

Reti e Sicurezza Informatica

Manuale del Cittadino Digitale: Guida
completa per navigare, lavorare e proteggersi.

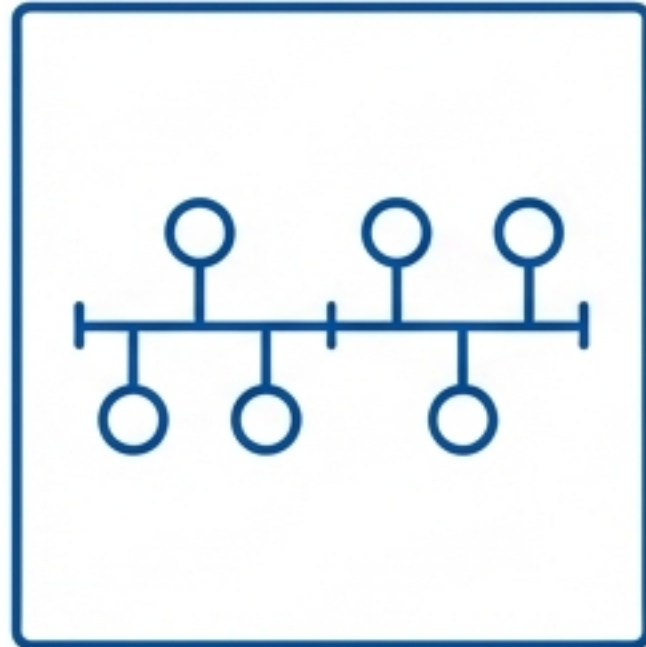


Che cos'è una Rete Informatica?

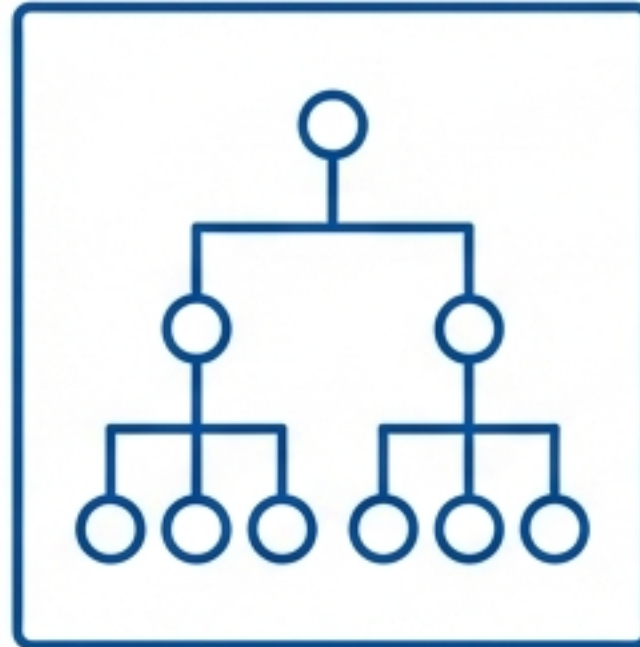
Una **rete** è un insieme di computer connessi che condividono risorse (dati, servizi, dispositivi) usando lo stesso protocollo.

Concetto Chiave:
Condivisione e
Comunicazione

Topologie di Rete



Bus
Inter Tight Semibold



Albero



Anello

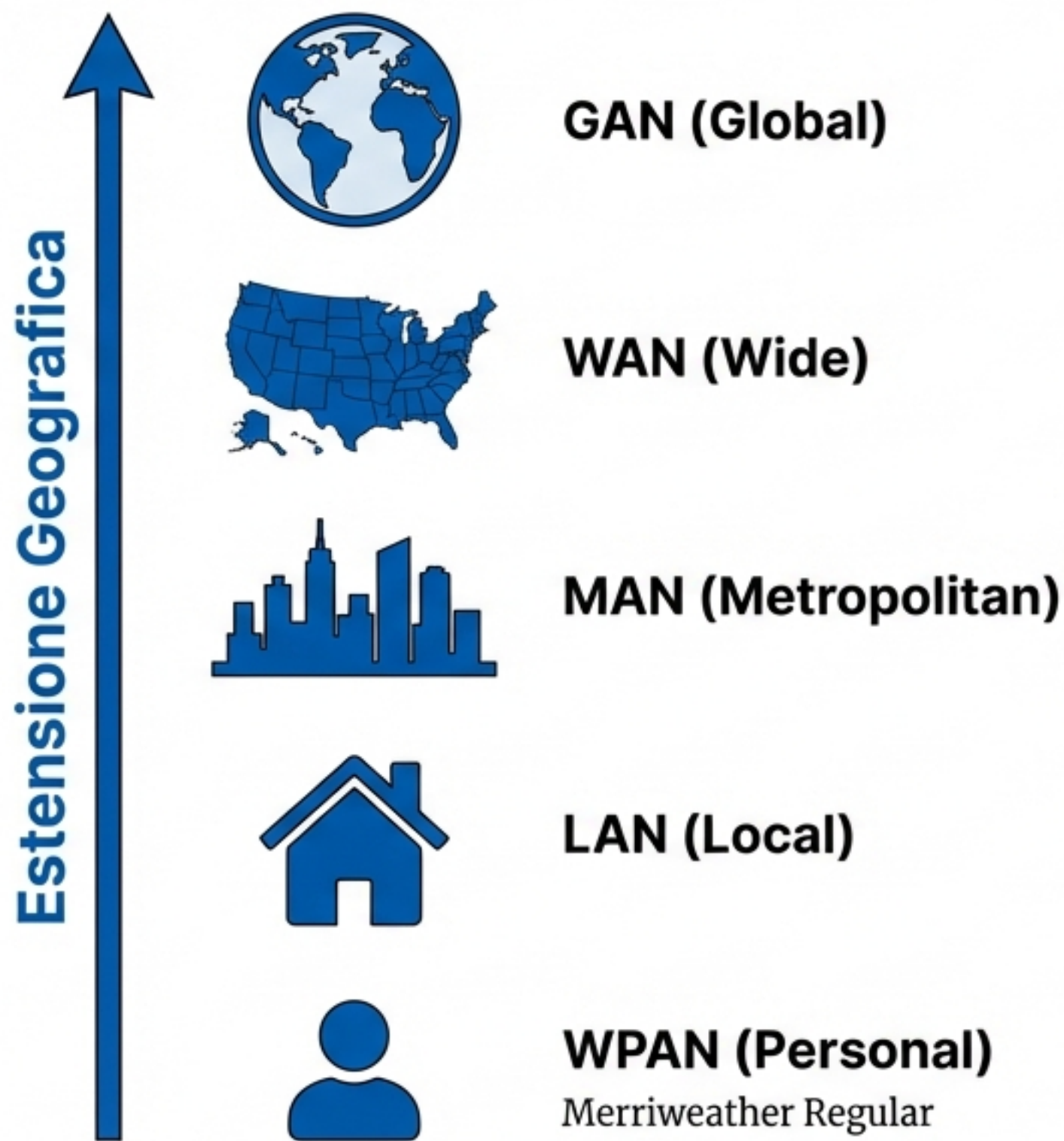


Stella

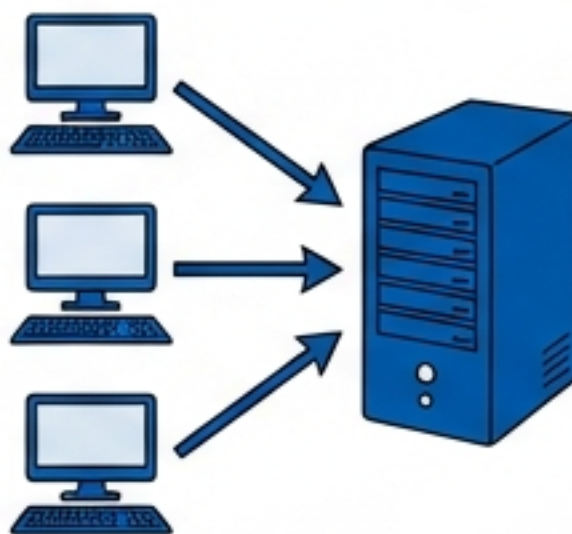


Maglia

La Geografia e l'Architettura delle Reti

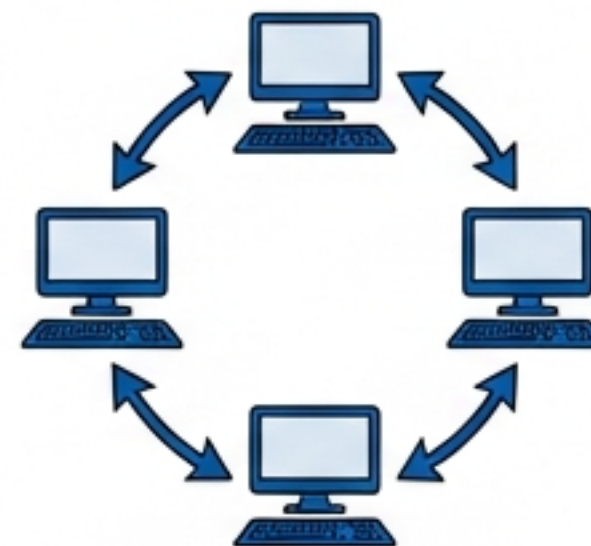


Client/Server



Gerarchico. Il Server offre risorse, il Client le richiede.
Merriweather Regular

Peer-to-Peer (P2P)



Paritario. Ogni computer è sia client che server.
Merriweather Regular

Security Note



VPN (Virtual Private Network):
Tunnel crittografato per garantire privacy su reti pubbliche.
Merriweather Regular

Internet: La Rete delle Reti



Connessione tramite ISP (Provider).

Tecnologie:

- **ADSL:** Cavi telefonici (Rame)  
- **Fibra Ottica:** Vetro e segnali di luce (Alta velocità)  

Protocollo globale: TCP/IP

`http://www.amazon.it/risorsa/esempio.html`



Vivere Online: L'Evoluzione dei Servizi

Web 1.0: Pagine statiche, consultazione passiva

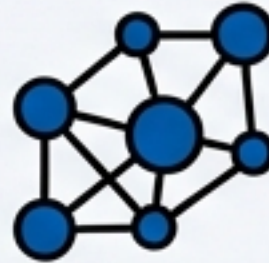


Web 2.0: Utenti autori, interazione, condivisione



E-mail

Protocolli: SMTP (invio), POP3/IMAP (ricezione).



Social Network

Relazioni e condivisione (Facebook, LinkedIn).



Wiki

Scrittura collaborativa (es. Wikipedia).



VoIP

Voce tramite Internet (Skype, Zoom).



Podcast

Audio on demand.

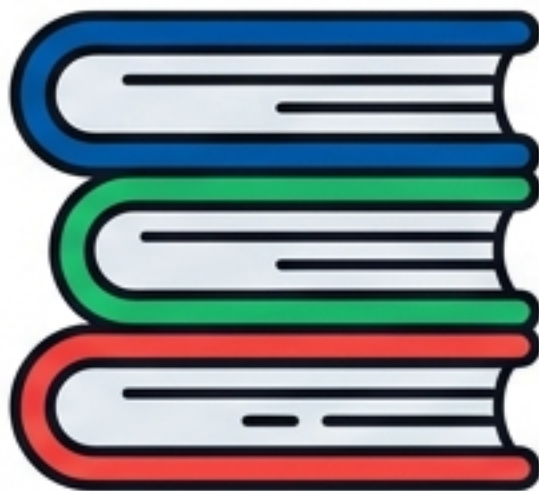


Forum

Discussioni asincrone.

La Nuova Frontiera: Studio e Lavoro

Formazione Digitale



MOOC (Massive Open Online Courses).
Corsi aperti, flessibili e certificati accessibili
a tutti tramite piattaforme dedicate.

Evoluzione del Lavoro



Telelavoro

Postazione fissa
a casa.

Smart Working

Senza luogo fisso, in
mobilità per obiettivi.

Conoscere il Nemico: Malware e Virus



Malware (Malicious Software):

Software creato per danneggiare il sistema o violare la privacy.

VIRUS



Si attacca ai file (.exe).
Si diffonde tramite
scambio file o download.
Richiede esecuzione.

WORMS



Si autoreplica via e-mail
o rete. Non ha bisogno di
un file ospite.

TROJAN HORSE



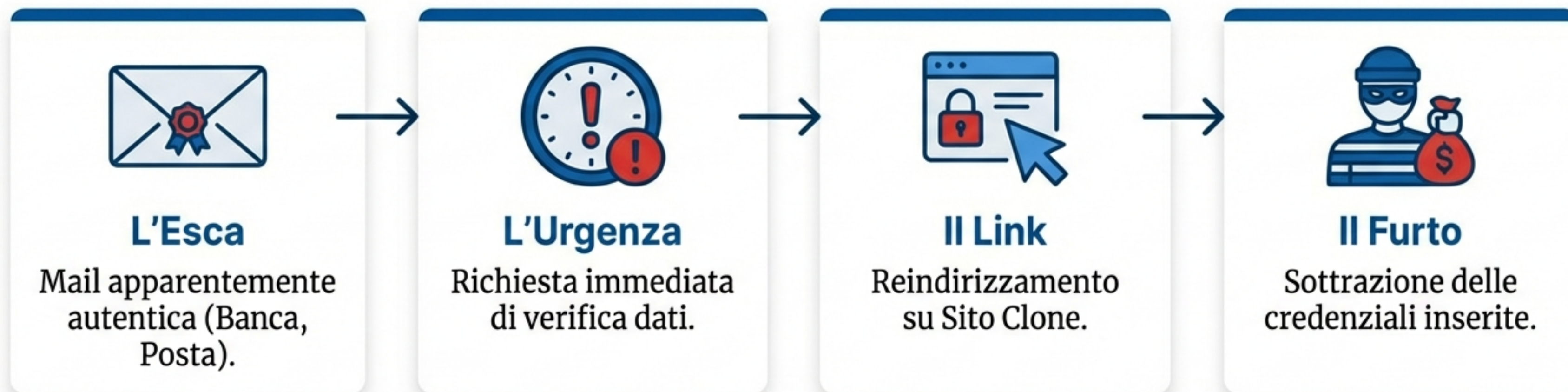
Software apparentemente
utile che nasconde una
minaccia. Apre una
'backdoor' per gli hacker.



L'Inganno del Phishing

Frode basata sul Social Engineering.

Anatomia della Truffa



REGOLA D'ORO: Le banche NON chiedono MAI dati riservati via e-mail.

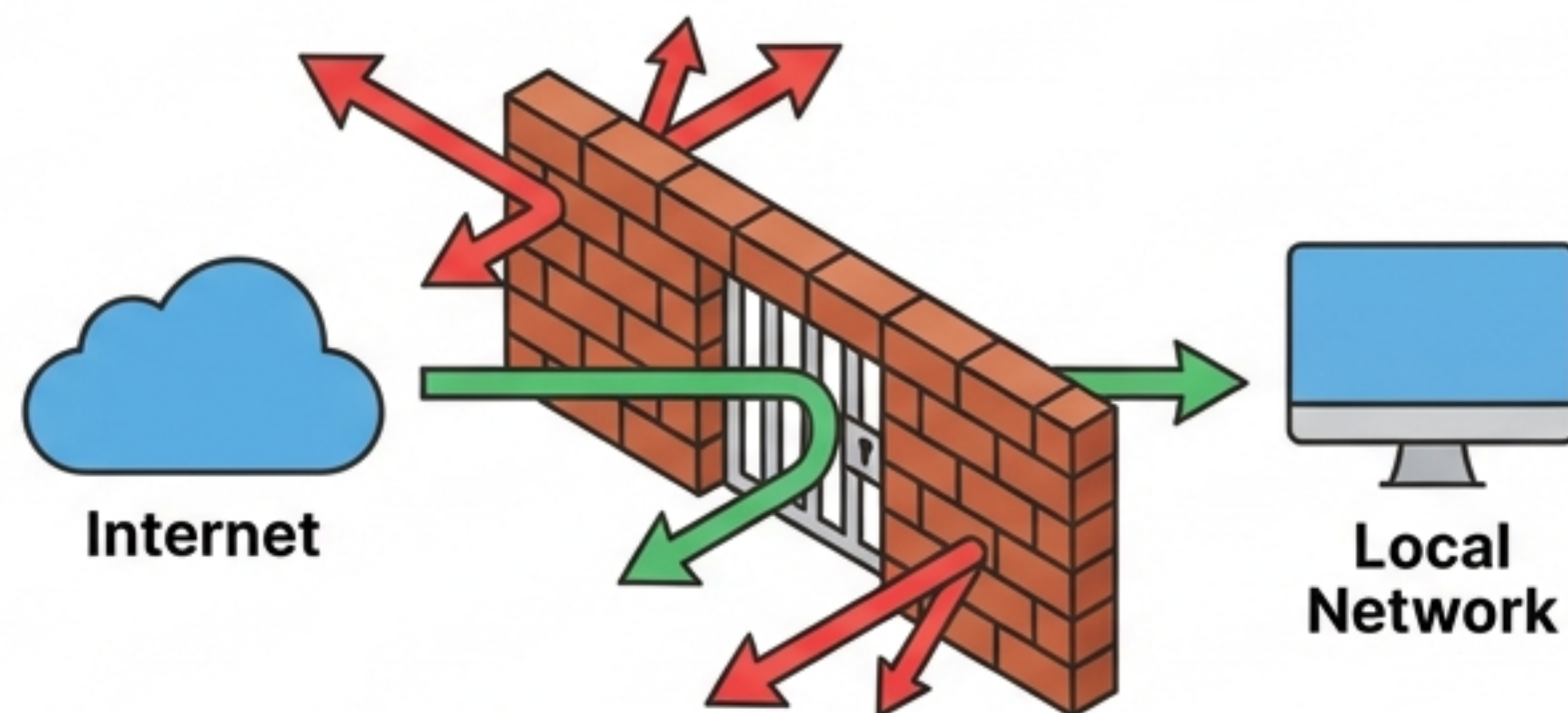
La Prima Linea di Difesa

Password Sicura



- Lunga e complessa (Maiuscole, numeri, simboli)
- Non riconducibile a dati personali
- Diversa per ogni servizio
- Cambio periodico

Firewall (Parafuoco)



Filtra il traffico in entrata e uscita. Può essere Hardware (difesa perimetrale) o Software (regole sul dispositivo).

Proteggere il Patrimonio: Il Backup



****Backup*:** Copia di sicurezza dei dati su supporti esterni (USB, Hard Disk, Cloud).

I Rischi (Perché farlo):

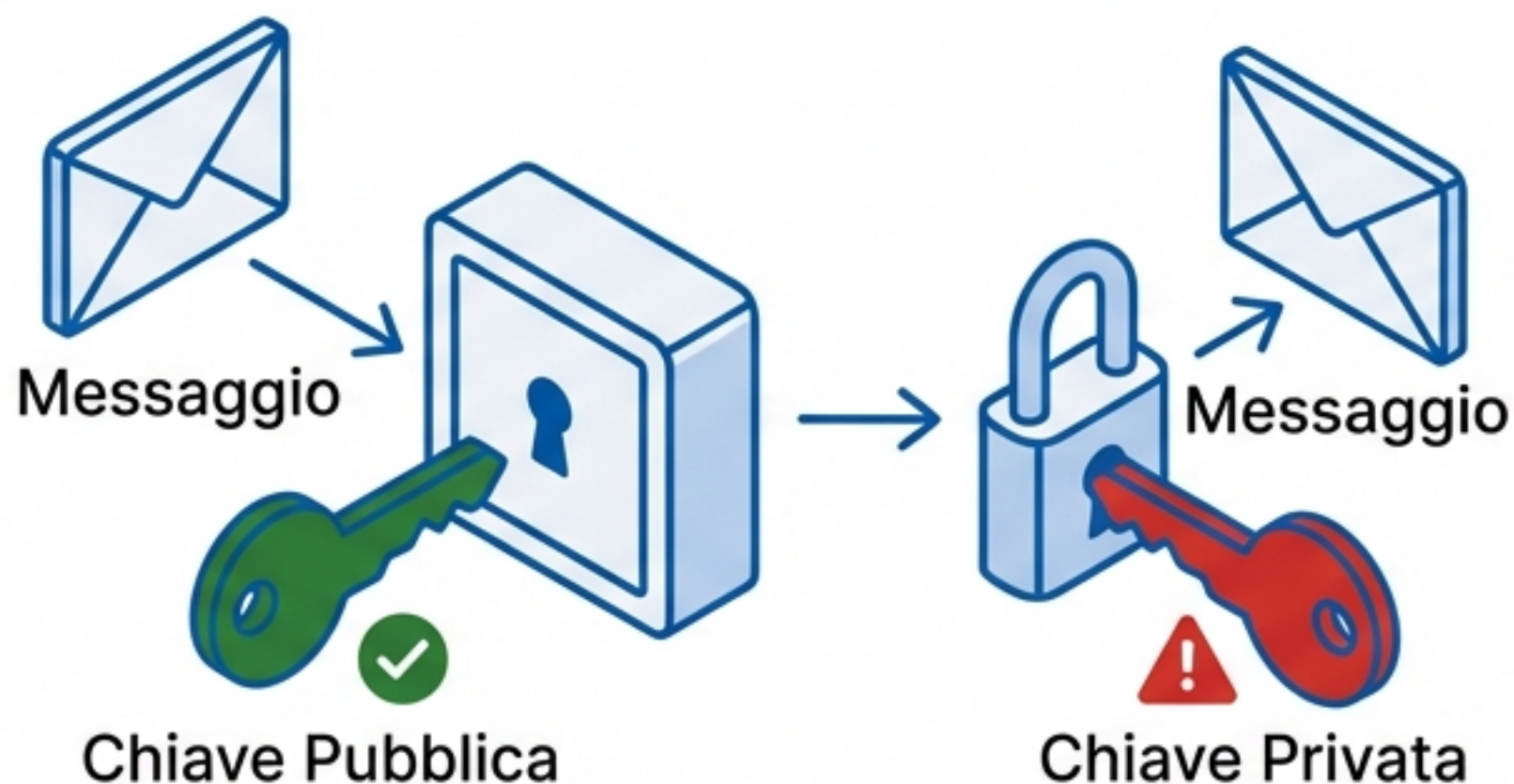
- – Rottura Hardware
- – Attacco Virus / Ransomware
- – Errore Umano
- – Furto o Disastri

Frequenza

Dipende dall'importanza dei dati. (Banca = Giornaliero; Personale = Settimanale).

Sicurezza delle Transazioni Online

Crittografia Asimmetrica



Concetti Chiave

- **HTTPS:** HyperText Transfer Protocol Secure. Garantisce trasmissione cifrata.
- **Certificato Digitale:** La “carta d’identità” del sito web rilasciata da un ente certificatore (CA).



<https://www.esempio.com>

Identità e Autenticazione

Firma Digitale

- ✓ Autenticità: Identità garantita.
- ✓ Integrità: Documento non modificato.
- ✓ Non Ripudio: Impossibilità di negare la firma.

I 3 Fattori di Autenticazione

Conoscenza (Cosa sai)



Password, PIN.

Possesso (Cosa hai)



Token, OTP via SMS.

Fisicità (Cosa sei)



Biometria.

Il Fattore Umano: Privacy e Netiquette

Privacy e Diritti

Tutela dei dati personali (GDPR).
Sui Social Network è fondamentale
gestire i livelli di visibilità e
bloccare utenti sconosciuti.

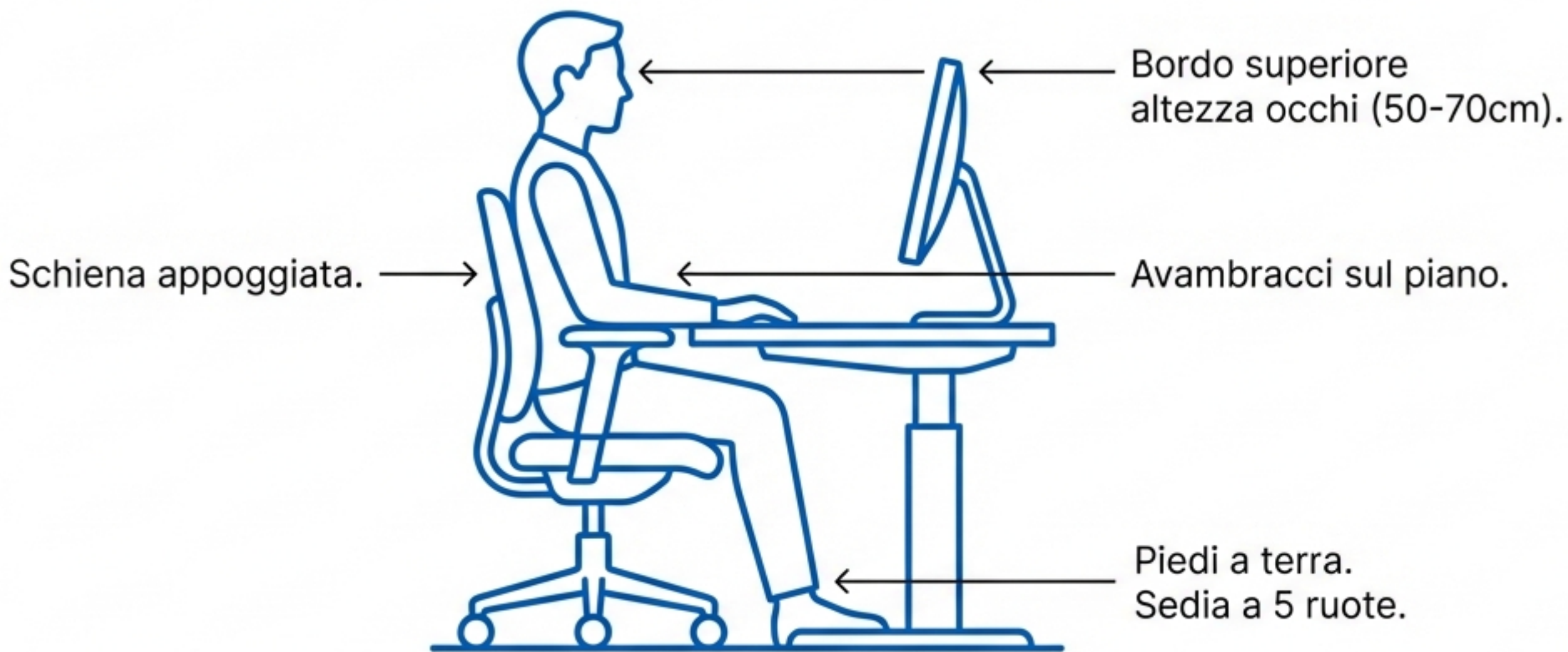


Netiquette (Galateo di Rete)

- ⚠️ No flame wars (toni polemici).
- ⚠️ NON SCRIVERE IN MAIUSCOLO (equivale a urlare).
- Rispettare la privacy altrui.
- Essere chiari e collaborativi.



Ergonomia e Salute



La Regola del Riposo

Fare una pausa di 15 minuti ogni 2 ore per evitare affaticamento visivo e disturbi muscolo-scheletrici.

Riepilogo: I Pilastri della Sicurezza

- ✓ **Password:** Usare password complesse e diverse per ogni sito.
(Merriweather Regular)
- ✓ **Software:** Mantenere Antivirus e Antimalware aggiornati.
- ✓ **Attenzione:** Verificare HTTPS e diffidare delle mail urgenti.
- ✓ **Protezione:** Eseguire backup periodici dei dati.
- ✓ **Comportamento:** Rispettare la Netiquette e la Privacy.
- ✓ **Salute:** Postura corretta e pause regolari.

