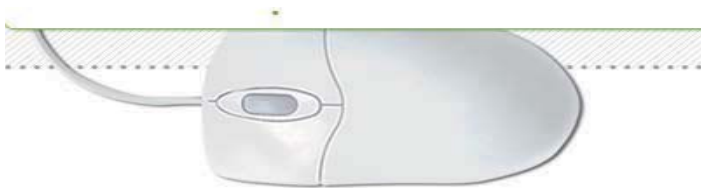


## Rischi e precauzioni nella navigazione



Per ripassare questa parte puoi consultare i video **Difendersi dalle minacce** e **Navigare sicuri** e a fare l'esercitazione **Sicurezza** nel **Modulo 7**

## La sicurezza in rete

- Sulla sicurezza della rete si dicono molte cose sbagliate
- In linea di massima i rischi esistono, ma bastano poche precauzioni, spesso di banale buon senso, per evitare guai
- I rischi si possono suddividere grosso modo in due categorie
  - Malfunzionamento del computer (molto difficile) causato da “virus”
  - Furto di dati personali (es. password, coordinate bancarie, dati della carta di credito...)

## I virus

I virus sono programmi capaci di “nascondersi” e “riprodursi” per “infettare” il computer e “contagiare” altri computer. Oggi i virus si trasmettono in prevalenza attraverso internet, navigando su siti che chiedono di installare programmi misteriosi o aprendo allegati a messaggi di posta elettronica inviati da sconosciuti. In particolare quest’ultima è proprio la **cosa da non fare mai**. Se ricevete un messaggio da un mittente sconosciuto, o scritto in inglese o in un italiano incomprensibile, o ricevete allegati sospetti, **nel dubbio cancellate il messaggio e non aprite gli allegati** (la semplice lettura del messaggio non è pericolosa)

In un computer basato sul sistema operativo Windows e che utilizza la rete Internet, è indispensabile proteggersi dai virus

L’installazione di programmi Antivirus e il loro aggiornamento costante è il miglior modo per proteggere il proprio PC sia dal punto di vista della prevenzione, sia per eliminare eventuali virus presenti

## Protezioni dai virus

Esistono validi programmi Antivirus gratuiti (spesso si usa il termine inglese *freeware*)

I 3 Antivirus utilizzabili gratuitamente più diffusi e probabilmente anche più validi al momento sono:

Avira AntiVir 

Avast   
avast! antivirus

AVG   
AVG  
Anti-Virus System

Il limite principale degli antivirus gratuiti è l'aggiornamento. Di continuo vengono messi in circolazione nuovi virus, i programmi a pagamento sono generalmente più aggiornati. Fra i più noti:



Norton Anti  
Virus

Kaspersky  


VirusScan Mc Afee

 McAfee

## Furti e simili

- Oggi il rischio più serio non è tanto il virus quanto il furto di informazioni e dati personali come le coordinate bancarie, il numero della carta di credito, le password per accedere a siti vari
- I sistemi usati dai criminali (attenzione: una volta i virus erano diffusi da buontemponi che si divertivano a dimostrare le loro capacità facendo un po' di danni. Oggi i tentativi di rubare dati personali sono opera di delinquenti spesso organizzati) sono diversi
  - Programmi simili ai virus che non vediamo e cercano sul nostro PC le informazioni (in inglese *spyware* o *malware*)
  - Messaggi finti di posta elettronica (*phishing*, dall'inglese *fish*=pesce) che chiedono di aprire un sito e inserire la propria password

## Protezione da furti e intrusioni

- L'antivirus non sempre è sufficiente a proteggersi. Sicuramente è utile un programma (in inglese *firewall*, "muro di fuoco") che impedisca ad altri quando siamo collegati ad internet di curiosare sul nostro computer. Alcuni antivirus forniscono anche questa protezione, non tutti però, meglio fare attenzione
- Ancora più seri però sono i rischi che corriamo a causa delle nostre disattenzioni. Oltre a quanto già detto per la scelta delle password, è bene fare attenzione a:
  - Messaggi che chiedono di collegarsi ad un sito e inserire la password del conto corrente bancario o bancoposta
  - Messaggio che chiedono soldi per fini benefici e umanitari
  - Siti che chiedono soldi a chi cerca lavoro
  - ...
- In generale: è bene diffidare di richieste di questo genere, se avete dei dubbi non fate niente, se ricevete messaggi sospetti cancellateli. Se non siete sicuri chiedete consiglio a qualcuno più esperto
- In fondo bastano poche precauzioni e non succede niente!