Quanto vengono percepite come spiacevoli le esperienze di autenticazione del cliente nei vostri istituti di servizi finanziari.

E cosa potete fare, in qualità di responsabili dell'esperienza del cliente.

eBook
Ripensare all'autenticazione del cliente

State perdendo il sonno per l'autenticazione dei clienti?

Non siete gli unici.

Se siete i responsabili dell'esperienza del cliente presso la vostra organizzazione, o la vostra funzione ha a che fare con l'autenticazione del cliente, è altamente probabile che questo processo vi faccia passare notti insonni.

Dopo tutto, il modo in cui un istituto di servizi finanziari verifica l'identità del cliente è fondamentale per come i clienti percepiscono il vostro brand. E se queste la loro esperienza si rivelano tutt'altro che positiva, i clienti potrebbero velocemente passare alla concorrenza.

Non siete però gli unici ad essere preoccupati. I processi di autenticazione, basati su conoscenza e token, ormai obsoleti, possono compromettere l'esperienza del cliente e provocano non pochi problemi anche ai responsabili della vostra azienda che si occupano del contact centre e ai responsabili dellaprevenzione delle frodi.

Nel corso delle prossime pagine, scopriremo come molti dei vostri problemi possano essere risolti, perché ricondotti ad unaorigine comune.

Vedremo anche perché vale la pena riunire tutte le parti coinvolte per ripensare la vostra strategia di identità e verifica (Identity and Verification: ID&V)– e parleremo dei vantaggi che tutti potrebbero ottenere passando a un processo di autenticazio ne più semplice e più sicuro: implementando la biometria vocale.

1 Gartner, tramite ID R&S, nel report sulla biometria come operazione di salvataggio.

Il 96%

dei clienti perde la fiducia o l'interesse in una compagnia quando leinterazioni con i servizi di cui hanno bisogno richiedono uno sforzo spropositato.

Gartner[1]

La "piramide del dolore" dell' autenticazione

Ogni volta che un cliente dimentica la sua password o è vittima di una truffa, la sua frustrazione e angoscia creano un effetto domino che ricade su tutta la compagnia.

Il 77%

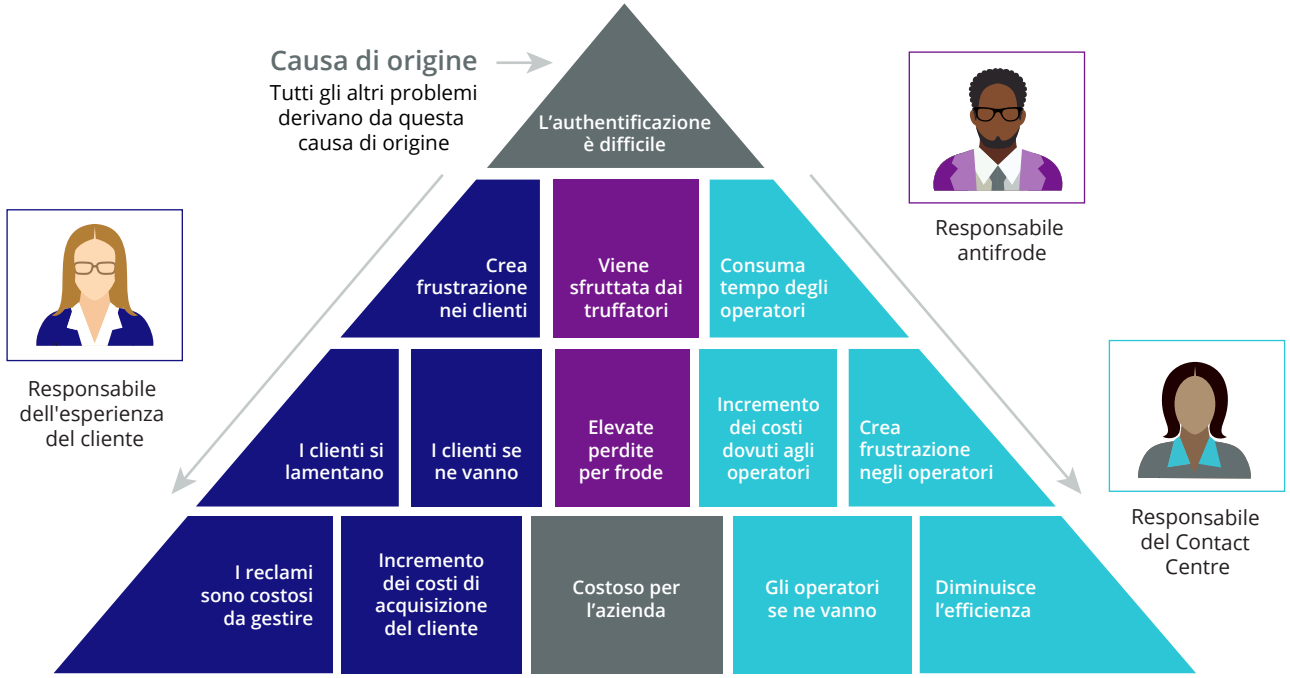
dei clienti voglia cambiare il provider di servizi[2]

Il dolore che provate *voi*

Le esperienze di autenticazione lente e difficili creano frustrazione nei clienti. Generano reclami che,al giorno d'oggi, sono spesso fatti circolare pubblicamente sui social media, e la vostra organizzazione deve dedicare tempo e risorse per rispondere con la dovuta sensibilità e velocità.

Peggio ancora, la frustrazione del cliente può convincerlo ad abbandonare per sempre la vostra compagnia. PwC segnala che un'unica interazione frustrante con un operatore è sufficiente a far sì che il 77% dei clienti voglia cambiare il provider di servizi.[2]

Per aggiungere dolore al dolore, è anche più difficile conquistare nuovi clienti quando le altre compagnieli possono tentare con esperienze di autenticazione più semplici, basate su tecnologie più moderne. La concorrenza in questo settore è sempre più feroce, con il 96% delle aziende che ora vede la verifica dell'identità come un valore di differenziazione fondamentale.[3]



2 PwC, sondaggio 2017 "L'esperienza è tutto", Ricerca completata nel 2018.
3 IDology 7th Annual Fraud Report (IDologia, 7° report annuale sulle frodi), ottobre 2019.

I problemi per i responsabili antifrode

I problemi che derivano dal lavorare con processi di autenticazione obsoleti sono sofferti altrettanto profondamente all’interno del team antifrode.

L’autenticazione basata sulla conoscenza richiede ai vostri operatori di lavorare come se fossero i guardiani della sicurezza. Anche un operatore con molta esperienza può subire un attacco tramite ingegneria sociale per mano di un truffatore esperto, consentendo così consenteaccesso criminale all’account di un cliente, o a informazioni personali che potranno essere utilizzate in attacchi successivi.

Molti criminali, però, non avranno bisogno di ingannare i vostri operatori per farsi rivelare informazioni sensibili:le avranno già acquistate nel dark web.

Anche se manca la password di un cliente, potrà probabilmente essere decifrata. Una recente analisi su >1 miliardo di credenziali trapelate, tra cui 168.919.919 password, ha riscontrato che il 42% di tali credenziali era vulnerabile ad attacchi non complessi e veloci come gli “attacchi dizionario”. E 1 su 142 password era “123456”.[5]

15
miliardi

Online, sono in vendita 15 miliardi di combinazioni nome utente-password di account, inclusi conti bancari.[4]

L’autenticazione basata su token – per esempio, che invia un codice al telefono del cliente – ha anch’essa i suoi problemi. Un truffatore con accesso all’account mobile del cliente può semplicemente scambiare il suo numero con un’altra SIM prima di attaccare.

La morale è questa: le tecnologie tradizionali di autenticazione vengono raggirate troppo facilmente, il che comporta elevati costi di prevenzione delle frodi e ingenti perdite in termini di frodi.

4 Ombre digitali studio segnalato tramite ZDNet, luglio 2020.
5 Segnalazione di ZDNet su un’analisi di >1 miliardo di credenziali trapelate che comprendevano 168.919.919 password, luglio 2020.

I problemi per i responsabili del contact centre

Porre domande di autenticazione basate sulla conoscenza richiede tempo: per alcune organizzazioni, richiede tra i due e i sette minuti.[6] Inoltre, fa sentire gli operatori del contact centre come degli investigatori e temono le conseguenze di non aver individuato un criminale.

Il risultato è un tempo medio di gestione (Average Handle Time: AHT) lungo e operatori scontenti e preoccupati. Il che, come potete immaginare, è l'ultima cosa che la persona incaricata di gestire un contact centre efficiente e produttivo vorrebbe vedere.

La durata di ogni conversazione con un cliente riduce l'efficienza dell'operatore e aumenta i costi legati al personale. Il morale basso degli operatori, nel frattempo, aumenta le possibilità ricambio degli operatori stessi. Oltre ai costi di acquisizione dei nuovi operatori per il contact centre, questo porta a una forza lavoro di nuovi operatori meno esperti , e ha, in ultima analisi, anche a un impatto sull'esperienza del cliente.

Con un numero crescente di interazioni con il cliente che stanno passando online, i responsabili dei contact centre hanno bisogno anche di un modo più efficiente per autenticare i clienti attraverso i vari canali; il 65% dei responsabili delle frodi riferiscono che gli attacchi ai canali digitali stanno creando costi aggiuntivi al contact centre, dovuti anche all'aumento dei volumi di richieste e incidenze che si accumulano aspettando una soluzione.[7]

Il problema finanziario che subisce la vostra azienda (un ottimo motivo per risolvere questa situazione insieme)

Riassumendo: un processo di autenticazione problematico contribuisce a creare:

- Costi per i reclami del cliente
- Costi di acquisizione di clienti
- Costi per la prevenzione delle frodi
- Perdite a causa delle frodi (e danni alla reputazione del brand)
- Costi operativi del contact centre
- Costi di acquisizione degli operatori

In poche parole, è estremamente costoso per la vostra azienda in generale..

Ecco però la buona notizia: come responsabili dell'esperienza del cliente, siete nella posizione perfetta per guidare il cambiamento e indirizzare benefici che si faranno sentire in tutto il vostro istituto di servizi finanziari.

6 Tempistiche basate sulle conversazioni con clienti di Nuance.
7 Studio Nemertes condotto nell'aprile 2020.

26%

Le aziende che riescono a tenere il ricambio degli operatori a <15% vedono un miglioramento del 26% nelle valutazioni dei clienti.[7]

Perché così tante compagnie leader del settore stanno passando all'autenticazione biometrica ?

Il problema fondamentale con i processi di autenticazione tradizionali è facile da capire: identificano le persone in base a quello che conoscono, o a quello che hanno, piuttosto che in base a chi sono realmente.

L'autenticazione biometrica affronta proprio questa questione. Utilizza infatti le caratteristiche *uniche* dei vostri clienti – le impronte digitali, il volto, il modo in cui usano il dispositivo, il modo in cui digitano, il suono della loro voce –per confermare la loro identità.

La biometria vocale, con la sua facilità di utilizzo e il suo elevato grado di precisione, sta diventando una soluzione sempre più popolare tra i principali istituti di servizi finanziari.

Una volta che il cliente ha registrato la sua "impronta vocale", la sua identità può essere verificata automaticamente in pochi secondi, sia che stia parlando con un operatore umano o con un IVR, o con un'applicazione mobile. Il cliente non deve ricordare una password né deve richiedere un codice OTP. E l'operatore non deve "giocare all'investigatore". Entrambi possono concentrarsi sul compito che devono portare a termine.

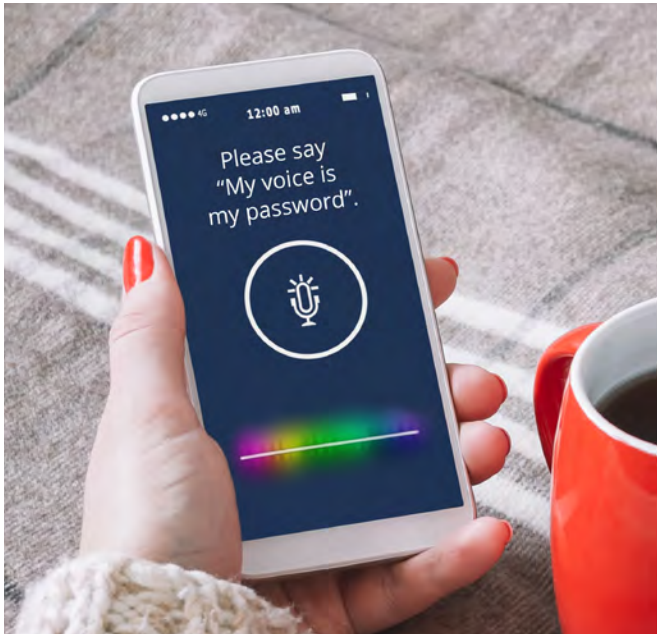
E c'è di meglio, è possibile utilizzare la biometria vocale per identificare in modo proattivo i criminali già noti, confrontando la loro voce con una "lista di controllo" di impronte vocali di frodatori seriali.

Proprio come un processo di autenticazione lento e debole provoca problemi durante un'operazione, la velocità e la sicurezza della biometria vocale possono portare innumerevoli benefici alla vostra azienda.

8 Intervista con il Responsabile antifrode globale e Responsabile dell'innovazione della produzione ID alla Experian, febbraio 2020.

L'81%

dei clienti considera la biometria come una forma più sicura di verifica dell'identità.[8]



I vantaggi per voi: un’esperienza cliente di livello superiore

Le soluzioni di autenticazione vocale possono essere “attive” o “passive”. Se sono attive, il cliente deve dire una semplice e specifica frase per far verificare la sua identità. Se sono passive, la soluzione ascolta l’inizio della conversazione tra il cliente e l’IVR o l’operatore, autenticando perfettamente il cliente in background, senza interruzioni. In ogni caso, è un’esperienza veloce, facile e sicura.

L’autenticazione vocale consente di gestire un volume molto più ampio di chiamate nella vostra IVR, accorciando i tempi di attesa dei clienti. Quando un cliente ha bisogno di parlare con un operatore, questa diventa un’interazione più semplice, più efficiente e meno problematica: il cliente non deve scervellarsi per ricordarsi una password, e l’operatore può rilassarsi e concentrarsi su come aiutare il cliente, entrambi sapendo di essere tutelati dalle frodi di ingegneria sociale.

Inoltre, il maggior livello di sicurezza garantito dall’autenticazione vocale consente a una compagnia di estendere la gamma di operazioni che un cliente può portare a termine senza dover ricorrere a un operatore umano. Per un istituto di servizi finanziari, una scelta popolare è per esempio dare supporto solo a transazioni a rischio più elevato, come l’impostazione di un nuovo beneficiario, mentre altre operazioni più quotidiane non hanno bisogno del lavoro attivo di un agente.

Il miglioramento delle esperienze grazie alla biometria vocale alla Barclays

— La soddisfazione del cliente e dell’operatore è aumentata

— Il 93% dei clienti ha attribuito un punteggio di 9 o 10 (su 10) al sistema di identificazione e verifica biometrica

— 90% di riduzione dei reclami

CSAT e ASAT

“L’utilizzo della tecnologia biometrica vocale di Nuance è entrata a far parte integrante della nostra missione, volta ad offrire un’esperienza eccellente al cliente. I risultati di soddisfazione del cliente e dei dipendenti parlano da soli. Non vediamo l’ora di lavorare con Nuance in futuro, per poter utilizzare la biometria vocale per validare ancora più processi e operazioni”.

— Anne Grim
Responsabile globale dell’esperienza del cliente, gestione patrimoniale e degli investimenti di Barclays

I vantaggi per il vostro contact centre: AHT inferiore, operatori più contenti

Un'autenticazione più rapida e robusta non è solo una vittoria per i clienti: è anche una vittoria per il contact centre.

Se le confrontiamo con l'autenticazione basata sulla conoscenza, le soluzioni di autenticazione vocale riducono l'AHT di una media di 53 secondi[9], e spesso di un minuto o più. Ancora meglio, dato che l'autenticazione non dipende più dalla memoria dei vostri clienti, ma dall'IA, meno clienti autentici falliscono l'autenticazione per un loro errore, e viene dedicato meno tempo alla gestione di questi casi.

Questo aumento dell'efficienza del contact centre si accompagna a una riduzione del tasso di abbandono da parte degli operatori.

Come abbiamo visto, l'autenticazione vocale riduce l'onere che grava sugli operatori e li protegge da critiche e situazioni frustranti. Questo consente loro di concentrarsi effettivamente sull'aiuto da prestare al cliente–aumentando la soddisfazione professionale dell'operatore e riducendo la probabilità che lasci il suo ruolo. Questo significa quindi meno tempo e denaro spesi per assumere e formare nuovi operatori. E quando arriva il momento di assumere un nuovo operatore, addestrarlo a condurre conversazioni conformi con i clienti è più rapido e facile che mai.

Ridurre l'AHT in tutto il mondo grazie alla biometria vocale

Biometria vocale di Nuance per i clienti	È stata riportata una riduzione dell'AHT
Australian Tax Office	48 secondi
Banco Santander	42 secondi
Eastern Bank	60 secondi
Royal Bank of Canada	43 secondi

9 Riduzione media dell'AHT calcolata sulla base dei risultati riferiti dai clienti Nuance.

Prevenzione delle frodi grazie alla biometria vocale, alla NatWest Group

17 milioni

di chiamate protette all’anno de llamadas protegidas al año

+2.500

chiamate fraudolente individuate llamadas fraudulentas detectadas

>300%

ROI nel corso del primo anno

I vantagii per il team di prevenzione delle frodi: riduzione di perdite e prevenzione attiva

Con l’autenticazione basata sulla biometria vocale, i criminali non possono più usare nomi utente e password rubati per lanciare i loro attacchi, e hanno meno possibilità di usare l’ingegneria sociale, come informazioni carpite agli operatori.

A questo si aggiunge la capacità della tecnologia di identificare i truffatori noti – e di segnalare in modo più efficace le chiamate sospette e le chiamate “bot”– e l’impatto di questa tecnologia sulle perdite causate dalle frodi e sulla prevenzione delle frodi può essere molto profondo.

Il sistema biometrico vocale di HSBC UK ha impedito tentativi di frode per un ammontare complessivo pari a 608 milioni di sterline in meno di due anni. La banca, ora, ha più di tre milioni di clienti del Regno Unito registrati nel suo sistema, che effettua circa nove milioni di verifiche ogni anno.[10, 11]

10 https://www.about.hsbc.co.uk/news-and-media/hsbc-voiceid-attempted-fraud (Accesso effettuato in data 8 febbraio 2021).
11 https://www.about.hsbc.co.uk/news-and-media/hsbc-uk-launches-new-voice-driven-technology (Accesso effettuato in data 24 marzo 2021).

“Il ROI derivante dall’implementazione di questa tecnologia probabilmente è ben superiore al 300%, così come il ritorno dovuto all’uso di questo metodo è stato davvero impressionante”.

— Jason Costain
Responsabile della strategia antifrode e della gestione delle relazioni NatWest Group (precedentemente Royal Bank of Scotland Group)

Il vantaggio reputazionale per l’intera azienda

L’introduzione dell’autenticazione vocale, o di altre tecnologie che migliorano il rilevamento e la prevenzione delle frodi, rafforza la reputazione del vostro istituto di servizi finanziari, mostrando chiaramente l’impegno che la vostra azienda mette nel proteggere e tutelare i suoi clienti.

Allo stesso tempo, questo aiuta a proteggervi dal danno reputazionale che può derivare da attacchi criminali andati a segno..

L’88%

dei consumatori dichiara che la sua percezione legata a un’impresa migliora quando l’azienda investe nell’esperienza del cliente, vale a dire, nella sicurezza.[12]

13 Report Experian 2020 su identità globale e frodi.

È ora di ripensare all’autenticazione.

Insieme.

Quando l’autenticazione causa problemi ai clienti o agli operatori, rappresenta un problema anche per la vostra azienda. La biometria vocale può aiutare, soprattutto se integrata in una soluzione multi-fattoriale che fornisce una visione unificata e globale dell’autenticazione – e dei tentativi di frode – su tutti i canali di interazione.

Come responsabili dell’esperienza del cliente, siete nella posizione ideale per coinvolgere i vostri colleghi e il vostro contact centre nella prevenzione delle frodi, ed avviare insieme una trasformazione che, alla fine, aiuterà tutti voi a raggiungere i vostri obiettivi.

Ma non dovete farlo da soli: Nuance è qui per aiutarvi, proprio come abbiamo aiutato tanti altre compagnia di servizi finanziari.

SCOPRITE DI PIÙ

Scoprite di più sulle soluzioni di autenticazione biometrica e di prevenzione delle frodi di Nuance sul nostro sito web.

Scoprite anche perché Opus Research ci ha nominato "leader indiscusso del mercato" nel suo Intelligent Authentication and Voice Biometrics Intelliview del 2020.

Informazioni su Nuance Communications, Inc.
Nuance Communications (Nuance) è un'azienda di tecnologia all'avanguardia, leader del mercato nell'ambito dell'IA conversazionale e dell'intelligence ambientale. Nuance, un partner a 360° gradi a cui si affida il 77% degli ospedali degli Stati Uniti e l'85% della aziende Fortune 100 in tutto il mondo, crea soluzioni intuitive che aumentano la capacità delle persone di aiutare altre persone.

ENT_4323_01_EB_IT, 6 settembre 2021