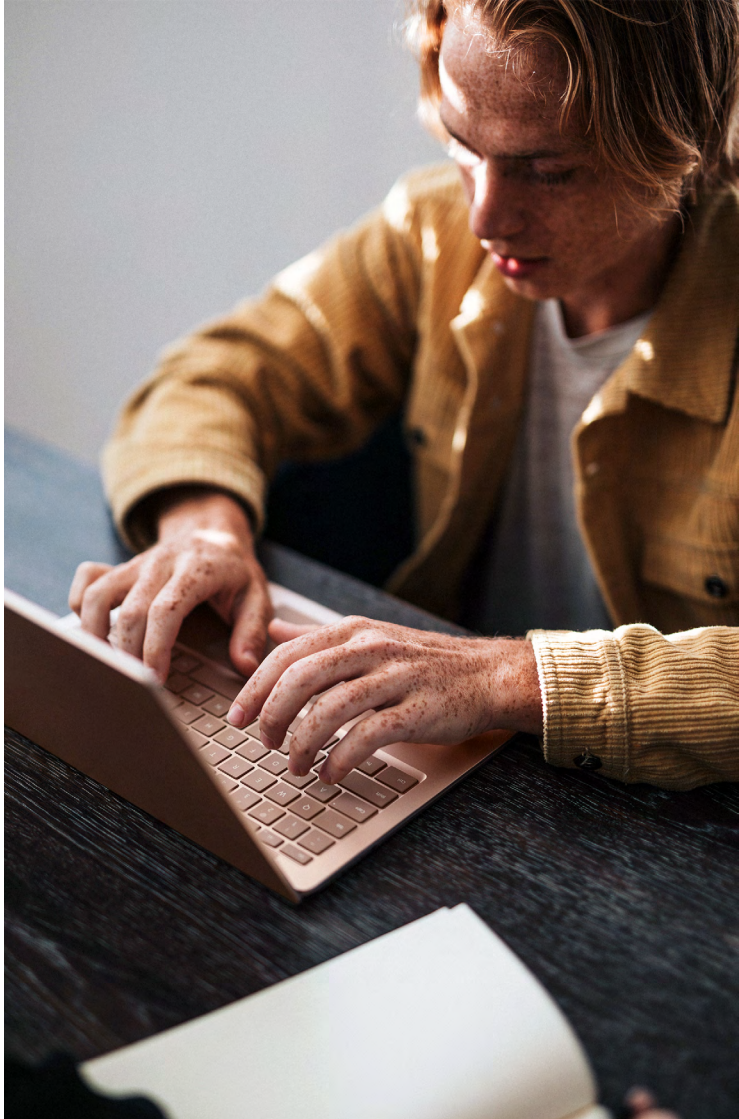
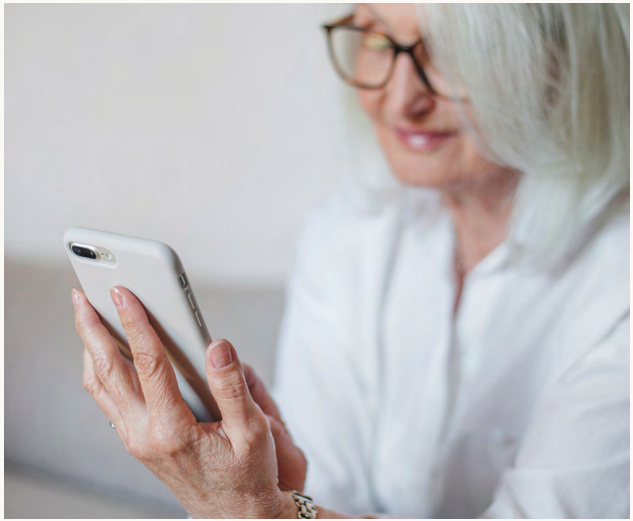
N26

La guida completa di N26 per gestire le tue finanze online in sicurezza



Sicurezza e online banking

Le conseguenze del COVID-19 hanno spinto le persone di tutto il mondo ad abbracciare sempre di più la tecnologia e l'innovazione per adattarsi alla nuova normalità. Sempre più clienti scelgono soluzioni digitali, effettuando pagamenti contactless invece che in contanti e prediligendo gli acquisti online. Non c'è da stupirsi del fatto che in molti stiano optando anche per soluzioni di digital banking: si prevede che entro il 2021 quasi il 39% della popolazione mondiale usufruirà di servizi bancari online.



Forse ti starai chiedendo: e la sicurezza?

In quanto banca tedesca dotata di regolare licenza bancaria, N26 è soggetta alle stesse regolamentazioni delle sue controparti tradizionali, investendo significativamente nella sicurezza e nell'integrità delle operazioni di online banking. Oltre a ciò che N26 fa dietro le quinte, anche tu puoi prendere alcune precauzioni per proteggerti dai crimini informatici. Con questa guida, contenente i nostri consigli e raccomandazioni, vogliamo fornirti uno strumento utile per contribuire alla sicurezza dei tuoi risparmi e delle tue operazioni bancarie online.

La sicurezza fa la differenza: in un mondo digitale deve essere una priorità

Nessuna banca è esente dal rischio di reati informatici. come qualsiasi altro istituto dotato di regolare licenza bancaria, N26 è soggetta a severe regolamentazioni in materia di sicurezza, adempimenti e prevenzione del crimine.

In un contesto digitale, la sicurezza diventa una priorità assoluta. I truffatori sono alla continua ricerca di nuovi modi per affinare le loro tecniche e colpire clienti ignari proprio quando meno se lo aspettano. Possono essere veloci, innovativi ed estremamente creativi nel loro modo di agire. Ad esempio, nel marzo 2020, il primo mese in cui il COVID-19 è stato dichiarato pandemia globale, gli attacchi di phishing correlati al coronavirus sono aumentati del 667% su scala mondiale.[1]

Ecco perché noi di N26 ottimizziamo continuamente le nostre misure di sicurezza. Tenere al sicuro i tuoi soldi è la nostra priorità assoluta e per farlo ci avvaliamo delle soluzioni più moderne del settore.

[1] Da una ricerca di Barracuda Sentinel - Threat Spotlight: Coronavirus-Related Phishing

5 minacce comuni nell'online banking

Anche se lavoriamo sodo per rendere sicuro il banking digitale con N26, i malfattori sono sempre alla ricerca di nuovi modi per adescare i clienti. La migliore prevenzione contro tali attacchi è l'informazione e la scrupolosità da parte tua, in quanto cliente. Ecco alcune delle tattiche criminali più comuni in cui ti puoi imbattere quando utilizzi l'online banking:

1

Il **phishing** è una tecnica fraudolenta utilizzata dai criminali informatici per indurre le loro vittime a condividere dati sensibili come credenziali di accesso, dettagli del conto e della carta di credito, così come altre informazioni per rubare la loro identità. Spesso utilizzano un linguaggio minaccioso, pensato per intimidire le loro vittime e cercare di manipolarle in modo che cedano alle loro richieste, ma sempre tentando di apparire legittimi, ad esempio spacciandosi per una banca o una grande azienda: quest'ultimo aspetto viene spesso reso più credibile mediante l'uso di loghi o indirizzi email che imitano quello delle controparti reali. Ma attenzione: queste ultime non chiederanno mai ai propri clienti di condividere informazioni così delicate o di accedere ai propri conti direttamente dalla mail! Normalmente, tali interazioni avvengono attraverso le email e gli SMS che solitamente contengono link a siti web fraudolenti.

2

Le tattiche della cosiddetta **ingegneria sociale (social engineering)** sono solitamente discrete e coercitive, oltre ad essere particolarmente efficienti quando si tratta di manipolare lo stato emotivo dell'individuo. I truffatori mettono in gioco una serie di tecniche per conquistare la fiducia delle persone per poi convincerle a farsi dare delle informazioni strettamente riservate e personali. Solitamente lo fanno richiedendo di effettuare operazioni entro precisi vincoli temporali per convincere le proprie vittime a cedere e a fornire i loro dati rapidamente.

3

La **truffa della falsa assunzione** è una tecnica con la quale i criminali pubblicano delle pubblicità contenenti informazioni fraudolente come mezzo per raccogliere dati personali da individui che non sospettano niente. Ad alcuni candidati viene addirittura chiesto di aprire dei conti in modo ingannevole, dicendogli di non rivelare a nessuno i motivi del loro operato. In questo modo i truffatori possono aprire e accedere a conti bancari con il nome delle persone truffate utilizzando la scusa di offerte lecite di assunzione.

4

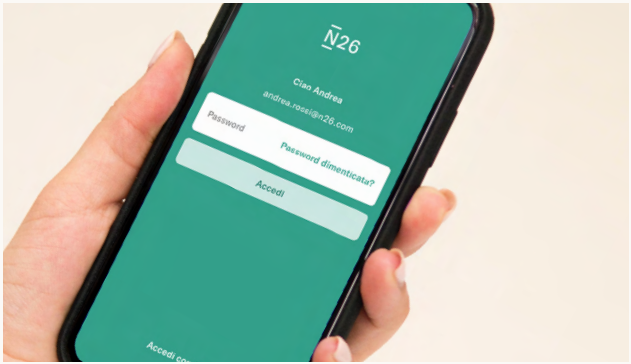
La **frode sui mercati online (marketplace fraud)** è un reato che i criminali informatici commettono dopo aver aperto dei conti bancari con delle identità rubate e/o impossessandosi dell'accesso a conti bancari grazie al phishing. I truffatori utilizzano tali conti rubati per creare dei profili falsi sui mercati online (marketplace), in modo che compratori ignari gli inviino dei soldi per prodotti non esistenti, falsi annunci immobiliari, auto di seconda mano e altri articoli fittizi.

5

Abbiamo invece un **furto di dati** quando i criminali informatici prendono di mira grandi aziende con l'intenzione di accedere a determinati dati dei loro clienti come nomi, indirizzi di residenza, dati assicurativi, dettagli su carte di credito, su alcune transazioni ecc. Invece di attaccare i sistemi di sicurezza delle banche, a volte i criminali informatici si accaniscono sulle aziende con cui vengono spesso effettuate transazioni online: dalle compagnie aeree, ai venditori al dettaglio, fino ai servizi di streaming online. Le informazioni rubate possono essere utilizzate per accedere ai conti bancari personali e quindi per effettuare acquisti e/o tentare altri tipi di frode.

Alcune funzionalità importanti che ci aiutano a garantire la sicurezza del tuo conto bancario digitale

N26 si impegna notevolmente affinché i propri clienti possano utilizzare il banking online in tutta sicurezza. Ecco alcune delle funzionalità più importanti che ci aiutano a tenere il tuo conto al sicuro.



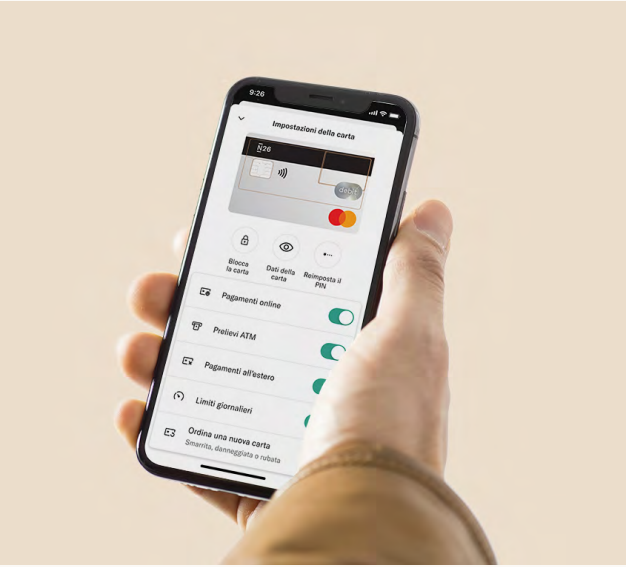
Un solo dispositivo associato: puoi gestire il tuo conto N26 solo attraverso lo smartphone che avrai associato ad esso. In questo modo, solo tu hai accesso ai tuoi soldi.

Autenticazione a due fattori: oltre a poter effettuare l'accesso al tuo conto N26 solo con il dispositivo associato, devi fornire la tua password o un'identificazione biometrica per dimostrare di essere veramente la titolare o il titolare del conto.

Impronta digitale e riconoscimento facciale: i dati biometrici ci aiutano a garantire che solo tu possa accedere al tuo conto. In questo modo non devi preoccuparti che la tua password possa essere rubata.

Notifiche in tempo reale: rimani sempre aggiornato sulle tue transazioni in tempo reale grazie alle notifiche in tempo reale. In questo modo puoi controllare immediatamente ogni transazione, direttamente dal tuo smartphone.

Blocco della carta attraverso l'app: se per qualsiasi motivo ritieni che i dettagli della tua carta siano stati compromessi, hai la possibilità di bloccare la tua carta o cambiare il PIN con pochi semplici clic sul tuo smartphone.



Tecnologia 3D Secure: questo passaggio di autenticazione richiede la tua autorizzazione tramite l'app N26 per processare qualsiasi pagamento online. In questo modo puoi identificare e prevenire un uso improprio della tua carta prima che il reato venga commesso.

Geolocalizzazione: quando dai il consenso all'app N26 per la geolocalizzazione, i nostri sistemi sono in grado di identificare se la tua carta viene utilizzata in un luogo diverso da dove sei tu, oltre a monitorare altre modalità di utilizzo potenzialmente sospette.

Verifica dell'identità: N26 lavora con regolari partner del settore per eseguire un controllo su ognuno dei clienti prima dell'apertura di un conto.

Blocchi di pagamento intelligenti: mantieni il controllo su come la tua carta può essere utilizzata disattivando pagamenti online, prelievi presso sportelli bancomat, transazioni tramite banda magnetica o pagamenti all'estero con un semplice clic.

Casella di posta sicura: se dobbiamo metterci in contatto con te per questioni importanti, ti invieremo un messaggio tramite la casella di posta all'interno dell'app, assicurandoci così che solo tu sia in grado di risponderci.

10 semplici consigli per garantire la tua sicurezza online

Ecco alcuni consigli utili per stare sempre al sicuro ogni volta che sei online, che sia per lo shopping, il banking o semplicemente per gestire la tua corrispondenza:

Effettua acquisti solo presso siti web affidabili di venditori riconosciuti

Crea delle password complesse contenenti lettere, numeri e simboli ed evita di usare la stessa password per accedere a diversi conti

Assicurati che i siti web siano sicuri, controlla che ci sia il simbolo di un lucchetto accanto all'URL e verifica le credenziali con un semplice clic

Non pubblicare mai informazioni personali sensibili online o sui social media

Tieni la tua app N26 e il sistema operativo del tuo cellulare sempre aggiornati in modo da evitare che possano verificarsi bug

Stai in guardia di fronte a offerte troppo belle per essere vere: probabilmente è proprio così!

Fai attenzione quando utilizzi una rete WiFi pubblica o una connessione condivisa e scegli sempre connessioni WPA2 sicure invece di connessioni WEP

Prediligi fornitori di servizi email con filtri per la sicurezza e per lo spam e che dispongono di un sistema di autenticazione a due fattori, come Gmail e Yahoo!

Consenti la geolocalizzazione sulla tua app N26, così possiamo individuare transazioni irregolari non effettuate da te

Utilizza metodi di autenticazione biometrici come la scansione dell'impronta digitale o il riconoscimento facciale per effettuare l'accesso

Campanelli d’allarme per messaggi sospetti

Se sei incerto sulla provenienza di un messaggio oppure un’email ricevuta sul tuo conto bancario, contatta sempre il Supporto Clienti N26 prima di fare qualsiasi cosa. Ecco alcuni elementi tipici dei messaggi fraudolenti o sospettosi:

Urgenza: se, per qualsiasi motivo, ti viene richiesto di fare qualcosa nell’immediato, fermati e controlla se c’è qualcosa che non quadra. I criminali informatici usano spesso avvisi con dei vincoli di tempo per ostacolare il processo con cui elaboriamo le decisioni. Ricorda: le aziende legittime non spingono mai i propri clienti a fare qualcosa “su due piedi”.

Piccoli errori e incoerenze: insospettisciti se leggi introduzioni troppo generiche e errori di ortografia e di formattazione palesi. Questi sono segnali di un potenziale tentativo di phishing.

URL errati: prima di cliccare su un link, controlla sempre l’URL del sito web in questione. Puoi farlo passando col cursore sul link per visualizzare la sua destinazione. Come se non bastasse, a volte anche URL legittimi vengono utilizzati per scopi fraudolenti. Verifica se ci sono lettere che non compaiono normalmente.

Siti web non sicuri: diffida dei siti web reindirizzati. Controlla che ci sia il simbolo di un lucchetto che indica che la connessione è sicura; cliccaci sopra per verificare le credenziali del sito web. In questo modo potrai controllare la validità del certificato Secure Sockets Layers (SSL) e da chi è stato emesso.

Richiesta di informazioni: fai particolarmente attenzione quando ti viene chiesto di fornire qualsiasi tipo di informazione personale. Ricordati sempre che N26 non ti chiederà mai di condividere dati sensibili se non all’interno di un contesto sicuro.

Dietro le quinte di N26: come le banche digitali combattono la criminalità informatica

Le divisioni Sicurezza, Anti-Criminalità Finanziaria e Prevenzione delle frodi di N26 sono composte ciascuna da numerosi specialisti ed esperti che aiutano a proteggere i nostri clienti dai crimini finanziari. Ecco le loro risposte alle domande più frequenti su come N26 affronta le frodi online.

Quali adempimenti sono richiesti dalle banche per prevenire le frodi?

Tutte le banche pienamente autorizzate devono adempiere ai requisiti di legge e segnalare alle autorità qualsiasi attività sospetta sulla propria piattaforma. N26 non è diversa dalle altre e deve rispettare tali obbligazioni, come qualsiasi altra banca.

Le banche digitali sono meno sicure di quelle tradizionali?

Le banche digitali possono operare con licenze diverse, il che significa che non tutte sono soggette agli stessi standard normativi in materia di sicurezza e prevenzione delle frodi, soprattutto se hanno licenze ad operare nella tecnofinanza (fintech) o con il denaro elettronico. Premesso questo, in quanto banca tedesca dotata di regolare licenza, N26 è soggetta alle stesse regolamentazioni delle nostre controparti tradizionali. Questo, in aggiunta alla nostra particolare attenzione al tema della sicurezza, ci rende sicuri come una banca tradizionale.

In che modo N26 rileva e monitora le frodi?

N26 dispone di un team di specialisti il cui lavoro si concentra sul monitoraggio e l'identificazione di transazioni sospette sulla nostra piattaforma. Con l'aiuto di modelli statistici e algoritmi avanzati, assieme ad analisi comportamentali, il nostro team di specialisti fa in modo che i tuoi soldi siano sempre in buone mani.

Perché le banche sono così reticenti su come affrontano le frodi?

C'è un duplice motivo. Prima di tutto, essendo soggette a severe leggi sulla protezione dei dati e di segretezza bancaria, alle banche non è permesso condividere i dettagli di un caso, se non con le autorità preposte all'applicazione della legge. In secondo luogo, le banche custodiscono gelosamente i dettagli su come prevengono le frodi proprio per non dare indizi a potenziali truffatori, che potrebbero utilizzare queste informazioni per eludere i controlli e colpire i clienti in modo efficiente.

In che modo la prevenzione delle frodi è diversa nel contesto di una banca digitale?

Nel mondo digitale le informazioni vengono trasmesse molto più velocemente e il contesto bancario non è certo un'eccezione. Noi di N26 cerchiamo di sfruttare questo fattore a nostro vantaggio con strumenti che ci permettono di monitorare e identificare in tempo reale le modalità con cui avviene un comportamento fraudolento sin da quando il cliente effettua l'accesso. Puntando su tecnologia, intelligenza artificiale, dati e algoritmi all'avanguardia, e combinandoli con l'intelligenza umana, siamo in grado di verificare e monitorare i singoli individui e assicurarci che qualsiasi attività sospetta venga affrontata velocemente.

Quali iniziative intraprende N26 quando rileva azioni fraudolente nelle attività dei propri clienti?

Non appena il nostro team di esperti rileva un'attività irregolare, prendiamo tutte le misure previste dalla legge per ridurne l'impatto e prevenire ulteriori danni. Ciò implica anche chiudere e denunciare alle autorità i conti bancari sui quali si verificano attività illegali. Se delle transazioni sospette fanno pensare a un riciclaggio di denaro, finanziamenti a organizzazioni terroristiche o qualsiasi altro atto criminale, N26 segnala immediatamente tali attività all'Unità di intelligence finanziaria tedesca (Financial Transaction Investigation Unit, FIU) o alle autorità locali di vigilanza.

Quali sono i modi in cui N26 ha investito sulla sicurezza?

Nel 2019, N26 ha apportato una serie di modifiche per migliorare ulteriormente il suo approccio alla sicurezza. Innanzitutto, abbiamo creato un nuovo team Trust & Safety, che lavora insieme al team Sicurezza Informatica per proteggere gli utenti, i loro account e i loro dati dai criminali informatici. Successivamente, abbiamo introdotto l'A-Team, una divisione di esperti specializzati che supportano i clienti quando vengono rilevate attività sospette o fraudolente sul loro account. Inoltre, N26 ha raddoppiato la dimensione della propria Unità Antiriciclaggio (AML) e dell'Unità contro i crimini finanziari, creando procedure per il monitoraggio delle transazioni e delle piattaforme. In questo modo possiamo rilevare e prevenire le attività illegali basandoci sullo storico dei dati, che in ultima istanza ci permette di essere sempre diversi passi avanti rispetto ai malfattori. Investiamo significativamente nella tecnologia e nell'intelligenza artificiale per implementare modelli e algoritmi avanzati, assieme ad analisi comportamentali.

Qual è la prossima svolta nel mondo della sicurezza e la prevenzione della criminalità informatica?

Dal momento che le persone hanno vite sempre più digitalizzate e interconnesse, il mondo della sicurezza informatica non può rimanere indietro. Con sempre più app di terzi non provenienti dal mondo bancario, ma che vi accederanno nel futuro, l'impiego dell'intelligenza artificiale e l'apprendimento automatico (machine learning) giocheranno un ruolo sempre più cruciale nel monitoraggio e nel rilevamento delle frodi ai fini di garantire la sicurezza su larga scala. Anche se noi di N26 utilizziamo già molti di questi strumenti, crediamo che gli innovatori digitali di oggi avranno un ruolo importante nell'aiutarci a delineare la sicurezza digitale di domani.

Qualcosa non quadra? Ecco a chi puoi rivolgerti

Se sospetti che il tuo conto o i dettagli della tua carta siano stati compromessi, cambia subito la tua password e blocca la carta immediatamente dall'app N26. In alternativa, puoi contattarci ai seguenti indirizzi:

PER SEGNALARE una transazione sospetta:
scrivici immediatamente sulla chat o per email a support@n26.com

PER CONTRASSEGNARE un messaggio o un sito web sospetto:
inoltra l'email o l'URL del sito web a phishing@n26.com

PER CONDIVIDERE un'idea su come migliorare la sicurezza di N26:
scrivici a security@n26.com

N26

La guida completa di N26 per gestire le tue finanze online in sicurezza