ORDINE
DEGLI INGEGNERI
DELLA PROVINCIA
DI ANCONA



Vademecum

del **cittadino digitale** consapevole

Sommario

Perché questo vademecum 3

01 Gli strumenti digitali 4
Identità digitale: SPID,CIEeIT-Wallet
I servizi pubblici online

02 Il lato oscuro dell'intelligenza artificiale 10
Il fenomeno in numeri
Due casi reali
Come funzionano queste truffe
Riconoscere deepfake e vishing

03 Regole pratiche 14
Proteggere i dati personali
Social, privacy e foto dei minori
Proteggere la casa connessa
Le dieci regole del cittadino digitale consapevole

04 Per gli Ordini: come organizzare un incontro con i cittadini 22
A chi si rivolge e con chi organizzarlo
Scaletta proposta
Consigli pratici

Fonti 23

Perché questo vademecum

Questo vademecum ha due scopi: aiutare i cittadini a usare in sicurezza i servizi digitali della Pubblica Amministrazione e a riconoscere le truffe rese possibili dall'intelligenza artificiale, e offrire agli Ordini degli Ingegneri una base pronta per organizzare incontri analoghi sul proprio territorio. Nasce dall'esperienza dell'Ordine degli Ingegneri della provincia di Ancona, che ha portato il tema in varie città marchigiane, da Senigallia a Fabriano, passando per Jesi e Ancona, con incontri su SPID, CIE, funzionamento dei portali pubblici e dinamiche delle truffe online. I contenuti sono curati dagli esperti della Commissione Innovazione Tecnologica e Digitalizzazione (ITD).

Il divario digitale è un problema concreto. Secondo i dati Istat 2026 citati dalla stampa, nelle Marche circa una famiglia su 10 non ha accesso a internet. Il motivo più frequente è la difficoltà d'uso (55,3%), e gli ostacoli maggiori riguardano anziani e persone con livello socio-economico più basso. Secondo la Mappa dei Comuni Digitali di Anci e Banca d'Italia, inoltre, circa un Comune su quattro ha subìto attacchi informatici con disservizi (Il Resto del Carlino, 11 novembre 2026).

DIGITALmeet 2026 è la 14ª edizione del progetto promosso dalla Fondazione Comunica: dal 19 al 24 ottobre, più di 150 eventi in 20 regioni e circa 200 speaker. Il tema dell'anno è «l'anno zero dell'alfabetizzazione AI». Il vademecum ne riprende il filo: gli stessi strumenti digitali che semplificano la vita ai cittadini, se non sono ben conosciuti, aprono la porta a nuove truffe, e conoscerli bene è la prima difesa.

Da qui la scelta di tenere insieme, in un unico percorso, gli strumenti e le difese: molti cittadini non conoscono SPID, CIE, i portali dei servizi pubblici o l'app IO, e chi li conosce ha spesso dubbi su come usarli in sicurezza. Il vademecum procede perciò in quattro passi, ciascuno costruito sul precedente:

- **Gli strumenti digitali:** cosa sono e come si usano SPID, CIE, IT-Wallet, App IO, SEND, pagoPA, domicilio digitale e ANPR, compreso il modo di ottenere certificati anagrafici senza andare allo sportello.
- **Il lato oscuro dell'AI:** come la stessa tecnologia può essere usata per ingannarci e come riconoscere truffe e deepfake.
- **Regole pratiche:** le abitudini concrete che permettono di difendersi, dalla verifica in due passaggi alla privacy dei social, dalla sicurezza dei dispositivi di casa fino alle dieci regole del cittadino digitale consapevole.
- **Per gli Ordini:** come trasformare tutto questo in un incontro pubblico con i cittadini.

01

Gli strumenti digitali

Tutto parte dall'identità digitale, la chiave che apre i servizi pubblici online. Questa parte spiega prima come ci si identifica (SPID, CIE, IT-Wallet), poi quali servizi si raggiungono con quelle credenziali e come usarli senza sportello e senza rischi.

Identità digitale: SPID, CIE e IT-Wallet

SPID, CIE eIT-Wallet sonotre strumenti con lo stesso obiettivo: dimostrare chi siamo online in modo sicuro, senza password deboli o ripetute ovunque.

Strumento	Cos'è	Stato
SPID	Sistema Pubblico di Identità Digitale: username, password e un secondo codice rilasciati da un gestore accreditato (Poste, Aruba, Namirial, InfoCert, TIM e altri)	Attivo dal 2016
CIE	Carta d'Identità Elettronica con chip, usata con l'app CieID e la lettura NFC della carta	Attiva oggi
IT-Wallet	Un'unica app per i documenti digitali (patente, tessera sanitaria, Carta europea della disabilità e, via via, altri documenti (ISEE, titoli di studio, tessera elettorale)), parte del progetto europeo EUDI Wallet previsto da eIDAS 2	Già attivo su App IO, con nuovi documenti in ar r ivo

Come accedere con SPID

1. Avere un'identità SPID attiva, rilasciata da uno dei gestori accreditati AgID.
2. Sul sito del servizio (INPS, Agenzia delle Entrate, il proprio Comune) cliccare su «Entra con SPID».
3. Scegliere il proprio gestore dall'elenco proposto.
4. Inserire username e password del gestore.
5. Confermare l'accesso con il secondo fattore: notifica sull'app o codice OTP.

SPID resta il sistema di accesso più usato, con 27,7 accessi annui per utente nel 2026, ma i dati dell'Osservatorio Digital Identity & Wallet del Politecnico di Milano mostrano un equilibrio che cambia: gli accessi con SPID calano, mentre cresce la CIE.

Indicatore	2025	2026
Identità SPID	41,5 milioni attive tra i maggiorenni (82%), a ottobre	43,4 milioni rilasciate, di cui 32 milioni attive, a settembre
Accessi con SPID	Oltre 1,3 miliardi nell'anno (stima)	873,6 milioni nei primi nove mesi, il 10% in meno dello stesso periodo del 2025
Carte d'identità elettroniche valide	48,4 milioni, a ottobre	57,4 milioni, a settembre (+19% in un anno)
Utenti CIE con credenziali digitali (CieID)	9 milioni, a ottobre	14,7 milioni di utenti attivi, a settembre

Fonte: Osservatorio Digital Identity & Wallet, Politecnico di Milano (dati presentati a novembre 2025 e a novembre 2026). Le rilevazioni non usano sempre le stesse definizioni (identità «rilasciate» o «attive»), quindi i confronti sono indicativi.

SPID ha tre livelli di sicurezza. Il livello 1 richiede solo username e password; il livello 2, il più diffuso, aggiunge un secondo fattore (codice OTP o notifica su app); il livello 3 prevede ulteriori soluzioni di sicurezza, come dispositivi fisici. Ogni servizio richiede un livello minimo. Usare SPID per accedere ai servizi è gratuito; l'attivazione presso i gestori può invece essere gratuita o a pagamento, con riconoscimento di persona, da remoto o con documento elettronico. Si possono avere più identità, anche con gestori diversi.

Come accedere con CIE

1. Avere la CIE 3.0 con il PIN a 8 cifre attivato.
2. Scaricare l'app ufficiale CieID sullo smartphone.
3. Sul sito del servizio cliccare su «Entra con CIE».
4. Inquadrare il QR code a schermo con l'app, poi appoggiare la carta sul retro dello smartphone (lettura NFC).
5. Inserire il PIN nell'app per confermare.

La CIE è ormai il documento più diffuso e il suo uso online cresce, ma resta inferiore a quello di SPID, anche perché PIN e PUK arrivano in due metà separate (una sulla ricevuta, l'altra inviata a parte) e spesso vengono smarriti. Conviene conservarli con cura. Se si perdono, il PUK si recupera con la funzione «Recupero PUK» dell'app CieID (serve uno smartphone con NFC e aver indicato un'email o un cellulare alla richiesta della carta) e poi si imposta un nuovo PIN; in alternativa ci si rivolge al Comune.

Oltre all'accesso con la carta, esistono le credenziali CIE di livello 1 e 2 (password e secondo fattore tramite SMS o app CieID), da attivare con il proprio PIN.

IT-Wallet: il portafoglio digitale

- **Già attivo:** dal dicembre 2024 si usa dentro l'App IO, nella sezione Portafoglio, accedendo con SPID o CIE. Oggi vi si possono aggiungere patente di guida, tessera sanitaria e Carta europea della disabilità; secondo gli osservatori, la versione digitale vale come l'originale per i servizi online e in presenza.
- **In arrivo:** altri documenti e attestazioni (ISEE, titoli di studio, tessera elettorale, certificati anagrafici). La carta d'identità digitale non è ancora nel portafoglio.
- **Si mostra solo ciò che serve:** si potrà provare la maggiore età senza rivelare la data di nascita esatta.

- **Un progetto europeo:** IT-Wallet anticipa l'EUDI Wallet previsto da eIDAS 2; entro il 24 dicembre 2026 ogni Stato membro dell'UE deve rendere disponibile un portafoglio digitale conforme. Secondo l'Osservatorio Digital Identity & Wallet, SPID e CieID potranno essere usati per attivare il wallet fino a febbraio 2028, previa verifica del possesso e dell'integrità della CIE.
- **Non è obbligatorio:** affiancherà SPID e CIE, che restano disponibili come alternative.

I servizi pubblici online

Con SPID o CIE si accede a una serie di servizi nazionali e regionali che evitano code e sportelli. Per ciascuno vale la stessa regola: partire sempre dal portale o dall'app ufficiale, mai da un link ricevuto per messaggio.

Servizio	A cosa serve	Attenzione
ANPR (anpr.interno.it)	Anagrafe Nazionale: certificati di residenza, stato di famiglia, nascita, cittadinanza, stato libero, con piena validità legale, accedendo con SPID, CIE o CNS	L'unico indirizzo ufficiale è anpr.interno.it: esistono siti-clone per rubare le credenziali
App IO	Documenti (patente, tessera sanitaria), avvisi di pagamento pagoPA, messaggi e notifiche degli enti pubblici	Installare, aggiornare e proteggere sempre l'app
SEND (cittadini.notifichedigitali.it)	Notifiche di atti degli enti, ad esempio una violazione del codice della strada, consultabili con SPID, CIE o App IO e pagabili con pagoPA. Esiste anche la versione per le imprese (imprese.notifichedigitali.it)	Usare solo il portale o l'app ufficiale
pagoPA	Pagamenti verso enti aderenti tramite canali e prestatori abilitati	Verificare ente creditore, importo, causale e codice dell'avviso; conservare la ricevuta; non partire da link anomali
ANNCSU (anncsu.gov.it)	Archivio Nazionale dei Numeri Civici delle Strade Urbane: indirizzi consultabili in mappa, utile per individuare e segnalare anomalie	Un indirizzo corretto migliora servizi e comunicazioni
Fascicolo Sanitario Elettronico	Documenti e informazioni sanitarie messi a disposizione dalla Regione (servizio regionale)	Diffidare di falsi messaggi su visite, prenotazioni o referti; usare il portale o l'app della propria Regione

Prima di ogni pagamento digitale, fermarsi e confrontare i dati dell'avviso: la comodità richiede sempre una verifica.

Certificati anagrafici senza andare allo sportello

Tra i servizi della tabella, l'ANPR è quello che più cambia la vita quotidiana: permette di ottenere online, in pochi passaggi e con piena validità legale, certificati di residenza, stato di famiglia, nascita, cittadinanza e stato libero.

1. Aprire il portale ufficiale anpr.interno.it, controllando l'indirizzo esatto nella barra del browser.
2. Accedere all'area cittadino con SPID, CIE o CNS.
3. Scegliere il certificato desiderato e seguire la procedura.
4. Scaricare il documento: niente appuntamento, niente coda.

Il download può essere gratuito o a pagamento a seconda dell'utilizzo del certificato. Anche i certificati anagrafici sono tra i documenti attesi in IT-Wallet.

Domicilio digitale: le comunicazioni della PA con valore legale

Un altro strumento che completa i precedenti è il domicilio digitale: un indirizzo di posta elettronica certificata (PEC) eletto per ricevere le comunicazioni ufficiali della Pubblica Amministrazione, con valore legale. Per le imprese e i professionisti iscritti ad albi è obbligatorio; per i cittadini maggiorenni è facoltativo e gratuito.

- **Come si registra:** sul portale domiciliodigitale.gov.it, accedendo con SPID, CIE o CNS e indicando una PEC già attiva. L'indirizzo scelto va confermato con il messaggio ricevuto nella casella.
- **Dove viene registrato:** nell'INAD, l'Indice Nazionale dei Domicili Digitali, realizzato da AgID, Dipartimento per la trasformazione digitale e InfoCamere.
- **Un'attenzione in più:** controllare con regolarità la casella PEC, perché le comunicazioni ricevute hanno valore legale, e usare solo il portale ufficiale per registrare o modificare il domicilio.

Sono strumenti pensati per semplificare la vita, ma proprio perché danno accesso a dati e pratiche importanti attirano chi vuole ingannarci. Ed è qui che entra in gioco l'intelligenza artificiale, come alleata e come minaccia.

02

Il lato oscuro dell'intelligenza artificiale

Gli strumenti visti finora funzionano anche grazie all'intelligenza artificiale, che lavora dietro le quinte per rendere i servizi più semplici, veloci e sicuri. La stessa tecnologia può però essere usata anche per ingannarci.

Usi utili, ogni giorno	Usi pericolosi, da riconoscere
Riconoscimento di documenti e volti per velocizzare l'accesso ai servizi	Voci clonate da pochi secondi di audio pubblico
Assistenti virtuali che rispondono ai cittadini	Video deepfake di persone reali o enti ufficiali
Sistemi antifrode che individuano pagamenti sospetti	Chiamate di vishing automatizzate su larga scala
Traduzione automatica e sottotitoli in tempo reale	Messaggi di phishing scritti su misura per la vittima

Il fenomeno in numeri

Quanto è diffuso il rischio? Alcuni dati aiutano a dimensionarlo.

Dato	Fonte
61% degli italiani teme che l'AI venga usata per truffarli	Sondaggio Ipsos
Circa 1 tentativo di frode biometrica su 5 coinvolge un deepfake; i selfie deepfake sono aumentati del 58% nel 2025	Entrust, Identity Fraud Report 2026
Almeno 36 milioni di € non recuperati, su circa 95 milioni trasferiti in poche ore, nel caso Fideuram (febbraio 2026)	Stampa nazionale (ANSA, Corriere della Sera), settembre 2026

Due casi reali

I numeri diventan opiù chiari guardando due casi recenti, molto diversi per bersaglio ma simili nel metodo.

- **Caso Fideuram (febbraio 2026, reso noto a settembre).** Un falso messaggio WhatsApp, attribuito all'amministratore delegato di Intesa Sanpaolo, proponeva a un dirigente della banca una presunta operazione finanziaria riservata. Per renderlo credibile i truffatori hanno aggiunto una telefonata con la voce, riprodotta con l'AI, di un avvocato noto alla vittima. In poche ore sono usciti circa 95 milioni di euro, in gran parte verso l'estero: una parte è stata recuperata, ma almeno 36 milioni, convertiti in criptovalute, risultano ancora da rintracciare e la Procura di Milano indaga. La lezione: nessun canale, da solo, basta più a confermare un'identità.
- **Video deepfake su Banca d'Italia (dal 2024, nuovi avvisi nel 2026).** Video manipolati riproducono volto e voce del Governatore per promuovere falsi investimenti, spesso con inserzioni a pagamento sui social e in stile trasmissione televisiva. Banca d'Italia ha pubblicato più avvisi, ha denunciato i falsi all'autorità giudiziaria e ricorda che le sue comunicazioni ufficiali escono solo sul proprio sito e sui canali istituzionali; nuove versioni dei video continuano però a comparire.

Come funzionano queste truffe

Dietro i due casi c'è uno schema comune, che si ripete con piccole varianti anche ai danni dei cittadini comuni.

1. **Raccolta della voce.** Bastano pochi secondi di audio pubblico (un video sui social, una videochiamata, un messaggio in segreteria) per addestrare un modello che riproduce timbro, accento e intonazione in modo quasi indistinguibile.
2. **Contatto e pressione.** Un messaggio o una chiamata che simula un dirigente, un familiare o un operatore bancario crea un'emergenza: un pagamento da sbloccare, una frode da fermare, una persona cara in difficoltà. La pressione psicologica è parte della truffa.
3. **Superamento dei controlli.** Voce o volto clonati possono ingannare anche i sistemi di riconoscimento biometrico (liveness detection) di alcune app bancarie.
4. **Richiesta di denaro o dati.** Si chiede un bonifico immediato verso un conto nuovo, oppure un OTP, un PIN o una password con la scusa di «verificare» o «sbloccare» un'operazione. L'urgenza serve a impedire ogni verifica autonoma.

Riconoscere deepfake e vishing

Conoscere lo schema aiuta a riconoscerlo mentre accade. Due principi valgono sempre: il numero visualizzato sul telefono non è una prova di identità e, a orecchio, un clone vocale può essere indistinguibile, quindi contano il contesto e la richiesta.

Vishing: telefonate truffa potenziate dall'AI

Il vishing (phishing telefonico) esiste da anni, ma l'AI lo ha reso più economico, credibile e diffuso.

- **Voce sintetica in tempo reale:** naturale, in italiano corretto, senza più gli errori grammaticali che smascheravano le vecchie truffe.
- **Numero falsificato:** lo spoofing fa apparire sul display un numero noto (banca, ente, familiare) anche se la chiamata arriva da altrove.
- **Automazione su larga scala:** molte chiamate in parallelo, con script che si adattano alle risposte della vittima.

In caso di dubbio si riattacca e si richiama un numero già noto, cercato autonomamente.

Segnali di un video deepfake

- Movimenti di labbra e occhi leggermente innaturali o non sincronizzati con l'audio.
- Illuminazione o ombre sul volto incoerenti con il resto dell'inquadratura.
- Voce quasi perfetta ma con intonazione troppo uniforme, priva delle piccole imperfezioni del parlato reale.
- Loghi, grafiche o contesti che imitano un canale ufficiale ma con dettagli leggermente sbagliati.
- Contenuto che promette guadagni facili o richiede un'azione urgente: anche il messaggio, non solo l'immagine, è un indizio.

03
Regole pratiche

Le truffe descritte sfruttano sempre le stesse leve: urgenza, fiducia e dati facilmente reperibili. Le difese sono di conseguenza poche abitudini, applicate sempre: proteggere gli account, non inviare mai documenti a chi ci contatta a sorpresa, ridurre ciò che di noi è pubblico sui social, curare la sicurezza dei dispositivi di casa e verificare ogni richiesta urgente attraverso un canale diverso.

Proteggere i dati personali

Il documento d'identità si mostra di persona a un servizio regolato dalla legge; non si invia mai a chi ci contatta a sorpresa, anche se sembra autorevole.

Documenti d'identità: quando sì, quando mai

- **Sì, per legge.** In hotel, B&B o affittacamere il gestore deve verificare il documento di persona e comunicare i dati alla Questura entro 24 ore (art. 109 TULPS, R.D. 773/1931). Una circolare del Ministero dell'Interno (novembre 2024), poi confermata dal Consiglio di Stato (2025), precisa che il check-in da remoto non basta senza una verifica visiva effettiva: la corrispondenza tra persona e documento va accertata di persona o con un videocollegamento che la consenta. È un obbligo di comunicazione dei dati, non un'autorizzazione a conservare copie del documento oltre il necessario.

- **No, mai.** Non si invia una foto o copia del documento via email, WhatsApp o SMS a chi telefona dicendo di essere una banca, un ente pubblico o le forze dell'ordine, nemmeno per un presunto controllo di sicurezza.

- **Il campanello d'allarme tipico:** «abbiamo rilevato un'operazione sospetta sul suo conto, ci mandi subito una foto del documento per bloccarla». La frase è costruita per impedire di verificare con calma.

- **Nessun ente ufficiale** chiede l'invio del documento per sbloccare un conto o una pratica con urgenza. Un vero controllo si svolge di persona, mai per telefono o chat.

Verifica in due passaggi (2FA)

La **2FA** aggiunge alla password un secondo codice, generato da un'app o inviato via SMS. Conta oggi perché, anche se l'AI aiuta a rubare una password con il phishing, senza il secondo fattore l'accesso resta bloccato.

- **Dove attivarla:** email, social (Instagram, Facebook), home banking. SPID la richiede già di default.
- **Come si fa:** nelle impostazioni dell'account, alla voce «Sicurezza» o «Verifica in due passaggi» / «Autenticazione a due fattori».

Social, privacy e foto dei minori

Dopo aver protetto gli account, resta da ridurre ciò che di noi è pubblico. Un profilo social aperto è la porta d'ingresso delle truffe con AI: foto, video e audio diventano materiale liberamente scaricabile per addestrare deepfake e cloni vocali.

- **Foto e video pubblici:** bastano poche immagini o pochi secondi di video per un deepfake credibile del volto.
- **Audio pubblico:** storie, reel e messaggi vocali forniscono il campione di voce necessario al voice cloning.
- **Informazioni personali:** nomi dei familiari, luoghi frequentati e abitudini rendono la truffa più credibile.

Come impostare la privacy (meno di un minuto)

- **Instagram:** Impostazioni e privacy → Privacy dell'account → Account privato.
- **Facebook:** Impostazioni → Privacy → Chi può vedere i tuoi contenuti futuri → Amici. Evitare «Pubblico».

Le voci di menù possono cambiare leggermente a seconda della versione dell'app.

Un pensiero in più per le foto dei minori

Una foto innocente di un bambino o di un ragazzo, pubblicata su un profilo pubblico, può essere scaricata e modificata con strumenti di AI per creare contenuti offensivi o pericolosi.

- Mantenere privati i profili propri e, quando possibile, quelli dei figli minorenni.
- Evitare di pubblicare foto di bambini in contesti pubblici o su profili non protetti, anche per amici e parenti.
- Non condividere informazioni che identificano scuola, luoghi abituali o percorsi quotidiani di un minore.
- Parlarne in famiglia con un linguaggio adatto all'età, senza allarmismo ma con chiarezza.

A chi rivolgersi

Se un genitore scopre che una foto di un figlio minorenne è stata usata in modo improprio, non deve gestirlo da solo: i canali sono gratuiti e riservati.

Chi	Cosa offre
Polizia Postale (commissariatodips.it, o il commissariato più vicino)	Riceve segnalazioni su materiale che ritrae minori diffuso online e coordina la rimozione tramite il Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO)
Telefono Azzurro, 1.96.96	Gratuito, attivo 24 ore su 24: ascolto e supporto a genitori e ragazzi, anche per contenuti online non autorizzati
Garante per la protezione dei dati personali (garanteprivacy.it)	Segnalazione dell'uso illecito dell'immagine di un minore e richiesta di rimozione dei contenuti

Proteggere la casa connessa

Dopo gli account e i profili, resta da proteggere la casa. Robot aspirapolvere, elettrodomestici, televisori, videocamere e router sono computer a tutti gli effetti: se vengono trascurati, diventano una porta d'ingresso per chi vuole spiarci o usare i nostri apparecchi per scopi criminali. Una singola casa vale poco per i criminali, che puntano sulla quantità: una falla presente in migliaia di modelli identici si sfrutta su larga scala.

Che cos'è una botnet

Una botnet è una rete di apparecchi infettati, a volte centinaia di migliaia, che obbediscono a un unico centro di comando senza che i proprietari se ne accorgano. L'apparecchio continua a funzionare, ma intanto può essere usato per sovraccaricare un sito fino a renderlo irraggiungibile, inviare spam, provare password rubate o nascondere chi commette truffe online. Per il proprietario le conseguenze sono invisibili ma concrete: connessione più lenta, indirizzo di casa segnalato come sospetto dai servizi online e un intruso stabilmente dentro la rete domestica.

Il caso di scuola è Mirai, che nel 2016 riunì telecamere e videoregistratori violati con le password di fabbrica. Più di recente, nel 2025, la botnet Aisuru, fatta soprattutto di router e apparecchi domestici compromessi, ha battuto più volte il record mondiale di traffico, e l'FBI ha lanciato l'allarme su BadBox 2.0, oltre un milione di dispositivi infetti, quasi tutti TV box, proiettori e tablet economici senza marchio.

Dispositivo per dispositivo

Dispositivo	Il rischio	Cosa fare
Robot aspirapolvere	Telecamera, microfono e mappa dettagliata della casa, di solito sui server del produttore; sono stati violati robot comandati a distanza	Disattivare visione remota e microfono se non servono; password unica e verifica in due passaggi; aggiornare il firmware; prima di venderlo o regalarlo, eliminarlo dall'account per cancellare le mappe
Frigoriferi, forni, lavatrici, climatizzatori, caldaie	Computer aggiornati di rado, quindi una porta d'ingresso nella rete di casa; un apparecchio connesso può essere fermato o alterato da lontano	Chiedersi se la connessione serve davvero (offline funzionano come prima); altrimenti rete separata e aggiornamenti; abilitare il controllo remoto solo quando serve
Smart TV e TV box	Bersagli preferiti delle botnet; i box economici possono arrivare con software malevolo già installato; molte TV profilano ciò che si guarda	Aggiornare, installare app solo dallo store ufficiale, disattivare riconoscimento dei contenuti e pubblicità personalizzata, spegnere telecamera e microfono se non servono; lasciare sullo scaffale i TV box senza marchio e senza aggiornamenti
Videocamere e baby monitor	Riprendono gli interni: un accesso abusivo significa qualcuno che guarda e ascolta; errori dei produttori hanno mostrato per sbaglio immagini di altre case	Cambiare la password di fabbrica al primo avvio; verifica in due passaggi; preferire otturatore fisico o modalità privacy e registrazione in locale; non inquadrare camere da letto e bagni; usare l'app ufficiale senza aprire porte sul router; per i neonati, un monitor a radiofrequenza non collegato a Inter net
Serrature, allarmi, videocitofoni	Controllano l'accesso fisico alla casa	Marchi con una politica di aggiornamento dichiarata; notifiche per ogni apertura; verifica in due passaggi; tenere sempre un'alternativa meccanica; se l'apertura da remoto non serve, lasciarle scollegate da Internet
Assistenti vocali, prese e lampadine	Gli smart speaker restano in ascolto; prese e lampadine sono i dispositivi più economici e più spesso senza marchio	Usare il tasto che spegne il microfono nelle conversazioni riservate e cancellare la cronologia dall'app; proteggere con un PIN i comandi vocali per serrature e allarmi; confinare prese e lampadine sulla rete separata

Il router: la porta d'ingresso della rete

Se il router viene compromesso, diventano raggiungibili tutti gli apparecchi e la navigazione può essere dirottata verso siti fasulli. Poche impostazioni, che si aprono dal browser con l'indirizzo riportato sull'etichetta, fanno la differenza:

- Cambiare la password di amministrazione, diversa da quella del wi-fi, e quella della rete, di almeno dodici caratteri, con cifratura WPA3 o WPA2 con protocollo AES.
- Disattivare il WPS, l'UPnP (che permette agli apparecchi di aprire varchi verso Internet senza chiedere il permesso) e la gestione remota del pannello.
- Collegare robot, elettrodomestici, telecamere e prese a una rete separata, come quella per gli ospiti: se uno viene violato, l'intruso non raggiunge computer e smartphone. Poi verificare che tutto funzioni, perché alcuni apparecchi devono dialogare con l'hub sulla rete principale.
- Una volta al mese controllare l'elenco dei dispositivi collegati ed eliminare quelli sconosciuti.
- Far sostituire un modem dell'operatore molto vecchio, che non riceve più aggior namenti.

Marchi sconosciuti e prezzi troppo bassi

Sui marketplace si trovano telecamere a 15 euro e TV box a 25. Dietro molti di questi prodotti c'è lo stesso schema: un unico fabbricante cede l'apparecchio a decine di rivenditori, che lo vendono con nomi diversi e la stessa app generica, così una falla colpisce insieme centinaia di migliaia di dispositivi di marche apparentemente diverse. Ricorrono password uguali per tutti e a volte non modificabili, aggiornamenti rari o assenti, server di società difficili da identificare e app che chiedono accessi senza motivo; nei casi peggiori il software malevolo è installato in fabbrica. Anche i marchi noti hanno avuto falle gravi: conta chi le corregge e per quanto tempo. Segnali d'allarme:

- un nome senza sito ufficiale;
- l'assenza di manuale e assistenza in italiano;
- nessuna indicazione sulla durata degli aggiornamenti;
- una dichiarazione di conformità europea introvabile;
- recensioni che lamentano un'app abbandonata.

Cosa prevede il Cyber Resilience Act

Il regolamento europeo 2024/2847 sulla sicurezza dei prodotti connessi obbliga dall'11 settembre 2026 i fabbricanti a segnalare entro 24 ore le vulnerabilità sfruttate e ad avvisare gli utenti coinvolti, anche per i prodotti già in commercio; in Italia la vigilanza è affidata all'Agenzia per la cybersicurezza nazionale. Dall'11 dicembre 2027 ogni nuovo apparecchio venduto nell'Unione dovrà avere una configurazione sicura di fabbrica e almeno cinque anni di aggiornamenti gratuiti, con la data di fine del supporto indicata all'acquisto. Gli apparecchi già installati nelle case restano però fuori dai nuovi requisiti: la prudenza del cittadino resta necessaria.

Regole valide per tutti i dispositivi

- Una password diversa e lunga per ogni account, gestita con un password manager: il riutilizzo è l'errore più pericoloso, perché le credenziali rubate a un sito vengono provate in automatico su migliaia di altri.
- Verifica in due passaggi prima di tutto sull'app che governa la casa connessa e sull'email; lo smartphone che fa da telecomando va tenuto aggiornato e protetto con un blocco schermo.
- Prima di comprare, cercare sul sito del produttore la data minima fino alla quale sono garantiti gli aggiornamenti e preferire dispositivi compatibili con lo standard Matter.
- Quando il supporto finisce, isolare o sostituire l'apparecchio; prima di venderlo, rimuoverlo dall'account e riportarlo alle impostazioni di fabbrica.
- Non ignorare i segnali: un dispositivo che si muove, parla o si accende da solo, una spia della telecamera accesa senza motivo, accessi all'account da luoghi sconosciuti. In questi casi scollegarlo, cambiare la password, chiudere le sessioni attive e ripristinarlo.
- In caso di accessi abusivi, immagini diffuse online o ricatti, presentare denuncia alla Polizia Postale, anche attraverso il Commissariato di P.S. online.

Le dieci regole del cittadino digitale consapevole

Tutto quanto visto in questo vademecum si riassume in diecireGole.
L'AI è potentissima e inarrestabile: la vera protezione è la consapevolezza, cioè fermarsi un attimo in più prima di agire.

01 **Non fidarsi solo di voce o volto**: un deepfake può essere indistinguibile a orecchio.

02 **Verificare su un canale diverso e ufficiale**: riattaccare e richiamare un numero già noto, cercato autonomamente, mai quello ricevuto.

03 **Non comunicare mai OTP, PIN, password o codici del dispositivo** a nessun operatore, per telefono, chat o email.

04 **Diffidare dell'urgenza**: «fallo subito» e «non dirlo a nessuno» sono i segnali d'allarme più chiari.

05 **Non inviare mai una foto del documento d'identità** a chi ci contatta a sorpresa, anche se si presenta come banca, ente o forze dell'ordine.

06 **Attivare la verifica in due passaggi** su email, social, home banking e app della casa connessa.

07 **Rendere privati i profili social** e limitare ciò che rivelano su volto, voce e abitudini.

08 **Proteggere le foto dei minori**: niente profili pubblici e niente informazioni su scuola, luoghi e percorsi abituali.

09 **Usare solo portali e app ufficiali**: controllare l'indirizzo prima di inserire SPID o CIE e confrontare i dati dell'avviso prima di pagare con pagoPA.

10 **Concordare una «parola di sicurezza»** in famiglia o in azienda per confermare le richieste urgenti di denaro, e segnalare i tentativi sospetti alla propria banca e alla Polizia Postale (consultando anche le indicazioni di ABI e CERTFin).

04

Per gli Ordini: come organizzare un incontro con i cittadini

Dopo aver visto che cosa sapere e che cosa fare, resta il passaggio più importante: portarlo ai cittadini. Il vademecum può essere il filo conduttore di un incontro pubblico, da replicare in altre città e province con gli esperti della propria Commissione o del proprio gruppo di lavoro sul digitale. Quella che segue è una proposta, da adattare al territorio.

A chi si rivolge e con chi organizzarlo

- **Pubblico:** cittadini di ogni età, con particolare attenzione ad anziani, famiglie e persone meno abituate al digitale, che secondo i dati sono le più penalizzate dal divario.
- **Partner possibili:** i Comuni (sede dell'incontro, anagrafe e sportelli al cittadino), la Polizia Postale o altre realtà del territorio per testimonianze e consigli, gestori di identità digitale e banche per le dimostrazioni.
- **Chi cura i contenuti:** gli esperti dell'Ordine in materia di innovazione tecnologica e digitalizzazione.

Scaletta proposta

La scaletta segue lo stesso ordine del vademecum, così che chi partecipa possa poi riprendere a casa ogni passaggio.

Momento	Contenuti	Spunto operativo
1. Apertura e contesto	Perché serve: divario digitale, dati Istat della propria regione, tema dell'alfabetizzazione AI	Usare dati locali per rendere il problema concreto
2. Gli strumenti digitali	SPID, CIE, IT-Wallet, App IO, SEND, pagoPA, ANPR, domicilio digitale	Mostrare le schermate reali dei portali ufficiali e invitare a provare dal proprio smartphone
3. Il lato oscuro dell'AI	Usi utili e usi pericolosi, casi reali, come funzionano le truffe	Scegliere casi recenti e riconoscibili dal pubblico
4. Dimostrazioni pratiche	Voce clonata dal vivo; come riconoscere un video deepfake	Per la voce, usare solo quella di un volontario consenziente e far confrontare originale e clonata
5. Le regole	Le dieci regole, la parola di sicurezza, la privacy dei profili social, la sicurezza dei dispositivi di casa	Consegnare il vademecum, stampato o in digitale
6. Domande e confronto	Dubbi e casi vissuti dal pubblico	Raccogliere le domande per costruire i prossimi incontri

Consigli pratici

- Usare un linguaggio semplice, con esempi concreti e pochi tecnicismi.
- Nelle schermate mostrate usare sempre portali e app ufficiali e non far comparire dati personali reali.
- Preparare i riferimenti locali: sportelli del Comune, servizi sanitari regionali, numeri utili come Polizia Postale e Telefono Azzurro (1.96.96).
- Prevedere un seguito, perché il format funziona meglio se ripetuto e portato in più Comuni.

Fonti

- Il Resto del Carlino, 11 novembre 2026: dati Istat 2026 sulle Marche e mappa Anci-Banca d'Italia dei Comuni digitali
- Osservatorio Digital Identity, Politecnico di Milano: comunicato su SPID, CIE e IT-Wallet (novembre 2025)
- Osservatorio Digital Identity & Wallet: report SPID, CIE e IT-Wallet nel 2026
- ItaliaOggi, Lo Spid arreta, la Cie avanza: dati dell'Osservatorio sui primi nove mesi del 2026
- AgID, Nasce INAD, Indice Nazionale dei Domicili Digitali
- AgID, Domande frequenti su SPID
- Ministero dell'Interno, recupero del PUK della CIE
- Agenda Digitale, IT Wallet: il mosaico dell'identità digitale
- Lentepubblica, IT-Wallet sull'app IO: cosa cambia da settembre 2026
- Smartworld, scadenza UE del 24 dicembre 2026 per il portafoglio digitale
- QuiFinanza, deepfake e truffe AI: i dati in Italia (sondaggio Ipsos)
- Accredity, statistiche su deepfake e frodi sui documenti (Entrust, Identity Fraud Report 2026)
- Il Post, 25 settembre 2026: il caso Fideuram
- Banca d'Italia, avviso sui falsi videomessaggi con tecniche di deepfake
- Altroconsumo, affitti brevi: stop al check-in da remoto (circolare del Ministero dell'Interno)
- Lentepubblica, check-in da remoto e Consiglio di Stato
- Articolo «Come proteggere casa da un attacco hacker: robot aspirapolvere, frigo, smart tv, videocamere di sicurezza e router», 13 novembre 2026 (aggiornato il 14 novembre)