Unità 2 – I virus informatici

(A) CONOSCENZA TERMINOLOGICA

Dare una breve descrizione dei termini introdotti:

- Virus
- Antivirus
- Disinfezione
- Quarantena
- Scansione periodica
- *Overclocking*
- Programma ospite
- *Malware*
- *Dialer*

(B) CONOSCENZA E COMPETENZA

Rispondere alle seguenti domande producendo anche qualche esempio

Conoscenza

1. Cosa è un *virus informatico*?
2. Quali sono i principali *tipi di virus*?
3. Come in genere avviene la *trasmissione di virus*?
4. Come agisce un *software antivirus*?

Competenza

1. Quali possono essere i *danni da virus informatici*?
2. Come avviene, in genere, la *trasmissione di virus*?
3. In cosa consistono l'*aggiornamento* e la *scansione con antivirus*?
4. Qual è, in generale, un comune *modo di operare di un virus informatico*?
5. Quali sono alcune possibili conseguenze di un *contagio da virus*?

(C) ESERCIZI DI COMPRENSIONE

1. La sicurezza informatica va garantita quando i dati sono ……, perché rappresentano una risorsa economica, o ……. , perché si riferiscono a persone e non possono essere divulgati, nel rispetto della …….
2. Un virus è un ……. scritto appositamente per alterare il funzionamento di un computer, senza che l'utente ne sia al corrente. La diffusione può avvenire attraverso un rete di ……, oppure attraverso ……..., come CD-ROM o pen drive e può provocare …… o semplicemente azioni di …….
3. La presenza di un virus può comportare la compromissione della funzionalità dell'intero ……. o la stampa di messaggi ……., o l'uso esagerato di ……..., come la CPU, la RAM o il disco. Normalmente i virus, una volta entrati nel sistema, si ……..., creando tante copie altrettanto pericolose.
4. Un virus entrato in un sistema può creare molti problemi come ……. file, alterandone il contenuto, ……. file o cartelle, rendendo impossibile l'esecuzione di programmi o, nei casi più gravi, ……. le unità a disco.
5. I virus possono differire per modo di ……, ossia la causa che produce l'infezione, per grado di ……, ossia la facilità di replicazione, e per la ……. dei danni generati.
6. Un software …… protegge il sistema dall'ingresso dei virus, purchè sia mantenuto …….. e si esegua la …… periodica dei dischi. L'antivirus è in grado di …… i virus conosciuti al momento e, in molti casi, di …….. l'infezione dal file infetto.
7. I virus più aggressivi, possono arrivare a ……. gli hard disk o a produrre il surriscaldamento della CPU, sia aumentando la frequenza del clock (tecnica detta …….), sia ……..… la ventola di raffreddamento.
8. I virus di tipo ……. alterano il software contenuto nl computer, in modo da essere eseguiti ogni volta che la macchina viene …….; spesso, si nascondono negli …… di posta elettronica, oppure in file che vengono ……. nella rete.

9. Un virus in genere infetta un programma, che viene detto programma …… che è in genere un programma ……Il codice del virus, in genere molto breve, viene eseguito subito all'avvio del programma …….. in modo che l'utente non si accorga della sua presenza
10. Per ciascuna delle seguenti frasi, indicare se è vera o falsa.

	Vero	**Falso**
Un antivirus deve essere aggiornato periodicamente		
La scansione periodica è dipendente dall'uso che si fa del computer		
Un file rilevato infetto, va sempre cancellato		
Se non si usa Internet, si può fare a meno di aggiornare l'antivirus		
Un virus si può presentare all'utente molto tempo dopo l'infezione		
Un virus può alterare il contenuto dei dischi		
Riavviando il computer, si eliminano i virus eventualmente presenti		
I virus sono tutti capaci di un comportamento autonomo		

10. Associare le proposizioni di sinistra con il tipo di virus appropriato riportato sulla destra, scrivendo nelle caselle la lettera corrispondente:

1		Si diffondono autonomamente	**A**	Trojan
2		Infettano installando applicazioni	**B**	Worms
3		Nascondono truffe sul traffico telefonico	**C**	Trojan
4		Non si diffondono autonomamente	**D**	Trojan
5		Sono usati per rubare informazioni	**E**	Dialer

(E) ESERCITAZIONI PRATICHE

Esercitazione 1 – Guida alla rimozione di virus
Obiettivi: utilizzo di software di manutenzione e di antivirus

1. Accendere il computer seguendo la procedura ACCENSIONE DEL SISTEMA
2. Procedere all'eliminazione dei file temporanei, cancellando le aree in cui il malware può salvare i propri file, ossia:
   a. la cache del browser;
   b. le cartelle temporanee utente e di sistema;
   Questa operazione può essere svolta scaricando e installando uno dei due software **ATFCleaner** o **CCleaner**. Altro vantaggio di questa operazione è la velocizzazione delle successive scansioni.
3. Se sul computer non è presente alcun antivirus, scaricarne uno free da Internet.
4. Successivamente, con l'antivirus installato:
   a. procedere al suo aggiornamento, con le ultime definizioni dei virusa attuali;
   b. interrompere il collegamento di rete locale e Internet;
   c. terminare tutti i programmi;
   d. chiudere tutte le finestre;
   e. lanciare una scansione completa del sistema.

Se un virus viene rilevato ma risulta impossibile eliminarlo, si può procedere come segue:

1. avviare il sistema in **Modalità Provvisoria** (all'accensione o riavvio del computer, tenere premuto il tasto F8 sulla tastiera subito dopo i test del BIOS). In questa modalità viene caricato il minimo insieme di componenti e di driver necessari per il funzionamento del

sistema e viene tralasciato tutto il superfluo, virus compreso. A questo punto l'antivirus che prima segnalava di non poter ripulire il file infettato potrà correttamente svolgere il proprio lavoro.

2. Interrompere il collegamento di rete locale e Internet;
3. terminare tutti i programmi;
4. chiudere tutte le finestre;
5. lanciare una scansione completa del sistema.