

# Guida all'uso dei mezzi informatici

Virus, spyware e tutti i tipi di malware mutano continuamente, per cui a volte sfuggono anche al controllo del miglior antivirus.

**Nessun pc può essere ritenuto invulnerabile**, quindi l'utente deve contribuire prestando attenzione alle mail ricevute e muovendosi in internet in modo "intelligente".

La presente guida fornisce alcune **regole da seguire per evitare problemi** durante l'utilizzo di posta elettronica e la navigazione internet.



# Indice

---

Posta elettronica ..... 3

Navigare sul web..... 5

Password ..... 6


Glossario ..... 7

# Posta elettronica

I virus arrivano, nel 90% dei casi, dai messaggi di posta elettronica interni ed esterni, prevalentemente sotto forma di "allegati". La sola apertura di un messaggio può causare infezioni; se poi questo contiene allegati (files di documento o di programma legati al messaggio), il rischio di infezione aumenta dal momento in cui si cerca di lanciare o visualizzare il contenuto dell'allegato (doppio click sull'allegato).

L'infezione del virus può essere invisibile all'utente, il più delle volte si continua a lavorare lasciando tempo al virus di moltiplicarsi, si può quindi rimanere infettati ed infettare gli altri senza averne sentore.

L'esigenza primaria del virus è quella di moltiplicarsi infettando più macchine possibile.



*“La sola apertura di un messaggio può causare infezioni”*

**Tutti i pc dell'azienda collegati in rete sono protetti da antivirus gestito centralmente.**

**Gli antivirus non offrono protezione totale,** non si deve quindi dimenticare il problema solo perchè si ha l'antivirus installato.

Regola primaria è essere sospettosi di fronte a qualsiasi messaggio, anche se inviati da una persona di nostra conoscenza con cui scambiamo regolarmente posta.

## Casi da trattare come sospetti:

- messaggi da mittente sconosciuto
- allegati con nome indecifrabile
- allegati con nome in inglese su messaggio in italiano
- messaggi in lingua straniera spediti da mittente italiano
- messaggi con allegato e con testo che non fa nessun riferimento all'allegato
- messaggi dal contenuto assurdo come "Clicca sull'allegato per vedere foto segrete di pinco pallino"
- comunque qualsiasi messaggio che risulti strano o diverso dal solito

## **In caso di dubbi sul contenuto, non aprire l'allegato e contattare il tecnico informatico.**

Sia i messaggi di mittenti interni all'azienda, sia quelli esterni devono ugualmente essere trattati con la dovuta cautela. Benché la più frequente via infettiva sia la posta, i virus sono frequentissimi nei documenti word o excel, sotto forma di macro, i cosiddetti macro virus.

**Stop ai messaggi inviati in serie**, come le catene di S. Antonio. I messaggi di auguri sono sempre graditi, ma è bene inviarli senza allegare programmi inutili e a volte pericolosi .

Tra la posta indesiderata rientrano anche i **messaggi "spam"**. Per limitarli il più possibile bisogna attuare alcuni accorgimenti:

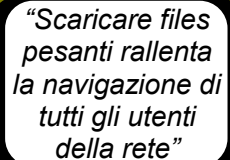
- evitare di diffondere il proprio indirizzo. Molti siti, non sempre affidabili, chiedono di iscriversi inserendo un indirizzo e-mail; indicare il proprio indirizzo solo quando è strettamente necessario.
- non attivare i collegamenti contenuti nei messaggi. Si rischia di segnalare che il proprio indirizzo e-mail è valido e usato frequentemente.
- non rispondere mai alle mail provenienti da sconosciuti, è un altro modo per far capire agli altri che esistete.
- nascondere i destinatari. Quando si spediscono numerose e-mail in copia carbone, usare la casella "copia nascosta" (Ccn), in modo da non mostrare a tutti la lista dei destinatari.

# Navigare sul web

**Tipologia di siti:** navigare nei portali istituzionali (libero, alice, ti-scali, google, ferrovie italiane, sole 24 ore, ecc.) non arreca problemi. Ma alcuni link, che si trovano su tali portali, dovrebbero essere evitati (suonerie dei telefonini, file musicali gratuiti, software pirata, giochi, pubblicità in genere, ecc...).

**Traffico di rete:** scaricare files di grosse dimensioni (maggiori di 50 Mb) è causa di rallentamento della navigazione per tutti gli altri utenti della rete aziendale. Naturalmente ci sono situazioni in cui questo non può essere evitato, in tal caso è bene scaricare il file una sola volta, mettendolo in rete per condividerlo con i colleghi, piuttosto che scaricarlo di nuovo, ogni volta che lo si vuole consultare.

La rete viene occupata non solo con il download diretto di un file, ma anche con l'ascolto o la visualizzazione di files in streaming (you tube, notiziari video, siti per ascolto di musica). Volendo ascoltare musica, è molto meglio farlo inserendo un cd nel lettore del proprio pc.



*“Scaricare files pesanti rallenta la navigazione di tutti gli utenti della rete”*

**Download sicuro:** un'altra via infettiva sono tutti i tipi di software scaricati da internet. Spesso si installano software non supportati dal reparto tecnico informatico; è bene tenere presente il rischio di infezione che questi comportano.

**Aggiornamenti di Microsoft:** con regolare cadenza, si viene avvertiti, dalla presenza di uno scudetto giallo vicino all'orologio (in basso a dx), della presenza di aggiornamenti del sistema operativo, pronti per essere installati. Tali aggiornamenti sono prevalentemente correzioni a vulnerabilità del sistema operativo. Per installarli basta cliccare col tasto dx del mouse sullo scudetto giallo e selezionare “installa aggiornamenti”. **Attenzione: Microsoft e gli altri produttori di software non inviano mai aggiornamenti via e-mail.** Nel caso riceveste una mail da Microsoft, che richiede di installare l'allegato, ignoratela e cancellatela.

# Password

Visto il continuo aumento delle password, necessarie per accedere ai servizi di rete e l'attuale mancanza di standardizzazione delle stesse, è bene specificare alcune regole da seguire.

**Le passwords sono personali** e vanno quindi tenute segrete, evitando di attaccare post-it, con appuntata la parola d'ordine, sotto la tastiera o, peggio, sul video. Tanta fatica per gestire e ricordare le password, per poi renderle pubbliche? In caso di necessità, si può riferire la propria password al collega che ha bisogno di collegarsi in vostra assenza, magari modificandola alla prima occasione. Si ricorda che ognuno è responsabile delle azioni effettuate dal proprio accesso alla rete aziendale.

**Per legge le password vanno cambiate**; vi verrà quindi richiesto di cambiarle ogni 3 o 6 mesi. Volendo evitare problemi per ricordarle, **una volta ricevuta la richiesta di cambio password, si potrebbero modificare anche tutte le altre, in modo da impostarle sempre tutte uguali**. Naturalmente questo non è obbligatorio.

**Come e dove memorizzarle.** Le password sono spesso troppo numerose per ricordarle a memoria, inoltre sono sempre legate a un nome utente. Due pratici sistemi per non dimenticarle sono i seguenti:

- scriverle in un foglio di carta da conservare sempre nel portafoglio e nel quale aggiornare, di volta in volta, le passwords modificate,
- creare un documento word, da memorizzare in rete nella propria cartella privata. Anche in questo caso, le password modificate vanno sempre aggiornate. Utente e password di accesso alla rete devono naturalmente essere scritti anche altrove.

# Glossario

## **Spyware**

È un tipo di software che raccoglie informazioni riguardanti l'attività on-line di un utente (siti visitati, acquisti eseguiti in rete etc...) senza il suo consenso, trasmettendole tramite internet a un'organizzazione che le utilizzerà per trarne profitto, solitamente attraverso l'invio di pubblicità mirata.

## **Malware**

Software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi *malicious* e *software*, ha dunque il significato letterale di "programma malvagio".

## **File di documento**

Insieme di dati raccolti in un unico documento digitale. Esistono file di testo, audio, video, di calcolo, ecc...

## **File di programma**

File che avvia un'applicazione o un programma. I file di programma hanno estensione exe, pif, com, cmd o bat.

## **Rete**

Una rete (in inglese network) è un insieme di sistemi per l'elaborazione delle informazioni messi in comunicazione fra loro.

## **Download**

Trasferimento di un file da un computer remoto (server o host) a un computer locale (client).

## **Streaming**

Trasmissioni video (con o senza audio) veicolate via web e fruite in diretta. Le immagini vengono inviate in sequenza dal server e immediatamente scompattate e visualizzate client.

## **Fonti:**

it.wikipedia.org — www.regionedigitale.net

Per dubbi e chiarimenti rivolgersi a:  
**Elisabetta Calzolari**  
**[e.calzolari@aspgiovanni23.it](mailto:e.calzolari@aspgiovanni23.it)**



ASP Giovanni XXIII

Progetto grafico e stampa:  
Ufficio Relazioni con il pubblico, comunicazione e qualità