










SMS  
ingannevoli:

# COME PROTEGGERSI

---



# Indice

|   |           |
|---|-----------|
|  <b>Introduzione.....</b>                                 | <b>3</b>  |
|  <b>Comunicazioni ingannevoli.....</b>                    | <b>4</b>  |
|  <b>In che forma si presenta un SMS ingannevole?.....</b> | <b>5</b>  |
|  <b>Come proteggersi dagli SMS ingannevoli.....</b>     | <b>7</b>  |
|  <b>Cosa possono fare le aziende.....</b>               | <b>9</b>  |
|  <b>Cosa fa Skebbby.....</b>                            | <b>9</b>  |
|  <b>I nostri servizi.....</b>                           | <b>10</b> |

# Introduzione

Complice l'accelerata del processo di digitalizzazione, **gli SMS, se già erano uno strumento perfettamente integrato nella nostra quotidianità, ora lo sono ancora di più.** Secondo i nostri dati, infatti, **il 38,5% delle aziende nel 2020 ha aumentato il volume di invio SMS** rispetto all'anno precedente.

Questo ha però portato con sé anche nuove minacce e i malintenzionati hanno visto nell'SMS uno strumento in più per compiere truffe.



Per questo abbiamo sentito l'esigenza di scrivere questo mini eBook e **dare a tutti gli strumenti giusti per scovare gli SMS ingannevoli e proteggersi** da questi. **Crediamo fermamente nella potenza della comunicazione via SMS.** Immediata e universale, ha permesso di migliorare le nostre vite ed ogni giorno riesce a semplificare le conversazioni tra aziende e clienti. **Per questo è fondamentale che clienti e aziende sappiano tutelarsi.** Ecco cosa troverai in questo mini eBook:



Come funzionano gli SMS ingannevoli



Come puoi individuare gli SMS ingannevoli e proteggerti

# Comunicazioni ingannevoli

Partiamo col dire che **le comunicazioni ingannevoli non sono solo appannaggio del mondo SMS**. Dalle email ai messaggi su Whatsapp, fino ad arrivare alle pubblicità che promettono la vittoria di ricchi premi, **ogni giorno siamo bombardati da messaggi di questo tipo**.

**I truffatori, infatti, sfruttano proprio i canali che ogni giorno usiamo per comunicare con amici, parenti e aziende**. Quelli quindi che ci sono più familiari.



# In che forma si presenta un SMS ingannevole?

I messaggi ingannevoli possono presentare sia **un mittente numerico che uno alfanumerico**. Nel secondo caso, spesso, i malintenzionati usano **mittenti che somigliano molto a quelli delle principali banche o di altre aziende molto conosciute e che, ad un occhio poco attento, potrebbero sembrare attendibili**.

Per quanto riguarda **il testo**, invece, contiene quasi sempre:

- Un invito diretto a fornire dei dati personali
- Una richiesta di fare donazioni
- Il link ad una pagina specifica sulla quale poi verranno richiesti dei dati sensibili

Anche **le pagine** alle quali verranno condotti i malcapitati **vengono costruite per sembrare originali**.

Questa specifica truffa si chiama *smishing* ed il termine indica proprio il tentativo di rubare dati sensibili inviando un SMS

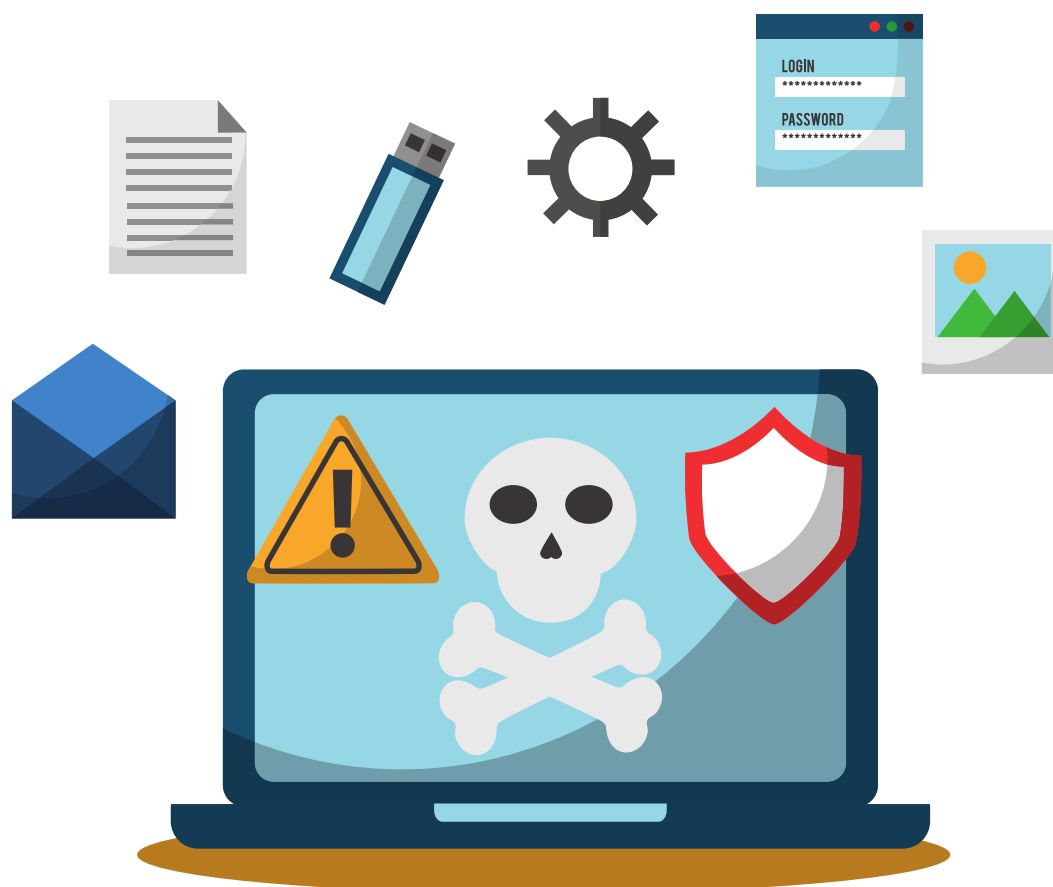
In altri casi, cliccando sul link presente nell'SMS, l'utente senza saperlo scarica un malware che consente la gestione da remoto del proprio dispositivo da parte dei malviventi.



## Focus: malware

Dall'inglese *malicious software* ovvero programma malevolo, per malware si intende un qualsiasi programma informatico usato per disturbare le operazioni svolte da un utente di un computer.

Questa strategia di per sé non è nuova, ma, negli ultimi mesi è l'esca ad essere cambiata. Infatti, i truffatori online fanno leva sulla paura delle persone che cercano informazioni su come combattere il virus o approfittano della confusione generale per accedere ai dati sensibili.

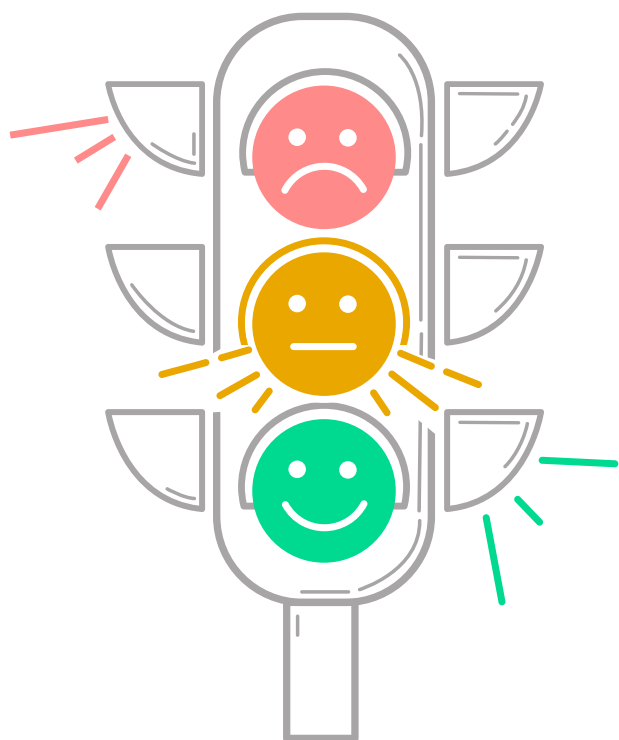


# Come proteggersi dagli SMS ingannevoli

Anche se l'Europa si è mossa recentemente per combattere queste truffe, tramite la direttiva PSD2, questo non significa che si possa abbassare la guardia.

## Focus: PSD2

L'introduzione della direttiva europea PSD2 ha previsto un doppio livello di sicurezza, con invio tramite SMS di un codice OTP, per accedere al proprio conto bancario. Questo secondo step dovrebbe aiutare a non accedere a siti bancari non reali.



Quindi, innanzitutto, se si individua un messaggio come quelli descritti in precedenza, è importantissimo **avvertire le forze dell'ordine e permettergli di scoprire l'eventuale truffa.**

Inoltre, dopo aver inviato la segnalazione, è **importante tutelare se stessi evitando di cliccare su qualunque link contenuto all'interno dell'SMS ritenuto sospetto.**

Se si è in dubbio sulla veridicità del messaggio ricevuto, è **sempre meglio contattare la propria banca oppure l'azienda che si presume ci abbia mandato l'SMS.** In questo modo si potrà verificare direttamente se il messaggio ricevuto era ingannevole oppure no.

Per aiutarti, abbiamo preparato una lista di 4 punti che ti possono supportare nell'individuare un SMS non affidabile:

## 1) Verifica l'accettazione delle comunicazioni

Perché aziende e organizzazioni possano inviarti comunicazioni, **devi aver appositamente accettato di volerle ricevere**; se non riconosci il mittente o non ricordi di aver dato il tuo consenso, meglio diffidare del messaggio.

## 2) Verifica il mittente del messaggio

Un altro espediente per scovare le truffe è quello di **fare attenzione a come è scritto il nome dell'azienda**. Spesso i truffatori usano mittenti numerici oppure **mittenti alfanumerici con nomi simili all'originale** ma non uguali.



## 3) Leggi attentamente il contenuto

Le comunicazioni truffaldine **invitano ad agire velocemente**; bisogna invece prendersi il tempo per leggere il contenuto del messaggio e se vengono chiesti dati personali è improbabile che sia un messaggio autentico

## 4) Verifica il formato del link

Gli indirizzi dei siti affidabili, sono preceduti dalla dicitura **https://** che indica la cifratura del contenuto presente nelle pagine e di conseguenza la sicurezza nel collegamento. **Quasi sempre i siti truffaldini non seguono questo protocollo e hanno un indirizzo preceduto da http://.**



# Cosa possono fare le aziende

Se i privati cittadini possono adottare diversi espedienti per difendersi dagli SMS ingannevoli, anche le aziende stesse possono fare la propria parte.

La prima cosa da fare è **far sapere ai propri clienti quali sono le modalità di comunicazione scelte per entrare in contatto con loro**. Molte banche, ad esempio, avvisano i propri correntisti che potranno ricevere SMS da loro ma che non gli verranno mai richiesti dati personali attraverso quel canale.

Ovviamente anche le aziende, gli enti governativi e le associazioni devono alzare le difese. Se già si usa l'SMS come canale per comunicare con i propri clienti, allora il consiglio è di **utilizzare un mittente alfanumerico**. Tutti i mittenti creati sono verificati dall'AGCOM e aiutano i destinatari a sapere subito chi gli sta scrivendo prima ancora di aprire il messaggio.



## Cosa fa Skebby

Crediamo negli SMS come strumento di comunicazione sicuro ed immediato tra aziende e clienti. Per questo da tempo abbiamo alzato ancora di più i livelli di sicurezza:

- Monitoriamo i nostri sistemi 24/7 e se i sistemi ci segnalano comportamenti sospetti, interveniamo subito
- Abbiamo integrato sistemi automatici di phishing/spam detection
- Controlliamo i pagamenti con appositi tool e abbiamo attivato controlli antifrode sempre attivi
- I nostri team di supporto, compliance e IT collaborano costantemente per garantire la massima sicurezza

# I nostri servizi

## La potenza della Piattaforma Skebbby al tuo servizio

### Servizio di Invio e Ricezione SMS

Inviare e ricevere SMS da pc non è mai stato così semplice e alla portata di tutti. Con il servizio di invio e ricezione di Skebbby in pochi step puoi inviare e ricevere SMS. Scrivi il testo, carichi la lista contatti e invii. Con il servizio di ricezione puoi anche ricevere SMS ed impostare risposte automatiche.

### SMS Gateway

Con SMS Gateway è possibile inviare e ricevere SMS direttamente dai tuoi applicativi (CRM, ERP, CMS), server/siti web o client email tramite API Rest. Le interfacce SMS di Skebbby sono semplici ed immediate e consentono di inviare e ricevere SMS in meno di 30 minuti.

### Landing Page

Le landing page sono mini pagine web con immagini, video, testo e collegamenti ai tuoi social. Le crei in pochi minuti grazie ai modelli pronti all'uso e all'Editor di Skebbby. Le landing page ti aiutano a rendere i tuoi SMS più interattivi. Aggiungile ai tuoi messaggi includendo il link nel testo!

### SMS ADV

Con SMS ADV puoi contattare nuovi potenziali clienti! Skebbby ti fornisce un database di numeri di cellulare consenzienti che puoi filtrare. Scegli tu chi contattare in base a genere, età e area geografica. Imposti il mittente personalizzato e parli con un nuovo pubblico.

### Email to SMS

Grazie ad Email to SMS è possibile inviare e ricevere SMS dal tuo programma di posta elettronica (Outlook, Mail, Gmail, Hotmail, Libero) preferito o app con funzionalità email. È compatibile con tutti i programmi desktop o webmail. Non richiede alcun software aggiuntivo.

### SMS Group

Con SMS Group è possibile creare gruppi / liste di numeri di cellulare in automatico via SMS. Comunicando e promuovendo l'iscrizione tramite il servizio di ricezione SMS si possono inviare SMS multipli a tutti i membri del gruppo!

" L'SMS è l'unico strumento  
che ti permette di contattare  
davvero tutti!"

**51.000+** aziende ci hanno già scelto



BOSCOLO



Lufthansa



LA  
SALUTE  
IN UN CLIC

Sistema Socio Sanitario  
Regione  
Lombardia  
ASST Cremona



[www.skebby.it](http://www.skebby.it)



[vendite@skebby.it](mailto:vendite@skebby.it)



0283508000