VADEMECUM

Buone pratiche di cybersecurity di base per i dipendenti delle PP.AA.

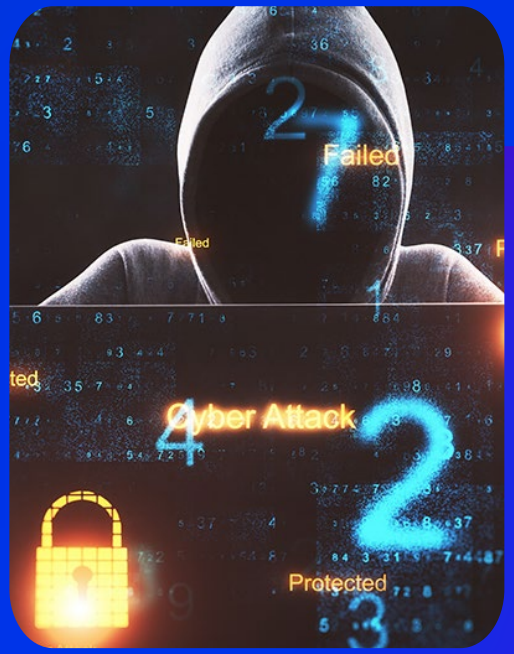
PERCHÉ SERVE PROTEGGERSI

Il contesto digitale è pieno di minacce

Le minacce informatiche crescono ogni giorno. Phishing, ransomware, furti di credenziali, intelligenze artificiali usate in modo malevolo. Spesso, però, non servono tecniche complesse: basta un clic sbagliato.

756

Eventi cyber contro la P.A. nel 2024*



più del 50% partiti da errori umani

OGNI GIORNO DECINE DI PP.AA. VENGONO ATTACCATE

*dalla Relazione annuale al Parlamento 2024 di ACN

CRISI GEOPOLITICHE

Dall’invasione russa dell’Ucraina alla guerra in Medio Oriente si moltiplicano gli attacchi informatici collegati ai conflitti in atto.

Le guerre sono localizzate, ma gli attacchi cyber colpiscono ovunque.

SIAMO SEMPRE SOTTO ATTACCO

LE GUERRE FANNO MALE, MA ANCHE GLI ATTACCHI HACKER

NEGLI ULTIMI ANNI ACN HA RILEVATO CHE CIRCA IL 20% DEGLI ATTACCHI SUBITI DALL'ITALIA HANNO RIGUARDATO LE PP.AA.

SONO STATE COMPROMESSE MOLTE STRUTTURE SANITARIE, BLOCCANDO I SERVIZI DI PRENOTAZIONE, L'OPERATIVITÀ DEI SISTEMI DIAGNOSTICI (TAC E RISONANZE MAGNETICHE), A DANNO DI MIGLIAIA DI CITTADINI E CON CONSEGUENZE REPUTAZIONALI ANCHE A SEGUITO DELLA PUBBLICAZIONE DEI DATI SANITARI DEI PAZIENTI.

SIAMO SEMPRE SOTTO ATTACCO

SONO STATI IMPATTATI FORNITORI DI SERVIZI DIGITALI SISTEMICI, CON RISCHIO DI GRAVI RITARDI DEI PAGAMENTI (IL CASO PIÙ ECLATANTE A DICEMBRE 2023 RIGUARDAVA ANCHE L'EROGAZIONE DELLE TREDICESIME).

SONO STATE IMPATTATE PIÙ VOLTE DIVERSE AMMINISTRAZIONI LOCALI E UNIVERSITÀ, CON RANSOMWARE DEVASTANTI CHE HANNO COMPROMESSO IL PATRIMONIO INFORMATIVO DEI SOGGETTI COLPITI DETERMINANDO CONSEGUENZE SULLA CONTINUITÀ DEI SERVIZI AMMINISTRATIVI E DELLA DIDATTICA.

LE STATISTICHE DICONO CHE IL PUNTO PIÙ DEBOLE DI UN SISTEMA INFORMATICO “SI TROVA TRA LA TASTIERA E LA SEDIA”

MA PUÒ ESSERE IL PRIMO E PIÙ IMPORTANTE PUNTO DI DIFESA

L’IMPORTANZA DEL FATTORE UMANO

La protezione digitale richiede attenzione costante su tre livelli:

GOVERNANCE DEI SISTEMI

TECNOLOGIE DI CYBERSECURITY

COMPORTAMENTI QUOTIDIANI

LE MINACCE DIGITALI COLPISCONO OGNI GIORNO, OVUNQUE

La maggior parte degli attacchi non nasce da un hacker: nasce da un nostro errore.

- PHISHING
- SOTTRAZIONE DI CREDENZIALI
- COMPROMISSIONE DI CASELLE EMAIL

UN LINK FASULLO

può fermare tutta l’Amministrazione

Una email finta. Un allegato aperto per errore.

E in pochi minuti tutti i sistemi vanno offline.

È già successo altrove.

Potrebbe succedere qui.

SERVE PIÙ CHE MAI UN APPROCCIO RESPONSABILE

Per difendere la sicurezza digitale dell'Amministrazione e la fiducia tra cittadini e istituzioni

Per evitare di incorrere in sanzioni amministrative e provvedimenti disciplinari

LE AMMINISTRAZIONI DEVONO AGIRE SUBITO

Per rafforzare la sicurezza digitale, ogni Amministrazione deve adottare misure chiare, continuative e documentate e vigilarne l’applicazione.

Non basta avere la tecnologia sicura: serve anche definire comportamenti e regole.

LA PRIMA DIFESA SONO LE CREDENZIALI

CREDENZIALI SICURE = SISTEMI PROTETTI

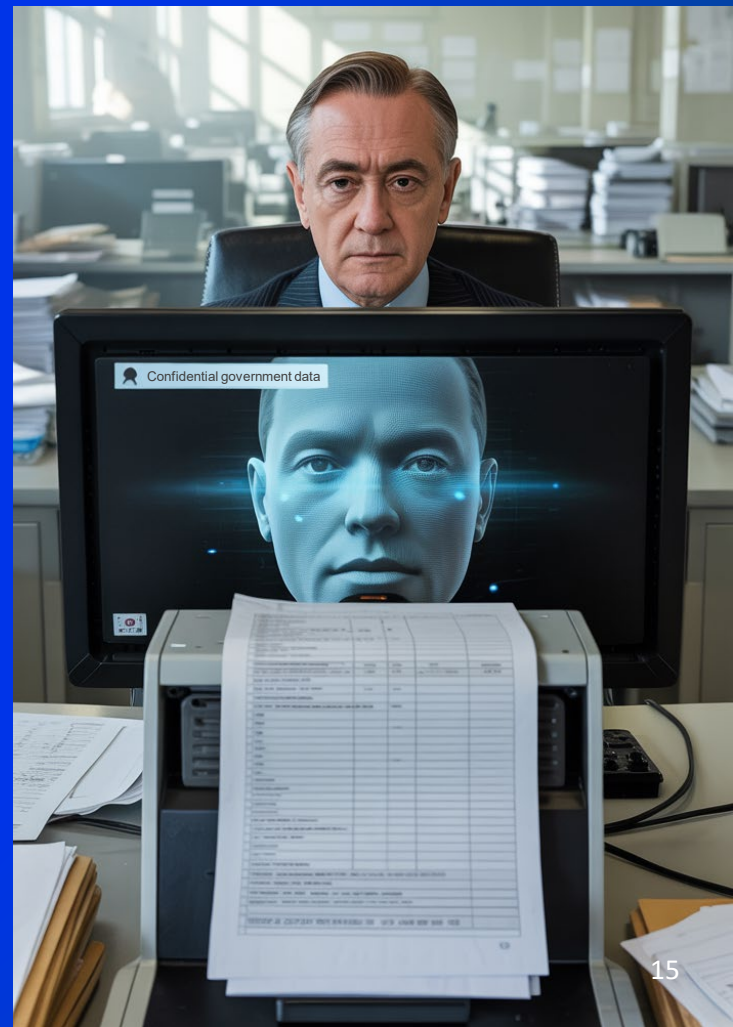
Password e token di accesso sono la prima barriera contro chi tenta di entrare nei sistemi informatici.

L’INTELLIGENZA ARTIFICIALE NON DIMENTICA

Molti sistemi di IA generativa (come chatbot e assistenti virtuali) sono progettati per raccogliere dati in modo indiscriminato. Ogni volta che un documento, un testo o un’informazione vengono incollati in una chat, entrano potenzialmente in un processo di addestramento.

Dentro questi sistemi oggi ci sono già documenti riservati, sanitari, legali, tecnici.
Spesso sono stati caricati — anche per errore — da dipendenti pubblici di tutto il mondo.

Questi contenuti possono riemergere in qualsiasi momento, offerti a chiunque faccia la domanda giusta.



12 BUONE PRATICHE

PER LAVORARE IN SICUREZZA OGNI GIORNO

Ecco 12 regole semplici e concrete che ogni dipendente pubblico dovrà applicare.

ATTIVA SEMPRE L’AUTENTICAZIONE A PIÙ FATTORI (MFA)

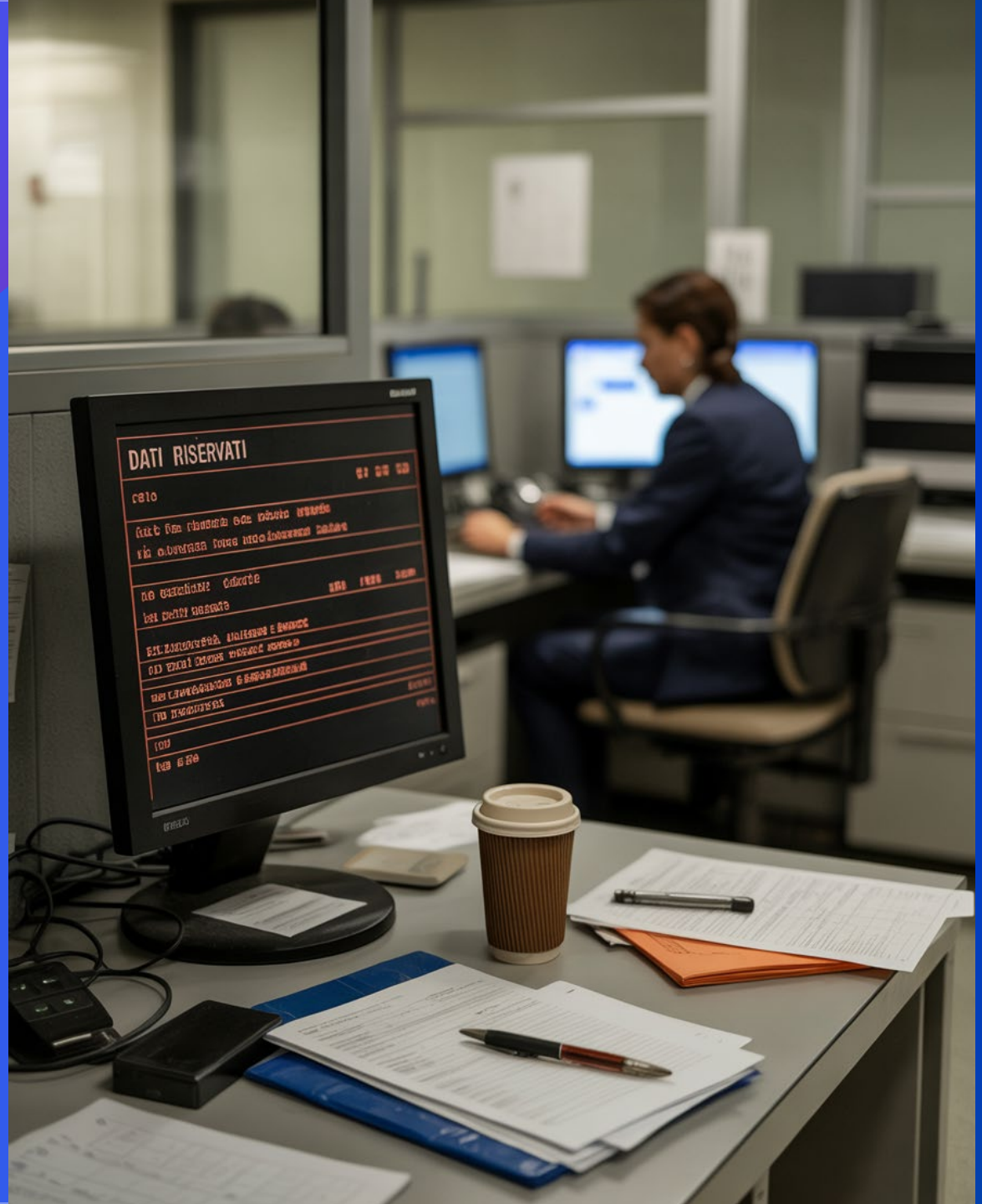
Non basta inserire una password.
Rendere disponibile e attivare sempre il secondo fattore di accesso: un codice temporaneo inviato via app o SMS.
È una barriera semplice, ma molto efficace contro gli accessi non autorizzati.

USA PASSWORD ROBUSTE E DIVERSE PER LAVORO E VITA PRIVATA

Non condividerle mai con nessuno.
Evita nomi, date di nascita o parole comuni.
Crea password robuste, uniche per ogni account.
Non usare la stessa password per servizi personali e accessi dell’Amministrazione.

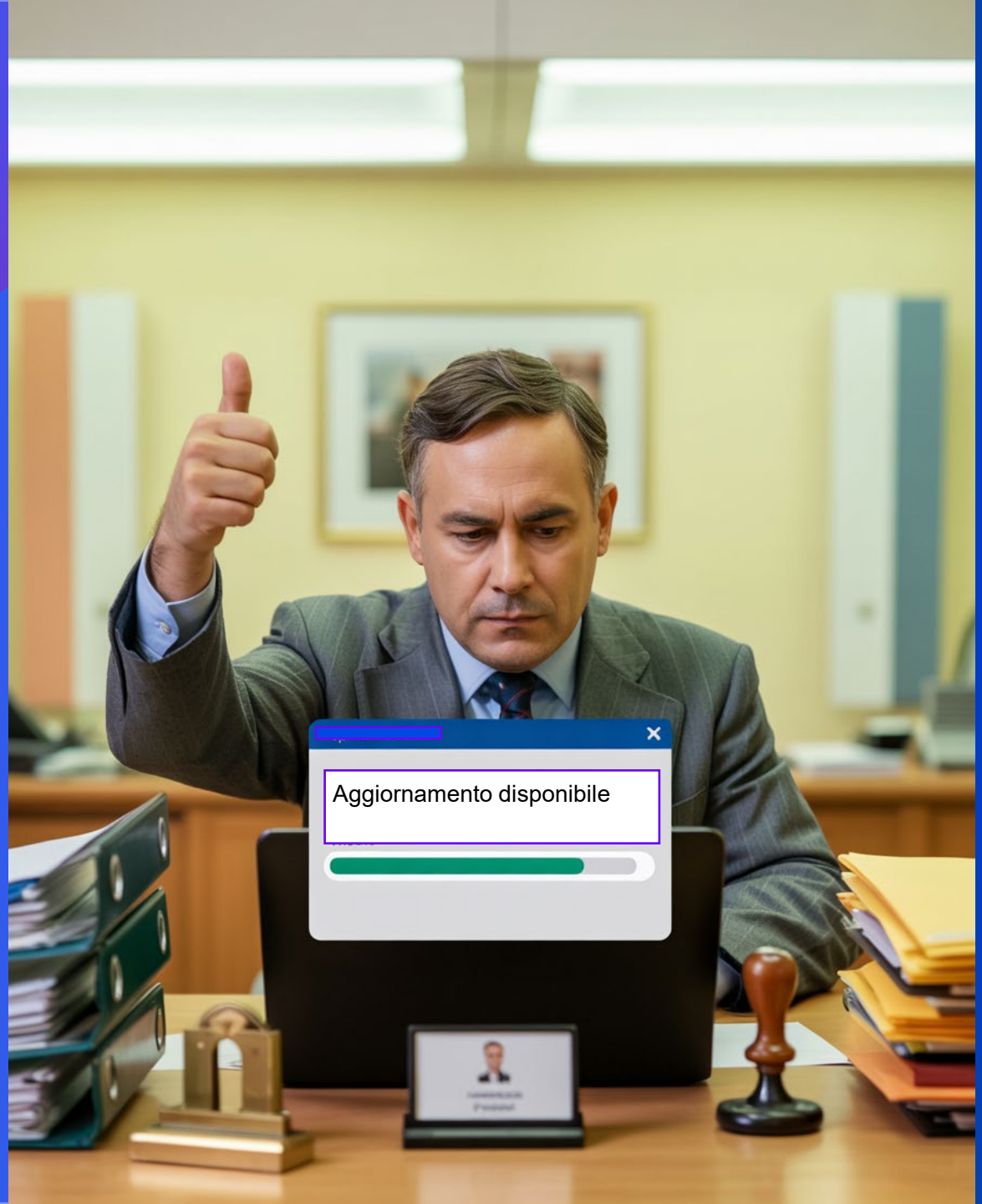
BLOCCA SEMPRE IL DISPOSITIVO QUANDO TI ALLONTANI

Un PC sbloccato è una porta aperta sui tuoi dati.
Anche pochi minuti lontano dalla scrivania bastano per compromettere la sicurezza.
Quando ti allontani dalla PDL disconnetti sempre la tua utenza.



AGGIORNA SEMPRE IL SISTEMA SENZA RIMANDARE

Ogni aggiornamento corregge falle di sicurezza note agli attaccanti.
Un dispositivo non aggiornato è come una porta lasciata socchiusa.
Quando richiesto dall'IT, installa sempre gli aggiornamenti appena disponibili.



INSTALLA SOLO SOFTWARE AUTORIZZATO DALLA P.A.

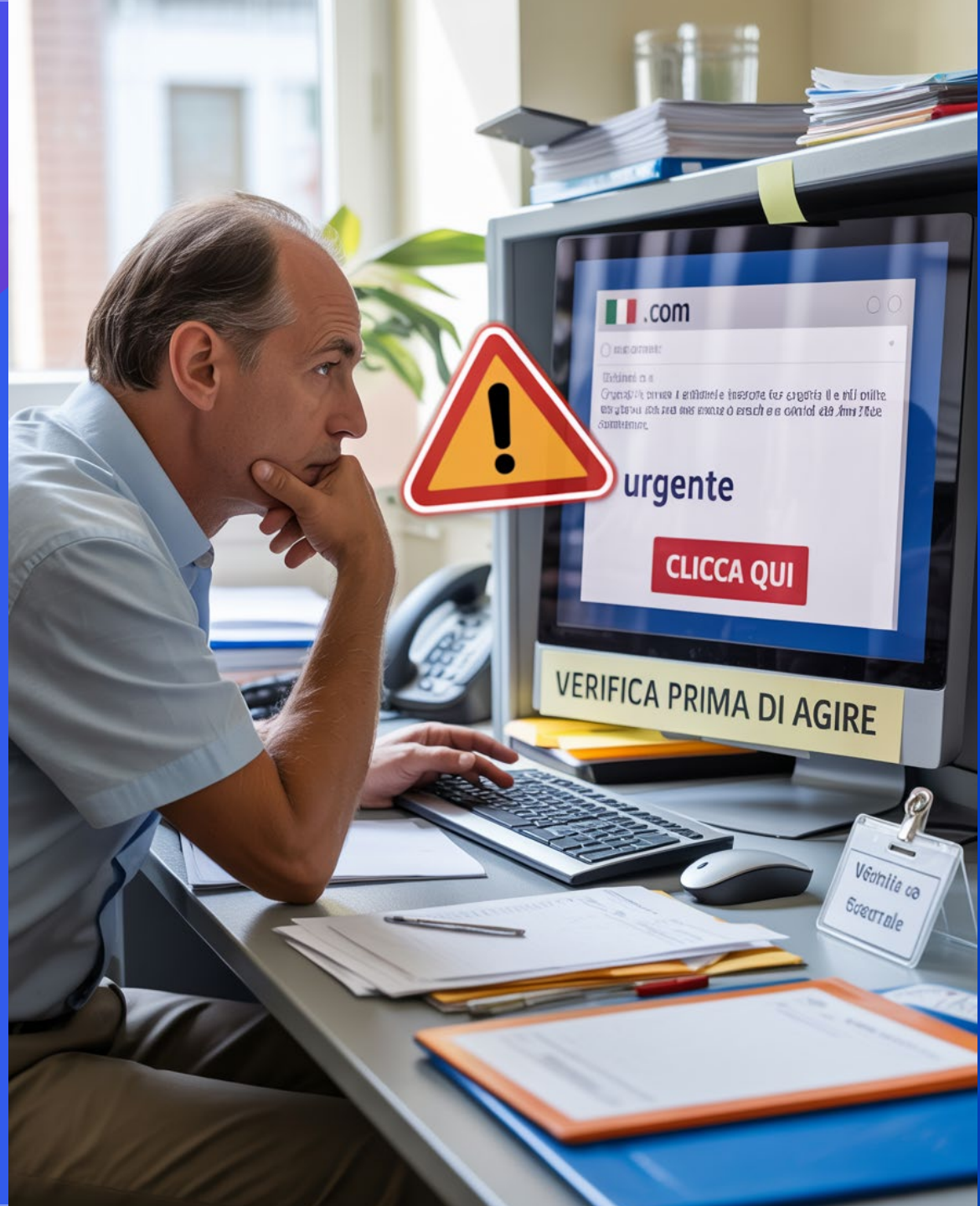
Anche un programma apparentemente innocuo può nascondere malware.
Non scaricare software da siti non ufficiali o su iniziativa personale.
Se serve un nuovo strumento, chiedi sempre l’autorizzazione.

USA SOLO SUPPORTI E DISPOSITIVI AUTORIZZATI DALLA TUA P.A.

Chiavette USB, hard disk esterni o dispositivi personali non autorizzati possono infettare l’intera rete.
Se non fanno parte della dotazione ufficiale, non usarli per memorizzare o trasferire dati.
La sicurezza inizia da ciò che colleghi.

NON FIDARTI MAI DI EMAIL URGENTI O CON LINK SOSPETTI

Molti attacchi iniziano con una email o un messaggio che sembrano legittimi.
Controlla sempre l’identità reale del mittente, anche se ti fidi.
Se hai un dubbio, non rischiare: segnala subito al team di sicurezza.



SE PERDI UN DISPOSITIVO AVVISA SUBITO IL TEAM DI SICUREZZA

Un computer, un telefono o una chiavetta smarriti possono contenere dati riservati. Anche pochi minuti senza protezione possono bastare a causare una violazione. Segnala immediatamente lo smarrimento: è un gesto di responsabilità, non di colpa.

EVITA DI CONNETTERTI A WI-FI PUBBLICHE NON PROTETTE

Le reti pubbliche (es. in bar, stazioni, hotel) possono essere usate per intercettare dati sensibili.
Se proprio devi collegarti, attiva una VPN, meglio se fornita dall'Amministrazione.
Meglio una connessione lenta ma protetta, che una veloce ma pericolosa.

SEGNALA SUBITO OGNI ANOMALIA, ANCHE SE SEMBRA PICCOLA

Un rallentamento, un accesso strano, un file che non riconosci: potrebbe essere l’inizio di un attacco.
Non ignorare mai un comportamento anomalo del tuo dispositivo.
Segnalare subito può fare la differenza tra un rischio contenuto e un danno grave.

USA LA EMAIL DI LAVORO SOLO PER ATTIVITÀ ISTITUZIONALI

Non iscrivere la tua email istituzionale a newsletter, siti commerciali o gruppi privati.
Evita di usarla per registrarti a servizi non autorizzati.
Ogni iscrizione esterna espone l’Amministrazione a rischi di tracciamento, spam e attacchi mirati.

NON INSERIRE MAI DATI SENSIBILI NELLE CHAT DI INTELLIGENZA ARTIFICIALE

Strumenti come chatbot, LLM o in generale l'IA generativa non sono ambienti protetti, a meno che non siano specificamente resi disponibli dalla P.A.

Usali solo per attività generiche, MAI per contenuti sensibili, critici o che riguardano la sicurezza nazionale.