Ludoteca
Registro.it

NABBOVALDO E IL RICATTO DAL CYBERSPAZIO

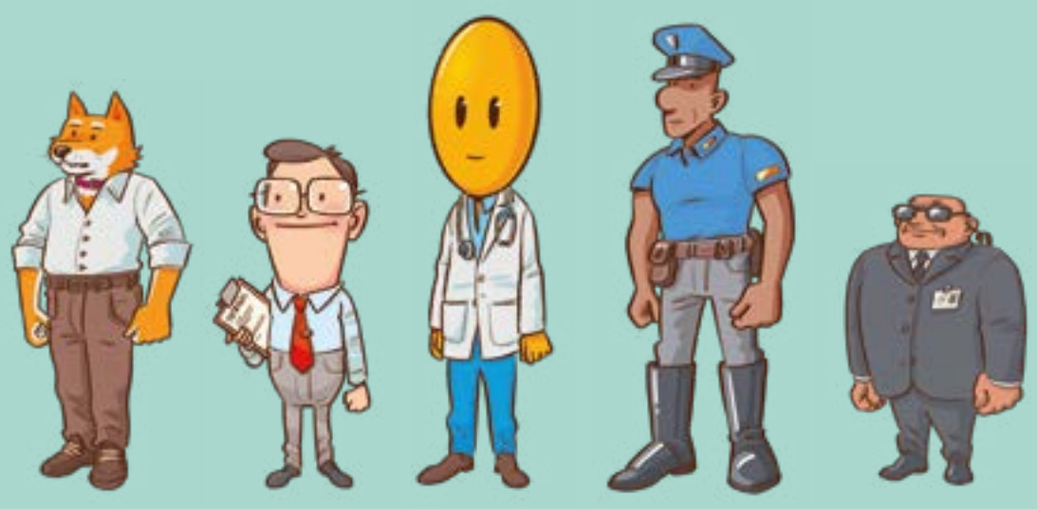
Guida
per gamers

Internet è come una grande città, fatta di indirizzi, luoghi e persone che la popolano ogni giorno. Ci offre molte **opportunità** - parlare con gli amici, studiare, giocare e tanto altro ancora - ma proprio come in una grande città ci sono **regole** di comportamento e di prudenza da rispettare e **pericoli** da cui guardarsi.
"Come mettere in sicurezza i nostri computer, i nostri cellulari", "come creare delle password difficili da indovinare" sono solo alcuni degli argomenti che potrete leggere in questo libro. Difendersi da tutto è difficile ma quello che conta è **conoscere i rischi** e le "**contromisure**". Questa guida è un buon punto di partenza per conoscere meglio la Rete e capire cosa fare se ci troviamo di fronte a un problema: infatti la soluzione non è scappare ma imparare ad **orientarsi** in sicurezza, godendosi il viaggio e arrivando a destinazione.

Buona lettura!

Alla scoperta di Internetopoli

Ciao ragazzi! Mi conoscete già? Per sicurezza mi presento: sono **Nabbovaldo**, per gli amici Nabbo. Vivo nella città di **Internetopoli** e di mestiere faccio… un po' di tutto. «Qualunque sia la matassa da sbrogliare, chiamate senza indugio Nabbo Tuttofare!». Vi piace questo slogan? L'ho inventato io! Forse mi avete già incontrato in qualche **fumetto**, e se non vi è capitato lo trovate qui: **www.ludotecaregistro.it/comics**. O forse mi avete visto in azione nell'avventura **Nabbovaldo e il ricatto dal cyberspazio**, un'app che potete scaricare da Internet e giocare sui vostri cellulari. Scommetto che sapete meglio di me come si fa. Anche perché, devo proprio ammetterlo, in queste cose io non sono molto in gamba, anzi! Il mio soprannome, Nabbo, significa proprio qualcuno che non se la cava molto bene fra computer, smartphone, Internet e videogiochi. Ma per fortuna ho molti amici e conoscenti che possono aiutarmi… Eccone qui alcuni, ve li presento:



MR. D | REGGIE | DOTTOR KAPPERSKY | IL POLIZIOTTO | L'UOMO IN NERO

Li conoscerete meglio giocando con l'app e leggendo questa guida che vi porterà alla scoperta di **Internet**, delle tante **belle cose** che potete trovarci e anche di qualche **pericolo**. Io passo molto tempo in Rete: chiacchiero con gli amici, ascolto musica, guardo video divertenti, a volte studio e naturalmente gioco, da solo o in compagnia. A volte ho rischiato di mettermi in qualche guaio, online, ma grazie a questi tipi in gamba, che avete visto nella pagina precedente, me la sono sempre cavata e ho anzi imparato a **evitare qualche trappola**. Li ho chiamati qui per dare qualche buon consiglio pure a voi. E allora, via! Incamminiamoci per **Internetopoli**. Per iniziare non c'è da andar lontano. Già alla **porta accanto** alla mia vive qualcuno che sa parecchie cose interessanti... Andiamo a interrogarlo!

Dal computer alla Rete

--> UN PO' DI STORIA <--

I primi **computer**, nati durante la Seconda guerra mondiale, erano enormi e costosissimi. Solo le organizzazioni militari, le università e le grandi aziende potevano permetterseli. ENIAC, uno dei primi, era lungo 30 metri, alto 3, e pesava ben 30 tonnellate! Per scambiarsi dati e programmi si spedivano nastri per posta. Nel 1969 è nata **Arpanet**, una rete militare che collegava quattro computer sotto il controllo del Dipartimento della Difesa americano. Man mano venne ampliata ad altri computer militari e universitari e nacquero altre reti.

A metà degli anni '70 arrivarono i **personal computer**, o PC, che chiunque poteva usare per lavorare ma anche per svago. Da allora si sono diffusi ovunque, nelle case e negli uffici. Mentre dal 1973 un "protocollo", cioè una serie di regole, consente ai vari dispositivi collegati di "parlare tra loro" e trasmettere dati.
È nata **Internet**, "la Rete delle reti", a cui chiunque può collegare il proprio computer o una rete di computer. I dati passano per i collegamenti più diversi: dai cavi telefonici alle fibre ottiche, dai ponti radio alle trasmissioni satellitari...

SPEZZATINO DI PAROLE

Gioco

Prova a riordinare la frase qui sotto, che è stata tagliata in blocchetti e mescolata: dopo il "Nonc..." iniziale, alterna un blocchetto di lettere in corsivo a uno in neretto. Ricostruirai cosa disse il dirigente informatico Ken Oleson nel 1977, quando ancora non immaginava il grande successo dei personal computer. E tu cosa ne pensi?

Nonc... _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____

bbades **cunode** *mputer* **iderar** *uiqual* **acasap** *ediave* **neperc** *ropria* **reunco** *eragio*

SOLUZIONE: La frase di Ken Oleson è: "Non c'è ragione per cui qualcuno debba desiderare di avere un computer a casa propria."

Tra miliardi di pagine

Il **Web è un enorme ipertesto**, cioè un insieme di documenti con informazioni di varia natura (immagini, testi, video, suoni, programmi…) collegati l'uno all'altro attraverso **parole chiave**: sì, possiamo immaginarlo proprio come un'enorme rete, i cui nodi sono costituiti da questi miliardi di documenti. Ma come ci si muove sul Web? Mentre per leggere un testo normale c'è una sola direzione possibile, dalla prima all'ultima pagina (come in un libro), la caratteristica di un ipertesto è che la lettura non si svolge in **maniera lineare**, ma cliccando sui vari **link** si può passare da un documento all'altro, seguendo i collegamenti che più interessano, e raggiungendo così pagine che si trovano in computer sparsi per tutto il mondo! Chiunque può creare un **sito** realizzando un po' di pagine e linkandole ad altri siti. E questo è bellissimo ma è anche un problema, perché non tutto quello che si trova in Rete è affidabile… ma di questo parleremo più avanti.

--> UN PO' DI STORIA <--

Il Web nasce nel 1991 al **CERN**, un centro di ricerca di Ginevra, per aiutare gli studiosi di tutto il mondo a condividere i risultati. Si diffonde subito e dal 1995 può essere usato anche per scopi commerciali.

Oggi esistono più di due miliardi di siti, anche se alcuni sono molto vecchi e non aggiornati, ed è usato da **cinque miliardi di persone** anche per attività quotidiane come informarsi, fare shopping, gestire il conto in banca, consultare le pagelle di scuola, vedere video, sentire musica, prenotare viaggi e alberghi, tenersi in contatto con amici e parenti, e per tanto, tanto altro…

Ogni pagina al suo posto

Quando è nata, la Rete collegava **università e centri di ricerca**. Non esisteva il problema della sicurezza perché Internet era utilizzato da studiosi di poche organizzazioni e non c'erano attività commerciali o finanziarie. Presto però la Rete si è allargata ed è diventata **accessibile a tutti**. Oggi in Rete trascorriamo **molto tempo**, cerchiamo notizie, giochiamo, studiamo, rimaniamo in contatto con gli amici, ascoltiamo musica, compriamo quello che ci serve… Da una parte quindi la cosa straordinaria è che chiunque può collegarsi utilizzando i servizi offerti, dall'altro qualcuno può farlo in maniera **anonima** o sotto **falsa identità**, con l'obiettivo di commettere delle azioni "malevoli" nei confronti di altri utenti. Chi naviga quindi deve stare attento a chi incontra e a dove capita, perché alcuni siti potrebbero essere stati realizzati a scopi ingannevoli o criminali.

*** PER APPROFONDIRE ***

Uno strumento per navigare

Per muoversi nella Rete, si utilizza un programma chiamato **browser**, capace di visualizzare i dati delle pagine Web e ricomporre testi, immagini e così via. Ogni dispositivo in Rete ha un **indirizzo IP** (Internet Protocol), formato da quattro gruppi di tre cifre, comprese fra 0 e 255, come 192.12.192.128. Poiché sono difficili da ricordare, i siti hanno anche un **nome a dominio** leggibile: per esempio **ludotecaregistro.it**. Passando il mouse su un link prima di cliccare, vedrete il vero indirizzo che non sempre è quello che si legge nella pagina. Perciò riscrivere gli indirizzi nel browser è sempre più sicuro che cliccare sui link.
Il nome finisce col **dominio di primo livello**: ad esempio .it, .com, .info. Alcuni indicano la nazionalità del sito: ad esempio ".it" per l'Italia o ".pl" per la Polonia. Altri indicano il tipo: ".com" i siti commerciali, ".gov" i governi. Prima dell'ultimo punto c'è il **dominio di secondo livello**, che in caso di dubbio è la parte da verificare: e così "servizi.senato.it" appartiene al Senato, ma "senato.servizi.it" potrebbe essere di chiunque!

--> UN PO' DI STORIA <--

Dal 1987 il Consiglio Nazionale delle Ricerche gestisce il **Registro .it**, che si trova presso l'Istituto di Informatica e Telematica del CNR di Pisa: a esso deve rivolgersi chiunque voglia registrare un dominio .it, modificarlo o cancellarlo, perché è il Registro .it che gestisce l'elenco dei nomi a dominio che finiscono per ".it".

Il malware in agguato

Sappiamo tutti che i virus sono pericolosi per l'uomo. Ma anche con cellulari e computer si deve fare attenzione! Alcuni programmi si comportano allo stesso modo, per questo vengono chiamati **virus**: infettano in segreto i nostri dispositivi, si riproducono e si moltiplicano dentro di essi, modificano o nascondono software e dati rovinandoli, passano ad altri computer e smartphone che entrano in contatto con quello infetto attraverso messaggi o allegati.
Con gli anni i malintenzionati hanno creato software sempre più dannosi, per arricchirsi o solo per il gusto di creare danni agli altri. Oggi si parla più in generale di **malware** (che deriva da **mal**iciuos soft**ware**) per indicare con un'unica parola ogni tipo di programma malevolo. E ce ne sono di tanti tipi! Ad esempio:

Worm che si moltiplicano sul disco del computer e si diffondono su altri dispositivi attraverso Internet.
Trojan che si nascondono in programmi apparentemente innocui e permettono di entrare nel computer per prenderne il controllo, come fecero i Greci a Troia col famoso cavallo.
Spyware che spiano cosa fa l'utente, per rubargli password e dati personali.
Adware che sommergono l'utente di pubblicità indesiderate.
Ransomware che bloccano dati o intere macchine, permettendo a chi li ha diffusi di chiedere un riscatto (anche se spesso, incassati i soldi, ne chiedono altri o spariscono senza sbloccare nulla).

Ecco allora un po' di buoni **suggerimenti**:
- Installate un buon antivirus e tenetelo aggiornato.
- Evitate di scaricare app da store non ufficiali.
- Evitate copie illegali di programmi, siti pirata con film e libri gratis, banner pubblicitari: possono portare virus e malware.
- Non fate "craccare" i vostri cellulari e dispositivi per sbloccarli e non installate ogni tipo di programma, perché queste azioni ne indeboliscono le difese e li espongono ad attacchi.
- Se trovate chiavette usb in giro, non inseritele nel vostro computer: qualche volta gli hacker fingono di smarrirle per infettare i computer altrui.
- Non cliccate su link sospetti che provengono da sconosciuti.
- Fate sempre una copia dei dati importanti (backup).

*** PER APPROFONDIRE ***

Attenti ai bachi!
I programmi dei computer possono presentare punti deboli, errori nel codice in cui sono scritti e così via. Gli informatici li chiamano **bug**, in italiano **bachi**. I malintenzionati possono approfittarsene e sfruttare queste imperfezioni per colpire i vostri dispositivi. Per evitarlo, **aggiornate spesso i sistemi operativi** dei vostri computer e telefonini installando le nuove versioni, che correggono gli errori precedenti. E scaricate le **patch**, piccoli aggiornamenti che rimediano ai problemi man mano trovati.

Hacker buoni e cattivi

Gli hacker – in italiano potremmo chiamarli "smanettoni", anche se la traduzione letterale è "pirata" – sono dei programmatori, veri appassionati di informatica, che tentano di violare i sistemi di sicurezza per **accedere a computer e reti**. Si tratta di un reato, certo, ma non tutti lo fanno per lo stesso motivo.
Alcuni hacker vogliono solo **mettersi alla prova**, spesso infatti lavorano per enti e aziende cercando di mettere in luce i difetti e i problemi delle loro protezioni informatiche, per correggerli e migliorarli. Altri hacker invece agiscono per **scopi ideali o politici**, cercando di sabotare in segreto i siti di organizzazioni e aziende per ostacolarne l'attività; così, ad esempio, combattono le aziende che fanno pagare programmi e software, sostenendo che devono essere gratuiti.
Altri hacker, purtroppo la maggioranza, danneggiano siti di aziende e persone per **guadagnare denaro**. Rubano dati privati per effettuare truffe e raggiri, oppure li rivendono, o addirittura ricattano i proprietari… Questi ultimi sono **autentici criminali informatici**, e tra tutti gli hacker sono quelli che fanno più notizia. Generalmente si tende a distinguere tra hacker buoni e cattivi, usando per i secondi il termine **cracker** che indica coloro che "rompono" i sistemi di sicurezza con intenzioni disoneste, a scopo di teppismo o per soldi.

Gioco

A volte alcuni malware fingono di essere un programma noto oppure di aiuto, come un antivirus, per farsi installare e in realtà rubare denaro o informazioni. Come si chiama questa categoria? Per scoprirlo aggiungete una lettera all'inizio di ognuna delle parole qui elencate, per trasformarla in un'altra parola. Ad esempio, a ETTO potete aggiungere R per trasformarlo in RETTO. Le lettere aggiunte, lette nell'ordine, vi sveleranno il nome di quei malware.

*R*__ETTO
___STIA
___AMBO
___DITO
___VENTO
___EST
___VERE
___OTTO
___SPIARE

SOLUZIONE: Retto, Ostia, Gambo, Udito, Evento, West, Avere, Rotto, Espiare = quel tipo di malware si chiama ROGUEWARE.

UN MESSAGGIO IN MARZIANO?

Gioco

Nabbovaldo ha ricevuto sul cellulare un messaggio misterioso:

TDSJQU LJEEJFT

Ma non sono stati i marziani: le due parole sono state codificate secondo una certa regola che riguarda la posizione delle lettere nell'alfabeto e che dovete indovinare. Se ci riuscirete, scoprirete come si chiamano gli hacker che nei loro attacchi si limitano a copiare e usare script fatti da altri.

SOLUZIONE: Ogni lettera del messaggio è stata sostituita con quella che la segue nell'alfabeto inglese. Per tradurlo, basta sostituire ogni lettera con la precedente: ad esempio, la T diventa S. La soluzione è quindi SCRIPT KIDDIES.

Dati personali e sensibili

Ci sono dei dati che è bene tenere **sempre riservati** e usare con molta attenzione. Primi tra tutti, quelli che permettono di **identificarci**, cioè nome, cognome, indirizzo, data di nascita e così via. Se infatti qualcuno ne entra in possesso, può spacciarsi per noi in Rete. Anche le informazioni sulle nostre **preferenze** e i nostri **gusti** sono preziose per le aziende che vendono prodotti o servizi. Per questo è importante fare sempre molta attenzione quando un sito chiede di registrarsi o chiede informazioni personali. Inoltre, c'è anche il pericolo che i nostri dati siano intercettati dai cracker, se non usiamo **sistemi sicuri** per navigare o scambiarci messaggi.

MESSAGGI CIFRATI

Gioco

Giulio Cesare usava un codice segreto nel caso i suoi messaggi cadessero in mano **nemica**. Sostituiva ogni lettera con quella che seguiva nell'alfabeto di un certo **numero** di posti, solitamente 3: così la A diventava D, la B diventava E e così via, ricominciando, fino alla Z che diventava C. Così, AIUTO diventava DNAZR. I suoi **odiati** nemici non ci capivano nulla, ma il destinatario conosceva il trucco e traduceva il tutto in un **lampo**. Non è un codice molto sicuro, oggi un hacker lo capirebbe in due secondi **netti**! Ma i nemici di Cesare spesso non sapevano nemmeno leggere... Nei secoli si sono inventati codici sempre più complessi, anche difficili e lenti da usare. Ma **ormai** i computer permettono di codificare messaggi e dati con livelli molto più **alti** di sicurezza, e di farlo in un **attimo**!

Anagramma (cambia l'ordine delle lettere cercando di creare una parola che abbia senso) ognuna delle otto parole sottolineate (una te l'abbiamo già anagrammata come esempio): le iniziali delle nuove parole ottenute, lette nell'ordine, ti diranno come si definisce un messaggio codificato e apparentemente illeggibile.

Rumeno _____ _____ _____

_____ _____ _____ _____

SOLUZIONE: Cinema, Rumeno, Idiota, Palmo, Tinte, Amori, Tali, Ottima: un messaggio codificato si dice "CRIPTATO"

*** PER APPROFONDIRE ***

Un protocollo sicuro

Per comunicare sul Web, tutti i computer usano un protocollo (cioè un insieme di regole) che si chiama Hyper Text Transfer Protocol, in breve **HTTP**. La sua versione sicura è l'**HTTPS**, con una "S" finale che sta per "secure", a cui magari non facciamo caso ma che può davvero fare la differenza. Significa che se anche qualcuno riuscisse a intercettare i dati, non sarebbe in grado di leggerli; è come se fossero scritti in uno speciale codice segreto! Avete mai usato un **codice cifrato** per scrivere messaggi ai vostri amici, sostituendo le lettere con simboli o numeri? Solo chi conosce il codice può capire cosa avete scritto. Quindi, se dovete inserire dati personali o delicati, può essere una buona idea controllare che l'indirizzo del sito cominci per https. Inoltre, evitate di digitarli in pubblico, dove qualcuno potrebbe osservarvi. Ed evitate di farlo su wi-fi pubbliche, come quelle dei centri commerciali, dove potete essere spiati molto più facilmente.

Sistemi di protezione dei dati

Per navigare su alcuni siti, bisogna prima registrarsi e creare i due codici che gli permettono di riconoscerci, le nostre "credenziali di accesso":
- un nome utente, o **username**;
- una parola d'ordine, o **password**.

La password in particolare, che deve sempre rimanere **segreta**, va scelta con molta cura: è importante che non sia troppo corta (**almeno 8 caratteri**), che al suo interno ci siano **sia numeri che lettere**, anche caratteri speciali e siano alternate maiuscole e minuscole, e soprattutto che non rimandi a parole facilmente ricollegabili a noi o ai nostri dati personali. Le buone norme da seguire?

- Se alla registrazione su un sito ricevete una **password iniziale**, cambiatela subito.
- Non usate le **stesse password su più siti e account** e cambiatele spesso.
- Per ricordarvi username e password dei vari siti, **non scriveteli in giro**. E se proprio non riuscite a ricordarli tutti, usate un apposito programma per gestirli: così vi basterà ricordare username e password solo di quello per recuperare tutti gli altri.
- Se scrivete password o dati personali fuori di casa, state attenti che **nessuno vi stia guardando**.

Gioco

Sulla pagina di login di un sito, un **hacker** sta cercando di entrare spacciandosi per un altro utente. Ne conosce il nome utente e cerca di indovinare la **password di quattro caratteri**. Finora ha effettuato quattro tentativi:

4E$c	zLE4
cz	c4cL

Sapendo che a ogni tentativo ha messo due caratteri che sono presenti nella password di quell'utente e due che non ci sono, e sapendo inoltre che non è mai stato messo un carattere giusto nella posizione giusta, riuscite a capire qual è la password vera?

SOLUZIONE: L4. Infatti la c è stata provata in tutte le posizioni: siccome sappiamo che nessun carattere giusto è stato provato nella posizione giusta, la c non può essere presente nella password. Quindi, nel quarto tentativo le due c sono sbagliate e i due caratteri veri sono 4 e L. Essendo stato provato in prima, seconda e quarta posizione, il 4 deve andare per forza al terzo posto. La L non può andare né al secondo né al quarto posto, quindi va al primo. Osservando il secondo tentativo sappiamo che, se L e 4 sono giusti, E e z sono sbagliati. Dal terzo tentativo, se c e z sono sbagliati, sappiamo che i due $ sono giusti e non possono che andare al secondo e al quarto posto.

Fake news e disinformazione

Il bello del Web è che **tutti possono accedere e mettere in Rete i propri contenuti**. Pensate che fatica può essere scrivere un giornalino, impaginarlo, stamparlo, diffonderlo in giro, e quanto può costare. Fare un sito è più rapido, facile, economico e potenzialmente arriva subito a chiunque nel mondo.
È davvero meraviglioso, ma ci sono dei problemi. Un giornale o un libro sono scritti da giornalisti e autori e, prima di essere pubblicati, una redazione controlla e verifica i contenuti. In Rete, invece, può scrivere chiunque, senza che ci sia alcuna verifica, ed è più facile che ci siano informazioni sbagliate e **fake news**, notizie non vere. Alcune messe per sbaglio, altre apposta, per scherzo o con intenti malvagi; magari per attaccare qualcuno, per ingannare le persone, per vendere qualcosa e influenzare le opinioni.
È dunque importante imparare a guardare con occhio critico quello che trovate in Rete, soprattutto se viene da siti sconosciuti. Bisogna fare attenzione a non cadere nella trappola di campagne d'odio, complottismi, disinformazione che in Rete sono purtroppo frequenti.

*** PER APPROFONDIRE ***

Suggerimenti per non infettarsi e non condividere fake news

- Attenzione alle **pubblicità**, alcune possono essere false e attendono solo un tuo clic per passarti un virus o toglierti dei soldi.
- Non credere ai **messaggi** che, mentre navighi, appaiono improvvisamente e sembrano provenire dal tuo computer o telefono per dirti che hai un virus e ti invitano a cliccare per toglierlo: non hai ancora nulla, ma è proprio cliccando che ci si può infettare!
- Prima di cliccare su un **link** o condividere una notizia, fai sempre attenzione all'indirizzo verificando il dominio: potrebbero essere pagine con dei malware, finti siti di informazione o di vendita.
- Non dare confidenza agli **sconosciuti**: in Rete non possiamo essere certi di chi si trova dall'altra parte della tastiera.
- Prima di **condividere** una notizia o un'informazione verifica bene il sito su cui è scritta, la data di pubblicazione e se contiene errori ortografici: sono tutti indizi che ci possono dire se è vera o no.

Gioco

Non sempre è facile riconoscere se una notizia è vera. Tra le cinque riportate, sapete riconoscere quali sono le tre vere e quali invece i due fake?

A Nel 1992 una nave ha perso 28.800 tra paperelle e altri giocattoli di gomma che galleggiando hanno percorso decine di migliaia di chilometri attraverso gli oceani, e in buona parte sono ancora in giro per i mari del mondo (fonte: wikipedia.org).

B Un uomo di 27 annni è decollato dal mOnte Rosa con uno deltaplano che si è costruito da solo e sfruttando i venti delle Alpi e dla Pianura Padana ha volato ininterrottamente fino a venezia, atterrando alla Piazza San Marco (fonte: republikka.com, 10 gennaio 2010).

C Le Suore Benedettine hanno trovato nelle Catacombe di Priscilla a Roma 3 cuccioli di coccodrillo, completamente bianchi perché cresciuti sottotera senza luce: discendono da un esemplare ke era stato liberato buttandolo nel gabinetto (fonte: kenesai.pl, 30 febbraio 2022).

D Quando la Covenant School di Dallas ha battuto la Dallas Academy per 100 a 0 al basket femminile, ha licenziato il proprio allenatore e chiesto di essere considerata sconfitta dicendo che aver attaccato senza tregua anche a vittoria certa, umiliando le avversarie, è contro il fair play (fonte: gazzetta.it, 15 giugno 2018).

E L'Unione Europea ha approvato l'uso alimentare degli insetti. I primi tre che potranno essere mangiati e utilizzati come ingredienti negli alimenti sono la larva della farina, la locusta migratoria e il grillo domestico (fonte: repubblica.it, 10 gennaio 2022).

SOLUZIONE: Soluzione: A - vera; B - fake; C - fake; D - vera; E - vera.

Dalla “chiocciola” al post

--> UN PO’ DI STORIA <--

Nel 1971, il programmatore **Ray Tomlinson** ha un’idea: inviare messaggi via Rete da un computer all’altro. Sceglie **il carattere @**, che si chiama “chiocciola” e si legge come “at” (in italiano “presso”), per gli indirizzi di posta.

Nasce così la **posta elettronica** o e-mail che ha un successo enorme. Ed è “informale”: i programmatori possono scrivere messaggi rapidi ai loro capi che non si offendono se il tono è colloquiale e se scappa qualche errore.
Già due anni dopo, tre quarti del traffico su Arpanet è composto da e-mail, e così su Internet appaiono altri programmi per comunicare in modo diverso. Si creano le **mailing list**, che permettono di mandare messaggi in un colpo solo a tutti gli iscritti, e le **chat** con cui ci si può scrivere e rispondere in diretta tra due persone o anche fra tanti, entrando in una “stanza” virtuale: è il servizio che oggi offrono **Whatsapp** e altri strumenti analoghi, come **Snapchat** che permette di condividere foto e messaggi usa-e-getta che dopo poco spariscono. Oggi si aprono pagine dedicate su **social** come **Tik Tok** in cui si condividono video, o **Instagram** immagini, su **Spotify** musica… Ce n’è per tutte le esigenze, personali e di lavoro. E da quando si sono affermati gli smartphone, tutti questi servizi sono a portata di mano.

Gioco

Su Tik Tok e sugli altri social si usano tante parole strane. Spesso sono inglesi, ma a volte in Rete acquistano un significato diverso da quello che avevano in origine.

Sapete collegare ogni parola della colonna di sinistra con il significato che le danno i TikToker? Lo trovate tra quelli indicati nella colonna di destra, ma sono stati mescolati…

cringe	fallire
extra	video molto personale
crush	inutilmente esagerato
floppare	non ti riguarda
nyob	cotta
storytime	imbarazzante

SOLUZIONE: Cringe: imbarazzante; Extra: inutilmente esagerato; Crush: cotta; Floppare: fallire; Nyob: non ti riguarda; Storytime: video molto personale.

Le buone maniere della Rete

Comportarsi con educazione e correttezza è sempre importante: non solo a scuola, in casa o con gli amici, ma anche quando **si naviga in Rete**. Anzi, esiste un insieme di regole di comportamento solo per Internet: si chiama **netiquette**, dei consigli per muoversi con giudizio evitando di risultare odiosi o di dover subire insulti dagli altri.
Contrariamente a quanto pensano alcuni, **in Rete non è tutto permesso**: chi non rispetta la netiquette rischia di farsi cacciare dai moderatori di un sito o di un social. E chi esagera con insulti o comportamenti aggressivi e fuori luogo, rischia anche di violare la legge.
Ecco alcune buone norme da rispettare:

- Prima di far notare un errore, valuta se è necessario e comunque fallo con delicatezza.
- Evita di insultare, di attaccare gli altri, di fare il bullo o rispondere alle provocazioni.
- Prima di diffondere una notizia, assicurati che sia vera controllando se proviene da fonti affidabili e se ci sono riscontri; inoltre, valuta bene se può danneggiare qualcuno.
- Evita di far girare lo spam, cioè la pubblicità indesiderata, e le varie "catene di sant'Antonio", i messaggi che chiedono appunto a chi li riceve di essere a loro volta diffusi.
- Leggi i regolamenti dei siti che visiti e rispettali.

Altre regole particolari valgono per i gruppi, per le mail e così via: ad esempio nei messaggi e nei post si considera maleducato scrivere tutto in maiuscolo, che è un po' come urlare.

Hater e troll

Imbattersi in qualcuno che **non si comporta bene** – nella vita reale come nel Web – non solo è fastidioso, ma può diventare anche sgradevole. Basta pensare a **Hypsta Holly**, perseguitata da una stalker, o a **Flint Flamer** che cerca in tutti i modi di provocare e insultare il povero Nabbovaldo.
Una figura davvero sgradevole è l'**hater**, odiatore per partito preso. Commenta e discute, ma non sa dialogare: non gli interessa un confronto onesto né è disposto a modificare la propria opinione in base a ciò che viene a sapere. Sa solo scaricare odio in **commenti feroci**. Ci sono hater che se la prendono con chiunque e altri che prendono di mira persone o categorie specifiche. Altrettanto spiacevoli sono i **troll**, che scrivono e commentano al solo scopo di **sabotare le conversazioni**. Anche loro provocano e insultano.
Hater e troll cercano **attenzione**: per zittirli, spesso basta non dargliela. Se pensi che valga la pena rispondere fallo, ma senza insistere. Meglio ignorarli. E se non smettono, puoi **bloccarli** o segnalarli agli amministratori del sito o della pagina.
In Rete sembra tutto permesso, ma non lo è affatto: calunnie e aggressioni sono reati, anche se avvengono sul Web. Spesso quando troll e hater vengono indagati dalle forze dell'ordine, abbassano la cresta: sono **leoni da tastiera** nascosti dietro computer e smartphone, ma messi davanti alle loro responsabilità si rivelano pulcini bagnati.

*** PER APPROFONDIRE ***

Personaggi in Rete

In Rete si incontrano le stesse figure che trovate nella vita di tutti i giorni: l'**imbroglione**, come Franco Forex, che cerca di raggirare gli altri; il **credulone** che diffonde qualsiasi notizia senza controllare se è vera, e il **complottista**, come Carla Cospira, che cerca di convincervi delle ipotesi più strampalate. Con loro valgono le stesse strategie utili nel mondo reale: farli ragionare o, se è impossibile, ignorarli. E se vi capita il **bullo**, non dategli soddisfazione e non reagite con violenza. Rispondete con fermezza senza dargli corda. Se poi insiste, fate fronte con i vostri amici e se è il caso rivolgetevi a un adulto.

IL MESSAGGIO CRIPTATO

Gioco

Questo testo è stato cifrato. Sostituisci ogni simbolo con una lettera: tutti i palloni corrispondono a una lettera, tutte le stelline a un'altra e così via. Prova a decifrarlo e otterrai una riflessione del giornalista Gianni Barbacetto su ciò che possiamo trovare in Rete.

SOLUZIONE: La considerazione è: «Internet è una grandissima ricchezza. Il pericolo è che, siccome vi si trova tutto e il contrario di tutto, compaiono anche molti errori. Internet è un mezzo prezioso solo se manovrato con cura: bisogna sempre controllare le notizie, mai fidarsi.»

Pirateria e crimini

Nella vita reale bisogna sempre fare attenzione a non lasciare incustoditi lo zaino, il portafogli o il nostro cellulare, perché in giro c'è sempre qualcuno che potrebbe rubarli. Allo stesso modo, in Rete c'è sempre qualcuno che può sfruttare i nostri errori o le debolezze a proprio vantaggio. **I criminali informatici** possono agire nei modi più diversi. Ad esempio, rubando i nostri codici di accesso ai siti, i dati della carta di credito, la nostra identità per compiere operazioni al nostro posto, impossessandosi dei nostri soldi. Possono anche ingannarci e convincerci a fare noi stessi operazioni che ci danneggiano a loro vantaggio, come comprare su un falso sito di commercio qualcosa che non riceveremo mai.
Oltre a evitare queste trappole, noi stessi dobbiamo stare attenti a **rispettare la legge**. Possiamo finire in guai seri, per esempio pubblicando immagini o testi di altri senza il loro consenso. E ricordiamoci che la diffamazione e l'ingiuria sono reati, anche sul Web. O cercando di guardare gratuitamente trasmissioni a pagamento, di scaricare film e musica coperti dal diritto d'autore: questa è pirateria. Senza contare che i file così scaricati possono contenere malware. Cosa fare per evitarlo?

- Non violare la privacy degli altri diffondendo notizie o immagini senza il loro consenso.
- Non fare cose vietate, come scaricare gratis contenuti a pagamento: non sono semplici scorrettezze, ma violazioni della legge che potrebbero metterci nei guai.
- Se scopri come si possono effettuare queste operazioni illegali, non spiegarlo ad altri.

Infine, in Rete non sempre sappiamo con certezza **chi abbiamo davanti** e questo può esporci a situazioni estremamente sgradevoli, come il **cyberbullismo**. La fiducia è una bella cosa, ma diamola solo a chi la merita!

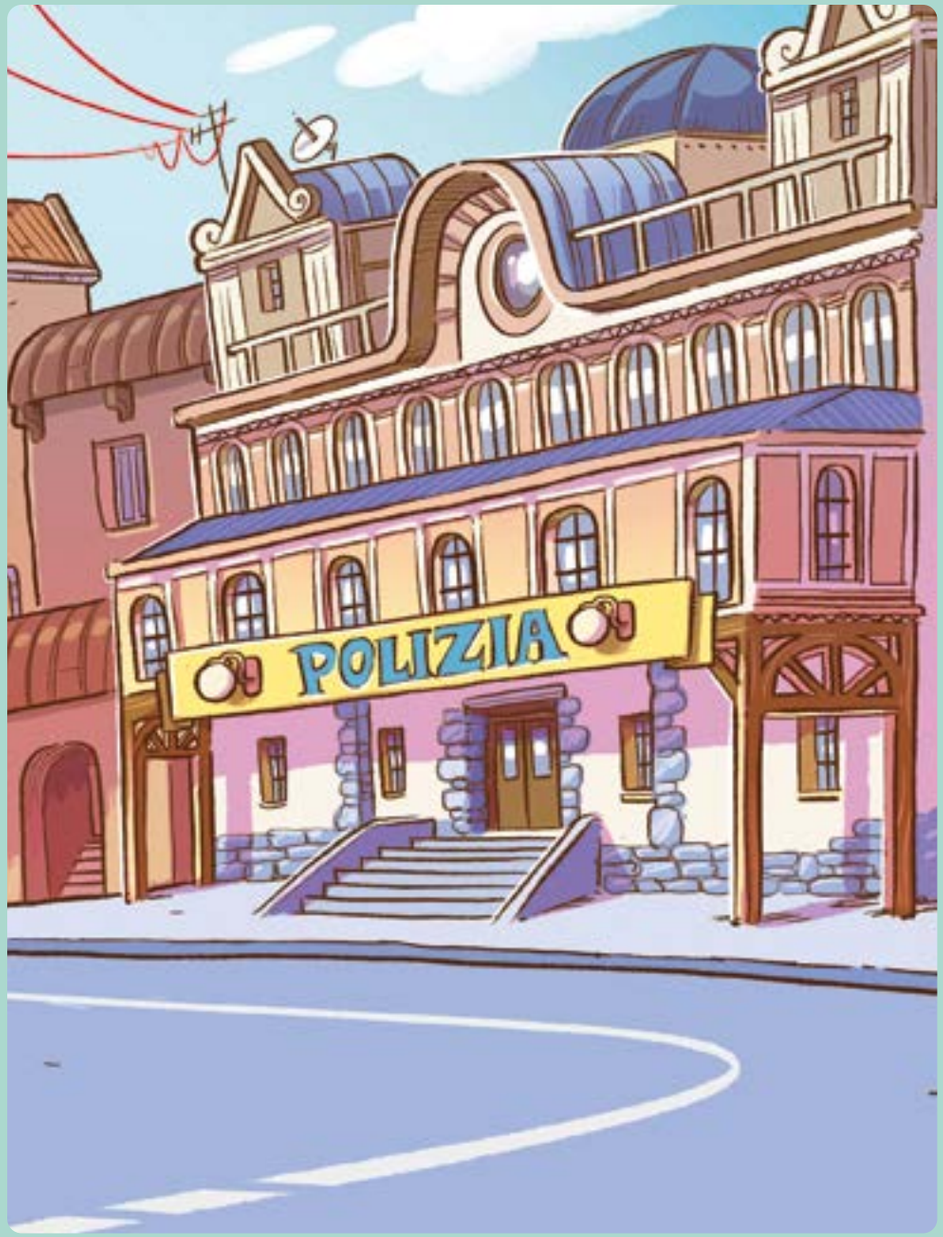
Grandi aiuti dai grandi

Abbiamo visto che la Rete è un posto molto bello ma **non privo di pericoli**. Frequentato da tante persone: amici e parenti, ma anche sconosciuti non sempre ben intenzionati. Proprio come il mondo reale. Per questo occorre sapersi muovere con attenzione, come ci hanno insegnato Nabbovaldo e i suoi amici nelle loro avventure.
A volte, come nel mondo reale, possiamo imbatterci in situazioni più grandi di noi. In questi casi, non dobbiamo esitare a chiedere **l'aiuto degli adulti**. È la cosa più corretta da fare: non possiamo sperare di risolvere sempre da soli le circostanze più difficili.
Ci sono anche casi in cui gli stessi adulti hanno bisogno di aiuto. Per fortuna c'è chi ci protegge, grandi e piccoli. Anche in Rete. Se si può avere la sfortuna di incontrare dei cybercriminali, è anche vero che esistono dei preparatissimi cyberpoliziotti! La **Polizia Postale e delle Telecomunicazioni** ha sedi su tutto il territorio italiano. Si occupa dei furti di dati e di identità, di violazioni del copyright, di gioco d'azzardo illegale, di cyberterrorismo e di altro ancora.
Su **www.commissariatodips.it** ci si può informare sulle ultime novità nel campo della sicurezza, si possono chiedere chiarimenti e si possono effettuare segnalazioni e denunce.
Anche la Guardia di Finanza ha un **Nucleo Speciale Tutela Privacy e Frodi Tecnologiche** che si occupa soprattutto di truffe, evasione fiscale e diritto d'autore. Insomma, siamo in buone mani. Quando serve, non esitiamo a chiedere aiuto!

*** PER APPROFONDIRE ***

Il manifesto per la sicurezza

Vuoi saperne di più? Vieni a scoprire il primo manifesto per la sicurezza online dedicato alle studentesse e agli studenti su: **https://www.ludotecaregistro.it/le-10-regole-per-navigare-consapevoli-e-sicuri**.



Testi: Andrea Angiolino
Contributo e supervisione ai testi: Giorgia Bassi
Impaginazione: Lorella Chiavacci per LCD

Prima edizione: gennaio 2023

Stampato presso Quintily S.p.A. –
Stabilimento di Roma