



# **GUIDA ALLA SICUREZZA DELL'UTILIZZO DEI SERVIZI BANCARI ONLINE**

In questa guida ti forniamo alcune indicazioni operative sull'utilizzo degli strumenti di sicurezza del tuo conto, seguite da informazioni utili alla sicurezza online e alla protezione della tua identità online.

## **1. COME ACCEDERE A WEBANK**

- 1.1 Per accedere all'area privata di [www.webank.it](http://www.webank.it)
- 1.2 Per accedere da app

## **2. ATTIVAZIONE APP WEBANK**

- 2.1 Come certificare l'app

## **3. COME UTILIZZARE L'APP CERTIFICATA**

- 3.1 Sul sito Webank
- 3.2 Sull'app Webank

## **4. ATTIVAZIONE DEL TOKEN**

- 4.1. Come si utilizza

## **5. IL TOKEN AUDIO**

## **6. CONSIGLI UTILI PER LA TUA SICUREZZA**

## **7. PROTEGGI LA TUA IDENTITÀ ONLINE**

- 7.1 - Cos'è il phishing
- 7.2 - Cos'è il crimeware

## **8. REGOLE PER LA TUA SICUREZZA**

## **9. UTILIZZARE IN SICUREZZA L'INTERNET BANKING**

## **10. UTILIZZARE IN SICUREZZA LE CARTE DIGITALIZZATE**

## **11. IN GENERALE QUANDO SEI ONLINE RICORDATI DI...**

## 1. COME ACCEDERE A WEBANK

### 1.1 Per accedere all'area privata di [www.webank.it](http://www.webank.it)

Inserisci il Codice Identificativo e la tua Password Personale, successivamente dovrai utilizzare uno strumento di Strong Authentication a scelta fra token digitale, integrato nell'App Webank, oppure token fisico.

### 1.2 Per accedere da app

Dopo aver certificato l'App, che verrà associata in maniera univoca al tuo smartphone e al tuo Codice Identificativo, per entrare nell'App e consultare la tua posizione sarà sufficiente inserire la Password Personale o, se abilitato, il riconoscimento biometrico. Per mantenere elevati livelli di sicurezza del tuo conto Webank, hai a disposizione due strumenti alternativi di Strong Authentication che ti serviranno per autorizzare gli accessi al conto e le operazioni dispositive: l'App Webank con token digitale (Token App) oppure il Token Fisico.

Di seguito trovi le informazioni operative in base allo strumento che hai scelto.

## 2. ATTIVAZIONE APP WEBANK

**Le funzioni di sicurezza sono integrate nell'App di Webank:** questo ti permette di avere la tua Banca sempre a portata di mano e con un unico strumento consultare il conto corrente, effettuare e autorizzare operazioni in qualsiasi momento, sia dall'App stessa che dal sito Webank. Ti ricordiamo che l'App Webank è disponibile gratuitamente su **Google Play, App Store** e **AppGallery**.

### 2.1 Come certificare l'app

Per utilizzare l'App di Webank sarà necessario procedere con la **certificazione**: ogni installazione dell'App viene così associata ad un unico cliente.



1. Se non l'hai ancora fatto, certifica il tuo numero di cellulare ed indirizzo email dalla tua area privata del sito Webank;
2. apri l'App Webank sul tuo smartphone ed inserisci Codice Identificativo e Password;
3. inserisci il codice OTP (One Time Password) che riceverai sul numero di cellulare certificato e conferma;
4. se hai scelto l'App come tuo strumento di Strong Authentication, crea ora il tuo Codice Dispositivo di sicurezza che può variare da 4 a 8 cifre. Per alcuni modelli di smartphone sarà possibile associare al Codice Dispositivo il riconoscimento biometrico che potrai utilizzare in alternativa al Codice Dispositivo.  
**Attenzione:** scegli bene il tuo Codice Dispositivo, ti verrà richiesto per disporre le operazioni e dopo cinque tentativi errati, per motivi di sicurezza, verrà bloccato; per sbloccarlo occorre disinstallare e reinstallare l'App e ripetere il processo di certificazione.
5. la tua App è ora certificata e puoi procedere con la configurazione delle funzioni veloci e con la normale operatività.

## 3. COME UTILIZZARE L'APP CERTIFICATA

### 3.1 Sul sito Webank

Hai scelto come strumento di Strong Authentication l'App? Anche quando accedi da web tieni a portata di mano il tuo smartphone. Le operazioni di login o dispositive, per essere autorizzate, generano automaticamente una notifica push che riceverai sul tuo smartphone:



per completare l'operazione di login dovrai fare un tap sulla notifica ricevuta;



per completare le operazioni dispositive dovrai fare un tap sulla push notification e inserire il Codice Dispositivo di sicurezza oppure il tuo riconoscimento biometrico, se abilitato;



una pagina di conferma sul sito ti avviserà del buon esito dell'operazione.

Se il tuo telefono non dovesse ricevere la notifica push potrai comunque generare, utilizzando l'App, un codice OTP (One Time Password) questa funzione è disponibile anche quando il tuo smartphone è offline:

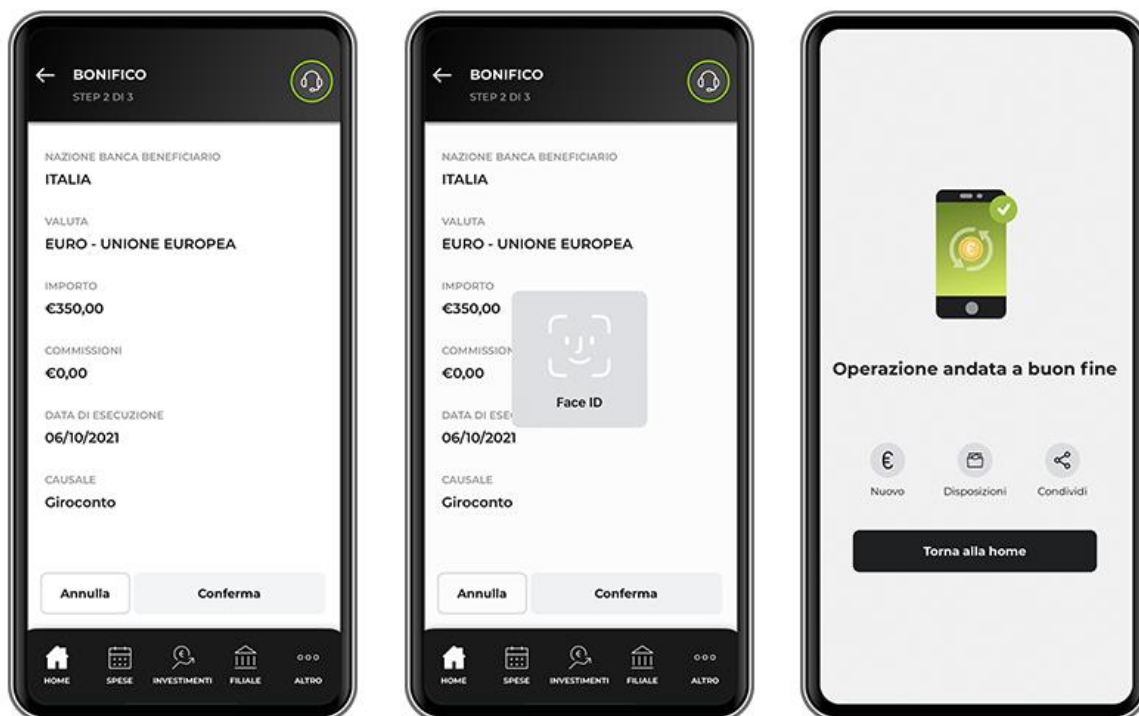


- seleziona il link "clicca qui" presente nella pagina web che compare per autorizzare l'accesso/la disposizione;
- apri l'App sul tuo smartphone e vai alla funzione "Genera OTP" e inserisci nella pagina web il codice generato dall'App.

## 3.2 Sull'app Webank

Il login viene effettuato con l'inserimento del riconoscimento biometrico, se abilitato, o con la Password Personale.

Le operazioni dispositivi vengono autorizzate con l'inserimento del riconoscimento biometrico, se abilitato, o con il Codice Dispositivo che hai scelto.



Con il Token App il tuo cellulare diventa uno strumento molto importante per la tua sicurezza: trattalo con la dovuta attenzione come fai per le tue carte di pagamento.

## FAQ

### 1. E SE PERDO O MI RUBANO IL TELEFONO?

Contatta subito il numero verde al numero 800 060 070. Inseguito potrai installare l'App su un nuovo smartphone.

### 2. E SE DISINSTALLO L'APP O CAMBIO TELEFONO?

Per motivi di sicurezza solo una installazione dell'App associata al tuo Codice Identificativo avrà attiva la funzionalità di Token App. Sarà la prima che certifichi.

Se hai cambiato telefono puoi procedere alla certificazione dell'App primaria sul nuovo dispositivo.

### 3. E SE HO PIÙ TELEFONI?

L'app può essere installata su più telefoni ma le installazioni successive alla prima non avranno attiva la funzionalità di token digitale per autorizzare le operazioni da web.

#### 4. IL MIO TELEFONO È ABBASTANZA EVOLUTO?



L'app che integra le funzionalità di sicurezza è disponibile per:

- iPhone con iOS versione 12.0 o superiore
- smartphone con Android versione 6.0. o superiore.

La possibilità di abilitare l'uso dell'impronta digitale verrà automaticamente proposta in fase di attivazione sui device che garantiscono un adeguato livello di sicurezza.

## 4. ATTIVAZIONE DEL TOKEN



Se hai scelto il Token fisico come strumento di Strong Authentication, accendilo tenendo premuto il pulsante  e contemporaneamente il pulsante .

Il token è protetto da un PIN di 4 cifre che potrai scegliere alla prima accensione e non è modificabile in futuro.

### 4.1. COME SI UTILIZZA

Una volta attivato il token, a ogni accesso al sito e per autorizzare le operazioni dispositive comparirà una schermata con la richiesta di un codice OTP di 6 cifre:



Attenzione: dopo cinque tentativi errati, per motivi di sicurezza, il Token fisico (Tastiera) viene bloccato. Chiama il Numero Verde 800 060 070 in caso di blocco del dispositivo.

Ti ricordiamo che il tuo token è uno strumento importante per la tua sicurezza e lo devi trattare con la dovuta attenzione: se dovessi perderlo o ti venisse rubato devi subito chiedere che venga sospeso, chiamando il Numero Verde 800 060 070. Ti verrà inviato tramite posta un nuovo Token fisico.

## 5. IL TOKEN AUDIO

Il nuovo Token offre un ritorno audio per tutte le icone, messaggi e numeri da immettere e visualizzare.

I messaggi audio possono essere trasmessi attraverso l'altoparlante interno del dispositivo, o tramite un auricolare per maggiore riservatezza.

È possibile modificare il volume, la lingua, la velocità di uscita delle parole audio, e può anche richiedere che l'uscita audio venga ripetuta.

Le funzionalità di uscita audio sono controllate premendo il tasto funzione insieme ad altri tasti, in modo simile a come il tasto shift sulla tastiera di un computer viene utilizzato per richiamare funzioni speciali.

Le combinazioni di funzioni e pressione dei tasti numerici per richiamare la funzionalità di controllo audio sono i seguenti:

- Tenendo premuto il Tasto funzione + il tasto 0: ripetizione ultimo messaggio audio.
- Tenendo premuto il Tasto funzione + il tasto 1: si passa alla selezione della lingua precedente nella lista, riproduce un messaggio audio con la lingua selezionata e continua.
- Tenendo premuto il Tasto funzione + il tasto 3: si passa alla selezione della lingua successiva nell'elenco, riproduce un messaggio audio con la lingua selezionata e continua.
- Tenendo premuto il Tasto funzione + il tasto 4: riduce la velocità audio, fornisce un feedback sulla nuova velocità e continua. Ci sono 8 possibili velocità.
- Tenendo premuto il Tasto funzione + il tasto 5: interrompe l'applicazione corrente e legge il numero di serie.
- Tenendo premuto il Tasto funzione + il tasto 6: aumenta la velocità audio, fornisce un feedback sulla nuova velocità e continua. Ci sono 8 possibili velocità.
- Tenendo premuto il Tasto funzione + il tasto 7: diminuisce il volume audio, e fornisce un feedback sul nuovo volume e continua. Ci sono cinque volumi differenti.
- Tenendo premuto il Tasto funzione + il tasto 9: aumenta il volume audio e fornisce un feedback sul nuovo volume e continua. Ci sono cinque volumi differenti.

Dopo che un controllo audio è stato eseguito, il Token Audio continua con il processo di applicazione corrente, (ad eccezione di 'tasto funzione + 5', spiegato in precedenza).

Se il tasto funzione viene premuto troppo a lungo senza che un altro pulsante venga premuto, la funzionalità del pulsante 'bloccato' inizia. Se il tasto viene rilasciato, il dispositivo torna operativo

**ASSISTENZA SERVIZIO CLIENTI 800 060 070**

*Dal lunedì al venerdì dalle 8:00 alle 22:00 e il sabato dalle 9:00 alle 17:00*

*Il numero è a disposizione per assistenza e informazioni in caso di furto, smarrimento blocco del token o dell'App*



## 6. CONSIGLI UTILI PER LA TUA SICUREZZA

La sicurezza è il risultato dell'azione combinata della Banca e del modo in cui utilizzi internet. Per garantire la sicurezza della tua operatività, la Banca ha adottato delle misure che:

- evolvono nel tempo, in funzione delle nuove minacce da contrastare e dell'evoluzione della tecnologia a supporto;
- non violano la privacy del cliente;
- non impattano in maniera significativa sull'usabilità del servizio;
- rispettano i requisiti normativi di settore\* e le best practice di sistema, in particolare per quanto riguarda l'utilizzo di meccanismi di autenticazione forte (Strong Authentication).

Il servizio Webank rientra nella categoria di servizi di pagamento via internet, questo implica responsabilità ed obblighi da parte della Banca e dei suoi clienti. Queste informazioni sono riportate nelle condizioni generali del contratto firmato dal cliente e dalla Banca in fase di apertura conto e sempre disponibili nella parte pubblica del sito Webank, nella sezione Trasparenza > Documenti precontrattuali.

Webank, al fine di rispettare i propri obblighi e, soprattutto, di permettere alla propria clientela di operare in semplicità e tranquillità, ha predisposto le misure di sicurezza che trovi descritte in questo manuale e sul sito. Le soluzioni adottate sono conformi alle migliori procedure in tema di sicurezza dei servizi di pagamento su internet ed a quanto definito dalle normative di settore.

In quanto cliente, anche tu hai degli obblighi che puoi facilmente rispettare seguendo le indicazioni che trovi di seguito. Inoltre, puoi costantemente reperire informazioni relative alla sicurezza sul sito di Webank e tramite le comunicazioni che ti inviamo via email.

Quello che noi ti **mettiamo a disposizione** sono degli strumenti che tu devi imparare a conservare ed utilizzare per **navigare sicuro**.

\* in particolare, gli "orientamenti finali sulla sicurezza dei pagamenti via internet" emessi dall'Autorità Bancaria Europea.

## 7. PROTEGGI LA TUA IDENTITÀ ONLINE

L'identità online è l'insieme degli elementi che permettono a chi fornisce un servizio internet di riconoscerti.

La tua identità online Webank è composta da:

- Codice Identificativo: è il tuo codice cliente di 7 cifre che resta invariato nel corso del tempo.
- Password iniziale: ti viene assegnata in fase di attivazione del servizio e devi modificarla al primo accesso con una di tua scelta.
- Password Personale: è la password che scegli al primo accesso in occasione del cambio password obbligatorio. Con questa operazione sostituisci la password iniziale con una di tua scelta composta da un minimo di 8 ad un massimo di 30 caratteri alfanumerici.

- Strong Authentication: il Token Fisico o il Token App (installato sul tuo smartphone) sono strumenti alternativi che permettono di realizzare un secondo livello di autenticazione ed autorizzazione nella tua operatività online generando dei codici temporanei OTP. Hanno sostituito la Carta dei Servizi Telematici utilizzata in precedenza.
- Il numero di cellulare e l'indirizzo email: sono fondamentali per tenere sotto controllo il tuo conto corrente. Ci permettono di contattarti velocemente per informarti o inviarti dati per completare le operazioni, per questo ti chiediamo che siano certificati e univoci e sempre aggiornati.

L'identità online può essere soggetta al **rischio di furto e utilizzo fraudolento da parte di terzi**.

Le frodi informatiche, tra cui le più diffuse sono il **phishing** ed il **crimeware**, consistono nell'utilizzare indebitamente informazioni personali di un soggetto, al fine di identificarsi, in tutto o in parte, nel soggetto stesso per compiere a suo nome azioni illecite (effettuare disposizioni bancarie oppure per ottenere credito tramite false credenziali).

**ATTENZIONE se pensi di essere stato oggetto di una frode informatica, quindi sia in caso di furto di identità online che di operazioni bancarie non riconosciute, contatta immediatamente l'Assistenza Clienti all'800 060 070 che si attiverà subito per:**

- mettere in sicurezza nuovamente il tuo servizio on line;
- richiamare, ove necessario e possibile, la disposizione non riconosciuta.

## 7.1 - Cos'è il phishing

Il phishing viene attuato da truffatori che, tramite l'invio di email portano l'utente su pagine fraudolente che richiedono l'inserimento di informazioni riservate. In genere sono pagine composte utilizzando il logo, il nome e il layout tipico dell'azienda imitata, come ad esempio una banca oppure una società emittente carte di credito.

I metodi più frequentemente utilizzati dai phisher sono:

- l'invio di false email o di falsi SMS contenenti link;
- pagine che si presentano durante la navigazione sul web;
- falsi annunci pubblicitari presentati sui motori di ricerca.

## 7.2 - Cos'è il crimeware

Il crimeware viene attuato diffondendo, presso postazioni non adeguatamente protette, un codice malevolo (malware) in grado di rubare informazioni riservate del cliente e a volte prendere il controllo da remoto della postazione contaminata.

I più diffusi tipi di malware sono: virus, worm, trojan, spyware, dialer, keylogger.

La diffusione dei malware può avvenire secondo varie modalità:

- attraverso un supporto, quali ad esempio CD-Rom oppure Pen Drive;
- attraverso la posta elettronica e gli allegati contenuti nelle email;
- scaricando dati e programmi da internet oppure navigando su siti non sicuri.

## 8. REGOLE PER LA TUA SICUREZZA

- Conserva tutti i dati che compongono la tua identità on line con la massima riservatezza: non memorizzare mai le tue password sul telefono, sul computer oppure sul browser;
- In generale Webank non ti contatterà mai per chiederti le tue credenziali d'accesso o OTP generate dagli strumenti di sicurezza, ricevute via SMS o email, non comunicare tali informazioni a nessuno;
- Non fermarti alle apparenze i messaggi di phishing possono essere inviati via email ed SMS e sembrare inviati dalla tua Banca. Non cliccare su link e/o allegati ricevuti via sms, e-mail o sistemi di messaggistica;
- la Banca non ti chiede mai di scaricare software o applicazioni utilizzando link inviati tramite sms o email; questa modalità viene usata dai truffatori per indurre i clienti a scaricare app pericolose per la sicurezza del telefono. Le app rese disponibili dalla Banca sono presenti solo sugli store ufficiali;
- non usare per i servizi bancari password già utilizzate per altri servizi;
- Abilita sempre sulle funzionalità di pagamento i servizi di notifica resi disponibili dalla tua banca tramite notifiche push, sms o email;
- non accedere al servizio da computer pubblici o utilizzando reti Wi-Fi non sicure. Utilizzare computer in Internet Cafè, biblioteche oppure luoghi simili è rischioso perché potrebbero contenere malware in grado di registrare ciò che stai digitando; se utilizzi una rete non sicura i tuoi dati potrebbero essere facilmente intercettati;
- Ogni volta che hai un sospetto su quanto sta accadendo contatta la tua Banca per chiedere chiarimenti e verifiche ai numeri ufficiali presenti sul sito.

## 9. UTILIZZARE IN SICUREZZA L'INTERNET BANKING

- quando scegli la Password Personale al primo accesso, che dovrà essere composta da un minimo di 8 ad un massimo di 30 caratteri alfanumerici, componila in maniera non banale e difficilmente riconducibile ad informazioni che riguardano te o la tua famiglia;
- accedi al sito digitando per esteso l'indirizzo del servizio direttamente nella barra del browser;
- ricordati sempre di mantenere aggiornati il tuo numero di telefono e il tuo indirizzo email: ti permetterà di operare in completa sicurezza e ci darà la possibilità di contattarti tempestivamente in caso di necessità;
- quando hai terminato di utilizzare il sito della tua banca effettua sempre il logout per disconnettere la sessione

## 10. UTILIZZARE IN SICUREZZA LE CARTE DIGITALIZZATE

1. Se digitalizzi una carta Imposta sempre un PIN/Password di accesso al telefono e preferisci una modalità di riconoscimento biometrico come l'impronta digitale o il riconoscimento facciale se il tuo device lo permette, per evitare un facile accesso ed utilizzo da parte di altri in caso di incustodita, smarrimento o furto;

2. Digitalizzare la tua carta solo sul tuo dispositivo personale, ricordati che, indipendentemente dal device utilizzato, sarai sempre ritenuto responsabile dei pagamenti effettuati con la tua carta digitalizzata;
3. Non rivelare mai i codici ricevuti via sms (OTP) relativi alla digitalizzazione delle tue carte a presunti operatori: la Banca non richiede mai tali codici, né telefonicamente né tramite e-mail

## 11. IN GENERALE QUANDO SEI ONLINE RICORDATI DI...

- utilizzare sul tuo PC, tablet o smartphone antivirus e antispyware e aggiornali frequentemente;
- non inserire mai dati richiesti in comunicazioni di dubbia provenienza;
- prestare particolare attenzione ai pop up che si aprono automaticamente e verifica sempre l'effettiva url del sito passando il mouse sul link e leggendo l'indirizzo che compare nella barra inferiore del browser;
- non aprire allegati di posta elettronica inviati da mittenti sconosciuti o contenuti in email non attese;
- prestare sempre attenzione ai dati che ti vengono richiesti in fase di sottoscrizione di un servizio. Tramite questionari molto lunghi, potresti essere indotto a fornire ad estranei delle informazioni personali non necessarie;
- **non divulgare sui social network informazioni che riguardano la tua identità** (data o luogo di nascita, indirizzo, numero di telefono);
- prestare attenzione ai permessi richiesti dalle applicazioni che usi sul telefono; potresti inavvertitamente autorizzare accessi alle informazioni contenute sullo smartphone (contatti, foto, documenti);
- non navigare e non scaricare materiali o applicazioni da siti non ufficiali o con una cattiva reputazione.

In qualsiasi momento trovi informazioni aggiornate in temi di sicurezza nel menù Sicurezza della pagina pubblica di [webank.it](http://webank.it)

**ASSISTENZA SERVIZIO CLIENTI 800 060 070**

*Dal lunedì al venerdì dalle 8:00 alle 22:00 e il sabato dalle 9:00 alle 17:00*