02-APR-2024
da pag. 19 / foglio 1 / 2

ItaliaOggi Sette
Settimanale - Dir. Resp.: Pierluigi Magnaschi
Tiratura: N.D. Diffusione: N.D. Lettori: 74000 (DS0006901)

DATA STAMPA
www.datastampa.it

Crescono i crimini informatici: così si corre ai ripari con polizze ad hoc e altri accorgimenti

Uno scudo contro i rischi cyber

Coperture varie: dalle spese legali all'assistenza psicologica

Pagina a cura
DI IRENE GREGUOLI VENINI

La tecnologia è sempre di più una parte integrante e irrinunciabile della vita quotidiana. A ciò si associano però maggiori rischi legati ai crimini informatici: sono molti, infatti, ad aver subito l'accesso fraudolento agli strumenti di pagamento, un furto di identità o la diffusione non autorizzata del proprio materiale digitale (si veda la pagina precedente). Per proteggersi ci sono diversi accorgimenti, come una gestione corretta delle password, l'attenzione ai siti su cui si naviga, oltre che alle e-mail con allegati o link da mittenti di cui non si è sicuri. Cominciano però anche a diffondersi dei prodotti assicurativi specifici, che propongono garanzie che vanno dalla rimozione dei contenuti lesivi dai social network alla copertura delle spese legali nel caso di un procedimento penale per un reato commesso utilizzando l'identità rubata fino all'assistenza psicologica in caso molestie o di attacchi subiti online.

I crimini informatici. La tecnologia si sta evolvendo sempre di più e con questo anche i possibili rischi. Da un'indagine che **Facile.it** ha commissionato agli istituti **mUp Research** e **Norstat** risulta che quasi 13 milioni di italiani sono stati vittima di un crimine informatico almeno una volta nella vita. In particolare, oltre 6 milioni e mezzo di individui hanno subito un accesso non autorizzato agli strumenti di pagamento personali, mentre quasi 2,5 milioni di persone si sono viste rubare la propria identità o l'immagine (o quella dei familiari) per poi essere usata da terzi per atti illegali.

Quasi 2,3 milioni, invece, sono stati vittime della diffusione non autorizzata di materiale digitale proprio o dei figli, mentre pochi meno, 2,2 milioni, sono coloro che hanno subito un furto di identità con la conseguente sottoscrizione di contratti a loro nome. Sebbene il problema riguardi tutte le fasce della popolazione, l'indagine ha evidenziato che la percentuale di chi è stato colpito da un crimine informatico aumenta tra i più giovani, toccando il picco tra i 18-24enni, fascia nella quale la percentuale di vittime raggiunge il 35%.

Il cyberstalking, il cyberbullismo e il revenge porn sono fenomeni molto diffusi, ma colpiscono in misura maggiore i più giovani. Sono circa 1,5 milioni le persone che hanno subito cyberstalking: se a livello nazionale la percentuale è pari al 3,4% dei rispondenti, tra i giovani con età compresa tra i 18 e i 24 anni si arriva fino al 7,1%.

Un trend analogo riguarda il cyberbullismo: le vittime sono 1,3 milioni, ma la percentuale passa dal 3,2% del campione nazionale al 13,1% tra i ragazzi 18-24enni (vale a dire 550 mila individui); simile è la situazione nel caso del revenge porn: ci sono 1,2 milioni di vittime, ma la percentuale passa dal 2,8% nazionale a oltre il 7% tra gli le persone con meno di 24 anni.

L'intelligenza artificiale: un'opportunità ma anche un rischio. Se molti percepiscono l'intelligenza artificiale come un'opportunità, c'è una fetta della popolazione che è preoccupata dai rischi anche sul fronte dei crimini informatici. Dall'indagine di Facile.it emerge che a livello nazionale il 34,5% vede dei vantaggi nell'utilizzo dell'IA, la percentuale sale al 40,4% tra i 25-34enni e al 53,5% tra gli appartenenti alla fascia 18-24 anni. Al contrario, al crescere dell'età aumentano anche i dubbi: dopo i 55 anni circa il 18% degli intervistati la considera solamente come una minaccia.

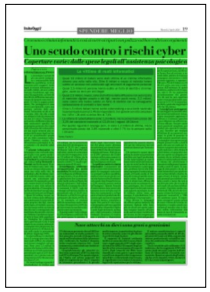
Considerando i rischi collegati all'intelligenza artificiale che più preoccupano le persone, il 52,6% degli intervistati teme che l'IA possa essere sfruttata da malviventi per azioni fraudolente e il 39,6% che diventi incontrollabile dall'uomo. Pochi di meno (il 39%) pensano che l'informazione online possa essere invasa da contenuti falsi creati dall'intelligenza artificiale.

Le polizze contro i crimini informatici. L'aumentare dei rischi online e del cybercrime ha spinto le compagnie assicurative a proporre polizze specifiche, anche se sono ancora pochi i privati che hanno scelto di sottoscrivere questo tipo di copertura (solo il 3% secondo quanto emerso dall'indagine). Queste formule di assicurazioni sono ancora abbastanza nuove in Italia ma l'offerta sta cominciando a svilupparsi: si tratta di prodotti che forniscono agli assicurati supporto di natura tecnica, economica e legale. Dal punto di vista tecnico propongono software specifici per difendere i dispositivi digitali usati dagli assicurati, proteggere i dati personali e valutare eventuali situazioni di rischio, sino a mettere a disposizione specialisti che possono intervenire per far rimuovere dal web contenuti dannosi per l'assicurato.

Chi sottoscrive questo tipo di polizza ha anche una protezione giuridica con legali professionisti che intervengono in caso di danni subiti online dall'assicurato, sia sui social network sia sui siti di e-commerce, o, più in generale, problemi dovuti alla diffusione impropria di contenuti personali, arrivando anche al rimborso di eventuali perdite economiche subite. Queste assicurazioni, in alcuni casi, offrono alle vittime anche un sostegno di natura psicologica, che si traduce nella copertura dei costi connessi al supporto psicologico in casi di violenza online come, per esempio, il cyberbullismo, il cyberstalking e il revenge porn.

Sono diverse le compagnie che offrono polizze dedicate alla sicurezza digitale delle famiglie; in alcuni casi queste coperture vengono inserite all'interno di assicurazioni multirischio per la casa, in altri vengono proposte come prodotti indipendenti. I prezzi sono accessibili: si va, per le coperture base, dai 60 euro l'anno, fino ad arrivare, a seconda della politica di ciascuna compagnia assicurativa e delle garanzie aggiunte, a superare i 160 euro. Più di 6 italiani su 10 (61,4%), però, non sono a conoscenza dell'esistenza di questi prodotti e, anche tra chi li conosce, solo il 3% ha sottoscritto un'assicurazione del genere. Tra chi non ha una copertura contro i crimini informatici, quasi uno su 3 (37,7%) è intenzionato a farla, quota che raggiunge il 43% tra i 25-34enni.

I consigli per proteggersi. Per proteggersi è possibile adot-



ItaliaOggi Sette
Settimanale - Dir. Resp.: Pierluigi Magnaschi
Tiratura: N.D. Diffusione: N.D. Lettori: 74000 (DS0006901)

tare alcuni accorgimenti: innanzitutto mantenere aggiornati il software e il sistema operativo e, poi, utilizzare un software anti-virus efficace. Occorre anche usare password complesse: per rendere più agevole il compito, si può ricorrere per esempio all'utilizzo di un password manager, in grado di generare in modo casuale password sicure. Un consiglio è non aprire mai gli allegati presenti nelle e-mail di spam, che sono un modo per infettare i computer attraverso attacchi malware e altre forme di cybercrimine, e in generale è meglio non aprire un allegato proveniente da un mittente sconosciuto. Un altro modo per divenire vittima del cybercrimine è cliccare sui collegamenti presenti nelle e-mail di spam, in messaggi di altro genere o in siti Internet sconosciuti: per questo occorre evitare di farlo. Inoltre, bisogna evitare di fornire i propri dati personali per telefono o tramite e-mail, a meno che non si sia del tutto certi che si tratti di un'e-mail o di una linea telefonica sicura. Conviene anche controllare gli URL dei siti che si visitano, evitare di cliccare su collegamenti sconosciuti o URL che sembrano spam. È importante accorgersi quanto prima di essere vittima del crimine informatico: è meglio quindi controllare gli estratti conto e chiedere subito informazioni alla banca in caso di transazioni sospette o sconosciute.

Le vittime di reati informatici

- Quasi 13 milioni di italiani sono stati vittima di un crimine informatico almeno una volta nella vita. Oltre 6 milioni e mezzo di individui hanno subito un accesso non autorizzato agli strumenti di pagamento personali
- Quasi 2,5 milioni di persone hanno subito un furto di identità o di immagine, usate da terzi per atti illegali
- Quasi 2,3 milioni, invece, sono stati vittima della diffusione non autorizzata di materiale digitale proprio o dei figli, mentre pochi meno, 2,2 milioni, sono coloro che hanno subito un furto di identità con la conseguente sottoscrizione di contratti a loro nome
- Circa 1,5 milioni italiani hanno subito cyberstalking e se a livello nazionale la percentuale è pari al 3,4% dei rispondenti, tra i giovani con età compresa tra i 18 e i 24 anni si arriva fino al 7,1%
- Le vittime di cyberbullismo sono 1,3 milioni, ma la percentuale passa dal 3,2% del campione nazionale al 13,1% tra i ragazzi 18-24enni
- Per quanto riguarda il revenge porn, ci sono 1,2 milioni di vittime, ma la percentuale passa dal 2,8% nazionale a oltre il 7% tra le persone sotto i 24 anni

Fonte: Facile.it

Nove attacchi su dieci sono gravi o gravissimi

C'è da tenere presente che nel 2023 sono aumentati, in modo costante, i cyber attacchi, secondo il Rapporto annuale sull'evoluzione della cybersecurity realizzato da Assintel (Associazione nazionale imprese Ict) - Confcommercio, costituendo un rischio serio per le imprese.

Geograficamente gli attacchi cyber sono aumentati al 50% in America e al 27% in Europa. Per quanto riguarda l'Italia, nel primo semestre del 2023 si è registrato un +85,7% rispetto al trimestre precedente e le piccole medie imprese, in particolare le piccole micro-aziende, sono tra gli obiettivi preferiti degli hacker.

Il rapporto di Assintel evidenzia inoltre un aumento del ricorso al malware, raggiungendo il 70% degli attacchi totali nel 2023. Gli impatti degli attacchi cyber preoccupano gli esperti: il 91% degli attacchi del 2023 viene classificato come grave o gravissimo e quelli con impatti critici rappresentano il 24%, evidenziando ripercussioni significative in termini economici, legali e di reputazione per le vittime.

Il settore manifatturiero è stato il più colpito, passando dal 5% al 16% degli attacchi totali nel 2023, seguito dal settore professionale scientifico tecnico, Ict, sanitario e finanziario e assicurativo.

Tra le tecniche più utilizzate c'è il malware, che ha raggiunto il 70% del totale degli attacchi, seguito dall'utilizzo di vulnerabilità e tecniche sconosciute. Quasi un quarto degli attacchi ha avuto impatti critici, mentre il 67% ha avuto impatti gravi.