchi informatici, mentre la corrispondente quota di chi ha 65 anni e oltre si ferma al 54,2%.

Infine, è tra i lavoratori autonomi (professionisti, lavoratori in proprio e imprenditori) che l'apprensione è maggiore. Il 74,3% di loro vedono nel *cyber risk* un ulteriore elemento critico che si aggiunge al contesto entro il quale esercitano la loro attività economica.

La consapevolezza di un potenziale ampliamento, in conseguenza delle azioni lesive di *criminal hacking,* delle possibili vulnerabilità sociali non

genera solo ansia, ma anche timore che la propria *privacy* sia violata con i risvolti materiali e immateriali che ne conseguono.

Il 53,2% degli italiani, per effetto del numero crescente di attacchi informatici, dichiara di aver paura che i suoi dati siano rubati e usati per altri scopi quando si collega a Internet per svolgere attività online – dagli acquisti, alle prenotazioni, alle operazioni in banca solo per citare le tipologie più ricorrenti – che oramai fanno parte della routine quotidiana di ognuno di noi.

Una paura che per circa un quarto della popolazione (24,4%) si traduce addirittura in una riduzione dei collegamenti a Internet per attività online, ovvero in un'autolimitazione precauzionale della propria esistenza digitale.

Se la paura è quel sentimento primitivo che aiuta ogni individuo ad anticipare un pericolo, possiamo allora affermare che sono i più giovani ad avere una percezione maggiore del *cyber risk* come di un pericolo immanente dei tempi che viviamo, ovvero quelle popolate dai nativi digitali, più avvezzi all'uso della tecnologia e dei social media, che in modo significativo incidono anche sul loro processo di socializzazione.

Il 66,3% dei 18-34enni teme, infatti, per l'incolumità dei propri dati personali e il 30,8% dichiara di collegarsi meno a Internet per compiere transazioni o beneficiare di servizi online, collocandosi in entrambi i casi sensibilmente al di sopra dei corrispondenti valori medi generali (53,2% e 24,4%, rispettivamente) (**tab. 6**).

4.2. La consapevolezza come arma di difesa

In parte per la narrazione che ne fanno i mass media, in parte per esperienza personale in seguito alle spiacevoli conseguenze di un'azione ostile di *criminal hacking*, i dati appena illustrati ci confermano che il *cyber risk* è oramai entrato a far parte della vita degli italiani, influenzandone stato d'animo e pratiche quotidiane.

Non altrettanto può essere detto della consapevolezza sociale sulla cybersicurezza, che, invece, può costituire un fondamentale antidoto culturale per arginare e contrastare l'impatto di attacchi ostili e attività criminose pervasivamente veicolati attraverso la rete.

È dal grado di cognizione che si ha di un fenomeno che si possono originare le adeguate condotte e prevenire gli errori, che ci possono trasformare nei bersagli di possibili reati cibernetici.

Per questa ragione abbiamo ritenuto opportuno verificare, ancora quest'anno, il grado di conoscenza degli italiani del termine cybersicurezza. Le risposte fornite al riguardo dagli intervistati sono sintomatiche della necessità di opportune campagne di informazione/formazione sulla popolazione e di azioni finalizzate a ridurre progressivamente la divaricazione e il divario sociale a essa riconducibile tra chi è pienamente consapevole e chi non lo è.

Analizziamo i dati nel dettaglio. Il 28,8% degli italiani dichiara di sapere precisamente cosa si intende per cybersicurezza, una quota cresciuta di 4,5 punti percentuali in confronto al 2022 (quando erano il 24,3%).

Più esperti sull'argomento sono gli uomini (35,4%), i laureati (40,5%) e i lavoratori autonomi (45,5%), seguiti dagli imprenditori (40,8%). Diminuiscono coloro i quali affermano di averne una conoscenza a grandi linee, che dal 58,4% passano a quota 50,6% (-8,2% punti percentuali rispetto al 2022).

Non diminuiscono, anzi crescono in numero, i cittadini che dichiarano, infine, di non conoscere il significato del termine, che dal 17,1% del 2022 salgono al 20,8% del 2023. Più ignari riguardo al tema risultano essere gli individui meno scolarizzati (53,9% con al massimo la licenza media) e i più anziani (51,8% con 65 anni e oltre) (**tab. 7**).

I dati sopra illustrati si mantengono su ordini di valore in linea con quelli dell'anno precedente e sono indicatori di una situazione ancora fluttuante, dove sotto il profilo semantico il termine cybersicurezza è dato per acquisito da una parte minoritaria della popolazione, avendo la maggioranza una conoscenza approssimativa del significato. Anziché ridursi, si incrementa, invece, la parte degli italiani che dichiara di ignorare l'accezione del termine stesso.

Se da un lato sono le competenze e i comportamenti dei singoli che fanno la differenza nel contrasto al *criminal hacking*; dall'altro, come già accennato, il grado di conoscenza terminologica del fenomeno oggetto di analisi ci dà la direzione del percorso da intraprendere per la costruzione di barriere

culturali contro il rischio informatico, che trovano il loro fondamento nella tutela personale.

4.3. Pratiche quotidiane di sicurezza

Sebbene il concetto di cybersicurezza debba ancora trovare una sua definitiva collocazione nella molteplicità dei nuovi fenomeni che popolano la società contemporanea, tuttavia, dai dati raccolti si ricavano evidenze di una certa abitudinarietà da parte degli italiani ad attuare pratiche di sicurezza informatica a tutela dei loro dispositivi informatici e a protezione di dati e informazioni personali che nell'attuale era digitale sono destinati per la gran parte a transitare in rete.

L'85,9% degli italiani, dichiara, infatti, di preoccuparsi della sicurezza dei propri dispositivi informatici e di questi il 58,8% prende anche delle precauzioni, a fronte del 27,1% che, nonostante sia preoccupato, afferma di non fare niente di concreto (**fig. 3**).

Scendendo nel dettaglio di quelle che sono le possibili misure di sicurezza che ogni utilizzatore informatico dovrebbe attuare, si osserva che oltre 7 italiani su dieci:

- utilizzano una password per il wi-fi di casa (75,2%);
- fanno uso di password diverse in funzione dei servizi utilizzati (posta elettronica, home banking, profili social, piattaforme di intrattenimento, ecc.) (71,5%);
- consentono l'aggiornamento periodico del sistema operativo e dei software di produttività del Pc di casa (70,8% e 74,6% per il Pc di lavoro);
- hanno un antivirus installato e aggiornato sul Pc di casa (70,3% e 75% sul Pc di lavoro).

Il backup dei propri file è, invece, una misura di sicurezza che accomuna il 59,5% degli italiani, realizzata per il 50,9% dei casi su dispositivi esterni per il 38,9% su cloud e, infine, per il 23% in locale (**fig.4**).

L'impiego di una password complessa (con almeno 12 caratteri alfanumerici e speciali) è praticato dal 56,8% degli italiani sul Pc di casa e dal 64,5% sul Pc di lavoro. I sistemi di autenticazione più complessi della password

(autenticazione biometrica oppure OTP via sms) sono, invece, utilizzati dal 54%, un impiego individuale incrementato anche dal ricorso da parte degli istituti di credito a questo tipo di procedure per le transazioni bancarie personali.

Il firewall, infine, come dispositivo di sicurezza della rete, è presente sul Pc domestico e di lavoro, rispettivamente, del 46,2% e del 59,6% degli italiani (**tab. 8**).

La maggiore o minore applicazione delle misure di sicurezza informatiche sopra illustrate è sensibilmente influenzata da due variabili strutturali: scolarizzazione ed età anagrafica. Il ricorso a tali misure è sempre maggiore tra i laureati e minore tra chi ha un basso titolo di studio, mentre è la coorte di individui con 65 anni e oltre di età quella più refrattaria all'applicazione di accorgimenti per l'integrità di dispositivi e dati.

Quanto stiamo osservando non è che la traslazione della diffusione delle più ampie competenze digitali tra la popolazione, dove i soggetti meno istruiti e più anziani rappresentano i gruppi sociali meno competenti e più a rischio di *digital divide*, con esclusione dalle connessioni online, al cui interno sempre più sono comprese attività quotidiane e interazioni sociali.

Essi, in definitiva, rappresentano l'anello più debole di tutto l'ecosistema digitale.

I dati sulla sicurezza informatica evidenziano nel complesso una realtà che va oltre la percezione che gli italiani hanno delle loro condotte in materia di prevenzione e tutela dal rischio di minacce informatiche, alcune delle quali con ogni probabilità introiettate oramai come automatismi, senza la piena consapevolezza della loro natura e della loro funzione.

4.4. La sicurezza degli smartphone, una condizione inderogabile

La sicurezza informatica e digitale si persegue anche, e in alcuni casi soprattutto, attraverso una gestione accorta e vigile del proprio smartphone, in quanto principale e costante punto di accesso alla rete.

Vediamo nel dettaglio quanto sono consapevoli di ciò gli italiani, dei quali:

- il 77,1% consente gli aggiornamenti periodici del software di sistema, con valori che arrivano all'82,8% tra i laureati e all'84,5% tra i 18-34enni, mentre si riducono al 48,2% tra i più anziani (65 anni e oltre);
- il 62,6% utilizza per accedere al proprio cellulare oltre alla password altri fattori (PIN, OTP, impronta digitale o riconoscimento facciale), una pratica che nel caso di utenti laureati supera quota 70% (72,2%) e di quelli più giovani sfiora l'80% (79,7%);
- il 36% degli occupati dispone di cellulari distinti per uso privato e per lavoro, una distinzione che ricorre nel 40,8% dei lavoratori autonomi;
- il 29,1% dispone di un sistema di cancellazione remota dei file in caso di furto o smarrimento; una quota da intendersi rilevante, tenuto conto della natura abbastanza sofisticata di tale misura, tra l'altro, principalmente utilizzata nel mondo Apple;
- il 36,8%, infine, applica al cellulare dei propri figli minorenni le stesse misure di sicurezza del suo cellulare personale, percentuale che tra i 35-64 anni arriva al 44,3% (**tab. 9**).

Essere costantemente connessi a Internet è oramai una necessità e la sicurezza dei dispositivi mobili e degli smartphone, in particolare, è dunque divenuta una condizione inderogabile.

Quest'ultimi, infatti, sono una componente integrante e onnipresente nella vita della quasi totalità degli individui, attirando le mire criminali degli hacker, interessati ad acquisire illegalmente dati, identità, beni online dei singoli utenti.

4.5. L'intenzionalità nella sicurezza

Una volta rilevato quanto siano utilizzate dagli italiani le principali misure di sicurezza per ridurre i rischi derivanti dall'utilizzo di sistemi informatici, il passo successivo è stato quello di ampliare lo spettro di analisi, cercando di analizzare non solo la quantità, ma anche la qualità e l'efficacia delle prassi di protezione messe in atto.

Lo abbiamo fatto, attraverso la selezione di una batteria di misure definite *sentinella,* a cui sono associabili comportamenti concretamente rilevabili e

misurabili, sintomatici di una maggiore intenzionalità a perseguire, a livello individuale, quell'insieme di condotte, che confluiscono concettualmente nella locuzione sintetica di igiene informatica.

L'adozione intenzionale di comportamenti conformi a un'adeguata igiene informatica indica in che misura le persone abbiano il profilo di un utente consapevole e responsabile dei rischi legati alla minaccia informatica.

Per questa ragione, tra le diverse misure di sicurezza precedentemente illustrate sono state selezionate quelle la cui adozione implica un maggiore coinvolgimento dell'utente, ovvero:

- la regolare esecuzione del backup dei file;
- l'impiego di password diverse in funzione dei servizi utilizzati;
- l'utilizzo di sistemi di autenticazione più complessi della password (biometrica, OTP, ecc.);
- la presenza di una password per il wi-fi di casa;
- l'installazione e l'aggiornamento di un antivirus su Pc di casa e cellulare.

Le evidenze raccolte per certi versi confermano, da un lato quell'introiezione di misure e prassi cui si faceva riferimento nel paragrafo precedente e che segna un passo in avanti rispetto a un'esplicita consapevolezza dei comportamenti messi in atto; dall'altro, una distribuzione asimmetrica tra i diversi gruppi sociali della succitata igiene informatica, per effetto di alcune variabili sociodemografiche.

Infatti, dall'analisi dei dati si evidenzia che quasi sei italiani su dieci, pari al 57,3% del totale, risultano adottare tra le quattro e le cinque misure sopra indicate e di questi il 32,4% è pienamente performante rispetto al mix nel suo complesso.

Il restante 42,7% di popolazione si suddivide tra un 26,4% di individui che adotta tra le 2 e le 3 misure e un 16,3% che ne adotta al più una (**fig. 5**).

Vale la pena osservare, però, che tra chi adotta tra le 4 o le 5 misure a più alto tasso di intenzionalità, il 55,8% aveva affermato di conoscere a grandi linee il termine cybersicurezza e il 20,4% di non fare niente di concreto per la sicurezza dei propri dispositivi, pur essendo preoccupato, evidenziando così una sottovalutazione della propria condotta.

Confrontando, poi, l'incrocio dei precedenti dati con le variabili strutturali della popolazione emerge che tra chi adotta al massimo una misura di sicurezza a più alto tasso di intenzionalità i gruppi meno performanti sono le donne (21%) rispetto agli uomini (11,3%), i più anziani (46,9% 65 anni e oltre) rispetto ai più giovani (3,6% 18-34enni), i meno istruiti (48,1% con al più la licenza media) rispetto ai laureati (5,9%).

Sono questi i gruppi bersaglio su cui intervenire con modalità differenziate e conformi alle loro caratteristiche e condizioni, così che acquisiscano per quanto possibile adeguati livelli di *cybersecurity*.

4.5.1. I gruppi per variabili sociodemografiche

Sulla base delle principali variabili sociodemografiche si è tentato di delineare un profilo tipologico che, pur in modo approssimativo, fornisse un'identità sociale a ciascuna delle posture di cybersicurezza precedentemente illustrate. I risultati di tale analisi hanno permesso la costruzione dei quattro gruppi di seguito elencati:

- **Attivi:** sono il gruppo di utenti che impiega tra le 4 e le 5 misure di sicurezza a più alta intenzionalità. Ne fanno parte, in prevalenza, individui uomini (62,3%) di età compresa tra 18 e 34 anni (74,3%) con alto livello di istruzione (laureati 70,9%), in gran parte occupati (71%) e inquadrati come impiegati (74,9%). La netta prevalenza di occupati dipendenti evidenzia l'impatto che il contesto di lavoro può sortire sui comportamenti individuali di *cybersecurity***.**
- **Proattivi**: sottogruppo del precedente, è composto da individui che impiegano tutte e cinque le misure di sicurezza a più alta intenzionalità, assumendo un approccio orientato alla prevenzione del rischio di minacce informatiche che possono alterare il funzionamento dei device e originare perdite di dati e informazioni. Sostanzialmente bilanciato sotto il profilo di genere, ne fanno parte in misura superiore al 40%, i giovani (43% 18-34enni) i laureati (40,4%) e gli individui occupati (43,9%). Tra questi ultimi sono più proattivi coloro i quali sono inquadrati come dirigente o quadro.
- **Adempienti**: la composizione del gruppo che accoglie chi adotta dalle due alle tre misure di sicurezza a più alta intenzionalità è abbastanza trasversale rispetto alle caratteristiche strutturali della popolazione e, in parte, speculare a quello dei proattivi. Infatti, si annullano le differenze

sotto il profilo della presenza di genere e della classe di età e prevalgono i livelli di scolarizzazione medio bassi. Di questo gruppo fa parte una quota soprattutto di disoccupati e dipendenti con mansioni esecutive.

- **Inconsapevoli**: quest'ultimo gruppo è quello con la minore numerosità e include coloro i quali dimostrano una ridotta consapevolezza del rischio informatico, adottando al massimo una sola misura di sicurezza. Ne fanno parte il 21% delle donne e soprattutto quei segmenti di popolazione che solitamente si caratterizzano per una più marcata *digital illiteracy*: soggetti con bassi livelli di istruzione (48,1% con al più la licenza media), più anziani (46,9% 65 anni e oltre) e classificati tra le non forze di lavoro, come casalinghe e pensionati (38,1%).

5. QUALCOSA SI STA MUOVENDO SUL FRONTE AZIENDALE

5.1. Target aziende

Come già illustrato in precedenza, la quota di imprese italiane con 10 e più addetti che nel 2022 ha avuto un problema di sicurezza ICT è stata pari al 15,7%, equivalente in valore assoluto a circa 30.000 unità.

Il rischio informatico, ormai, può essere equiparato a un'esternalità negativa di cui necessariamente le imprese devono tenere conto nell'esercizio delle loro attività.

Possiamo affermare ciò non solo sulla base dei dati dell'Istat, ma anche attingendo dalla diretta esperienza degli italiani, in quanto testimoni delle disavventure informatiche occorse nell'ultimo anno nei loro luoghi di lavoro, dove per il 20,6% si è verificato un problema e più nello specifico:

- un sabotaggio e una sospensione dei servizi aziendali nel 12,8% dei casi;
- un attacco informatico agli account social e al sito aziendali con danni conseguenti (11,7%);
- una perdita di dati e informazioni a causa di un attacco informatico (10,3%);
- un furto di identità e di dati sensibili (9,1%) **(fig. 6)**.

Ad un tempo però, come già osservato in precedenza, gli italiani che affermano di avere un antivirus installato e aggiornato sul Pc di lavoro sono il 75%. Se, invece, a titolo di esempio, consideriamo alcune misure di sicurezza più sofisticate messe in atto dalle imprese con 10 e più addetti, si rileva (fonte Istat) che quelle che adottano l'identificazione e l'autenticazione dell'utente tramite metodi biometrici sono l'8,2% (21,3% nel caso di imprese con 250 addetti), mentre quelle che ricorrono alla combinazione di almeno due meccanismi di autenticazione, sono il 27,1%. L'assicurazione contro incidenti di sicurezza Ict, infine, è una pratica che ha accomunato nel 2022 il 16,4% delle imprese italiane (quota in crescita rispetto al 2019, quando quelle assicurate contro questo tipo di rischio erano il 13%).

Questi dati, letti nella loro consequenzialità, ci confermano come la sicurezza informatica dipenda necessariamente dal combinato disposto di tecnologie, procedure e persone.

Se la sicurezza informatica, per essere efficace deve affondare le sue radici in una responsabilità diffusa, la formazione è una scelta necessaria, anche se talvolta non sufficiente, per rendere consapevoli gli addetti sui loro obblighi e su quali debbano essere le corrette posture da tenere.

La *cyber resilience* di un'organizzazione non può, pertanto, prescindere da un ampliamento del perimetro della formazione del personale, che deve comprendere tutti, senza limitarsi al solo team di *cybersecurity.*

5.2. La formazione aziendale come reazione al *cyber risk*

Sul fronte della formazione in azienda in realtà sembra che qualcosa si stia muovendo. Si osserva, infatti, una spinta alla formazione, interpretabile come sintomo di una reazione aziendale all'incremento della minaccia informatica, a cui è stato fatto cenno sopra. A fronte del 44,6% dei dipendenti intervistati, che dichiara di non aver mai avuto una formazione specifica sulla *cybersecurity*, il restante 55,4% dei rispondenti, invece, è stato o sarà formato per contrastare o prevenire eventuali attacchi informatici di cui:

- il 27,3% partecipando ad almeno uno specifico corso nell'ultimo anno;
- il 14,6% andando in formazione nei prossimi mesi;
- il 13,5% di dipendenti, frequentando corsi che sono stati erogati oltre un anno fa.

La numerosità dei soggetti formati o in procinto di esserlo sale al 63% per i laureati (a fronte del 50,1% dei diplomati).

Sotto il profilo geografico, il numero maggiore di dipendenti formati o da formare si ha tra quelli residenti nelle Regioni del Centro (59,6% a fronte del 50,6% di quelli residenti nel Sud e nelle Isole), mentre è nelle Regioni settentrionali che si registrano le quote più alte di addetti formati nell'ultimo anno (29,4% nel Nord-Ovest e 30,2% nel Nord-Est) (**tab.10**).

Se, dunque, ben oltre un quarto dei dipendenti formati ha ricevuto una specifica formazione contro i rischi informatici solo nell'ultimo anno e quasi

un ulteriore 15% la riceverà nei prossimi mesi, è verosimile ritenere che da parte aziendale sia stato avviato un processo di consapevolizzazione dell'importanza della qualificazione del capitale umano impiegato, poiché ogni addetto, ogni individuo, può essere una fonte di rischio informatico.

TABELLE E GRAFICI

Tab. 1 - Reati informatici denunciati all'Autorità giudiziaria dalle Forze di Polizia ([1]), 2012-2021 *(v.a. e var. %)*

Anno	Reati informatici	Totale reati
2012	124.113	2.818.834
2013	150.035	2.892.155
2014	144.107	2.812.936
2015	154.867	2.687.249
2016	162.292	2.487.389
2017	174.743	2.429.795
2018	202.387	2.371.806
2019	228.254	2.301.912
2020	267.565	1.900.624
2021	316.716	2.104.114
Var.%		
2019-2021	38,8	-8,6
2020-2021	18,4	10,7
2012-2021	155,2	-25,4

(1) Sono considerati, oltre ai delitti denunciati all'Autorità giudiziaria da Polizia di Stato, Arma dei Carabinieri e Guardia di Finanza che alimentavano il modello cartaceo 165 in uso fino all'anno 2003, anche quelli denunciati dal Corpo Forestale dello Stato, dalla Polizia Penitenziaria, dalla Direzione Investigativa Antimafia e da altri uffici (Servizio Interpol, Guardia Costiera, Polizia Venatoria e altre Polizie Locali)

Fonte: elaborazione Censis su dati Ministero dell'Interno

Tab. 2 - Prime 10 province (*) per numero di reati informatici denunciati all'Autorità giudiziaria dalle Forze di polizia 2021 *(v.a., val. per 1.000 abitanti e val. %)*

Province	Totale reati informatici			Val. % popolazione sul totale Italia
	v.a.	per 1.000 abitanti	% sul totale	
Milano	24.077	7,5	7,6	5,4
Roma	21.637	5,1	6,8	7,1
Torino	17.165	7,8	5,4	3,7
Napoli	16.016	5,4	5,1	5,1
Brescia	8.323	6,6	2,6	2,1
Palermo	6.253	5,2	2,0	2,0
Firenze	6.063	6,1	1,9	1,7
Bari	5.891	4,8	1,9	2,1
Bologna	5.833	5,8	1,8	1,7
Venezia	5.519	6,6	1,7	1,4
Totale 10 Province	116.777	6,1	36,9	32,4
Totale reati informatici	316.716	5,4	100,0	100,0

(*) Relativo a 92 Province (la Regione Sardegna è ripartita nelle quattro vecchie Province: Sassari, Cagliari, Oristano e Nuoro) e 14 Città Metropolitane

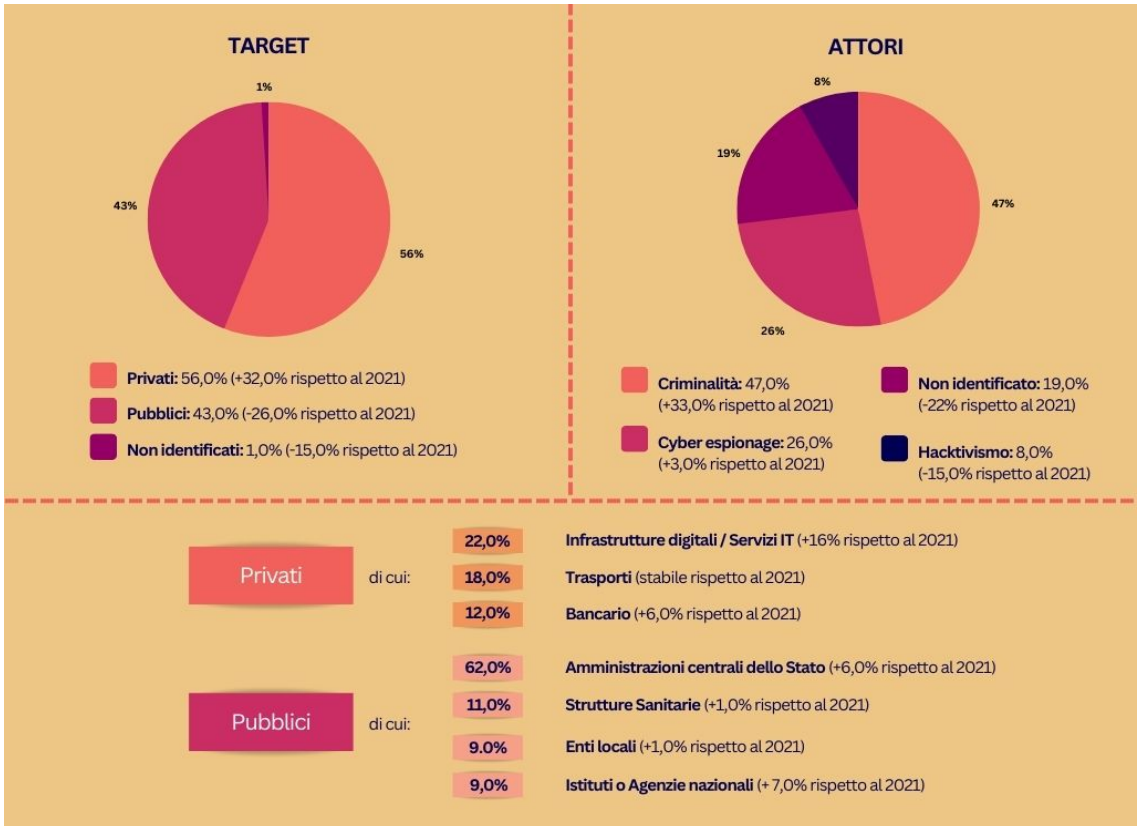
Fonte: elaborazione Censis su dati Ministero dell'Interno

Tab. 3 - Imprese che hanno avuto almeno un problema di sicurezza ICT (indisponibilità dei servizi ICT, distruzione o danneggiamento dei dati, divulgazione di dati riservati), per tipologia di danno e classe di addetto, 2022
(val.%)

	Classe di addetti				10 addetti e più
	10-49 addetti	50-99 addetti	100-249 addetti	250 addetti e più	
Divulgazione di dati riservati	0,8	1,7	2,6	4,3	1,0
Distruzione o danneggiamento dei dati	3,2	3,8	6,0	4,9	3,3
Indisponibilità dei servizi ICT	13,4	17,7	23,1	30,7	14,4
Divulgazione di dati riservati a causa di intrusioni, *pharming*, attacchi di phishing, azioni intenzionali dai propri addetti	0,5	1,2	1,9	2,9	0,6
Divulgazione di dati riservati a causa di azioni non intenzionali da parte dei propri addetti	0,4	1,2	1,0	2,3	0,5
Distruzione o danneggiamento dei dati a causa di infezione di software dannoso o intrusione non autorizzata	1,7	1,3	3,0	2,9	1,7
Distruzione o danneggiamento dei dati a causa di guasti hardware o software	2,1	2,9	3,7	3,2	2,3
Indisponibilità dei servizi ICT a causa di attacchi dall'esterno	2,9	2,6	5,7	7,8	3,1
Indisponibilità dei servizi ICT a causa di guasti hardware o software	12,1	16,3	20,5	27,1	13,0
Almeno un problema di sicurezza ICT	14,5	20,1	25,8	33,1	15,7
2019					*10,1*

Fonte: elaborazione Censis su dati Istat - Rilevazione sulle tecnologie dell'informazione e della comunicazione nelle imprese

Fig. 1 - 1 Attività cibernetiche ostili contro assetti informatici rilevanti per la sicurezza nazionale, 2022



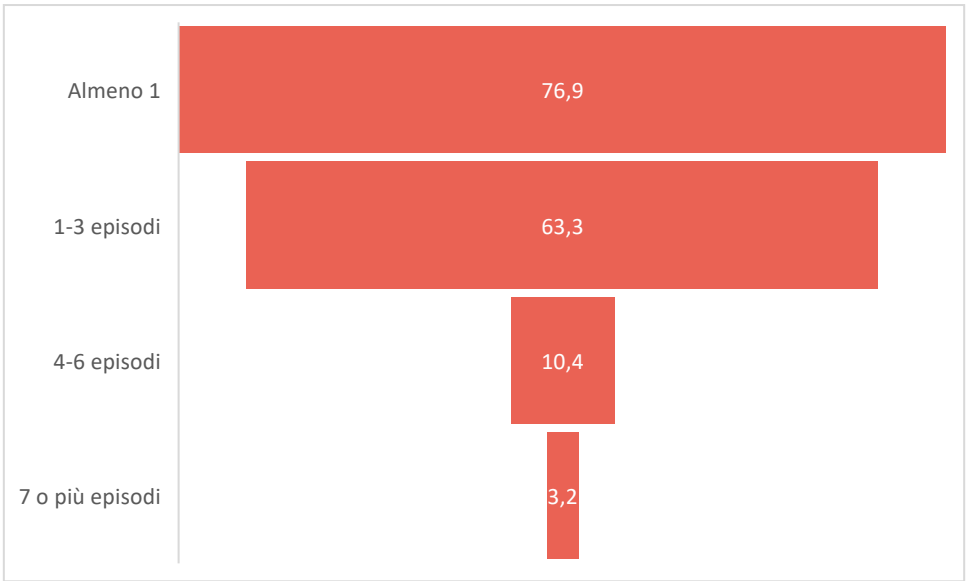
Fonte: elaborazione Censis su dati della Presidenza del Consiglio dei ministri – Sistema di informazione per la sicurezza della Repubblica

Tab. 4 - Il mercato della *cybersecurity* in Italia, 2022 *(v.a. e val.%)*

Valore Mercato *cybersecurity* (1)	1,86 miliardi
Imprese > 250 addetti che hanno aumentato investimenti in *cybersecurity* (1)	61,0
Rapporto spesa *cybersecurity*/Pil (1)	0,10
Imprese antihacker (2)	3.147
Incremento Imprese antihacker (2) (sett.2021 – giu. 2022)	+5,4%
Prime 3 Regioni per numero imprese antihacker (2):	
Lazio	22,5
Lombardia	18,5
Campania	10,5

Fonte: elaborazione Censis su dati (1) Osservatorio Cybersecurity & Data Protection del Politecnico di Milano e (2) Unioncamere-InfoCamere.

Fig. 2 – Minacce informatiche capitate agli italiani nell'ultimo anno *(val.%)*



Fonte: indagine Censis, 2023

Tab. 5 - Italiani che hanno subìto minacce e truffe informatiche *(val.%)*

Nell'ultimo anno le è capitato di:	%
Ricevere un SMS o un messaggio su WhatsApp con invito a cliccare su un link sospetto/malevolo	60,9
Essere bersaglio di e-mail ingannevoli per truffarla, per convincerla a dare informazioni sensibili che la riguardano (ad esempio, con mittente banche e/o aziende di cui lei è cliente)	56,0
Ricevere richieste di denaro, prestiti da persone conosciute sul web	15,9
Avere il suo Pc/laptop infettato da un virus	15,7
Essere truffato facendo acquisti online su siti web fraudolenti o all'interno di piattaforme con annunci legittimi (per esempio Facebook, eBay, Instagram)	8,9
Avere conversazioni e/o frequentazioni con persone conosciute sul web scoprendo poi che avevano una falsa identità	8,8
Scoprire sui social account fake con il suo nome/identità/foto	8,5
Subire una violazione della privacy (ad esempio a causa di un furto di un *device*, di una copia di dati personali non autorizzata, condivisione di video, foto, non autorizzate da parte di altri ecc.)	8,2
Scoprire pagamenti di acquisti online fatti a suo nome e con la sua carta	6,6
Vedersi clonata carta di credito e/o bancomat	6,6

Fonte: indagine Censis, 2023

Tab. 6 - Reazioni degli italiani al numero crescente di attacchi informatici a enti e istituzioni, per classi di età *(val.%)*

Il numero crescente di attacchi informatici a enti e istituzioni verificatosi durante i mesi passati, quali delle seguenti situazioni le ha provocato?	18-34 anni	35-64 anni	65 anni e oltre	Totale
Ulteriore preoccupazione rispetto all'attuale situazione di crisi	67,9	65,6	54,2	62,9
Quando mi collego a Internet per svolgere attività online (per. es. acquisti, prenotazioni, operazioni con la banca) ho più paura che i miei dati personali siano rubati e usati per altre cose	66,3	59,4	32,5	53,2
Mi collego meno a Internet per svolgere attività online (per esempio acquisti, prenotazioni, operazioni con la banca)	30,8	24,9	19,0	24,4

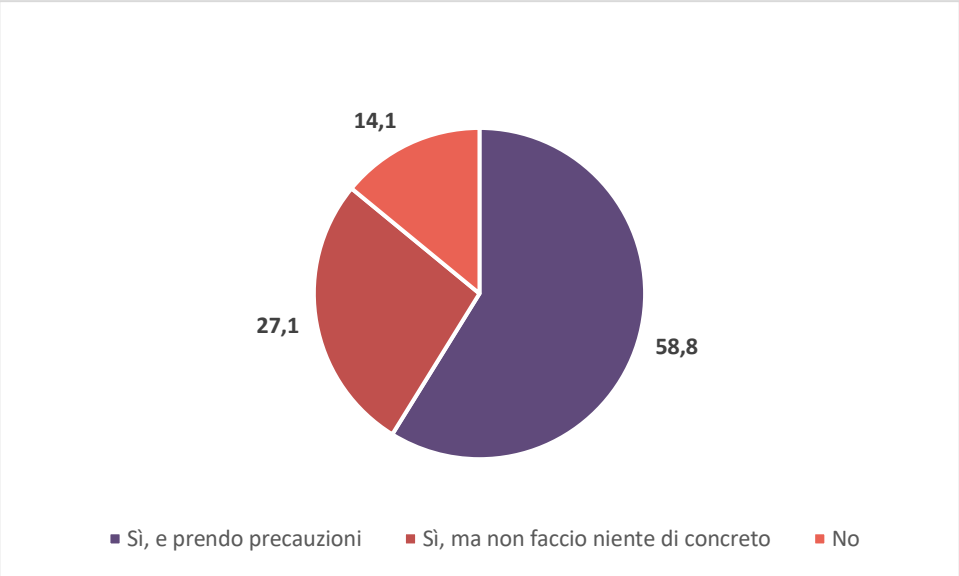
Fonte: indagine Censis, 2023

Tab.7 - Italiani che dichiarano di sapere cosa si intende per cybersecurity *(val.%)*

	2023	*2022*
Sì, precisamente	28,8	*24,3*
Sì, a grandi linee	50,4	*58,6*
No	20,8	*17,1*
Totale	100,0	*100*

Fonte: indagine Censis, 2023

Fig.3 - Italiani preoccupati della sicurezza informatica *(val.%)*



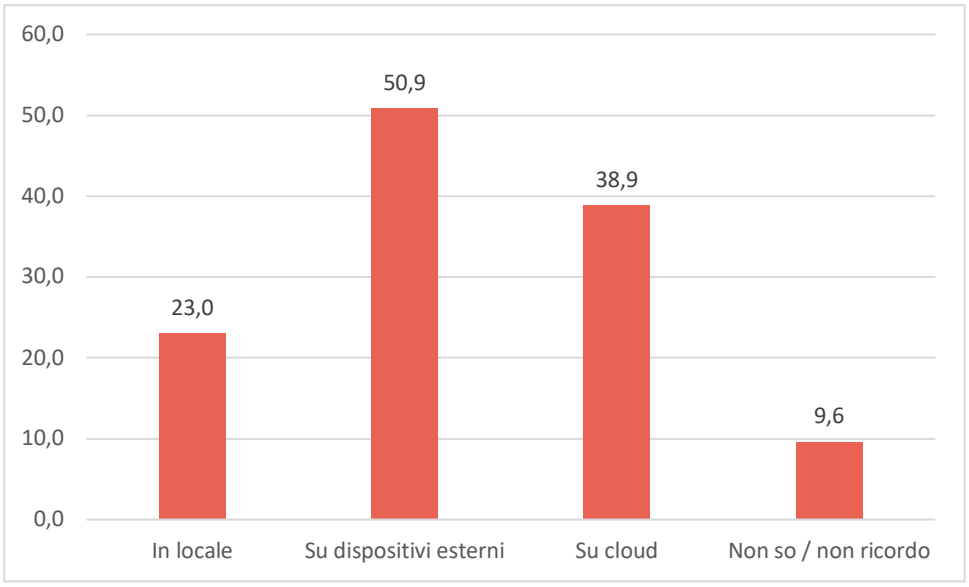
Fonte: indagine Censis, 2023

Tab.8 - Misure di sicurezza informatica utilizzate dagli italiani *(val.%)*

Tra le misure di sicurezza di seguito indicate quali utilizza?	Totale	Dispositivi di lavoro
Utilizza una Password per il suo wi-fi di casa	75,2	
Fa uso di password diverse per i vari servizi che utilizza (posta elettronica, home banking, profili social, piattaforme di intrattenimento ecc.)	71,5	
Consente l'aggiornamento periodico del sistema operativo e dei software di produttività (es. Office) del Pc di casa	70,8	*74,6*
Ha un antivirus installato e aggiornato sul suo Pc di casa	70,3	*75,0*
Effettua di solito un backup dei suoi file	59,5	
Fa uso di una password complessa, con almeno 12 caratteri sia alfanumerici sia speciali, sul suo Pc di casa	56,8	*64,5*
Utilizza sistemi di autenticazione più complessi della password per es. autenticazione biometrica con le impronte digitali o codice OTP via sms, ecc.	54,0	
Utilizza un firewall sul Pc di casa	46,2	*59,6*

Fonte: indagine Censis, 2023

Fig.4 - Modalità di backup utilizzate dagli italiani *(val.%)*



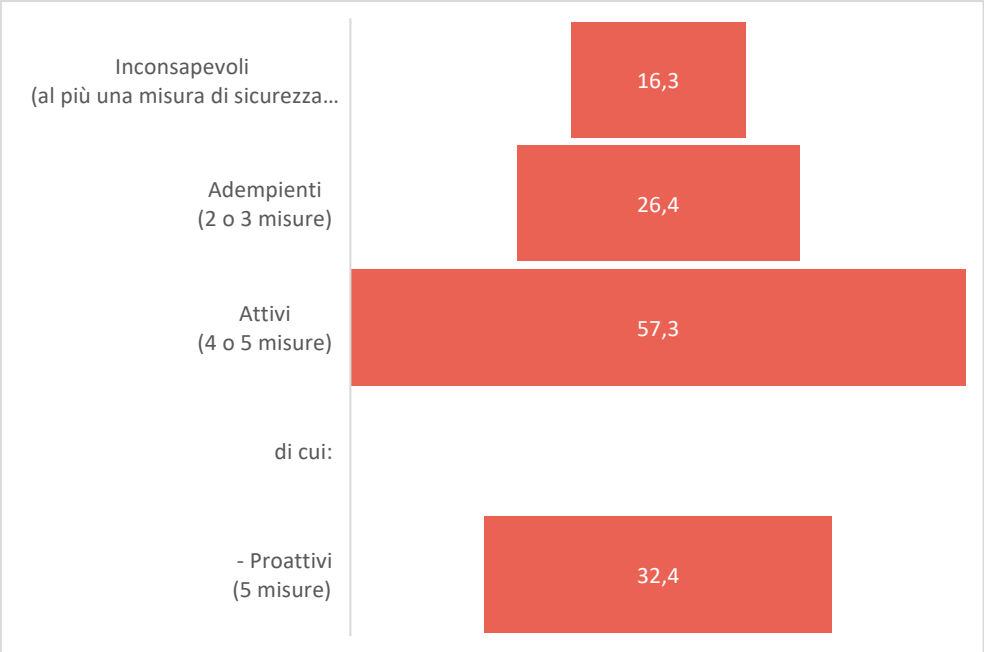
Fonte: indagine Censis, 2023

Tab. 9 - Misure di sicurezza applicate dagli italiani al proprio telefono cellulare, per classi di età *(val.%)*

	18-34 anni	35-64 anni	65 anni e oltre	Totale
Accede al cellulare con altri fattori e utilizza oltre alla password (per es. PIN, codice OTP, impronta digitale o riconoscimento facciale)	79,7	72,2	32,6	62,6
Ha applicato un antivirus	51,7	55,6	28,5	47,2
Consente gli aggiornamenti periodici del software di sistema	84,5	90,1	48,2	77,1
Dispone di un sistema di cancellazione remota dei file in caso di furto o smarrimento	37,3	33,3	15,3	29,1
(solo se occupato) Dispone di cellulari distinti per uso privato e per lavoro	39,1	35,5	16,7	36,0
(solo per chi ha figli minorenni) Al cellulare dei suoi figli minorenni applica le stesse misure di sicurezza del suo cellulare personale	29,7	44,3	0,0	36,8

Fonte: indagine Censis, 2023

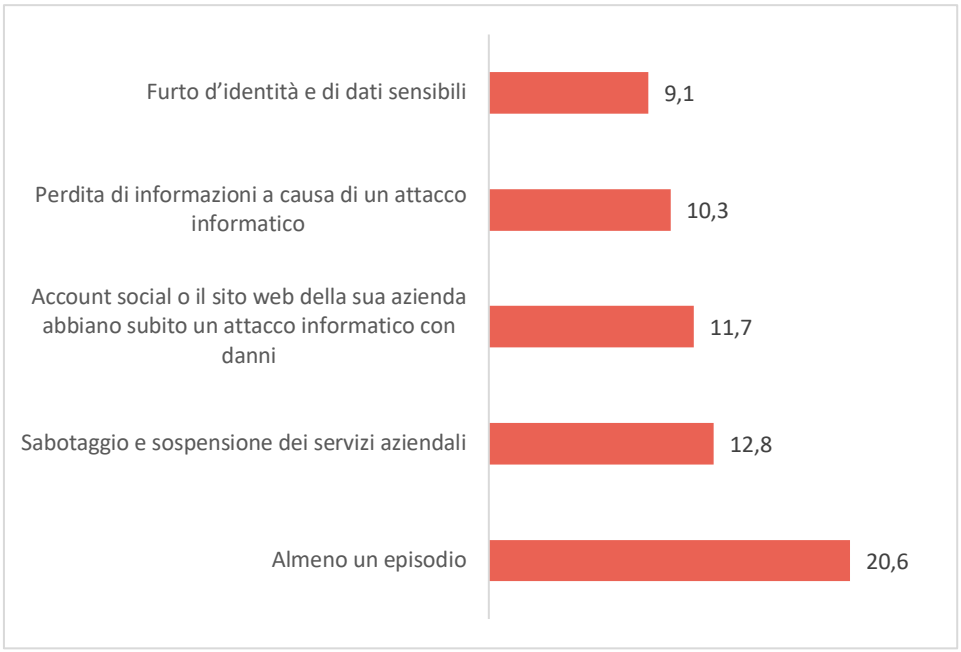
Fig. 5 – Misure di sicurezza a maggiore intenzionalità adottate dagli italiani (*) *(val%)*



(*) Sono considerate le seguenti 5 misure:
- Fa uso di password diverse per i vari servizi che utilizza;
- Utilizza sistemi di autenticazione più complessi della password per es. autenticazione biometrica con le impronte digitali o codice OTP via sms, ecc.;
- Utilizza una password per il suo wi-fi di casa;
- Ha un antivirus installato e aggiornato sul suo Pc di casa e/o sul cellulare
- Effettua di solito un backup dei suoi file

Fonte: indagine Censis, 2023

Fig. 6 – Lavoratori la cui azienda ha subito nell'ultimo anno attacchi informatici *(val.%)*



Fonte: indagine Censis, 2023

Tab. 10 - Occupati che hanno avuto formazione specifica sulla cybersecurity nell'ultimo anno, per ripartizione geografica *(val.%)*

	Nord-Ovest	Nord-Est	Centro	Sud-Isole	Totale
Sì, nell'ultimo anno	29,4	30,2	27,4	22,6	27,3
Sì, più di un anno fa	10,8	9,3	22,6	13,6	13,5
No, ma è prevista nei prossimi mesi	15,3	18,2	9,6	14,4	14,6
No, mai	44,6	42,3	40,4	49,4	44,6
Totale	100,0	100,0	100,0	100,0	100,0

Fonte: indagine Censis, 2023