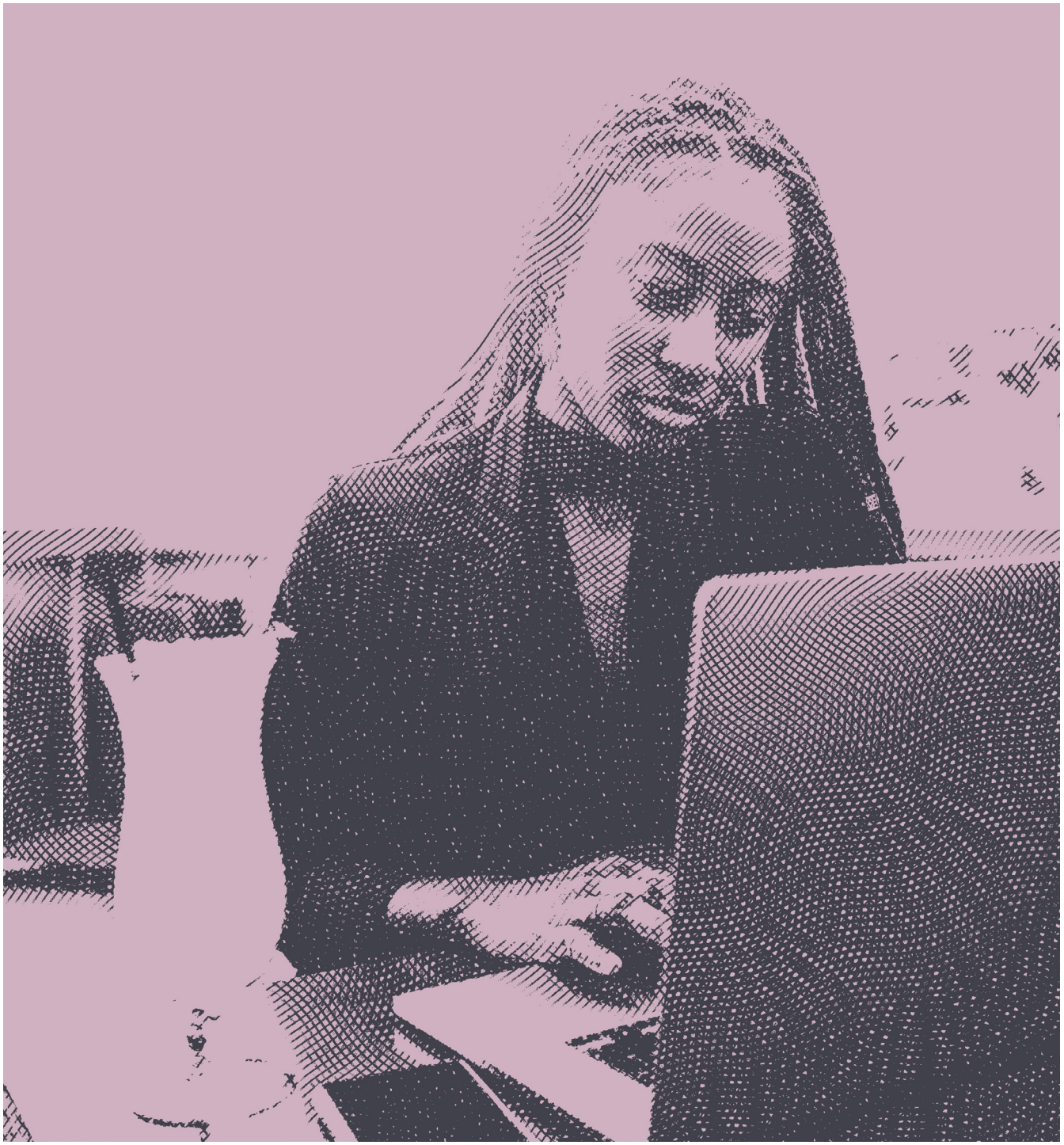
Okta Digital Trust Index

Esplorare la fiducia in un mondo in rapido cambiamento



okta

Sommario

> La fiducia è una scommessa umana.
>
> Maria Michela Marzano, Avere Fiducia, Mondadori, 2014

Introduzione

La fiducia inizia dalla sicurezza

Gli eventi del 2020 hanno messo in primo piano il concetto di fiducia nelle nostre vite. Quasi da un giorno all'altro, hanno trasformato la fiducia nei governi e nelle istituzioni in una questione significativa per la maggior parte delle persone; hanno reso la fiducia dei clienti nei brand estremamente importante per i profitti in un periodo di grave recessione economica; hanno condotto molte organizzazioni a superare obiezioni di lunga data, dando fiducia ai propri dipendenti per il lavoro da casa, trasformando i canali digitali nell'unico mezzo per offrire un servizio ai propri clienti.

Tutto ciò si inserisce in un contesto di crescenti preoccupazioni per la sicurezza, innescate da quantità di violazioni dei dati e da minacce informatiche mai viste prima, da una rigorosa applicazione normativa della legislazione sulla protezione dei dati, da truffe opportunistiche di ingegneria sociale e da livelli di privacy verso cui i consumatori hanno aspettative sempre più alte.

Secondo una valutazione INTERPOL, le frodi di phishing sono aumentate del 59% dopo la pandemia, insieme all'aumento di malware, ransomware, domini malevoli e notizie false: un segno di come i criminali cercano di sfruttare la paura e l'incertezza causate dalla situazione sociale ed economica.

Per le aziende, la sicurezza inizia con la fiducia. Vale a dire che, perché la sicurezza sia effettivamente tale, è necessario innanzitutto comprendere, come organizzazione, di quali dipendenti, partner e clienti al di fuori del perimetro tradizionale e centrato sull'ufficio ci si può fidare, fornendo loro accessi a dati e sistemi sensibili.

Tuttavia, è vero anche il contrario: la fiducia inizia con la sicurezza. In altre parole, il modo migliore per stimolare la fiducia tra i principali stakeholder è quello di offrire strumenti e policy di sicurezza efficaci, in particolare quelle focalizzate sulla gestione continua dell'identità degli utenti. Questa è la via più rapida per aumentare la produttività e costruire fedeltà e impegno, non solo tra i dipendenti e i partner, ma anche tra i clienti.

Per saperne di più, Okta ha condotto questa nuova indagine su oltre 13.000 impiegati, di cui oltre 2.000 nel Regno Unito, a cui ha chiesto di rispondere alle seguenti domande:

Quanta della nostra fiducia è costruita, mantenuta e tradita nel mondo digitale?

Al di fuori dei legami umani, quanto ci fidiamo quando ci rapportiamo solo attraverso i nostri schermi?

I brand, le aziende e i governi fanno abbastanza per costruire la fiducia?

Quali fattori esterni stanno cambiando la nostra disponibilità a fidarci attraverso i canali digitali?

Metodologia:

Tutti i dati, salvo diversamente specificato, sono di YouGov Plc. Il campione totale è stato di 13.163 impiegati provenienti da Regno Unito, Stati Uniti, Australia, Germania, Francia, Italia, Spagna, Svezia, Paesi Bassi e Giappone.

Tra questi, 2.041 impiegati provenivano dal Regno Unito. Il lavoro sul campo è stato svolto tra il 26 novembre e il 10 dicembre 2020. Il sondaggio è stato effettuato online.

Ciò che segue è l'Okta Digital Trust Index, il nostro report che esplora il confine umano della fiducia digitale in un mondo sempre più modellato dagli effetti della pandemia. Concludiamo con le raccomandazioni per i singoli, le aziende e gli enti pubblici su come costruire e trasmettere una fiducia reale e umana.

> La fiducia arriva a piedi, ma se ne va in Ferrari.
>
> Mark Carney, governatore della banca centrale canadese

Sezione uno

Cosa porta i consumatori a fidarsi dei brand?

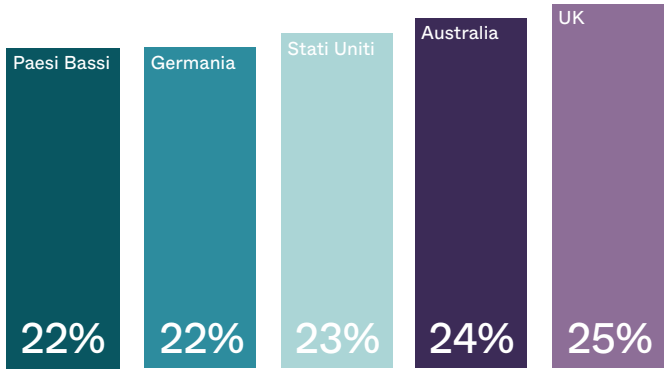
Nel 2020, con l'inevitabile passaggio al telelavoro, gli impiegati sono diventati degli esperti digitali, trascorrendo molto più tempo e spendendo molto più denaro online. **Nel 2020, sono 46,5 milioni i consumatori multicanale italiani, cioè gli utenti che hanno usufruito di servizi di eCommerce o per i quali il digitale ha un ruolo nel proprio percorso di acquisto, +6% rispetto all'anno precedente**.

Il 2021 è l'anno di transizione verso pratiche online più istituzionalizzate, e i marchi sono chiamati a costruire con sicurezza nuovi modelli di fiducia e fedeltà con i loro stakeholder.

Oggi la fiducia si conquista con fatica, ma si perde facilmente, e sebbene i valori etici siano sempre più apprezzati da azionisti, investitori e consigli di amministrazione, abbiamo scoperto che quando si tratta di clienti, è più importante che a essere solide siano le basi.

Circa il 38% degli intervistati dell'Italia ha dichiarato che l'affidabilità del servizio, come la garanzia che gli articoli arrivino in tempo e in buone condizioni, è il criterio che più li spinge a riporre la propria fiducia in un marchio digitale.

Anche la sicurezza è fondamentale: il 15% ha affermato che l'esistenza di opzioni di accesso sicure, come l'autenticazione multifattoriale (MFA) e altre misure in atto, contribuisce ad alimentare la fiducia nel marchio. Questo bisogno di sicurezza è emerso anche dagli intervistati in Australia (24%), negli Stati Uniti (23%), in Germania (22%) e nei Paesi Bassi (22%).



Percentuale delle persone intervistate che credono che avere un sistema di sicurezza aggiuntivo come MFA – autenticazione multifattore – possa aumentare la fiducia nei confronti di un brand.

Le violazioni pesano

Ciò non vuol dire che l'etica non abbia alcuna importanza: il 6% degli intervistati in Italia ha citato questo come fattore il più importante nella fiducia. L'etica svolge un ruolo importante anche quando i consumatori devono decidere a quali marchi non affidarsi, in particolare in termini di "etica dei dati".

I due principali comportamenti citati dagli intervistati italiani che li rendono più propensi a diffidare di un marchio, sono l'abuso o la vendita intenzionale di dati personali (29%) e l'affidabilità del servizio (15%).

Entrambi non rappresentano solo una questione etica per i marchi digitali, ma sono anche pratiche che metterebbero in allarme le autorità garanti ai sensi del GDPR in Italia. Per sfuggire all'ira dei clienti e a una potenziale grave perdita di reputazione e di risorse finanziarie, le organizzazioni devono garantire che la sicurezza dei dati sia adeguata, iniziando con una gestione dell'identità basata sulle migliori pratiche.

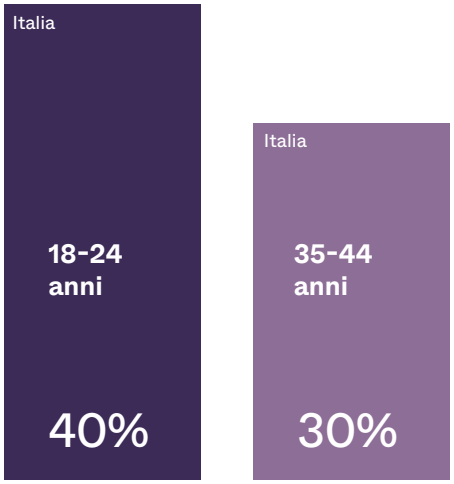
L'uso improprio intenzionale o la vendita di dati sono due comportamenti similmente capaci di generare diffidenza nei confronti di un marchio da parte di tutti gli altri mercati. Ma mentre le violazioni dei dati sono state la seconda maggiore fonte di preoccupazione per gli intervistati in paesi come l'Australia (16%), gli Stati Uniti (15%) e i Paesi Bassi (13%), i disagi o gli errori sono stati un fattore più importante nella perdita della fiducia per gli intervistati in Francia (23%), Spagna (21%) e Svezia (16%). Un altro forte richiamo al fatto che, mentre l'etica dei dati rimane della massima importanza, un servizio clienti sempre presente non deve essere dimenticato.

Quando la fiducia viene meno

È chiaro che la fiducia è vitale per i marchi digitali, per avere successo nell'attuale panorama di business altamente competitivo.

Il 72% degli intervistati italiani ha dichiarato che difficilmente acquisterebbe da un'azienda di cui non si fida.

Il 51% degli intervistati non crede che le immagini caricate sul sito web corrispondano al prodotto reale.



Percentuale di intervistati che ha smesso definitivamente di usare i servizi di un'azienda a seguito di una violazione.

Una volta guadagnata la fiducia, i marchi devono essere consapevoli che dovranno lavorare sodo per mantenerla, e che un'ottima sicurezza informatica è la chiave per farlo. Il 40% degli intervistati italiani ha dichiarato di aver perso fiducia in un'azienda a causa di una violazione dei dati o simili, con un dato ancora più alto negli Stati Uniti (56%).

A seguito di un simile evento, il 38% degli utenti italiani ha smesso definitivamente di utilizzare i servizi dell'azienda, e il 37% ha cancellato il proprio account presso la medesima. Il 36% ha, invece, hanno modificato le impostazioni utente, come password e indirizzi e-mail, evidenziando l'importanza di un login sicuro per mantenere la fiducia.

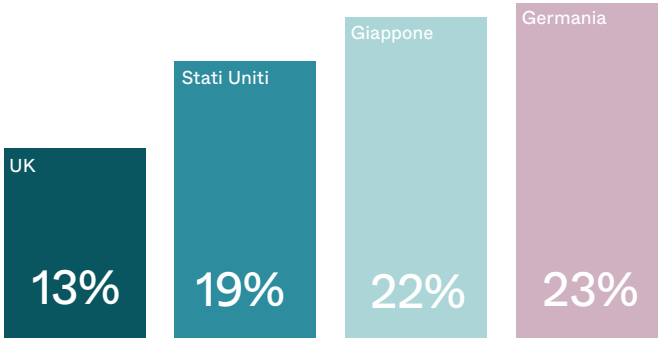
È interessante notare che gli intervistati più giovani dell'Italia hanno una minore tolleranza per la cattiva gestione dei dati e una sicurezza scadente dei marchi presso cui fanno acquisti. Circa il 40% dei giovani tra i 18 e i 24 anni ha dichiarato di aver smesso definitivamente di utilizzare i servizi di un'azienda in seguito a una violazione, contro il 30% dei 35-44enni.

Dato che le giovani generazioni diventeranno il motore della crescita economica di domani, i marchi devono garantire che le loro priorità di business siano allineate con queste crescenti aspettative in termini di sicurezza informatica.

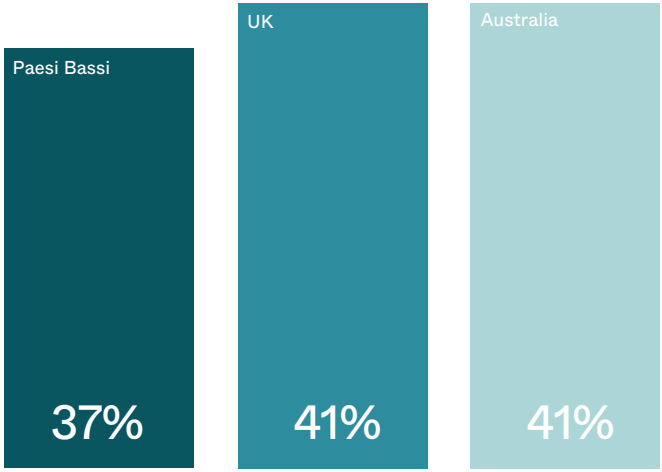
> Le generazioni più giovani diventeranno i decision-maker del futuro, quindi è importante predisporre tutto affinché sia garantito un buon servizio, e la sicurezza informatica è al centro delle operazioni per allineare le esigenze dei clienti con le priorità di business.
>
> Jesper Frederiksen, VP e GM EMEA, Okta

C'è molto lavoro da fare

C'è ancora molto lavoro da fare Una significativa minoranza (11%) degli intervistati italiani ha dichiarato di credere che nessun canale digitale gestisca i dati in modo sicuro, analogamente a quanto avviene in Germania (23%), Giappone (22%) e Stati Uniti (19%). Ed è chiaro che le app per la comunicazione sul posto di lavoro (13%) sono ritenute più affidabili di quelle personali (4%).



Percentuale degli intervistati che non ha fiducia in nessun canale digitale per la custodia dei loro dati.



Percentuale degli intervistati che hanno fiducia dei siti web governativi.

Il più affidabile tra tutti i canali digitali in Italia è il sito web governativo (28%), cosa percepita nello stesso modo dagli intervistati in Australia (41%) e nei Paesi Bassi (37%). Si tratta senza dubbio di un fatto positivo. Nonostante le preoccupazioni iniziali sulla gestione dei dati personali e relativi al COVID-19 dei cittadini, non ci sono state finora violazioni di rilievo, e un controllo continuo sembra essere alla base di un miglioramento degli standard di sicurezza dei dati.

> Ottimo che la gente si fidi dei siti web governativi per la gestione dei propri dati più che di ogni altro canale digitale. È importante che il governo continui a dare priorità alle misure di sicurezza informatica e a mantenere i dati dei cittadini al sicuro.
>
> Dott.ssa Jessica Barker

Sezione due

Come la pandemia ha cambiato i comportamenti degli utenti

Il 20% degli intervistati in Italia ha dichiarato di lavorare spesso da casa, e questi stessi dipendenti richiederanno una maggiore flessibilità nelle politiche di telelavoro una volta che la crisi sarà passata.

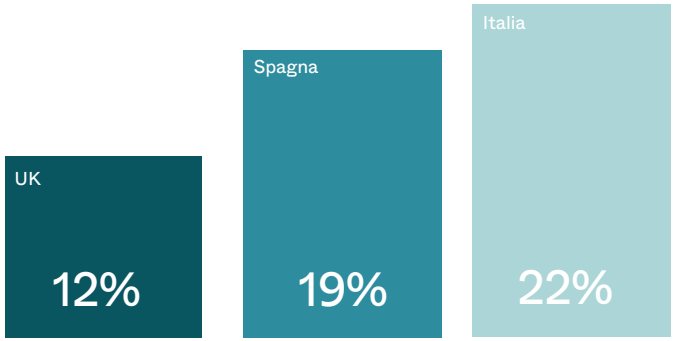
Eppure, benché chiusi in casa, molti sono stati esposti a un aumento delle minacce informatiche, volte a rubare sia i dati di accesso aziendali che quelli relativi all'identità personale.

Il phishing è diventato la tattica preferita da molti hacker nel 2020. Hanno avuto grande successo usando come esca informazioni sui vaccini COVID-19, o aggiornamenti urgenti (ma falsi) da istituzioni affidabili come l'OMS, inducendo così i destinatari a cliccare. **Già in aprile, solo Google ha dichiarato di** bloccare 18 milioni di e-mail giornaliere di malware e phishing relative al COVID-19.

Di conseguenza, probabilmente non sorprende che il 42% degli intervistati italiani abbia dichiarato di essere diventato più cauto nel fornire informazioni personali online, mentre appena il 3% afferma di essere meno cauto nel farlo. Il telelavoro ha inoltre reso gli intervistati più consapevoli nei confronti delle e-mail di phishing (37%), delle violazioni di dati (41%) e persino dei "deepfake" generati dall'IA e utilizzati per diffondere informazioni false (36%).

Gli intervistati ritengono di essere più esposti al rischio di furto d'identità (24%), il che è comprensibile dato l'aumento degli attacchi phishing a cui molti sono stati sottoposti.

I malware (15%) e le violazioni dei dati (10%) completano il quadro delle tre principali fonti di preoccupazione.



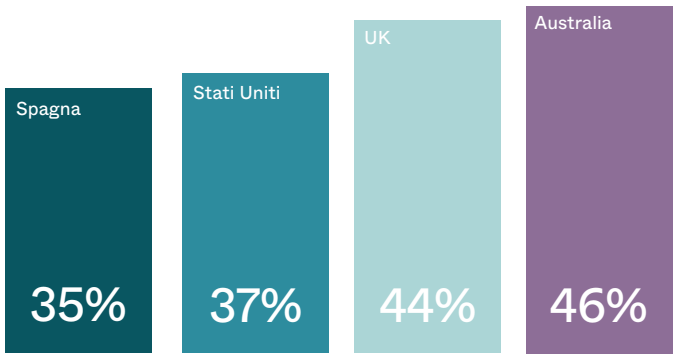
Percentuale di intervistati preoccupati per il furto della password.

Gli impiegati in Italia (22%) e in Spagna (19%) si sono sentiti molto più a rischio circa il rischio del furto di password, dimostrando che la transizione verso l'autenticazione senza password si renderà necessaria. Vale la pena ricordare che un individuo può essere esposto a minacce informatiche non solo attraverso attacchi mirati a lui stesso e ai propri dispositivi, ma anche ai propri coinquilini, che possono adottare comportamenti a rischio online.

> "Le possibilità di minaccia quando si lavora da casa sono aumentate per molteplici ragioni complementari. Le persone si sono ritrovate a condividere dispositivi e reti domestiche nonché spazi fisici, aumentando il rischio e compromettendo la riservatezza di materiali scritti e chiamate audio. Gli attuali "colleghi" possono variare da familiari fidati a coinquilini poco conosciuti, mentre la sicurezza di avere colleghi e un helpdesk IT a portata di mano viene meno. Inoltre, i modelli comportamentali e di sicurezza adottati in precedenza dai lavoratori possono essere inconsciamente compromessi, soprattutto quando devono destreggiarsi tra impegni lavorativi e domestici.
>
> Ben King, CSO EMEA, Okta

È ora di essere trasparenti

La motivazione principale addotta dagli intervistati italiani per la loro maggiore cautela online è l'aver cercato più informazioni o letto termini e condizioni durante la pandemia (36%) mentre il 23% ha notato una maggiore copertura mediatica sull'argomento, la stessa ragione che ha reso più cauti gli intervistati in Australia (46%), negli Stati Uniti (37%) e in Spagna (35%). Il ruolo dei mass-media è senza dubbio importante nell'educazione del pubblico; al contempo, emerge una chiara opportunità per i marchi digitali di migliorare la consapevolezza di tali problematiche tra i clienti, costruendone così la fiducia. Combinando questi sforzi con strumenti come l'MFA, si può trasmettere un maggiore senso di sicurezza ai consumatori ansiosi, aumentando le entrate e attuando una differenziazione competitiva.



Percentuale degli intervistati che hanno evidenziato una copertura mediatica sull'argomento durante la pandemia.

Anche i datori di lavoro giocano un ruolo in tutto ciò. Sensibilizzando le persone, aggiornando le tecnologie legacy che possono essere vulnerabili alle minacce online e dimostrando l'efficacia delle misure di sicurezza, come gli anti-malware endpoint, possono dare ai dipendenti la certezza di essere protetti sia a casa che in ufficio. Così non ci si limita solo ad avvantaggiare indirettamente marchi digitali terzi, ma i benefici si estendono anche alla propria organizzazione: aumentare la fiducia negli strumenti che i dipendenti utilizzano per il telelavoro contribuirà in ultima analisi ad aumentare la produttività.

Sezione Tre

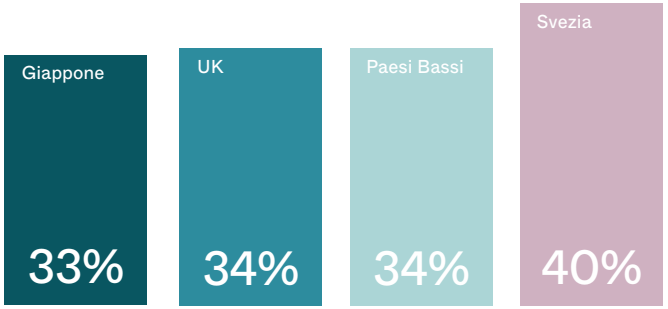
Come stanno rispondendo le organizzazioni?

Molti datori di lavoro hanno effettivamente adottato misure per affrontare la crescita delle minacce informatiche che gravano sui dipendenti che lavorano da casa. Le nuove applicazioni e tecnologie di sicurezza, come l'MFA, (32%) si sono rivelate la misura più popolare, seguita da una maggiore formazione del personale (22%). Entrambe sono di vitale importanza per contribuire a rafforzare la fiducia dei dipendenti, elemento fondamentale per le aziende di successo.

Tuttavia, più preoccupante è il fatto che il 25% degli intervistati ha affermato che il proprio datore di lavoro non ha fatto nulla finora per combattere un'ondata di minacce online legate alla pandemia. La cosa è ancora più marcata nel settore legale (34%) e Vendita al dettaglio (33%).

> Nei settori che non sono nativi del digitale, i dipendenti spesso si trovano a lavorare da una base tecnica inferiore, il che significa che potrebbero non notare o riflettere sui controlli aggiunti per combattere i rischi online. Coloro che hanno tradizionalmente affrontato livelli più elevati di minacce informatiche, come banche, tecnologia e vendita al dettaglio, hanno probabilmente avuto anche un budget per la sicurezza proporzionalmente più elevato rispetto ad altri settori intervistati. In tutti i settori, i CIO e i CSO hanno dovuto dividere il loro tempo tra il supporto di esigenze specifiche del settore e le richieste di sicurezza, due compiti spesso molto diversi.
>
> Ben King, CSO EMEA, Okta

Inoltre, il 19% degli impiegati ci ha detto di non sapere se il loro datore di lavoro avesse adottato misure di sicurezza proattive, con cifre più alte in Svezia (40%), nei Paesi Bassi (34%) e in Giappone (33%).
La cosa è particolarmente deludente in quanto indica una mancanza di trasparenza e fiducia tra i responsabili business, quelli IT e i loro dipendenti.
Si possono gestire i migliori sistemi di sicurezza informatica del mondo, ma se il personale non ne è a conoscenza, la propria azienda non sarà in grado di promuovere una maggiore fiducia.



Percentuale degli intervistati che non sanno se i lori datori di lavoro hanno preso ulteriori misure di sicurezze.

> Gli hacker imparano sempre nuovi trucchi, e i dipendenti ne sono consapevoli, tanto che molti diventano sempre più cauti nei confronti del phishing, delle violazioni dei dati e dei nuovi rischi, come le truffe deepfake. Le aziende devono quindi assicurarsi di essere il più avanti possibile e combattere queste nuove minacce con nuovi approcci.
>
> Ben King, CSO EMEA, Okta

È chiaro che, se non l'hanno già fatto, i responsabili IT devono iniziare a sviluppare soluzioni di gestione delle identità continue e basate sul rischio per ottenere, nel 2021, una sicurezza basata sulla fiducia, e per migliorare la produttività del personale e ridurre al minimo il rischio informatico. Inoltre, devono essere più trasparenti riguardo a qualsiasi nuova tecnologia e alle policy di sicurezza che sono state progettate a supporto della medesima.

Sezione Quattro

Conclusioni e raccomandazioni

IDC definisce la fiducia come la condizione che "consente di prendere decisioni tra due o più entità, riflettendo il livello di fiducia tra di loro" ed è un "innalzamento del dialogo sulla sicurezza per includere attributi quali il rischio, la conformità, la privacy e persino l'etica aziendale". È un concetto che oggi nessun responsabile IT o business può ignorare, poiché la trasformazione digitale aumenta gli obiettivi degli attacchi informatici e contemporaneamente apre nuovi canali per coinvolgere i clienti e supportare i dipendenti. Se ottenuta nel modo giusto, la fiducia non solo mitigherà il danno, ma incrementerà le entrate e il valore per le organizzazioni.

Nell'impresa si inizia con un approccio Zero Trust incentrato sull'identità e sull'obiettivo finale delle policy di accesso basate sul rischio, dell'autenticazione continua e adattiva e dell'accesso frictionless.

La pandemia ha sottolineato la necessità di tali approcci, in modo che le organizzazioni possano fidarsi del fatto che i loro utenti da remoto siano chi dicono di essere, dato che gli hacker cercano sempre più di infiltrarsi nelle reti aziendali. È necessario inoltre promuovere la fiducia tra i dipendenti in modo che possano lavorare in modo più produttivo.

Ma la nozione di fiducia si estende anche alle interazioni con i clienti. Le odierne aziende digitali devono costantemente coltivare questa fiducia, proponendosi come amministratori responsabili dei dati dei clienti. In questo modo si raggiungeranno fedeltà e successo, nonostante i furti di dati e di identità siano aumentati durante la pandemia. Anche in questo contesto, la fiducia inizia con la sicurezza, con l'identità come pilastro centrale: ossia i marchi digitali devono fornire ai loro clienti gli strumenti necessari per l'autenticazione continua e sicura.

Le nostre principali raccomandazioni

I responsabili business e IT devono essere trasparenti con i dipendenti che lavorano a distanza sulle misure di sicurezza informatica e sulle politiche che stanno attuando, così da promuovere la fiducia e il buy-in del personale.

Nuovi strumenti di sicurezza come l'MFA e la biometria per l'autenticazione senza password sono vitali per la protezione contro i furti di identità dei consumatori, e per garantire l'accesso da remoto ai dipendenti..

È necessaria una maggiore formazione interna sulla protezione dal phishing e sulle migliori pratiche di sicurezza per mitigare i rischi del lavoro a distanza.

Bisogna mantenere aggiornata la propria strategia di sicurezza per garantire che tenga conto di un panorama di minacce in continua evoluzione, del contesto normativo e dell'attitudine alla fiducia.

Bisogna dimostrare l'efficacia delle misure di sicurezza a chi lavora da remoto, per dare loro la certezza di essere protetti sia a casa che in ufficio.

I governi e i servizi digitali devono continuare a dare priorità alle misure di sicurezza informatica e relativa alla privacy per mantenere i dati dei cittadini al sicuro durante la pandemia e nella nuova normalità.

L'etica dei dati è importante per i clienti, per cui le aziende devono garantire il rispetto delle linee guida normative, prevenendone l'uso improprio e riducendo il rischio di violazioni.

È necessario assicurarsi che la propria organizzazione soddisfi le maggiori aspettative in termini di sicurezza e privacy dei consumatori più giovani, per favorire la fidelizzazione di un gruppo economicamente importante.

"

La fiducia è un impulso umano - prezioso, benefico e rischioso - e come molti dei nostri impulsi, può sembrare difficile da capire.

Questa affascinante ricerca ci aiuta a comprendere la fiducia digitale in un momento in cui il mondo sta cambiando rapidamente e la nostra percezione di fiducia è stata sconvolta anche riguardo qualcosa di semplice, come la stessa aria che respiriamo. Questi risultati mostrano che le persone non si fidano delle parole, ma si fidano dei fatti. Dal punto di vista della cybersecurity, ciò rafforza l'importanza di una sicurezza forte come fattore abilitante per il business, in un momento in cui la continuità e la resilienza del settore informatico sono così importanti. I risultati sottolineano anche l'importanza della fiducia nella cultura della sicurezza: la necessità per le organizzazioni di essere trasparenti con dipendenti, clienti e media non è mai stata così evidente. I leader non possono ignorare la fiducia, o loro e le loro organizzazioni saranno lasciati indietro.

Dott.ssa Jessica Barker

Sezione Cinque

Rendere sicura l'impresa del futuro con Okta

L'identità è la base per costruire organizzazioni sicure e basate sulla fiducia. Con Okta Identity Cloud, i leader aziendali di tutto il mondo possono creare con fiducia le migliori esperienze digitali per i loro dipendenti e clienti.

Mettete al sicuro i vostri collaboratori, ovunque si trovino, con le **soluzioni Okta per l'identità dei dipendenti**. Ottenete gli strumenti per rendere sicuro e automatico l'uso del cloud, con pieno supporto per gli ambienti ibridi.

Utilizzate le **soluzioni per identità dei clienti** di Okta per costruire un'esperienza sicura e continua, che i vostri sviluppatori e utenti adoreranno.

Informazioni su Okta

Okta è il principale fornitore indipendente di identità per l'impresa. Okta Identity Cloud consente alle organizzazioni di collegare in modo sicuro le persone giuste alle tecnologie giuste e al momento giusto. Con oltre 6.500 integrazioni pre-costruite ad applicazioni e fornitori di infrastrutture, i clienti Okta possono utilizzare in modo semplice e sicuro le migliori tecnologie per il loro business. Oltre 9.400 organizzazioni, tra cui Engie, JetBlue, Nordstrom, Takeda Pharmaceutical, Teach for America, T-Mobile e Twilio si affidano a Okta per proteggere l'identità dei loro dipendenti e dei loro clienti.

Okta.com