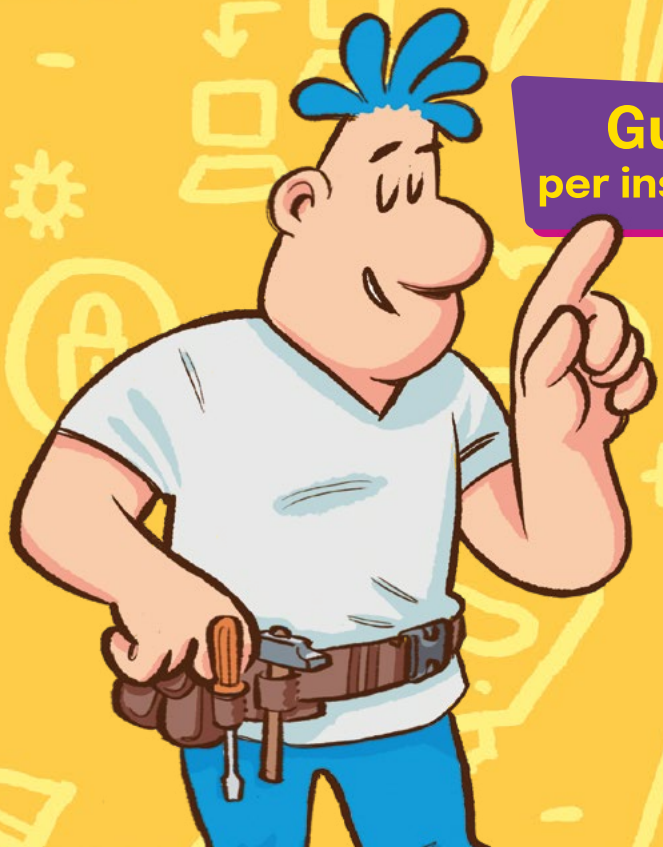
Ludoteca
Registro.it

NABBOVALDO E IL RICATTO DAL CYBERSPAZIO



Guida
per insegnanti

INTRODUZIONE

Registro .it (www.registro.it) è l'anagrafe dei domini internet italiani. Opera nell'ambito dell'IIT – Istituto di Informatica e Telematica del Consiglio Nazionale delle Ricerche di Pisa ed è da sempre impegnato nella diffusione della cultura di Internet.
Dal 2011 ha avviato un progetto di educazione digitale nelle scuole, la **Ludoteca del Registro .it**, per spiegare agli studenti come funziona la Rete e diffonderne l'uso consapevole.
Ecco i **punti di forza** del progetto:

- i contenuti sono curati direttamente dai ricercatori e tecnici dello IIT del CNR;
- è un progetto gratuito per le scuole che aderiscono;
- le attività proposte rompono lo schema della lezione frontale con giochi di gruppo, cartoni animati, lezioni aperte nella sede pisana del CNR.

I laboratori della Ludoteca si basano sul **gioco** e il **coinvolgimento attivo** di ragazzi e ragazze, rendendoli protagonisti di un'avventura che ruota intorno al mondo di Internet, a cominciare dai suoi meccanismi di funzionamento.
Tra gli obiettivi del progetto c'è anche la ricerca di **strumenti innovativi per la didattica del digitale**, adatti ai diversi ordini e gradi delle scuole coinvolte. Da qui la scelta di sviluppare risorse di vario tipo come fumetti, giochi da pavimento, web app, cartoni animati.

La cybersecurity spiegata ai ragazzi

Internet è un "luogo" in cui passiamo una parte sempre maggiore del nostro tempo. Per lavorare, informarci, rilassarci, restare in contatto con gli amici, fare acquisti.
Il **mondo virtuale** è sempre più in grado di affiancare e integrare il mondo reale in tante funzioni quotidiane. Ma, come nel mondo fisico, anche qui non mancano **trappole e minacce**, con il problema che si presentano in forme spesso nuove e difficili da riconoscere. Ancor più per i giovanissimi, navigatori entusiasti ma poco consapevoli dei rischi.
Per questo la Ludoteca dedica un focus ai temi della **cybersecurity** cercando di spiegare, attraverso attività di gioco educativo, le principali **minacce online** e soprattutto le tecniche e i comportamenti per evitarle.
La scelta di realizzare un videogioco su questi temi mira a sensibilizzare i ragazzi e le ragazze tra i 10 e i 13 anni con un linguaggio a loro particolarmente familiare. "**Nabbovaldo e il ricatto dal cyberspazio**" è un **single player adventure**, un gioco di esplorazione e abilità che porta il giocatore a confrontarsi con un caso di cybercrimine, incontrando personaggi e situazioni divertenti. Tutto avviene a **Internetopoli**, la città della Rete. Qui il protagonista, ispirato al Marcovaldo di Calvino, si propone come "tuttofare" e si trova a risolvere una serie di problemi di sicurezza informatica, coinvolto in una grande sfida con un misterioso avversario.
Il gioco è disegnato da Gabriele Peddes su sceneggiatura di Giovanni Eccher con

i toni ironici e accattivanti di un fumetto. Non è un caso, perché è il seguito ideale di "**Nabbovaldo ovvero le stagioni a Internetopoli**" e "**Nabbovaldo contro i pc zombi**": due storie a fumetti che si possono leggere su **www.ludotecaregistro.it/comics**.

La struttura del gioco

Il gioco è diviso in quattro capitoli e contiene i seguenti elementi:

- una **mappa** di Internetopoli, la città di Nabbovaldo, che mostra la posizione del giocatore e gli consente di passare da una location all'altra;
- una serie di **ambienti** che rappresentano i luoghi più significativi di Internetopoli;
- in ciascun ambiente, di norma, Nabbovaldo incontra un **personaggio** con cui il giocatore interagisce in un **dialogo**, durante il quale sceglie man mano le risposte da dare;
- **minigiochi** collegati al tema, segnalati sulla mappa con icone blu in movimento;
- il giocatore può raccogliere le pagine sparse negli ambienti della **Nabbopedia**, un dizionario che gli permette di familiarizzare con i termini e i concetti della sicurezza informatica.

Il gioco prevede una struttura ibrida tra il **percorso fisso** e l'**open world**. Il giocatore può infatti muoversi liberamente nella mappa, parlare con i personaggi e risolvere i minigiochi nell'ordine che preferisce, ma la trama del gioco si sviluppa in **quattro capitoli** principali, più un **epilogo** in cui il giocatore può solo effettuare un dialogo finale. Ogni volta che il giocatore risolve tutti i minigiochi e gli obiettivi del capitolo corrente, si passa al capitolo successivo. Questo permette anche di "resettare" il mondo del gioco tra un capitolo e l'altro. Visivamente, i capitoli sono separati l'uno dall'altro da **filmati** che portano avanti la storia principale.

Per quanto riguarda il **sistema di ranking**, i punti sono chiamati "**like**" e sono rappresentati dalla classica icona con il pollice alzato. Essi si ottengono:

- giocando ai minigiochi;
- rispondendo in maniera corretta nei dialoghi a scelta multipla;
- raccogliendo le pagine della Nabbopedia sparse negli ambienti di gioco;
- leggendo i nuovi termini aggiunti alla Nabbopedia.

Al contrario, si perdono:

- rispondendo in maniera sbagliata in alcuni dialoghi a scelta multipla;
- giocando più di una volta al minigioco "Slot Machine".

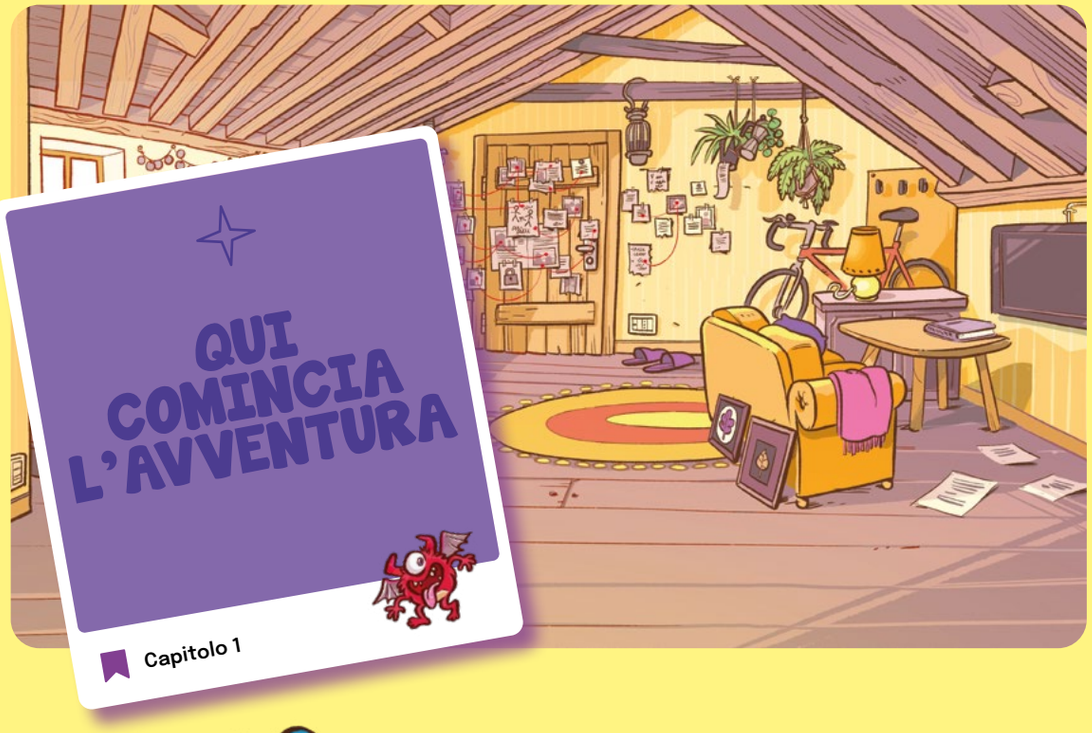
Alla fine del gioco (le partite possono essere salvate) viene conferito un "ranking" a seconda di quanti like il giocatore ha accumulato in totale.
La **Hall of fame** mostra la classifica dei giocatori di tutta Italia.

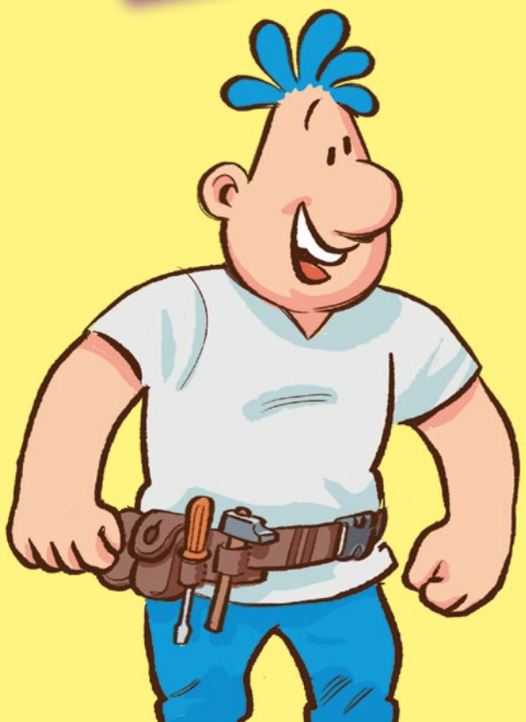
Lanciare l'avventura

L'app "**Nabbovaldo e il ricatto dal cyberspazio**" è disponibile sui principali store, come l'App Store di Apple per i cellulari iOS e Google Store per quelli Android. Innanzitutto installatela voi stessi sul vostro **cellulare** o **tablet** e giocate almeno una partita di prova, per farvi un'idea dei meccanismi e del linguaggio del gioco. Quindi proponetelo ai vostri alunni, chiedendo loro di installarlo sui propri device e di giocarci a casa, cercando di portare l'avventura sino in fondo. Annunciate che dopo un certo periodo di tempo, ad esempio una o due settimane, ne parlerete tutti insieme in classe, per rispondere anche a eventuali domande. Per supportarli nel gioco e consentire loro di soddisfare i principali dubbi mentre giocano, potete subito distribuire i **libretti per la classe** che avete trovato nel kit.
Durante l'avventura, i ragazzi e le ragazze si trovano a fronteggiare situazioni in cui devono applicare il buonsenso per capire quali siano i **comportamenti corretti** da tenere in Rete. Inoltre rispondono a **quiz mascherati da dialoghi**, da cui possono apprendere interessanti nozioni sulla cybersecurity. Ciascuno dei vostri alunni effettuerà percorsi diversi nell'avventura, prendendo scelte e vivendo **esperienze differenti**. Inoltre, raccoglierà elementi e spunti con le definizioni della **Nabbopedia**, utili come primo riferimento per comprendere le molte sfaccettature dell'argomento.
Lo scopo del **libro per la classe** è quindi quello di **rispondere alle curiosità** suscitate dal gioco, offrendo al tempo stesso una **panoramica generale** dei temi trattati. Da questo punto di vista è una lettura preziosa anche per gli insegnanti, dal momento che offre una **visione sistematica** dei temi.

Come procedere in classe

L'attività in classe servirà a approfondire e contestualizzare quanto appreso durante il gioco. Nella didattica, il **dopogioco** è utile almeno quanto il gioco. A introduzione delle attività potete far raccontare ai vostri alunni l'avventura che hanno giocato, ciascuno per la parte che ha visto e vissuto. Potete **rispondere alle curiosità** sollevate dai vari episodi del gioco, grazie agli approfondimenti che troverete in questa guida, magari dopo aver chiesto agli alunni stessi di provare a rispondere ai compagni in base a quanto hanno appreso durante il gioco.
Starà poi a voi stimolare e indirizzare ulteriormente le curiosità e le domande della classe, contestualizzandole nel quadro generale dei temi della sicurezza informatica. Per aiutarvi a farlo, o per procedere in attesa che i ragazzi e le ragazze manifestino dubbi e desideri di approfondimento, la guida propone una serie di **percorsi di approfondimento** tratti dal gioco. Oltre a riassumere la **trama**, si sofferma sui **personaggi** e sui **luoghi** più significativi di ogni sezione agganciando la spiegazione di temi specifici da proporre alla classe. Sono suggerite anche alcune **attività** da inframezzare al dialogo con gli alunni, e un gioco a squadre che utilizza le definizioni della Nabbopedia. Potete infine chiedere ai ragazzi e alle ragazze in quali momenti del gioco si sono trovati a fronteggiare i pericoli della Rete, così da poter collegare a tali situazioni le indicazioni contenute nella sezione "**Attenti ai pericoli!**". Buona lettura, buona navigazione e buon gioco!





Riassunto del capitolo

Il primo capitolo del gioco introduce il protagonista, **Nabbovaldo** detto Nabbo, un ragazzo che vive a Internetopoli e che si è inventato un lavoro di "tuttofare" a domicilio. Lo slogan è promettente: "Se hai un problema, rivolgiti a nabbovaldotuttofare.it!".
Il giocatore si immedesima in lui. Ad accoglierlo nelle prime schermate è **Reggie**, la guida del Registro .it, che in una breve panoramica illustra i meccanismi e i contenuti del gioco. Quando Reggie termina le spiegazioni introduttive e lo saluta, Nabbo è accanto alla propria casa. Intanto la **mappa** della città evidenzia con apposite icone i luoghi in cui è richiesto il suo aiuto. Man mano che incontra i personaggi che abitano la città, vediamo Nabbovaldo impegnato a risolvere vari **problemi tecnici**: installare computer e periferiche, disinfestarli da worm e altri malware. Intanto veniamo a sapere che la sua ragazza, **Linda**, è in viaggio per lavoro. Effettuati tutti i lavori richiesti, Nabbovaldo incontra sua cugina **Ada** che gli racconta di aver visto un pacco abbandonato sulla soglia della casa di Linda. Nabbo vi si reca e lo apre: ne esce un enorme lucchetto che purtroppo blocca la porta della casa di Linda.

I personaggi

Nabbovaldo è il tuttofare di Internetopoli, volonteroso ma pasticcione. Il nome è ispirato a Marcovaldo, protagonista della raccolta di novelle di Italo Calvino: un ingenuo alle prese con la vita di un'immaginaria metropoli italiana degli anni '60. "Nabbo" è anche un termine usato dai ragazzi e dalle ragazze per indicare un "pivello", un **principiante** dei videogiochi. Viene dall'inglese *noob*, che ha lo stesso significato e che è apparso a metà degli anni '90. In italiano si dice anche "niubbo", dall'inglese *newbie*: un vocabolo radicato da più tempo (era già attestato nel 1970) per indicare un principiante in qualsiasi settore. Nabbo e niubbo sono spesso usati come sinonimi, ma per qualcuno c'è una sfumatura in più: il *newbie* è inesperto e per questo poco abile, ma può anche essere di talento e disposto a imparare; il *noob* è anche goffo e poco propenso a migliorare. Talvolta è ritenuto offensivo e per questo scritto *n00b*, o anagrammato in *obon*, o ribaltato in *boon*, così da sfuggire alle liste nere di parole non ammesse dai vari siti.

>> IN CLASSE <<
Chiedete ai ragazzi e alle ragazze di descrivere il **carattere di Nabbovaldo**, poi confrontatevi sui significati di nabbo e niubbo. Nabbovaldo a quale categoria appartiene?

Nel gioco **Reggie** è il portavoce di Registro .it, l'anagrafe dei domini internet con estensione .it che ha sede nell'Istituto di Informatica e Telematica del CNR di Pisa. Nel 1987 l'organizzazione IANA, Internet Assigned Numbers Authority, ha assegnato al Consiglio Nazionale delle Ricerche il compito di gestire gli indirizzi di **primo livello .it** e la loro associazione con i relativi indirizzi IP (Internet Protocol), codice numerico che identifica in modo univoco tutte le risorse e i dispositivi collegati alla Rete internet. Un nome a dominio è ad esempio **ludotecaregistro.it**. La parte finale del nome ".it" è il dominio di primo livello che, in questo caso, si riferisce alla nazionalità. Per poter essere riferimenti efficaci nell'individuazione e nella localizzazione di macchine e risorse, sia gli indirizzi IP che i nomi di dominio devono essere **univoci**, non ce ne possono essere due uguali.
Se Internet è una grande città, i **nomi a dominio** sono gli indirizzi di case, negozi e uffici. Un **indirizzo**, nel linguaggio della Rete e dei computer, è una sequenza di numeri. Questo indirizzo, che identifica

in modo univoco una risorsa della Rete, si chiama **indirizzo IP**, dove IP sta per Internet Protocol. I calcolatori possono memorizzarlo senza problemi. Gli esseri umani, invece, hanno bisogno di associare agli indirizzi parole o espressioni semplici da ricordare.
I nomi a dominio non sono altro che **sequenze di lettere e/o numeri**, combinate dagli utenti secondo fantasia ma in modo che possano essere facilmente memorizzate. Anch'essi, come gli indirizzi veri e propri, sono unici e non possono essere duplicati.

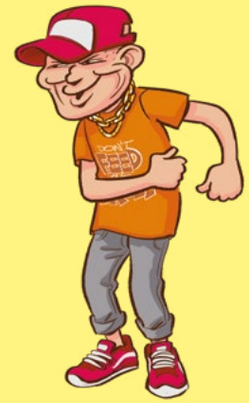
A tradurre i numeri in lettere e viceversa è un sistema chiamato **Domain Name System**, paragonabile a un elenco telefonico, perché associa ogni indirizzo IP al suo nome a dominio.
Come tutte le città che si rispettino, anche la Rete ha le sue strade e i suoi "quartieri": questi ultimi, in particolare, si contraddistinguono per la targa associata al nome a dominio, chiamata **Top Level Domain**. Ce ne sono a centinaia: ".it", ".com", ".net", ".org"... e servono a identificare alcune caratteristiche del nome, come l'ambito cui si riferisce o l'area geografica.

*** PER APPROFONDIRE ***
www.nic.it/it/trova-il-tuo-it/come-registrare.

>> IN CLASSE <<
Potete chiedere ai ragazzi e alle ragazze se conoscono alcuni esempi di **domini internet di primo livello nazionali**, come ".fr", ".de"... Poi, per farli ragionare sull'importanza dell'univocità dei nomi a dominio e degli indirizzi IP, introducete la metafora degli indirizzi postali in una città, anche loro univoci. Le case sono le risorse, ogni casa ha un solo indirizzo altrimenti si farebbe molta confusione... Potete infine proporre agli alunni di **creare il proprio nome a dominio**: fate scrivere nomi a dominio .it di fantasia, dando un tema come il nome di una collana di fumetti di fantascienza, quello di un bioparco... Poi verificate insieme su Registro .it che il dominio sia libero (servizio whois in home page).

*** PER APPROFONDIRE ***
https://bit.ly/3QvDrjW
(carpe digital sui nomi a dominio).

Gli ambienti

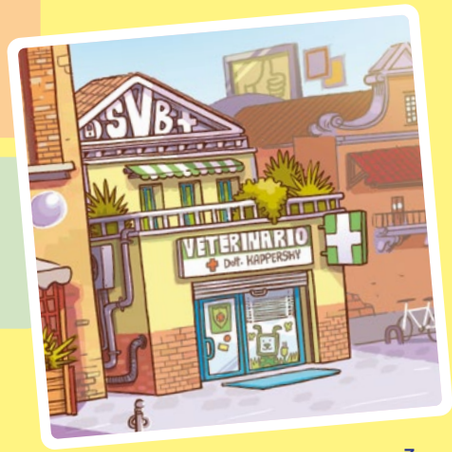


Lo studio del Dottor K., esperto informatico specializzato in cybersicurezza, è il posto davanti al quale Nabbo incontra **Troll**, un ragazzo molto arrogante che, apostrofandolo come "sempliciotto", inizia a fargli delle domande sulla cybersecurity per dimostrargli di saperne molto di più.

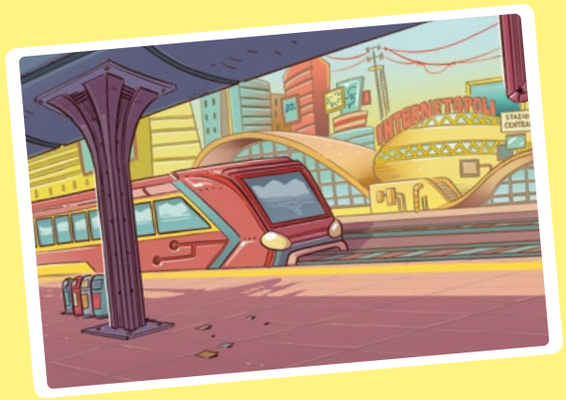
>> IN CLASSE <<
Partendo dal dialogo, date alla classe la definizione di "cybersecurity" e "malware" riprendendole dalla **Nabbopedia** (si veda pag. 11). In particolare, nel dialogo si parla anche di **spyware**, un malware in grado di registrare l'attività di un utente/vittima su un particolare dispositivo digitale. Può anche essere l'aggancio per presentare l'approfondimento sui malware, che trovate alla fine di questo capitolo.

~ PROPOSTA ATTIVITÀ ~
Proiettate o fate recitare la tavola n. 7 delle **Tavole Cyber Quiz**, che trovate su www.ludotecaregistro.it/per-le-scuole/cybersecurity. Quindi, fate scegliere alla classe - per alzata di mano - il comportamento da tenere.

*** PER APPROFONDIRE ***
Guardate insieme alla classe un video sul perché occorre non abbassare mai la guardia quando si tratta di **cybersicurezza**: https://bit.ly/3qvCFZy e https://bit.ly/3TVl6yA.

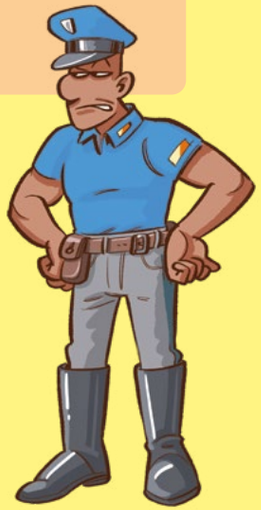


Alla **Stazione centrale** Nabbo incontra un poliziotto esperto in reati informatici che gli parla di alcune mail sospette: sono i tentativi di truffa effettuati tramite la tecnica del phishing.



>> IN CLASSE <<
Partendo dal dialogo, spiegate ai ragazzi e alle ragazze cosa significa "**phishing**" (ne trovate una definizione e una descrizione a pag. 23). Approfondite il tema, soffermandovi sull'importanza delle frasi che cercano di convincere l'utente a fare qualcosa, come: "clicca qui", "inserisci la password", "registrati". Potete fare riferimento anche a "**Non aprite quella posta!**", che trovate nella sezione di "**Attenti ai pericoli!**" (si veda pag. 29).

~ PROPOSTA ATTIVITÀ ~
Dividete la classe in gruppi e chiedete a ciascun gruppo di provare a scrivere una **mail di phishing** su un foglio di carta. Poi ogni gruppo lo passa a un altro, che a sua volta cerca di individuare le ingenuità che possono insospettire chi la riceve. A conclusione dell'attività ogni gruppo legge la mail dell'altro gruppo ed espone gli indizi che a suo parere smascherano il tentativo.



*** PER APPROFONDIRE ***
Guardate insieme il video per approfondire il tema dello **spamming** sul sito della Ludoteca di Registro .it: https://bit.ly/3B38b6d.

Alla **gelateria di Freddy**, il gelataio chiede a Nabbo che cos'è un "trojan horse" promettendogli in cambio un gelato gratuito.

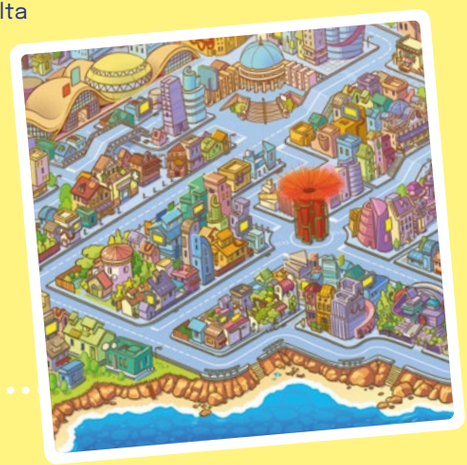
>> IN CLASSE <<
Raccontate o fate raccontare da un alunno la leggenda dello stratagemma di Ulisse a Troia, che dà il nome a un particolare **malware**, il **trojan horse**. Ragionate sul concetto di vulnerabilità, di accettare regali da sconosciuti, di promesse ingannevoli. Riflettete poi su quali siano i link su cui non cliccare. È possibile fare riferimento a "**Navigare in sicurezza**" nella sezione di "**Attenti ai pericoli!**" (si veda pag. 30). Fate riferimento anche al minigame **Whack a worm** in cui questo tipo di malware è rappresentato in forma di vermi infestanti i giardini degli abitanti di Internetopoli.

~ PROPOSTA ATTIVITÀ ~
Proiettate o fate recitare la tavola n. 8 delle **Tavole Cyber Quiz**, che trovate su www.ludotecaregistro.it/per-le-scuole/cybersecurity. Quindi, fate votare per alzata di mano il comportamento.

*** PER APPROFONDIRE ***
Qual è la differenza tra **virus**, **malware** e **spyware**? Guardiamo insieme un video su: https://bit.ly/3L2myfR.

Approfondimento: malware e principali attacchi informatici

I **virus** informatici sono programmi dannosi che si comportano proprio come i virus biologici: infettano computer e smartphone e si riproducono al suo interno, intaccando programmi e dati nonché predisponendosi a passare sulle altre macchine con cui vengono in contatto. Oggi ci sono molti più tipi di software malevolo e si preferisce il termine generico **malware**. Vengono realizzati appositamente per danneggiare computer, smartphone e, in generale, dispositivi collegati alla Rete, nonché i loro utenti, a scopo di lucro o di interruzione dei servizi. Per teppismo, per bravata o per motivi ideologici: c'è ad esempio chi ha sabotato le librerie di software **open**, cioè a disposizione gratuita, perché voleva danneggiare le aziende che le usano per creare software finalizzati al profitto.
I **worm** sono malware che, riproducendosi, danneggiano i dati riuscendo anche a cancellarli. I **trojan**, dal nome del celebre cavallo di Troia, sono malware che una volta entrati nei sistemi informatici consentono agli attaccanti di installare altri programmi o rubare dati. Gli **spyware** consentono di spiare le attività dell'utente, per seguirne il comportamento e impossessarsi di dati personali, come ad esempio password e dati bancari. Gli **adware** sono malware che attivano fastidiosi messaggi pubblicitari che difficilmente possono essere disattivati. I **ransomware** sono una categoria di malware oggi molto diffusa e di cui si è sentito molto parlare a seguito di casi eclatanti che hanno riguardato importanti organizzazioni pubbliche e private. Sono in grado di bloccare file (criptandoli, rendendoli cioè illeggibili) o interi sistemi informatici: a quel punto, chi li ha creati esige il pagamento di un riscatto in cambio dello sblocco. Il riscatto (in inglesse *ransom*) è richiesto in **criptovalute**, come i Bitcoin, che consentono di mantenere l'anonimato di chi le utilizza. Non sempre, però, al pagamento segue lo sblocco dei dati: a volte i malintenzionati spariscono senza effettuarlo o rinnovano le richieste o richiedono un ulteriore riscatto per non diffondere i dati rubati.



Nabbopedia

Questa **attività a squadre** può essere ripetuta alla fine di ogni capitolo, possibilmente scegliendo le parole che i ragazzi e le ragazze hanno trovato, riferite ai personaggi incontrati e ai luoghi visitati.
Dividete gli alunni in squadre e leggete le **definizioni** riportate qui sotto. Tutta la classe cerca di indovinare il termine a cui la definizione si riferisce. Nessuno può fare più di un tentativo per la stessa definizione. Ogni termine indovinato vale 1 punto, vince la squadra che fa più punti. In caso di pareggio, potete leggere un'ulteriore definizione. Se volete giocare con più definizioni, cercatele nel gioco.

Virus: termine generico per indicare un malware che, installato inconsapevolmente dall'utente, cerca di diffondersi su altri dispositivi. Spesso dannoso per il sistema.

Malware: programma in grado di apportare danni a un sistema informatico, in genere mascherato da programma innocuo, documento o messaggio.

Adware: un tipo di malware che ci bombarda di pubblicità non richieste. Spesso viene installato inconsapevolmente insieme a programmi gratuiti.

Spyware: un tipo di malware che raccoglie informazioni su di noi e le trasmette ai loschi figuri che lo hanno diffuso, in genere a scopo pubblicitario ma non solo…

Trojan horse: malware travestito da programma innocuo, che permette a un utente esterno di manovrare i nostri dispositivi. Entra nel nostro computer proprio come il cavallo di Troia.

Bug: errore di funzionamento di un programma o di un dispositivo elettronico.

Hacker: operatore molto esperto in uno o più programmi. Spesso viene usato impropriamente per definire un cracker, cioè uno che viola sistemi informatici.

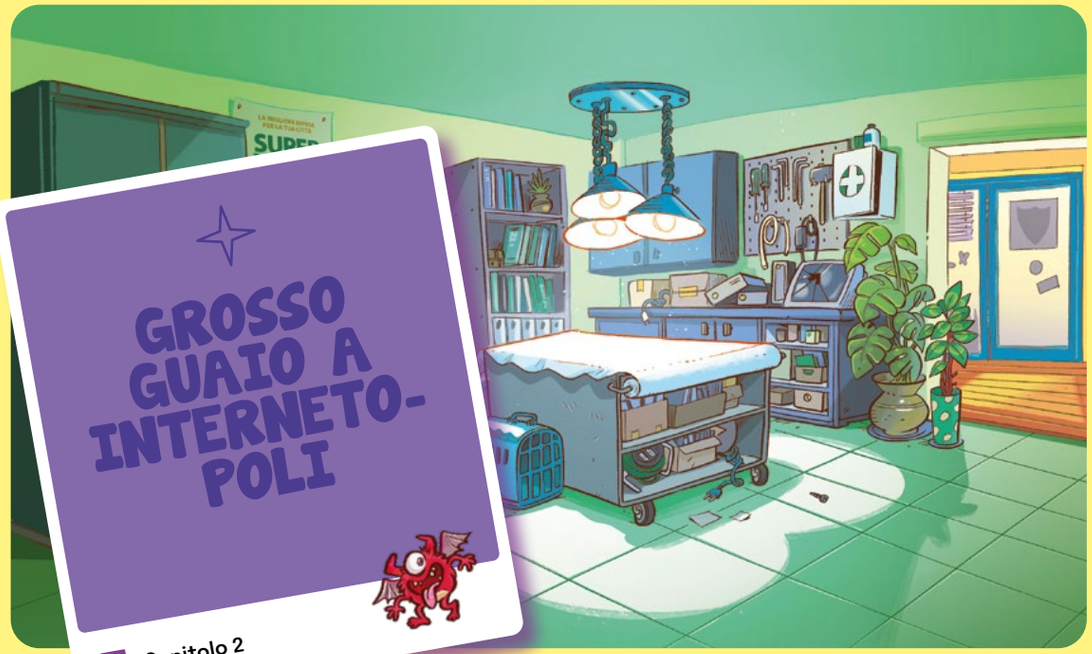
Cybersecurity: è una parte della sicurezza informatica, che dipende solo dalla robustezza e resilienza della tecnologia (e non dai nostri comportamenti).

Cybercrime: attività criminale compiuta attraverso mezzi informatici.

Dati sensibili: dati personali riguardanti caratteristiche intime dell'individuo come l'origine etnica, le convinzioni religiose o politiche, lo stato di salute ma anche pin e password.

Username: nome con il quale possiamo entrare in un sito, in un servizio di posta elettronica, in un computer… collegato a una password che conosciamo solo noi.

Password: parola d'ordine supersegreta che, associata al nostro nome utente o nickname, permette a un sistema informatico di identificarci e consentirci l'accesso.



Riassunto del capitolo

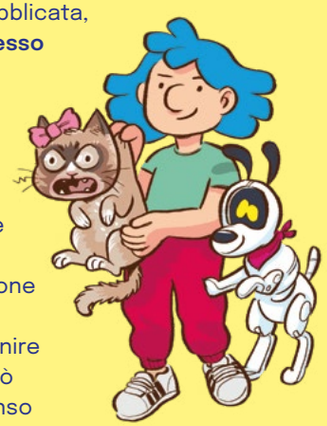
Dopo che Nabbovaldo ha incautamente aperto il pacco destinato a Linda, la casa di quest'ultima è bloccata da un enorme **lucchetto**. Aggirandosi per la città si scopre però che non è la sola: anche le **case di Kitty Kathy e di Mr. D** sono sigillate allo stesso modo. Risolvendo il minigioco nella piazza principale, il giocatore scopre che l'attacco alla casa di Linda è opera di un **ricattatore anonimo** che chiede un pagamento di 50.000 like per togliere il blocco. Nabbovaldo si rivolge allora a diversi esperti che potrebbero dargli una mano: il **dottor Kappersky (detto dottor K)**, la **polizia**, **Super Virus Blocker**. Ma ogni volta scopre che l'interpellato non sembra in grado di aiutarlo. Una volta che Nabbovaldo ha parlato inutilmente con tutti e tre, gli giunge la notizia che Linda sta tornando in città. Nabbovaldo decide di andarla a prendere alla stazione e di spiegarle quello che è successo.
Intanto, il giocatore potrebbe anche attivare una **sottotrama** della vicenda, non necessaria alla soluzione del caso ma che offre un punteggio aggiuntivo. Questa sottotrama tocca alcuni temi legati al mondo dei **social network**. All'interno del Social Club può scoprire che **Hypsta Holly** è perseguitata da una follower: **Bimba**. Si tratta di un vero e proprio caso di **stalking**, che il giocatore può sventare parlando con Bimba e convincendola a comportarsi meglio. Allo stesso modo, ai **Giardini Wi-Fi** può insegnare ad **Ada** a usare in modo più rispettoso le foto dei minori che scatta, nel Casinò a **Pop Polly** può suggerire di ignorare le catene di mail.

I personaggi

Gli **Uomini in nero** lavorano nel settore della sicurezza e bloccano l'accesso di Nabbovaldo ad alcuni luoghi di Internetopoli: il Social Club e il Casinò. Nel gioco gli chiedono di tornare quando avrà abbastanza like da essere famoso, ma in realtà sono la metafora dei meccanismi di autenticazione che su Internet permettono di accedere a siti e risorse solo se si è autorizzati. Lo strumento più tipico per ottenerlo è il login con un nome utente, o **username**, e una **password**: ne parliamo nell'approfondimento di questo capitolo. Siti bancari, di servizi pubblici e altri ancora possono richiedere sistemi ancor più sofisticati, con ulteriori passaggi o con procedure dedicate come lo SPID. Sistemi alternativi di riconoscimento sono quelli biometrici, con il riconoscimento del volto o delle impronte digitali.

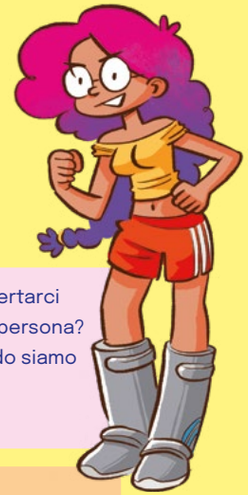
>> IN CLASSE <<
Potete far raccontare ai ragazzi e alle ragazze le loro esperienze con il meccanismo di **autenticazione**. Qualcuno si è mai registrato a un sito? È risultato facile o difficile? Si è fatto aiutare? È mai successo a qualcuno di perdere la password? Come ha risolto?

Ada è la cugina di Nabbovaldo appassionata di fotografia, venuta a Internetopoli per studiare. Abita da lui, che le ha regalato il PC-cane Hub. Durante l'avventura la incontriamo più volte, e in un paio di casi pone dei dubbi sull'**opportunità di pubblicare** le foto che ha scattato: una volta si tratta di un minore, un'altra del titolare dell'autoscuola signor Guido che ha avuto un incidente. In realtà per pubblicare una foto, così come per taggare qualcuno su una foto pubblicata, occorre sempre **il permesso della persona ritratta**, che può anche ritirarlo in seguito. Non è sufficiente il consenso generico dato a parole a farsi fotografare: serve proprio un consenso specifico alla pubblicazione di quella foto, che per **i minori di 14 anni** deve venire da genitori o tutori. Si può pubblicare senza consenso esplicito la foto di chi ha partecipato a eventi pubblici, ma comunque **mai se danneggia** l'immagine e la reputazione di chi vi è ritratto.



>> IN CLASSE <<
Chiedete ai ragazzi e alle ragazze se è mai capitato che qualcuno abbia scattato loro delle **foto** che non vorrebbero far vedere in giro, di quando erano piccoli o di adesso. E se ci sono foto pubblicate che, anche se ora mostrano senza problemi, potrebbero diventare inopportune in futuro.

Gli ambienti



Il **Social Club** è finalmente accessibile a Nabbovaldo perché lui è ormai considerato abbastanza noto. Ma possiamo essere sicuri dell'identità di chi incontriamo in Rete?

>> IN CLASSE <<
Fate riflettere su quali siano gli elementi che ci permettono di **identificare** le persone per riconoscerle. La faccia, il modo di muoversi, il tono della voce? E cos'altro? E in Rete, quante di queste cose sono utilizzabili? Come possiamo fare quindi per accertarci dell'identità di una persona? Cosa cambia quando siamo online?

~ PROPOSTA ATTIVITÀ ~
Per far capire che in Rete potremmo anche trovarci davanti a **persone inesistenti**, facciamo il gioco "Identità nascosta", che trovate sul sito della Ludoteca del Registro .it: https://bit.ly/3Rz6mF2.

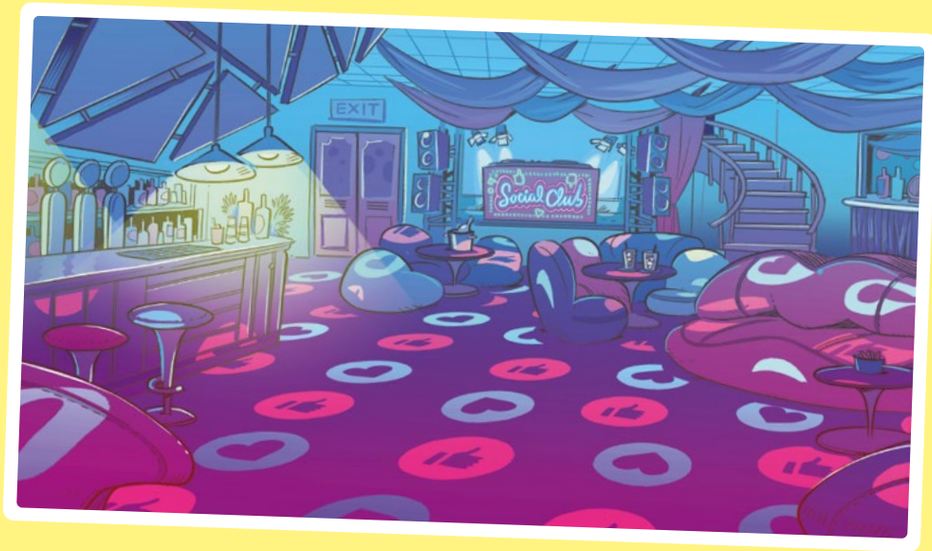
❋ PER APPROFONDIRE ❋
In questo video si parla della **biometria** e delle sue potenzialità per integrare l'identificazione sicura degli utenti; guardatelo insieme sul sito della Ludoteca del Registro .it: https://bit.ly/3RyoM8Z.

La **casa di Linda** è bloccata da un enorme lucchetto: si tratta del **ransomware**, un software che blocca i dispositivi e dunque i dati dell'utente che, per riavere l'accesso, è costretto a pagare un riscatto ai malintenzionati che lo hanno predisposto. Nel gioco, l'ignoto ricattatore chiede di essere pagato in like; nella realtà l'attaccante chiede alla vittima una somma in **criptovalute**, in modo che il pagamento non possa essere tracciato. Linda e Nabbovaldo sospettano di varie persone, ma non sono in grado di riconoscere con certezza il ricattatore.

>> IN CLASSE <<
Introducete il concetto di "backup", la copia dei nostri dati. Riflettiamo su quante volte **una copia** di qualcosa può salvarci dai problemi. Per esempio, se perdete le chiavi di casa o del motorino e non ne avevate una copia siete nei guai, ma se avete messo da parte un esemplare ne potete fare anche altre. Così se vi copiate da qualche parte numeri di telefono e indirizzi, o altri dati per voi importanti. Da qui passate a parlare dei **backup** di computer e cellulari: gli alunni li fanno spesso? È proprio grazie al backup della casa che Mr. D, il vicino di Nabbovaldo, risolve il problema del ransomware.

~ PROPOSTA ATTIVITÀ ~
Questo video introduce alle buone pratiche di **cybersecurity**: https://bit.ly/3eryUSg.

❋ PER APPROFONDIRE ❋
Per comprendere cosa siano le **criptovalute**, potete guadare insieme il video sul sito della Ludoteca del Registro .it: https://bit.ly/3eFOuK0.



La fabbrica dei meme è protetta da un firewall, dei sistemi hardware e software dedicati ad analizzare i dati e le richieste che arrivano su una Rete aziendale o privata in modo da rilevare e bloccare quelli sospetti. In pratica il firewall è una barriera che protegge da alcuni tipi di attacchi dall'esterno.

>> IN CLASSE <<
Difficilmente i ragazzi e le ragazze conoscono i **firewall** e quindi altrettanto difficilmente li installano sui loro dispositivi, ma ci sono altri modi per **proteggere computer** e altri tipi di dispositivi da molti altri tipi di rischi. Potete chiedere loro se proteggono gli strumenti e come: il loro computer ha un antivirus? Un sistema di controllo parentale? E il telefono è protetto da una password? O dall'impronta digitale? Oppure chiunque può aprirlo?

~ PROPOSTA ATTIVITÀ ~
Proiettate o fate recitare la tavola n. 9 delle **Tavole Cyber Quiz**, che trovate su www.ludotecaregistro.it/per-le-scuole/cybersecurity. Poi fate votare per alzata di mano.

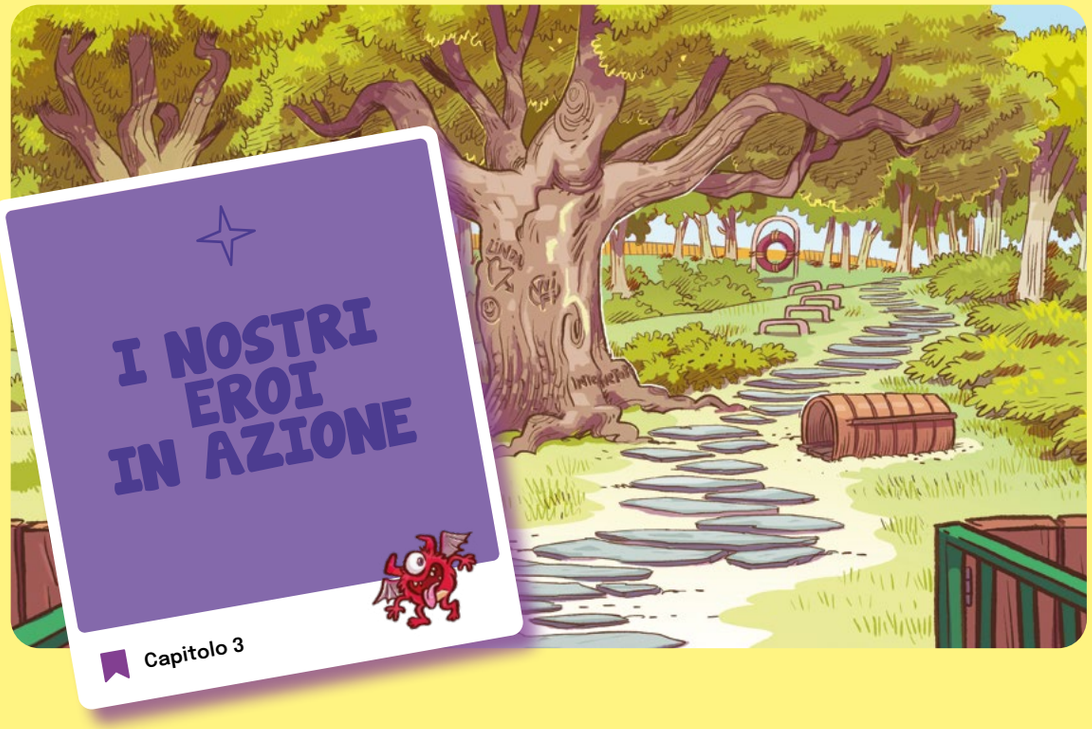
*** PER APPROFONDIRE ***
Le tematiche della **sicurezza** sono qui trattate in un fumetto di Nabbovaldo e in articoli di approfondimento, sul sito della Ludoteca di Registro .it: https://bit.ly/3L4sGUU.

Nabbopedia

Prendendo spunto dall'**attività di pag. 11**, dividete la classe in squadre e leggete alcune definizioni di parole che i ragazzi e le ragazze hanno trovato nel gioco, come ad esempio: stalking, bannare, firewall, white hat, bug, chat, HTML, router e altre ancora. Troverete le definizioni da leggere all'interno del gioco.

Approfondimento: il meccanismo di autenticazione

Per evitare che i malintenzionati si sostituiscano a noi accedendo a informazioni riservate o effettuando operazioni al nostro posto, spesso i siti e i servizi chiedono una registrazione in cui scegliamo un nome utente, o **username**, e una parola d'ordine, o **password**. Il login che ci permette di entrare in quel sito e servizio con le credenziali scelte non è altro che l'attivazione del meccanismo di autenticazione, una delle principali contromisure in sicurezza informatica. È essenziale che le password siano scelte con cura: lunghe, complesse, non di senso compiuto. Lo stesso vale anche per le risposte alle domande di controllo che a volte i siti aggiungono all'identificazione o al recupero della password, per rendere più difficile l'accesso a chi dovesse riuscire a impossessarsi delle chiavi di un utente. Talvolta, come password o domanda di controllo vengono usati **dati personali** come la data di nascita o il codice fiscale. Nel primo caso siamo di fronte a una scelta molto scontata e dunque poco sicura. Nel secondo caso è vero che il codice fiscale ha anche il vantaggio di essere univoco. Attenzione, però: si tratta di informazioni che i malintenzionati possono riuscire a trovare molto facilmente. O anche a calcolare: esistono siti e programmi che consentono di elaborare il codice fiscale di qualcuno se si conosce il nome, il cognome, la data e il luogo di nascita. Tutto questo è anche un motivo in più per **trattare con riservatezza** le informazioni sulla propria persona. La ragione per cui i siti ci chiedono spesso di utilizzare password complicate è per prevenire i tentativi ripetuti di forzatura da parte dei **cybercriminali**. Grazie alla potenza dei computer, gli attaccanti possono cercare di indovinare una password facendolo fare in modo automatico a dei programmi specifici, che fanno tantissimi tentativi al secondo. È questo il cosiddetto attacco di "forza bruta". Per questo è importante che le password scelte dagli utenti **siano lunghe** (minimo 8 caratteri), siano **alfanumeriche** (distinguendo maiuscole e minuscole e aggiungendo caratteri speciali) e **non rimandino a parole di senso compiuto**. Questo aumenta moltissimo la quantità di possibili combinazioni che i cybercriminali devono tentare prima di indovinare quella giusta. Inoltre molti siti chiedono, oltre a username e password, anche di trascrivere una serie di caratteri distorti o di indicare in una fotografia quali riquadri contengono oggetti particolari come ad esempio alberi, semafori, automobili: serve a garantire che chi prova ad accedere sia un **essere umano**, non un programma automatico. E gli esseri umani ci mettono molto di più a effettuare ciascun tentativo, digitando ogni volta la password. Sempre per prevenire questi attacchi, diversi siti **bloccano l'accesso** dopo un certo numero di tentativi falliti: a quel punto occorre aspettare un lasso di tempo o effettuare una procedura di sblocco.

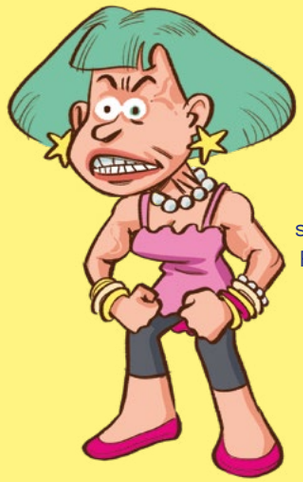


Riassunto del capitolo

Nabbo racconta a **Linda** quello che è successo e i due si confrontano sulla strategia da adottare per risolvere il problema del **ransomware**. Lui le promette che lavorerà a testa bassa per guadagnare tutto ciò che occorre per pagare il riscatto. Linda però non è d'accordo: sostiene che non è corretto cedere al ricatto e incoraggiare così colui che ha diffuso il malware. Secondo lei, invece, occorre impegnarsi indagando sul caso in modo da riuscire a smascherare il colpevole. A suo parere il ricattatore è qualcuno che la conosce bene e vive vicino a lei: sospetta di Franco Forex, Heather Hater, Flint Flamer e Troll. Nabbo concorda con questa linea di azione, ma ricorda che nel frattempo dovrà continuare a fare i suoi lavori perché se fallissero i loro tentativi è intenzionato a pagare il riscatto di tasca propria.
I due si aggirano per la città vedendo che il ransomware ha bloccato diversi edifici. L'unico che è riuscito a liberarsene è **Mr. D**, grazie al fatto che aveva eseguito un **backup** completo della propria casa: ha buttato via tutte le informazioni diventate inaccessibili, e ha utilizzato i dati di backup (cioè la copia della sua casa) per ricostruirla. Alla fine, i due si rendono conto di non essere arrivati ad alcun risultato. Decidono allora di tendere una **trappola al ricattatore**, fingendo di obbedire alle sue indicazioni: mettono una valigetta sotto un albero dei **Giardini Wi-Fi** come se contenesse il riscatto – la valigetta invece è piena della biancheria di Nabbo – e poi si nascondono tra i cespugli pronti a balzare addosso a chi verrà a ritirarla.

I personaggi

Flint Flamer è un provocatore che insulta Nabbovaldo cercando di farlo arrabbiare. I **flame** sono infatti messaggi aggressivi che gli utenti di una comunità online rivolgono a un altro membro o al gruppo. Tra gli altri incontri sgradevoli che si possono fare in Rete ci sono gli **haters** e i **troll**, rappresentati nel gioco appunto da **Heather Hater** e dal ragazzino **Troll**.
I primi sono gli odiatori a tutti i costi, che non sono interessati a una discussione aperta e onesta ma si limitano a criticare senza ascoltare le argomentazioni altrui: con loro il dialogo è inutile.
Peggio ancora i troll, che vogliono solo provocare e creare scompiglio per far deragliare le conversazioni altrui. Parlare con loro è addirittura dannoso: sono in cerca d'attenzione, infatti con loro la strategia migliore è non considerarli e continuare come se non ci fossero. Finiranno per stufarsi e andarsene.

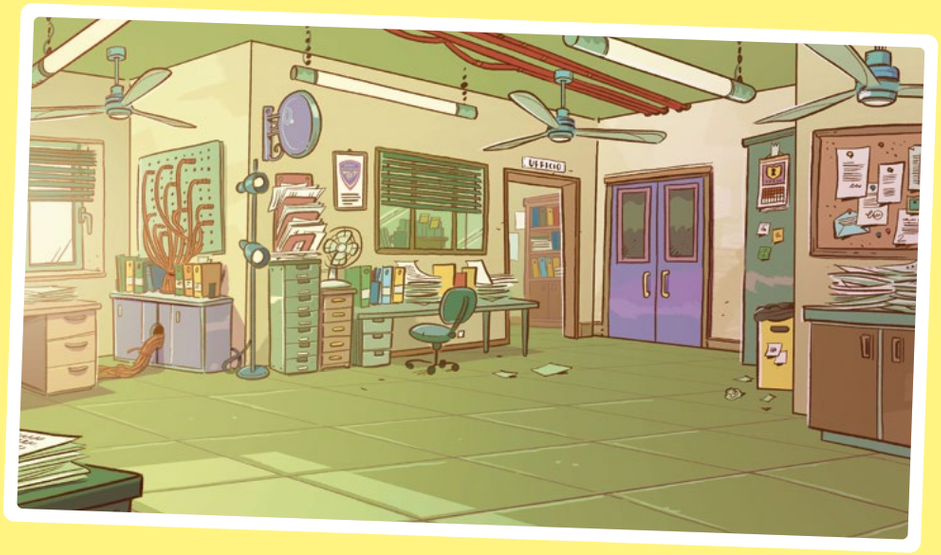


>> IN CLASSE <<
Potete chiedere se qualcuno è stato vittima di **attacchi** e **provocazioni** gratuite o vi ha assistito, in Rete o nella vita reale, per poi parlare di come ha reagito e di come risolvere questi problemi. Fate notare che il fatto di essere sul web non autorizza a calunniare e offendere: i commenti fuori luogo possono portare a denunce e condanne anche qui.

Franco Forex è un approfittatore e un imbroglione. Cerca di convincere Nabbovaldo a investire in titoli online, mentre questa è un'attività riservata a broker autorizzati. Inoltre è un appassionato di **sistemi piramidali**. Come lui, sono tanti i personaggi in Rete che cercano di far soldi sulle spalle degli altri. Per questo occorre la massima attenzione. Pubblicare **informazioni sulla nostra vita privata**, come l'indirizzo e le indicazioni sui nostri spostamenti, è rischioso perché possono essere preziosi per ladri e malintenzionati. **Registrarsi** su siti sconosciuti significa regalare i propri dati personali a chi li gestisce, che li può utilizzare a scopi criminosi o rivendere a terzi. **Imitazioni di siti affidabili** possono addirittura indurci a inserire i nostri dati bancari e delle carte di credito, esponendoci a truffe e raggiri. Così anche **siti di e-commerce falsi** possono indurci a inviare soldi o impossessarsi delle nostre credenziali per poi attingere al nostro conto in banca o alla nostra carta.
Il poliziotto di Internetopoli simboleggia la **Polizia Postale e delle Telecomunicazioni**,

con sedi capillari in tutte le regioni e nella maggior parte delle province. La Polizia Postale previene e persegue ogni **crimine in Rete** e opera anche per tutelare la **privacy degli utenti** contro abusi dei loro dati personali e furti di identità. Il suo campo d'azione spazia quindi dalle truffe online alla lotta contro i **crackers** (i pirati informatici capaci di introdursi illegalmente in reti di computer, server e dispositivi allo scopo di fare danni), dalla prevenzione della pedopornografia a quella del gioco illegale, dalle violazioni di copyright al cyberterrorismo. Il sito www.commissariatodips.it è a disposizione del pubblico per raccogliere segnalazioni e denunce, per informare sulle ultime novità relative alla sicurezza online e per rispondere a richieste di delucidazioni, oltre che per consentire l'invio telematico delle normali denunce di furto e smarrimento.
Analogamente alla Polizia Postale, in Rete opera anche il **Nucleo Speciale Tutela Privacy e Frodi Tecnologiche** della Guardia di Finanza specializzato in truffe, evasione fiscale, diritto d'autore e tutela dei marchi, controllo delle attività finanziarie in Rete di malavita organizzata e terrorismo.

>> IN CLASSE <<
Per parlare insieme di **cyberbullismo** e altri potenziali rischi, guardiamo insieme https://bit.ly/3d51h8l.



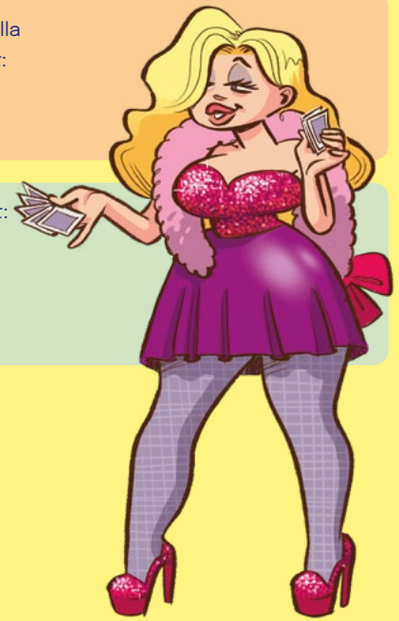
Gli ambienti

Nel **Commissariato**, Nabbovaldo parla con il poliziotto della possibilità che i propri computer e cellulari siano infettati da un virus, nonché del modo in cui è bene reagire se un virus riesce a intrufolarsi.

>> IN CLASSE <<
Domandate agli alunni se hanno avuto qualche esperienza di computer o cellulari **infettati**, e nel caso come hanno risolto la situazione. Poi esaminate le buone pratiche riportate in "Tra hardware e software", che trovate nella sezione finale "Attenti ai pericoli!" (si veda pag. 28).

~ PROPOSTA ATTIVITÀ ~
Giocate a "Indovina l'errore" sul tema dei dati personali, usando le strisce 2, 4, 6 e 7 reperibili sul sito della Ludoteca di Registro .it: https://bit.ly/3L0ubDc.

*** PER APPROFONDIRE ***
Guardate insieme questo video che esamina il problema del **social engineering** sul sito della Ludoteca di Registro .it: https://bit.ly/3TY17jN.

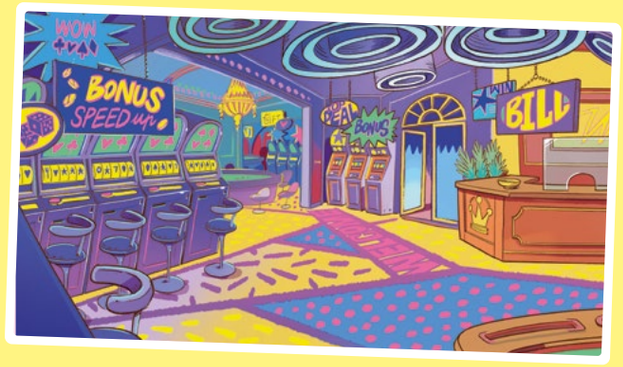


All'interno del **Casinò**, Pop Polly racconta a Nabbovaldo di aver ricevuto una mail con l'annuncio di una grande vincita a una lotteria, a cui però lei non ha mai partecipato! Secondo il messaggio, deve solo rispondere inviando un modulo con tutti i dati personali.

>> IN CLASSE <<
Quello subito da Polly è un tentativo di **phishing**: chiedete alla classe la definizione. Potete anche chiedere da dove viene il nome: si legge infatti *fishing*, proprio come pescare: i criminali lanciano la lenza e sperano così che qualcuno abbocchi (per approfondire, si veda pag 23). Più in generale il problema è il **social engineering**: gli anonimi malintenzionati non cercano di rubare i dati di Polly, ma di convincere lei stessa a mandarli: discutete prendendo spunto dall'approfondimento che trovate nella pagina accanto. I dati possono essere usati per forzare accessi e anche per il furto d'identità, cioè per agire in Rete spacciandosi per la vittima.

~ PROPOSTA ATTIVITÀ ~
Giocate a "**Indovina l'errore**" sul tema dei dati personali, usando le strisce 2, 4, 6 e 7 reperibili sul sito della Ludoteca di Registro.it: https://bit.ly/3eD539r.

*** PER APPROFONDIRE ***
Guardate insieme questo video che esamina il problema del **social engineering** sul sito della Ludoteca di Registro .it: https://bit.ly/3RvPsHx.

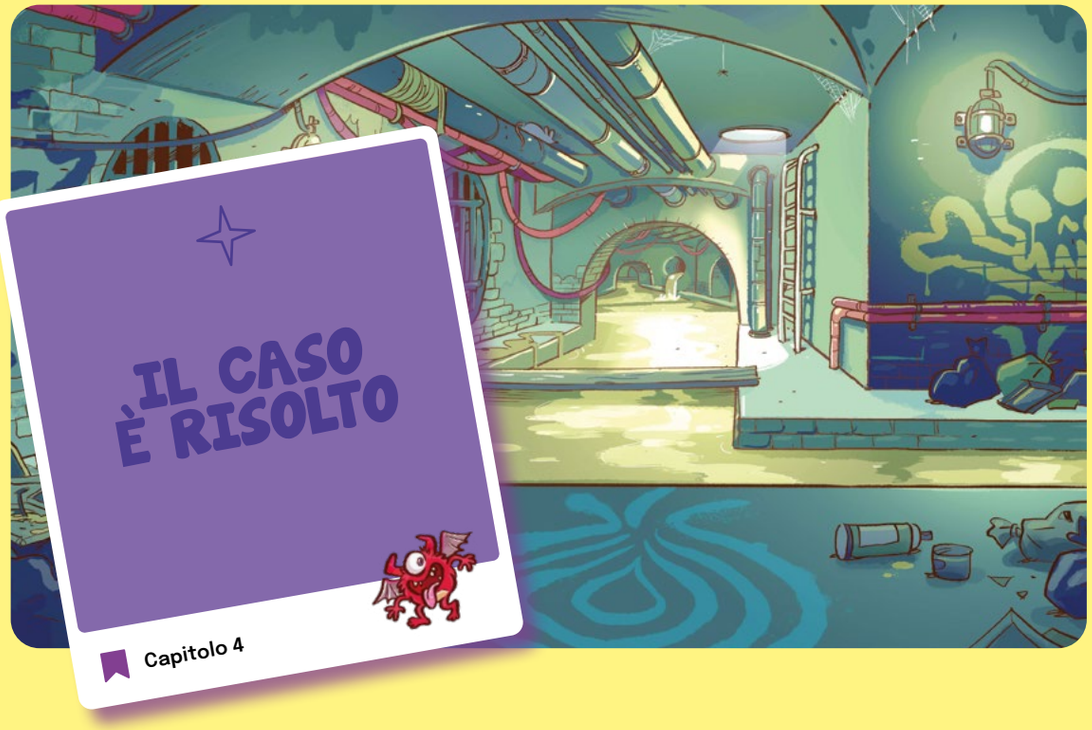


Nabbopedia

Prendendo spunto dall'**attività di pag. 11**, dividete la classe in squadre e leggete alcune definizioni di parole che i ragazzi e le ragazze hanno trovato nel gioco, come ad esempio: file, PIN, bot, spyware, hotspot, ipertesto, defrag e altre ancora. Troverete le definizioni da leggere all'interno del gioco.

Approfondimento: la difesa dai virus e dall'ingegneria sociale

Reti e computer sono difesi da **antivirus** e **firewall**: questi ultimi sono filtri che proteggono una Rete locale da intrusioni non autorizzate e dall'invio di contenuti pericolosi. Anche questi sistemi di protezione possono avere falle e debolezze ma il punto più debole di tutti può essere l'**utente**, che in un momento di leggerezza o di distrazione può vanificare ogni difesa, magari aiutando lui stesso gli aggressori. Tra le tecniche più insidiose dei **cybercriminali** vi sono quindi quelle di **social engineering**, o **ingegneria sociale**, con cui si cerca di ingannare le persone per convincerle a fornire i dati che i malintenzionati vogliono ottenere, a installare i malware, a inviare il proprio denaro e così via.
Le diverse tattiche hanno nomi differenti a seconda delle modalità. Si parla ad esempio di **baiting** quando si adescano le persone facendo leva sulla loro curiosità, abbandonando un dispositivo come una chiavetta USB in un posto dove si conta che venga ritrovato. Spesso la chiavetta è contrassegnata con marchi noti, o comunque familiari alla vittima predestinata in modo che sembri affidabile. Device abbandonati presso un'azienda, con etichette e diciture che incuriosiscono, come ad esempio "licenziamenti" o "buste paga", possono fare ulteriormente leva sulla curiosità di chi le trova. Chiavette o device abbandonati, una volta che sono stati collegati al proprio computer (per studiarne il contenuto o anche solo per individuarne il proprietario con la buona intenzione di restituirle) provvedono immediatamente a infestarlo con qualche malware.
Il **phishing** è una delle tecniche di social engineering più diffuse: si cerca di spingere l'utente a inviare o immettere i propri dati in un form attraverso mail ingannevoli. È il tipo più pericoloso di **spamming**, messaggi mail indesiderati che spesso costituiscono semplicemente pubblicità non voluta ma che possono celare insidie assai più pericolose. Queste mail sono studiate per sembrare messaggi di conoscenti o di entità autorevoli: una banca, le Poste, corrieri, grandi aziende di e-commerce, fornitori di servizi come elettricità e gas. I contenuti spesso fanno riferimento a **premi**, **guadagni e sconti**, magari sostenendo che è rimasto poco tempo per ottenerli, oppure a una falsa **urgenza**: un conto bloccato, un pacco che rischia di essere mandato indietro, un account che scade. In altri casi nel messaggio è richiesto di digitare le credenziali di accesso a un sito o i dati della carta di credito, oppure ci si può trovare inconsapevolmente ad accedere a un sito malevolo o a scaricare un allegato che nasconde malware.
Esistono anche tecniche di phishing con chiamate telefoniche (anche automatiche) o semplici sms denominate rispettivamente **vishing** e **smishing.** Le modalità degli attacchi si moltiplicano e con essi le etichette, ma la sostanza rimane sempre la stessa: i cybercriminali cercano di spacciarsi per aziende rispettabili, tentando di far cliccare link verso pagine infette o di farsi cedere dati preziosi.



Riassunto del capitolo

Nabbo e **Linda** sono in agguato nei **Giardini Wi-Fi** quando vengono attaccati da uno stormo di **Adware**. Si danno da fare per sconfiggerli, ma poi si rendono conto che qualcuno ne ha approfittato: la valigetta sotto l'albero è aperta e abbandonata con tutta la biancheria di Nabbo. Il ricattatore ha scoperto il trucco. Nei giardinetti c'è però anche **Ada** con il suo **cane-PC Hub**, che è riuscito a percepire l'odore del ricattatore in fuga. Da quel momento è lui a guidare Nabbo e Linda sulle tracce del colpevole. Dopo varie peripezie, il cane li conduce all'interno del **Dark Web** dove il gruppetto scopre un passaggio segreto. Seguendolo, si ritrova all'interno della casa di **Kitty Kathy** che quindi non è inaccessibile per il ransomware come sembrava. Nella scena che segue si scopre che Kitty Kathy è in realtà un robot, controllato da **Rosilda** e dagli altri gatti che si danno alla fuga mentre il robot attacca Nabbo e Linda, ma viene messo fuori uso mandandolo in cortocircuito con l'acqua di un vaso da fiori. Ada cattura Rosilda, costringendola a restare inerme. Rosilda non può far altro che rivelare i codici di sblocco del ransomware e Internetopoli è salva.

I personaggi

Carla Cospira crede a qualunque bufala e **fake news** presente in Rete. I cosiddetti "cospiratori" credono alle teorie del complotto, convinti che alcuni eventi e situazioni siano manipolati in segreto da "poteri forti". Nelle teorie del complotto l'insieme di dati e notizie veri è confuso con falsità, qualsiasi "prova" si adatta così alla tesi della teoria rendendo difficile confutarla, perché chiunque ci provi è visto come parte della cospirazione.

>> IN CLASSE <<
Potete chiedere se i ragazzi e le ragazze hanno mai trovato in Rete **notizie strane e quasi incredibili**. Prendono tutto per vero o verificano? Hanno mai provato a confrontare le fonti per imparare a capire quali sono le più affidabili? Si sono mai rivolti a qualcuno per un suggerimento, ad esempio a un adulto affidabile? Alla stampa? Alle enciclopedie?

Gli ambienti

Nei **Giardini Wi-Fi** uno stormo di adware assale Nabbo e Linda che sono costretti a difendersi.

~ PROPOSTA ATTIVITÀ ~
Proiettate o fate recitare la tavola n. 10 delle **Tavole Cyber Quiz**, che trovate su www.ludotecaregistro.it/per-le-scuole/cybersecurity. Fate scegliere alla classe il comportamento da tenere per alzata di mano.

*** PER APPROFONDIRE ***
Il problema del **vero** e del **falso** in Rete riguarda pubblicità e le notizie, si veda a tal proposito www.ludotecaregistro.it/2021/06/21/le-fake-news.

Hypsta Holly è un'**influencer** e ha un grande seguito, ma ha anche un problema con una stalker che la perseguita ovunque vada. Anche le persone pubbliche hanno diritto alla loro privacy: interferire con essa non è solo maleducazione, ma può sconfinare nel reato. In Rete tutti sembrano a portata di mano, ma non bisogna approfittarne.

>> IN CLASSE <<
Parlate di comportamenti corretti e **netiquette** con l'approfondimento "Saper stare al mondo e sul Web", che trovate nella sezione "Attenti ai pericoli!" (si veda pag. 32).

>> IN CLASSE <<
Gli **adware** che bombardano di pubblicità sono un problema. Fate riflettere i ragazzi e le ragazze sul concetto di **gratuità in Rete**. Da cosa guadagnano i curatori di siti e di software gratuiti? Se non ci sono altre entrate, è la **pubblicità** a pagare. Noi vediamo spot, pagando con il nostro tempo o con quello necessario a caricare banner e inserzioni, con il rischio di cliccare per sbaglio su qualche banner di pubblicità ingannevole e attivare servizi a pagamento.

Il **Dark Web** di Internetopoli, come quello vero, è un posto oscuro dove si commercia di tutto in totale anonimato: medicine e sostanze illegali, armi, segreti industriali. In realtà occorre distinguere tra dark web e deep web. Il **deep web** è una grande parte del web che si stima contenga tra il 90 e il 99% dei contenuti presenti in Rete, non indicizzata dai motori di ricerca, per cui non la troveremo mai tramite Google. In questa parte del web però non è tutto illegale, qui si trovano contenuti privati accessibili solo su login, pagine dinamiche create ogni volta sul momento, pagine non collegate ad altre, contenuti non testuali, siti troppo recenti e quindi non ancora indicizzati. Ad esempio nel deep web possiamo trovare una casella di posta, il nostro account di online banking, ed è bene che siano nascosti, se chiunque potesse trovarli i nostri dati non sarebbero certamente al sicuro. Il deep web non va quindi confuso con il dark web, che ne è una piccola parte ed è formato da pagine accessibili attraverso appositi software come Tor, creato apposta per garantire l'anonimato. È nel dark web che prosperano gli **aspetti più illegali**: dal traffico di documenti, armi e droghe alla pedopornografia, dal terrorismo al commercio di dati riservati rubati nei siti.

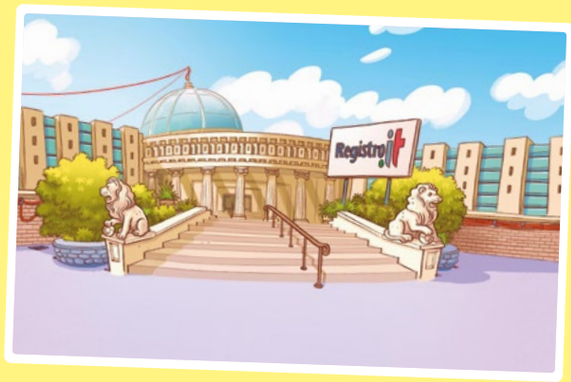
>> IN CLASSE <<
Nella metafora del gioco, il **Dark Web** è la fogna di Internetopoli. Sotterranea, oscura, puzzolente, fuori dalla vista dei cittadini. Provate a censire con i ragazzi e le ragazze le altre metafore del gioco: il Social Club per i social, i casinò per i siti di gioco, la piazza principale con i cavi per i collegamenti della Rete, i worms rappresentati come vermi e i meme come oggetti fabbricati in serie. È l'occasione per una carrellata sui vari argomenti trattati nell'avventura.

~ PROPOSTA ATTIVITÀ ~
Riflettendo sul fatto che i **dati personali** sono un bene prezioso, tanto da costituire un pagamento per beni o servizi, e possono essere rivenduti ad aziende senza scrupoli, utilizzate la tavola n. 2 delle **Tavole Cyber Quiz** che trovate su: www.ludotecaregistro.it/per-le-scuole/cybersecurity. Poi fate votare le possibili risposte per alzata di mano.

*** PER APPROFONDIRE ***
Per capire la distinzione tra "buoni" e "cattivi" nel mondo di quelli che sono chiamati genericamente **hacker**, è disponibile il video "Hacking Etico" su https://bit.ly/3Qu8zR2. Potete inoltre guardare il novo video di WdW sul **dark web** che trovate su https://bit.ly/3L3mnkd.

Approfondimento: la verifica delle fonti

La grande forza del web è che tutti possono pubblicare i propri contenuti: l'enorme ipertesto che ne risulta è di una ricchezza e varietà mai viste prima.
È una vera **rivoluzione culturale**: una occasione incredibile di condivisione, crescita e democrazia. Al tempo stesso, però, questa totale apertura ai contributi di chiunque può creare non pochi problemi e può **esporre a pericoli**.
Innanzitutto, c'è il tema dell'**attendibilità** delle notizie trovate. In buona o in mala fede nei blog o sui social possono essere caricate informazioni scorrette che, prese come vere dagli utenti, possono indurre a comportamenti errati mettendone a repentaglio la tranquillità, la salute e la sicurezza. Informazioni tendenziose, scherzi presi sul serio e fake news di ogni genere possono infatti influenzare le scelte individuali, anche politiche, e aprire la porta a truffe o campagne d'odio. Per questo è sempre importante verificare la fonte da cui proviene una notizia, dando così maggiore credibilità ai canali istituzionali e ai giornali; parallelamente una notizia di cui sono sconosciuti l'autore e/o la data, o che riporta errori grammaticali, può essere di dubbia provenienza e quindi non credibile.



Nabbopedia

Prendendo spunto dall'**attività di pag. 11**, dividete la classe in squadre e leggete alcune definizioni di parole che i ragazzi e le ragazze hanno trovato nel gioco, come ad esempio: phishing, cracker, freeware, nome a dominio, ram, debugging e altre ancora. Troverete le definizioni da leggere all'interno del gioco.

ATTENTI AI PERICOLI!

In questa ultima sezione riportiamo una serie di **consigli** e **buone pratiche** per evitare problemi e utilizzare in maniera sicura computer e telefonini, anche quando si naviga in Rete. Chiudono il tutto alcuni consigli di netiquette, il buon comportamento di chi naviga e frequenta i social.
A ogni sezione premettiamo la citazione di alcune **situazioni del gioco** che potrebbero suscitare la curiosità sui temi che vengono proposti e a cui si può agganciare la spiegazione delle buone pratiche nella discussione in classe.

Tra hardware e software

L'**installazione dell'hardware** viene chiesta da Bimba nel primo capitolo del gioco, da Forex nel secondo, da Mr. D e dall'uomo in nero nel terzo. Alcune buone pratiche aiutano a evitare problemi con l'hardware: tra queste, fare **backup** frequenti, tanto che anche nel videogioco Mr. D riesce a evitare le conseguenze del ransomware perché ne ha a disposizione uno aggiornato di tutta la propria casa! Software e sistemi operativi vanno tenuti sempre aggiornati e vanno tenute aggiornate anche le copie di sicurezza dei dati.

- Non lasciate mai cellulari, tablet e computer portatili **incustoditi**. In ogni caso, potete attivare **sistemi di localizzazione** che vi aiuteranno a trovarli se verranno smarriti o rubati.
- Usate **password d'accesso** ai vostri dispositivi e utilizzate il sistema di blocco dei vostri dispositivi quando non li state usando. Se qualche malintenzionato dovesse metterci le mani sopra, non potrebbe accedere ai vostri dati.
- Le **chiavette USB** sono comode per trasportare dati, ma non fidatevi di quelle di dubbia provenienza. A volte vengono abbandonate apposta per farle trovare: chi le collega al proprio device per vedere cosa contengono installa senza accorgersene pericolosi malware. Lo stesso può accadere con hard disk, cellulari e altri dispositivi.
- Aggiornate spesso i sistemi operativi. Può essere fastidioso dover aspettare i tempi di un **aggiornamento** e abituarsi a nuove modalità di utilizzo, ma le nuove versioni pongono rimedio a errori precedenti e tappano le falle di sicurezza. È importante installare anche le **patch**, piccoli aggiornamenti fra una versione principale e l'altra, meno impegnativi da installare.
- Fate frequenti **backup** dei vostri dati. In caso di guasti, smarrimenti, furti o attacchi ransomware, avere una copia recente dei vostri dati vi consente di evitare brutte conseguenze e di ricominciare come se niente fosse.
- Software e programmi sono coperti da brevetti e **diritto d'autore**. Evitate di scaricare e utilizzare programmi e file pirata. Oltre a essere illegali, c'è il forte rischio che nascondano pericolosi malware.

Non aprite quella posta!

Il poliziotto alla stazione nel primo capitolo del gioco cita i pericoli che possono arrivare con la **posta elettronica**; se ne riparla anche nel commissariato di Internetopoli.
Evitate leggerezze con i messaggi: spesso non vengono da chi sembra. Inoltre, attenzione all'**ingegneria sociale**. Nel gioco, Franco Forex è un truffatore di piccolo cabotaggio, ma almeno ci mette la faccia! Su Internet c'è chi invece si spaccia per altri: come gli autori della mail ricevuta da Pop Polly nel terzo capitolo, che si fingono organizzatori di una lotteria di cui lei avrebbe vinto un grosso premio. O chi ha creato il sito che chiede a Hypsta Holly di installare un'app di ottimizzazione delle prestazioni sul cellulare prima di scaricare un catalogo di moda. Calma e sangue freddo possono aiutare a sventare questi tentativi di attacco.

- Cercate sempre di capire se messaggi e comunicazioni che vi spingono ad agire vengono davvero da quel **mittente**. Per verificare se un mittente appartiene davvero a un'organizzazione o a un'azienda, valutate il dominio di secondo livello del suo indirizzo (ad esempio nell'indirizzo internet del Registro che è registro.it, registro è il dominio di secondo livello): a volte è solo molto simile a quello originale, magari cambia solo una lettera, ma è quella piccola diversità a fare la differenza.
- La presenza di **errori** di ortografia e sintassi in messaggi apparentemente provenienti da banche, enti, grandi aziende è spesso un indizio della loro falsità.
- Non cliccate su **link** oppure posizionate il cursore del mouse sull'indirizzo, senza cliccare, per verificare se l'indirizzo è veramente quello che vi aspettereste.
- Attenzione agli **allegati eseguibili**, cioè ai programmi: se vengono da mail sospette, non scaricateli. Possono contenere virus.
- Allo stesso modo, attenzione a **file di testo**, fogli di calcolo e simili che possono contenere istruzioni macro. Anche quelle sono eseguibili e possono contenere virus. Così pure i file protetti da password.
- Diffidate da messaggi che fanno leva sull'**urgenza**: per sventare un pericolo, per riscuotere una somma o un premio, per sbloccare una spedizione che sta per essere respinta. È una delle tecniche base dei cybercriminali.
- Anche la semplice **curiosità** è una leva utilizzata spesso.
- Non cliccate sui link: eventualmente, se l'indirizzo che leggete vi pare affidabile, **ridigitatelo** voi nel browser. E meglio ancora, se si tratta di enti o società con cui avete rapporti, passate attraverso siti o numeri di telefono già noti e sperimentati.
- Diffidate di **banche** o **aziende** che vi chiedono tramite messaggi o

telefonate di fornire i vostri dati di accesso: quelle vere non lo fanno mai.

Navigare in sicurezza

Degli **indirizzi** e della loro registrazione si parla nel gioco proprio davanti alla sede di Registro .it, che è uno dei luoghi visitabili durante l'avventura. Ne accenna poi Freddy in gelateria nel secondo capitolo. Ma non sempre i siti web sono sicuri e spesso non sono ciò che sembrano: le apparenze ingannano, anche online. Il web è un posto affascinante ma pericoloso, in cui è bene osservare diverse precauzioni.

- Come i sistemi operativi, anche i **browser** devono essere continuamente aggiornati per rimediare alle eventuali criticità. Potete settarli perché si aggiornino in automatico; altrimenti verificate di utilizzare sempre la versione più recente.
- Controllate di avere sempre un **antivirus** efficiente e aggiornato.
- Sulle **reti wi-fi pubbliche**, non fate operazioni sensibili come acquisti con carta di credito od operazioni bancarie. Potreste essere intercettati da malintenzionati.
- Su wi-fi pubbliche, non scaricate o inviate file con dati personali e fate particolare attenzione a chiudere ogni collegamento con un **logout**.
- Se possedete una **Rete wi-fi casalinga**, mettete sempre una password e datela solo a persone fidate. Renderla disponibile a tutti è generoso ma vi espone a pericoli.
- Se usate computer condivisi, come quelli di un albergo o una scuola, usate la **navigazione in incognito**; al termine non lasciate finestre e programmi aperti o in cui vi siete loggati (soprattutto browser), o file con vostri dati.
- Evitate di cliccare su **banner** o annunci pubblicitari, che potrebbero portarvi su siti pericolosi o attivare malware.
- Quando dovete effettuare operazioni sensibili, come acquistare qualcosa od operare sull'home banking, assicuratevi di essere su pagine sicure con il suffisso **https**.
- Uscite sempre dai siti in cui vi loggate effettuando un **logout**, non limitatevi a chiudere la finestra.

Tra password e accessi

Gli uomini in nero bloccano a Nabbo l'accesso al Social Club, almeno fino a quando non diventa abbastanza famoso raccogliendo i like. Nella realtà, questo mestiere è svolto dalle procedure di accesso sotto **login** e **password**, che fanno entrare nel sito solo chi si è registrato ricevendo l'approvazione del gestore. Le password sono una difesa efficace se vengono scelte bene.

- Se un sito o un servizio vi fornisce una **password iniziale**, cambiatela sempre appena possibile: non lasciate mai quella di default generata dal sistema.
- **Cambiate** le password dei siti più importanti con frequenza: più passa il tempo, più c'è il rischio che vengano scoperte o violate.
- Le password semplici sono più facili da forzare con attacchi di forza bruta (sono i tentativi di decifrarle) da parte degli hacker, che con semplici programmi possono provare tutte le combinazioni possibili di caratteri. Più la password è **lunga** e contiene **caratteri insoliti**, più le combinazioni crescono in misura esponenziale e più lungo e difficile sarà forzarle per chi non le conosce.
- Non create password che corrispondano a dati personali **facilmente intuibili** come data di nascita, nome e cognome o che siano facilmente ricollegabili a voi.
- Non lasciate **scritti su fogli** incustoditi username e password, così come i PIN di carte di credito e bancomat.
- Se proprio non riuscite a ricordare tutte le vostre password, utilizzate un **programma** fidato che le memorizzi e vi consenta così di ricordare un'unica password molto robusta, quella necessaria ad accedervi.
- Usare la **stessa password** su più siti è molto pericoloso. Se infatti qualcuno riesce a forzare un sito e a rubare le chiavi di accesso degli utenti, molto probabilmente cercherà di utilizzarle su altri siti o di venderle a qualcuno che farà poi la stessa cosa.
- Valutate **altre modalità** di riconoscimento sicuro per l'accesso ai vostri dispositivi, come le impronte digitali.
- Quando digitate in pubblico password o dati sensibili, fate molta attenzione a **non essere osservati**. Anche davanti ai bancomat, coprite bene con la mano la tastiera mentre digitate il PIN: potrebbe esserci qualcuno in agguato o una telecamera nascosta.

Tutte le trappole del malware

Il malware può essere un problema, per noi come per gli abitanti di Internetopoli: tutto il gioco si incentra su un caso di **ransomware**. È un virus a bloccare più volte la fabbrica del signor Hashtag, mentre Mr. D ha problemi con i worm. Di spyware parla il troll davanti allo studio del Dr. Kappersky, nel primo capitolo del gioco; di trojan Freddy in gelateria. Con gli adware si batte Nabbo nel quarto capitolo, ai Giardinetti Wi-fi. Osservare il comportamento del proprio computer o cellulare può aiutare a scoprire eventuali malware che abbiano superato lo schermo di protezioni e antivirus.

- Scaricate app sul cellulare solo da **store ufficiali**.
- Attenzione a **sintomi sospetti** come un eccesso di pop-up pubblicitari sul vostro computer o cellulare, strani messaggi di sistema, surriscaldamento (nel computer segnalato anche dalla ventola sempre in azione), rallentamenti e blocchi, tentativi di connessione automatica: possono essere indizio di un malware all'opera.
- Il cambio non voluto della **homepage** del browser e la comparsa di app sconosciute sul cellulare possono essere ulteriori indizi di un malware in attività.

- Controllate periodicamente con attenzione il **traffico dati** del vostro device: se cresce in maniera immotivata, potrebbe esserci un malware in attività.
- Allo stesso modo, controllate con cura gli **addebiti telefonici** e i servizi attivati sul vostro cellulare: talvolta i malware attivano essi stessi servizi a pagamento senza che ve ne accorgiate.
- Evitate di **craccare** i vostri dispositivi, ad esempio gli iPhone per poter usare app non ufficiali: questo apre le porte ai malware.

Saper stare al mondo e sul web

Nabbovaldo incontra più volte un troll, Heather la hater, il pessimo Flint Flamer. Del **comportamento** con questa categoria di persone parla Ted Tuber al Social Club, nel secondo capitolo. Carla Cospira introduce il tema delle **notizie false**. Hypsta Holly è perseguitata da Bimba, che non rispettando la sua privacy arriva a diventare una **stalker**. Inoltre, Ada si interroga più volte sull'opportunità di pubblicare certe foto che potrebbero essere imbarazzanti per il soggetto ritratto. Seguire la **netiquette** e muoversi con giudizio in Rete aiuta anche a evitare complicazioni legali.

- Leggiamo i **regolamenti dei siti** cui accediamo e comportiamoci di conseguenza.
- **Non insultiamo** e non aggrediamo.
- Non diffondiamo **notizie false** o che comunque non abbiamo verificato.
- Non spieghiamo come effettuare **attività illegali** di qualsiasi tipo né istighiamo a farle.
- **Rispettiamo** sempre gli altri; se dobbiamo far notare errori valutiamo se sia davvero opportuno e facciamolo con delicatezza.
- Rispettiamo il diritto d'autore e il **copyright**, evitando di diffondere illegalmente contenuti protetti.
- Non violiamo la **privacy** pubblicando informazioni personali o immagini altrui senza consenso.

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

Prima edizione: settembre 2022

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

**Una guida ricca di informazioni,
curiosità e attività didattiche per condurre
i ragazzi e le ragazze alla scoperta di**

“Nabbovaldo e il ricatto dal cyberspazio”

e introdurli a un uso consapevole della Rete.

Registro.it

Consiglio Nazionale
delle Ricerche

CM 51934A