Cybersecurity

Sicurezza informatica

www.tecnologiaedidattica.com


INTERNET

Cos'è internet?

INTERNET → rete di computer (o altri dispositivi) che possono comunicare tra loro e scambiare dati attraverso dei **protocolli comuni** *(TCP/IP, http://...)*

Grazie a internet, possiamo utilizzare una **serie di servizi**:

- il **world wide web** (www): insieme di pagine digitali *(ipertesti)* da visitare o in cui caricare contenuti (web 2.0)
- la **posta elettronica**: inviare e ricevere e-mail
- **servizi cloud**: spazi di archiviazione per i nostri dati
- **servizi finanziari** (*home banking, e-commerce, etc.*)

Un protocollo di rete è un insieme di regole e di procedure che **regolano lo scambio di informazioni** tra dispositivi elettronici connessi tra loro.

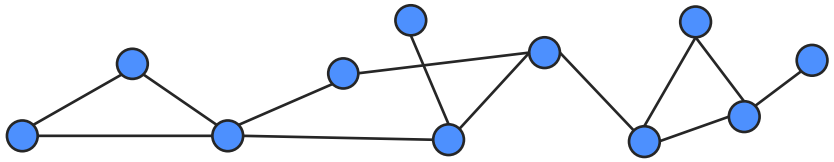
Come funziona?

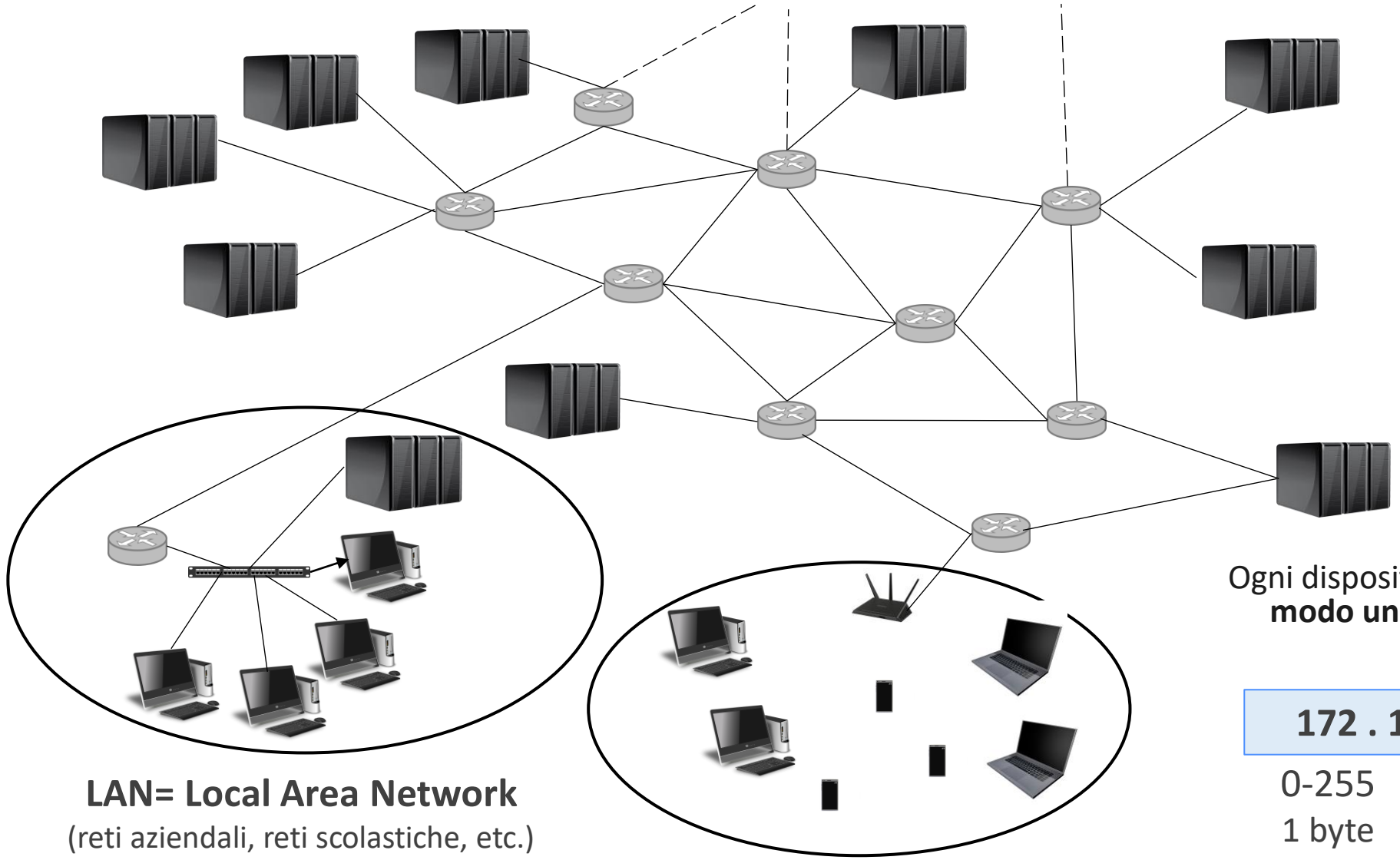
INTERNET si basa su un sistema (architettura) **client/server**

- il **client** è il nostro dispositivo *(computer, laptop, smartphone)*
- Il **server** è un computer più potente con un diverso sistema operativo che gli permette **di far funzionare una serie di servizi** *(motori per il web, posta elettronica, gioco online, app di messaggistica, etc.)*

Il nostro dispositivo client **può trovare i servizi che sta cercando** grazie ai **router,** che indirizzano i pacchetti di dati dal client al server e viceversa.

INTERNET possiamo rappresentarla come una **struttura a nodi connessi** tra loro.





server

client

router

MODEM/router

LAN= Local Area Network

(reti aziendali, reti scolastiche, etc.)

WLAN=Wireless Local Area Network

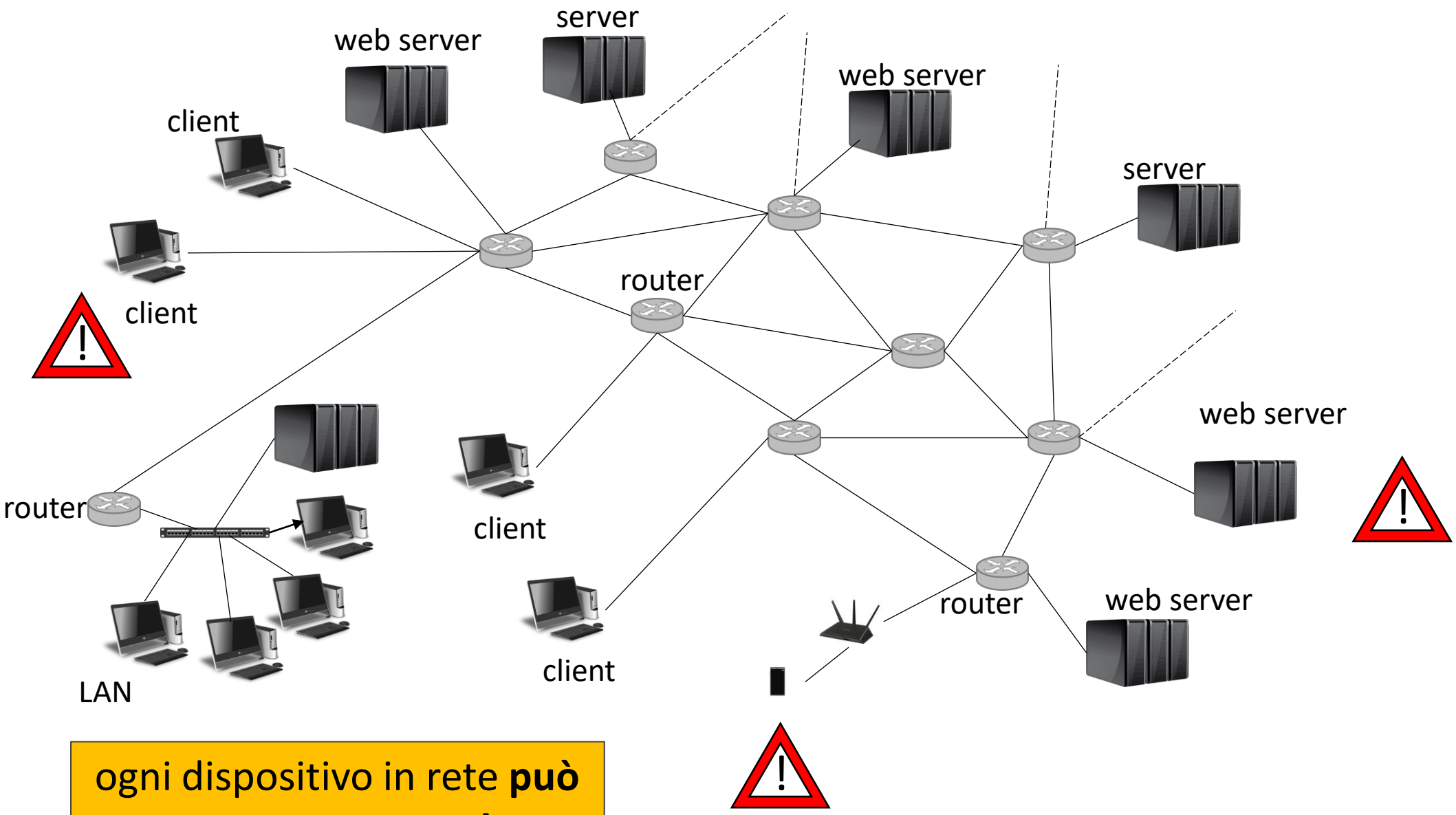
(reti private domestiche, parti di reti aziendali)

Ogni dispositivo in rete **viene individuato in modo univoco da un codice numerico** *(indirizzo IP).*

172 . 122 . 254 . 17

0-255

1 byte



ogni dispositivo in rete **può essere attaccato!**

Hacker?

No…criminali informatici.

Un hacker **è un profondo conoscitore dei sistemi informatici** e spesso lavora per **individuarne le vulnerabilità**, ma non lo fa necessariamente per commettere reati.
Il termine *hacker,* in sé, **non ha significato positivo né negativo.**

Quali sono i reati informatici?

1. **Minacce alla sicurezza dei dati**
2. **Furto di identità**
3. Interruzione di servizio
4. Frodi elettroniche

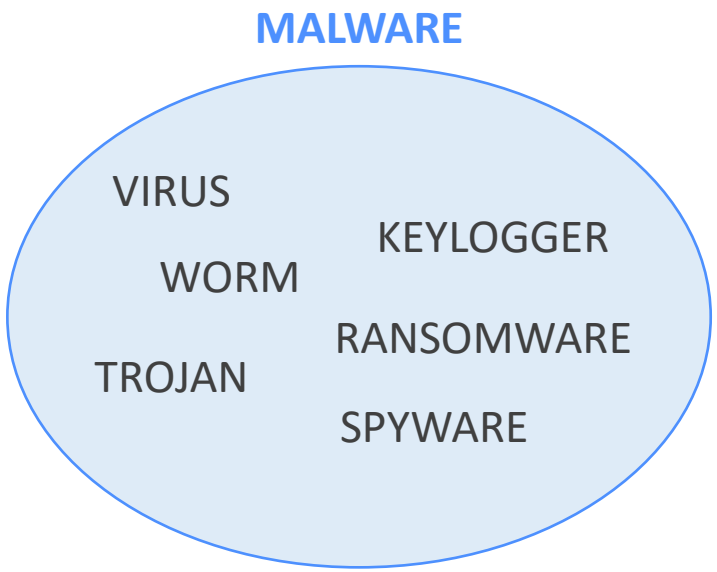
- Accesso non autorizzato
- **Cancellazione/alterazione dei dati**
- **Intercettazione dati in rete**
- Deterioramento e manomissione dei supporti fisici
- **Diffusione di malware**

Cosa sono i malware?

Sono programmi informatici creati per **disturbare le attività di un utente**, sottrargli dati e informazioni e usarle per attività illecite

*mal*icious *soft*ware = software malevolo

conoscere i **principali tipi di malware è fondamentale per difendersi** dagli attacchi informatici!



Tipi di malware:

virus

è un software che, una volta scaricato e installato**, si replica e si diffonde in altri computer**. Il virus **deve essere portato da un vettore** (es. un file) e **deve essere eseguito dall'utente**, che spesso lo attiva senza rendersene conto.

worm

è infettivo come il virus, **ma è più pericoloso** (non ha bisogno di vettori o di azioni da parte dell'utente).

trojan horse

di solito si nasconde in un altro programma **e non ha bisogno di azioni dell'utente**. Una volta che inizia la sua attività, il trojan può **aprire la porta ad altri malware finalizzati al furto di dati o altre azioni malevole.**

Tipi di malware:

spyware

traccia l'attività online di un ignaro utente **raccogliendo informazioni sulle sue preferenze** per alimentare campagne di spam, di *phishing* o altre frodi.

keylogger

è in grado di registrare quanto digitato sulla tastiera, permettendo ai malintenzionati di **rubare password e codici di sicurezza**.

ransomware

è un malware che **cripta i dati del computer** o di una rete rendendoli illeggibili e inutilizzabili; i criminali cedono alle vittime la chiave per recuperare i dati **solo dopo il pagamento di un riscatto**.

allo stato attuale della tecnologia, **non è possibile decodificare dati criptati senza la chiave**

Come proteggersi?

Proteggersi dai malware:

- ✗ **NON** aprire **MAI** allegati di mail sospette, specie se file eseguibili (.exe)
- ✗ **NON utilizzare versioni OBSOLETE** di programmi e **sistemi operativi non aggiornati** (specie se non più supportati!)
- ✗ **evitare** di installare programmi o giochi «craccati» (attenzione ai **CHEAT**!)
- ✓ installare un **buon programma antivirus** e tenerlo sempre aggiornato.
- ✓ **aggiornare sempre il SO e i programmi** del nostro computer

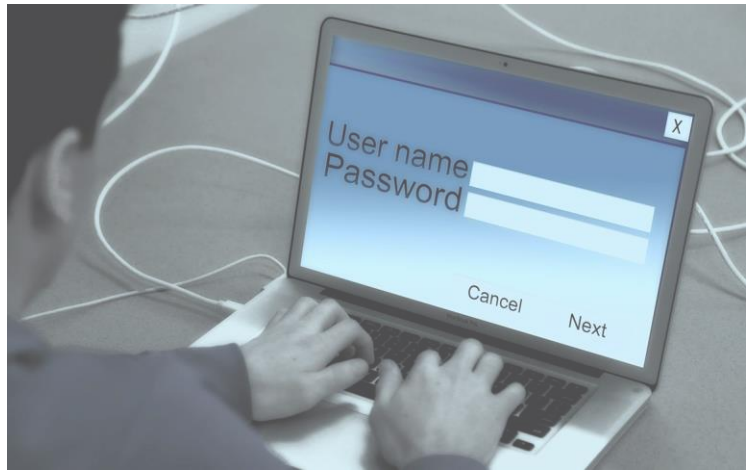
avere un programma antivirus non aggiornato **NON protegge il computer** dai malware!

sicurezza degli accessi

Sicurezza degli account

Tutti i servizi che utilizziamo richiedono **l'uso di credenziali**…posta elettronica, social media, servizi di **e-commerce** (es. *Amazon, etc.*).

Le credenziali (*username* e *password*) servono anche per gli accessi degli utenti alle reti aziendali; **la loro violazione può portare alla diffusione di malware**, al furto e/o alla grave compromissione (es. criptazione) di dati e informazioni.



Proteggere le password utilizzate è fondamentale per non esporci **ai più pericolosi attacchi informatici!**

Proteggere gli accessi:

❌ **NON** utilizzare la stessa password per servizi diversi

❌ **NON** utilizzare **password deboli**

PippoPluto ❌

Andrea2011 ❌

Polpetta123 ❌

123456 ❌ deboli

Maradona10 ❌

SXdXeE3gQi$m?a$h ✔ forte

Una password forte si compone di **almeno 16 caratteri casuali** con:

- lettere MAIUSCOLE e minuscole
- simboli (%,!ì#]…
- cifre numeriche 3,8,5,…
- usa una **passphrase** invece di una semplice **password**

❌ **NON** conservare **MAI** le password in un file sul PC o nella chiavetta USB

…e non vanno nemmeno scritte in agenda o su un foglio di carta!

Proteggere gli accessi:

- **modificare** spesso le password (ogni 3 mesi)
- utilizzare **applicazioni o software** per la creazione e la gestione delle password (molti antivirus hanno la «cassaforte delle password»)
- attivare, quando possibile, **l'autenticazione a 2 fattori (2FA)** o l'autenticazione con la **biometria** *(es. impronta digitale)*

Reti sociali

Alcune delle conseguenze più spiacevoli derivano, purtroppo, **dalla condivisione di informazioni personali** attraverso le applicazioni di **social networking**.

- ✗ NON condividere foto, informazioni sulle proprie abitudini, altri dati personali come l'indirizzo di casa o dei posti frequentati
- ✗ NON accettare richieste di contatto da persone sconosciute
- ✓ verificare le impostazioni di riservatezza dei propri account social
- ✓ disattivare la geolocalizzazione