GUIDA ALLA SICUREZZA DIGITALE

Proteggi i tuoi dati, il tuo denaro e la tua tranquillità

Ogni giorno utilizziamo smartphone, computer e servizi bancari online per gestire attività personali e professionali. Per questo motivo **è fondamentale conoscere le principali minacce informatiche** e **adottare semplici comportamenti** che permettono di navigare e operare online in modo sicuro.





LE REGOLE D'ORO DELLA SICUREZZA ONLINE



Custodisci con attenzione le tue credenziali

- **Password, PIN, codici temporanei (OTP) e dati delle carte sono strettamente personali.** Non condividere mai queste informazioni con nessuno.



Accedi ai servizi solo attraverso canali ufficiali

- **Digita sempre l'indirizzo del sito nella barra del browser** o utilizza esclusivamente l'**applicazione ufficiale**.



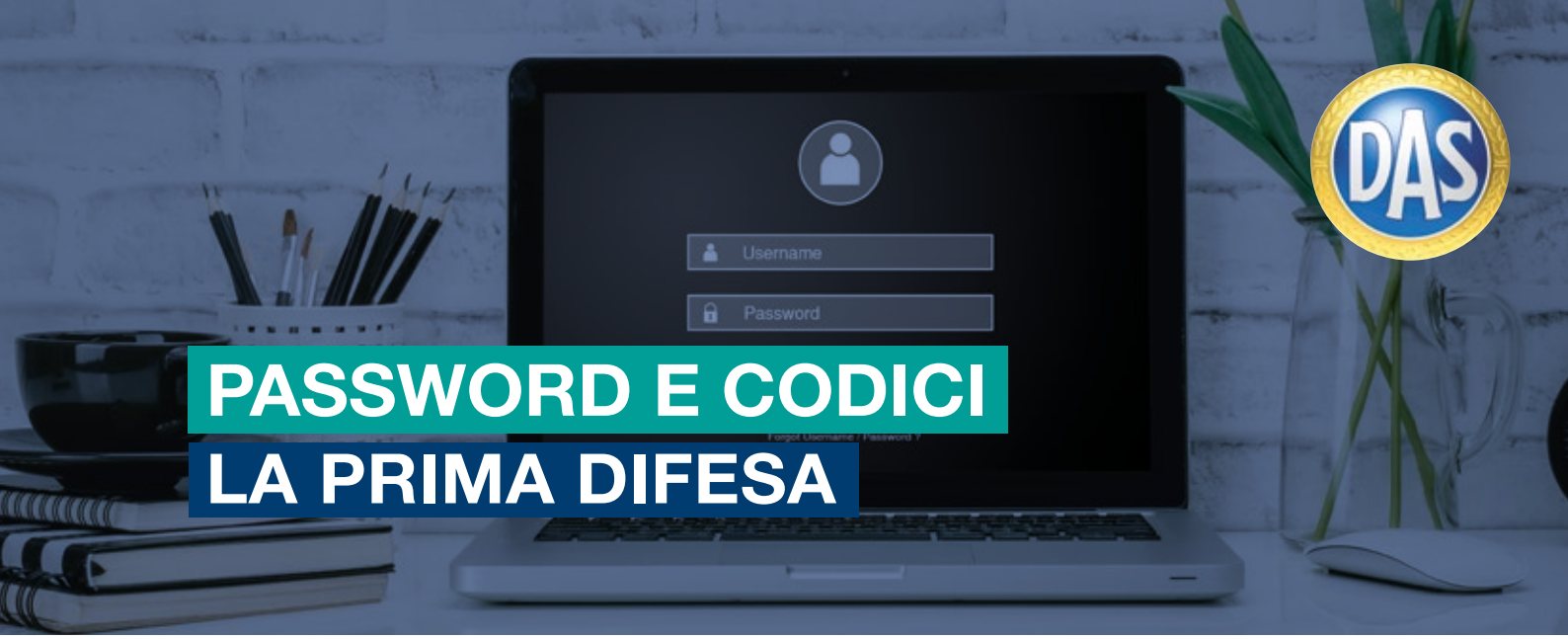
Mantieni alta l'attenzione

- Prima di autorizzare un'operazione, **verifica attentamente l'importo, il beneficiario e la causale**.



Controlla periodicamente i movimenti

- **Monitorare con regolarità il conto corrente e le carte di pagamento** permette di individuare tempestivamente eventuali anomalie.



PASSWORD E CODICI
LA PRIMA DIFESA

Una corretta gestione delle credenziali rappresenta il primo livello di protezione.

Consigli utili:



Utilizza **password diverse** per servizi differenti.



Cambia periodicamente le credenziali più importanti.



Evita di annotare PIN e password insieme alle carte.



Attiva, quando possibile, **l'autenticazione a due fattori**.



Ricorda:

Nessun operatore legittimo ti chiederà di comunicare password, PIN o codici OTP.



ATTENZIONE AI MESSAGGI FRAUDOLENTI



IL PHISHING

Il **phishing** è una tecnica utilizzata per sottrarre informazioni personali attraverso email, SMS o messaggi apparentemente affidabili. I **criminali informatici** cercano di **creare urgenza e preoccupazione** per spingere la vittima ad **agire senza riflettere**.



Segnali di allarme

- ! **Richieste urgenti.**
- ! **Errori grammaticali o contenuti poco chiari.**
- ! **Link sospetti.**
- ! **Promesse o minacce insolite.**
- ! **Richiesta di dati personali o bancari.**



Come comportarsi

- ✓ **Non cliccare sui collegamenti ricevuti.**
- ✓ **Non scaricare allegati inattesi.**
- ✓ **Contatta direttamente il servizio clienti tramite canali ufficiali.**

SMISHING
IL PHISHING VIA SMS

COS'È LO SMISHING

Lo **smishing** utilizza **SMS o messaggi di chat** per indurre gli utenti a fornire informazioni riservate.



Obiettivo dei truffatori

- **Ottenere credenziali di accesso.**
- **Recuperare dati delle carte.**
- **Convincere a effettuare bonifici o ricariche.**
- **Installare software dannosi.**



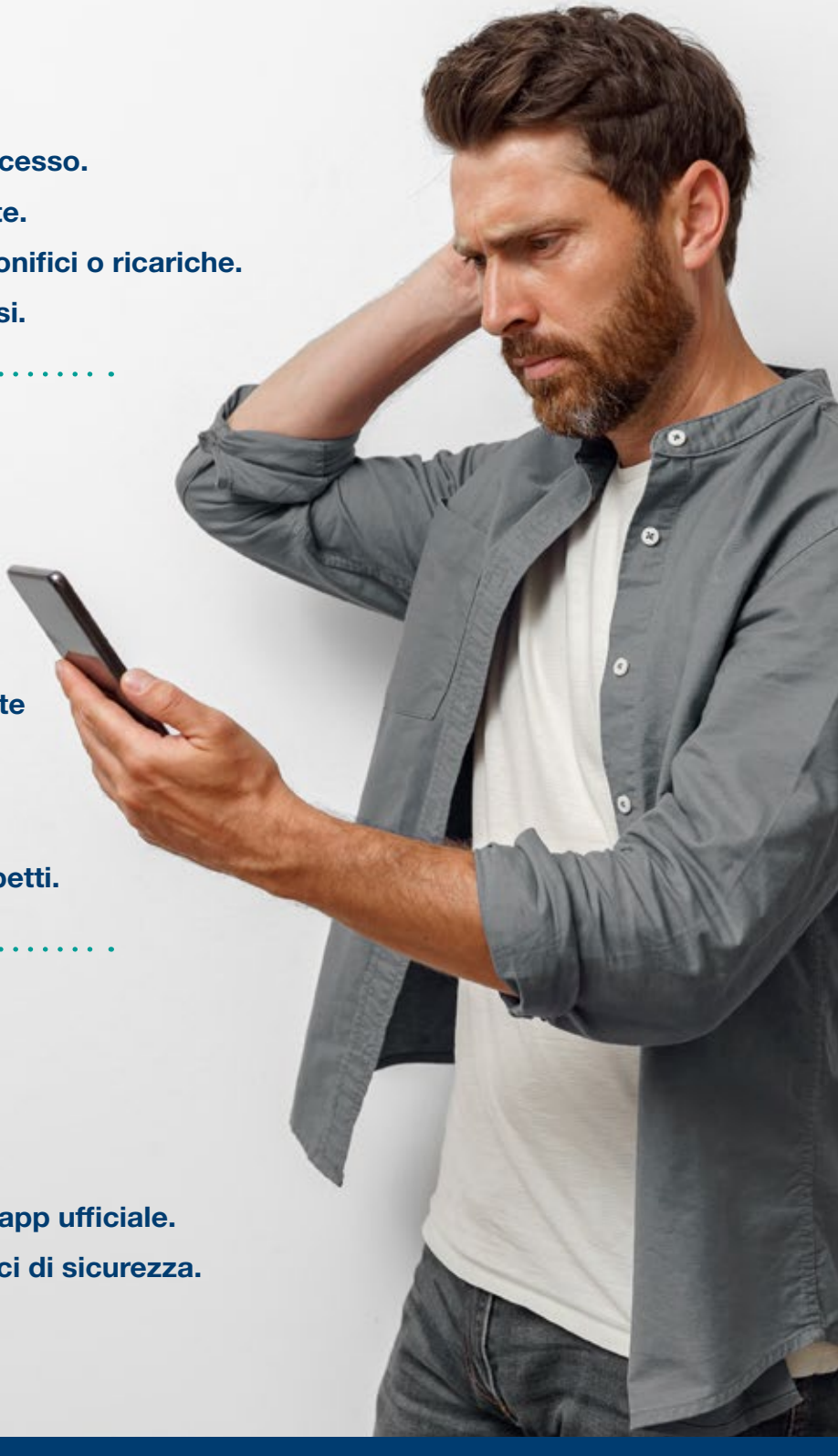
Come riconoscerlo

- **Messaggi che segnalano blocchi imminenti.**
- **Richieste di verifica urgente del conto.**
- **Link abbreviati o poco riconoscibili.**
- **Numeri sconosciuti o sospetti.**



Buone pratiche

- **Ignora il link.**
- **Verifica direttamente dall'app ufficiale.**
- **Non condividere mai codici di sicurezza.**



SMISHING
IL PHISHING VIA SMS

ESEMPIO DI TENTATIVO DI FRODE ONLINE

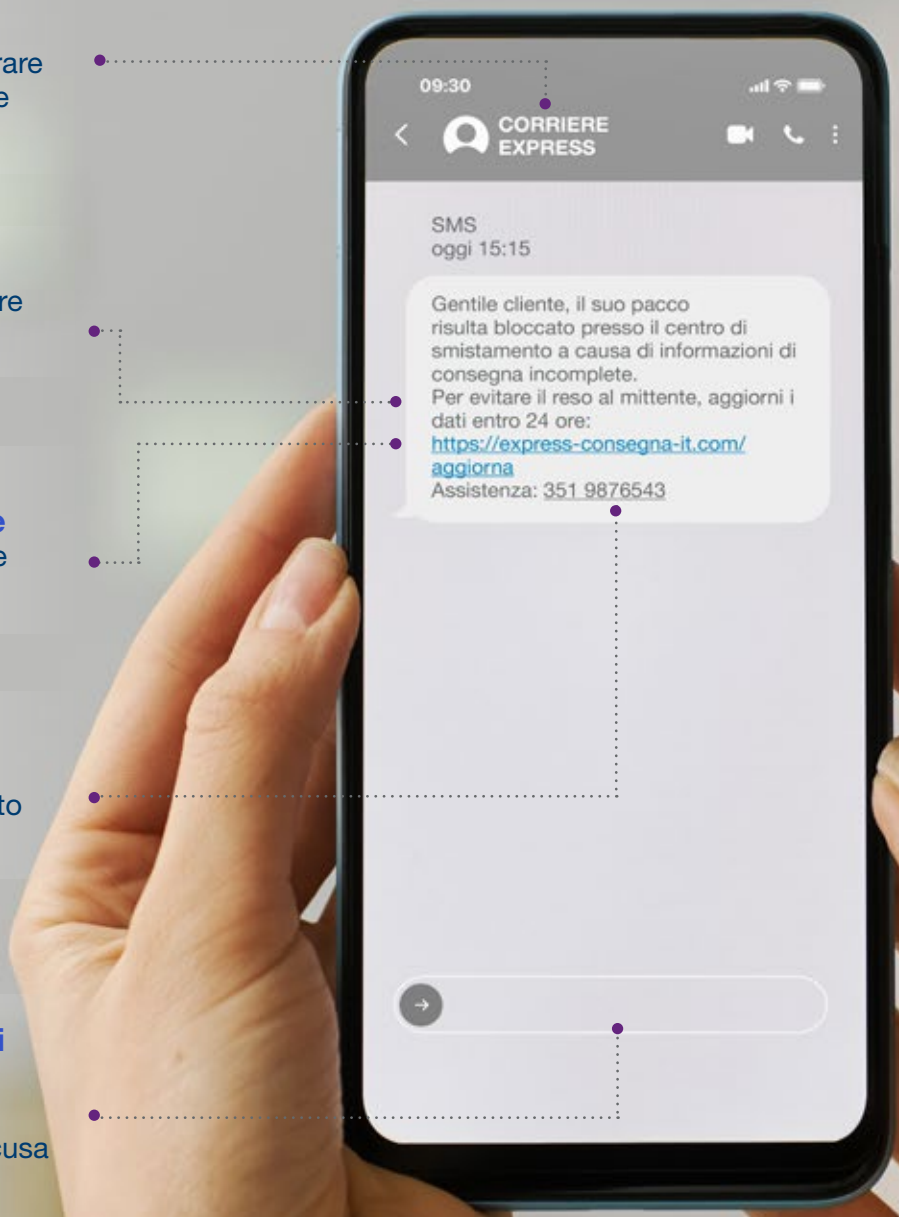
Attenzione!
Il nome del corriere può sembrare autentico ma essere facilmente falsificato.

Il testo crea urgenza
L'invito ad agire entro poche ore spinge a fare scelte impulsive.

Il link non appartiene al sito ufficiale del corriere
Controlla sempre attentamente l'indirizzo web.

Il numero indicato non è un contatto ufficiale
Verifica sempre i recapiti sul sito ufficiale dell'azienda.

Non inserire dati personali o di pagamento
I truffatori possono richiedere informazioni sensibili con la scusa della consegna.





VISHING
LE TRUFFE TELEFONICHE

IL VISHING

I truffatori possono fingersi operatori bancari, consulenti tecnici o addetti all'assistenza clienti.



Le tecniche più comuni

- ! Simulazione di emergenze.
- ! Segnalazione di operazioni sospette.
- ! Richiesta di trasferimenti di denaro.
- ! Invito a installare software di controllo remoto.



Ricorda sempre

Un operatore autentico non ti chiederà mai:

- ⊗ Password.
- ⊗ PIN.
- ⊗ Codici OTP.
- ⊗ Disposizioni di pagamento.
- ⊗ Trasferimenti di denaro verso "conti sicuri".

In caso di dubbio...

Chiudi la chiamata e richiama tu stesso il numero ufficiale dell'organizzazione.

DIFENDITI DAI MALWARE

COSA SONO I MALWARE

I **malware** sono **programmi dannosi** progettati per compromettere dati e dispositivi.

Possono essere diffusi attraverso:

- **Allegati email infetti.**
- **Download da siti non affidabili.**
- **Software contraffatti.**
- **Applicazioni provenienti da store non ufficiali.**



Come proteggersi

- ✔ **Installa un antivirus affidabile.**
- ✔ **Mantieni aggiornato il sistema operativo.**
- ✔ **Scarica applicazioni solo da fonti ufficiali.**
- ✔ **Evita siti web poco attendibili.**
- ✔ **Esegui backup periodici dei dati.**





Scegli di navigare in sicurezza

Proteggi i tuoi dati, il tuo denaro e la tua tranquillità



UTILIZZA RETI SICURE

Le reti Wi-Fi pubbliche possono rappresentare un rischio per la sicurezza.



Per una connessione più sicura

- Preferisci la tua rete domestica.
- Evita di effettuare operazioni bancarie su Wi-Fi pubblici.
- Disattiva la connessione automatica alle reti aperte.
- Aggiorna regolarmente i dispositivi.



Prima di ogni operazione online chiediti:

- Sto utilizzando un canale ufficiale?
- Ho verificato il mittente del messaggio?
- Mi stanno chiedendo dati riservati?
- L'operazione è realmente autorizzata da me?
- Il dispositivo è aggiornato e protetto?

Se hai anche solo un dubbio...

interrompi l'operazione e verifica attraverso i canali ufficiali.

LA NOSTRA SOLUZIONE PER TUTELARTI:

DAS PER TE



DAS per TE ti assiste negli imprevisti legali della vita quotidiana e ti rimborsa le spese necessarie per far valere i tuoi diritti.

Puoi scegliere tra **due soluzioni**:

DAS PER TE MOBILITÀ & TEMPO LIBERO

Protegge la tua famiglia nell'ambito della **mobilità**, dello **sport**, dei **viaggi** e delle **vacanze**.

DAS PER TE VITA PRIVATA & LAVORO

Offre una **tutela completa nell'ambito della vita privata e lavorativa**.

- Puoi affidarti ai nostri legali con l'opzione "**Affidati a DAS**"
- **Tutela opzionale** degli **immobili dati in affitto**

Le garanzie innovative per la tua tutela digitale

Cosa ti offre

*** CERTIFICAZIONE CONTENUTI DIGITALI**

Per dare valore di prova autentica a foto, video e altri contenuti acquisiti con un supporto digitale.

Tecnologia

Metodologia forense brevettata contro ogni tipo di manipolazione

Certificazione

Acquisizione in tempo reale di foto, video, screenshot, e audio

Valore

Garantisce **autenticità e immutabilità dei dati con valore legale**

Prove

Raccogli **prove valide** per la tua difesa e per un'**azione legale**

*** INVIO TELEMATICO QUERELA**

Per presentare una denuncia alle autorità, senza dover uscire di casa, seguendo una semplice procedura guidata. Utile per denunciare truffe e violazioni online.

1. **Accedi alla piattaforma DAS**
2. **Seleziona la tipologia di reato**
3. **Compila con i dati necessari**
4. **Trasmetti la querela per la validazione e ottieni la conferma di deposito**

*** DIGITALE SICURO**

(disponibile con la forma di garanzia "Vita privata e Lavoro")

Per tenere sotto controllo i tuoi dati personali e finanziari ed evitare il rischio che siano utilizzati sul web in modo fraudolento. Puoi utilizzare la piattaforma Digitale Sicuro anche per scaricare strumenti di navigazione online sicura sui tuoi dispositivi digitali. La copertura di assistenza digital completa la tua protezione.

Scopri il prodotto DAS PER TE al seguente link e richiedi un preventivo gratuito
https://www.das.it/prodotti/das-per-te

D.A.S. SpA - Assicurazioni Difesa Legale
Sede e Direzione Generale: Via Enrico Fermi, 9/B · 37135 Verona
Tel. 045 8372611 · Fax 045 8300010

dasdifesalegale@pec.das.it
www.das.it

Messaggio pubblicitario con finalità promozionale. Prima della sottoscrizione leggere il set informativo disponibile su www.das.it