The Cyber Security Issue

Donne e uomini. Adulti e bambini. Istituzioni e persino Stati. Si parla di sicurezza e riguarda tutti.

Comics & Science

PER UN RAPPORTO TRA SCIENZA E INTRATTENIMENTO

2018

EDIZIONE SPECIALE FUORI COMMERCIO

ISBN 978-88-8080-328-7

Cajelli
Saracino
Ziccardi

"NABBOVALDO contro i PC ZOMBI"

di Giovanni Eccher e Gabriele Peddes

2018

GIOVANNI ECCHER
È sceneggiatore di fumetti, e regista per il cinema. Ha firmato il documentario "Magnus - Il segno del Viandante".

GABRIELE PEDDES
È nato e risiede a Bologna, dove si è diplomato presso l'Accademia di Belle Arti e lavora come fumettista e illustratore.

DIEGO CAJELLI
È sceneggiatore di fumetti e insegna "Crossmedialità e storytelling" presso l'Università Cattolica del Sacro Cuore (MI).

GIOVANNI ZICCARDI
È professore di Informatica Giuridica e componente del Comitato di Sicurezza presso l'Università degli Studi di Milano.

ANDREA SARACINO
È ricercatore presso l'Istituto CNR-IIT di Pisa, dove si occupa di sicurezza informatica.

Comics & Science

Una pubblicazione di
Cnr edizioni
Consiglio Nazionale delle Ricerche
in collaborazione con
Istituto per le Applicazioni del Calcolo "Mauro Picone" del CNR (bookshop@cnr.it) e Istituto di Informatica e Telematica del CNR

DIREZIONE EDITORIALE
Roberto Natalini
Andrea Plazzi

REALIZZAZIONE
Symmaceo Communications (MI)
facebook.com/Symmaceo
comics-science@symmaceo.com

PROGETTO GRAFICO
Lorenzo Ceccotti e Marianna Rossi

IMPAGINAZIONE
Alessio D'Uva

HANNO COLLABORATO
Per IIT-CNR: Stefania Fabbri, Domenico Laforenza, Anna Vaccarelli; Mattia Di Bernardo, Antonio Mirizzi

RINGRAZIAMENTI
Sara Di Marcello

Illustrazione di copertina di Gabriele Peddes

Il ritratto di Giovanni Eccher è di Tuono Pettinato

NABBOVALDO contro i PC zombi
Testo di Giovanni Eccher, disegni e colori di Gabriele Peddes

Prima edizione: Dicembre 2018

Cnr Edizioni, 2018
Piazzale Aldo Moro 7
00185 Roma
www.edizioni.cnr.it
ISBN 978 88 8080 327-0 (print edition)
ISBN 978 88 8080 328-7 (electronic edition)

Stampa
A4 Servizi Grafici snc
Chivasso (TO)

Comics&Science
è una co-produzione
Lucca Comics & Games e
Symmaceo Communications

FSC
www.fsc.org
MISTO
Carta da fonti gestite in maniera responsabile
FSC® C115584

INTRO

Secondo capitolo delle avventure di Nabbovaldo, Nabbo per gli amici. Anche grazie alla sveglissima Linda, non è più il ragazzone ingenuo e inesperto degli inizi (be', diciamo che non è più inesperto) e sa come muoversi a Internetopoli. Anche per questo è felice di ospitare la cuginetta Ada, che... ma stiamo facendo spoiler... quando basta cominciare a leggere! Volevamo dire una cosa molto semplice: è un piacere che un fumetto di *Comics&Science* – e con esso la filosofia comunicativa che gli gira intorno – sia piaciuto abbastanza da avere un seguito. Lo dobbiamo anche alla lungimiranza di CNR-IIT, l'Istituto del CNR che gestisce Registro .it, l'anagrafe dei domini ".it", né più né meno che l'immagine dell'Italia in Internet: da anni si rivolgono ai giovanissimi sui temi dell'identità e della cittadinanza *online*, cruciali per arrivare a operare in Rete in sicurezza e consapevolezza. E Internetopoli, in compagnia di Nabbo e Linda, è un ottimo punto di partenza per conoscere la Rete e i suoi pericoli: la soluzione non è scappare ma imparare a rivolgersi a persone esperte. È quanto ci aiutano a capire gli autori Giovanni Eccher e Gabriele Peddes, con una narrazione a fumetti agile e godibilissima che dà lustro al "comics" in *Comics&Science*.

Roberto Natalini
Andrea Plazzi

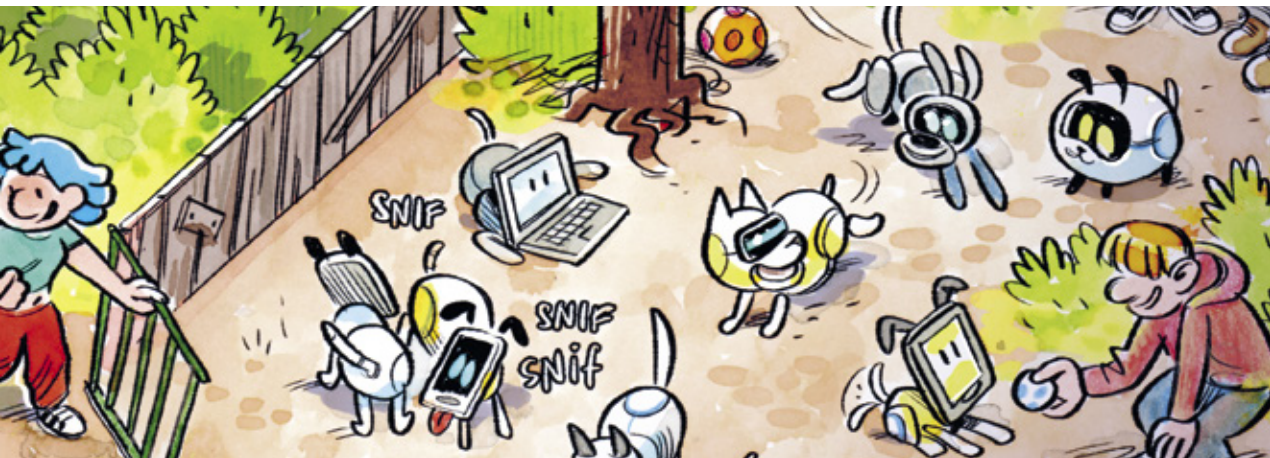
The Cyber Security Issue

SOMMARIO

5

NABBOVALDO CONTRO I PC ZOMBI

GIOVANNI ECCHER
GABRIELE PEDDES



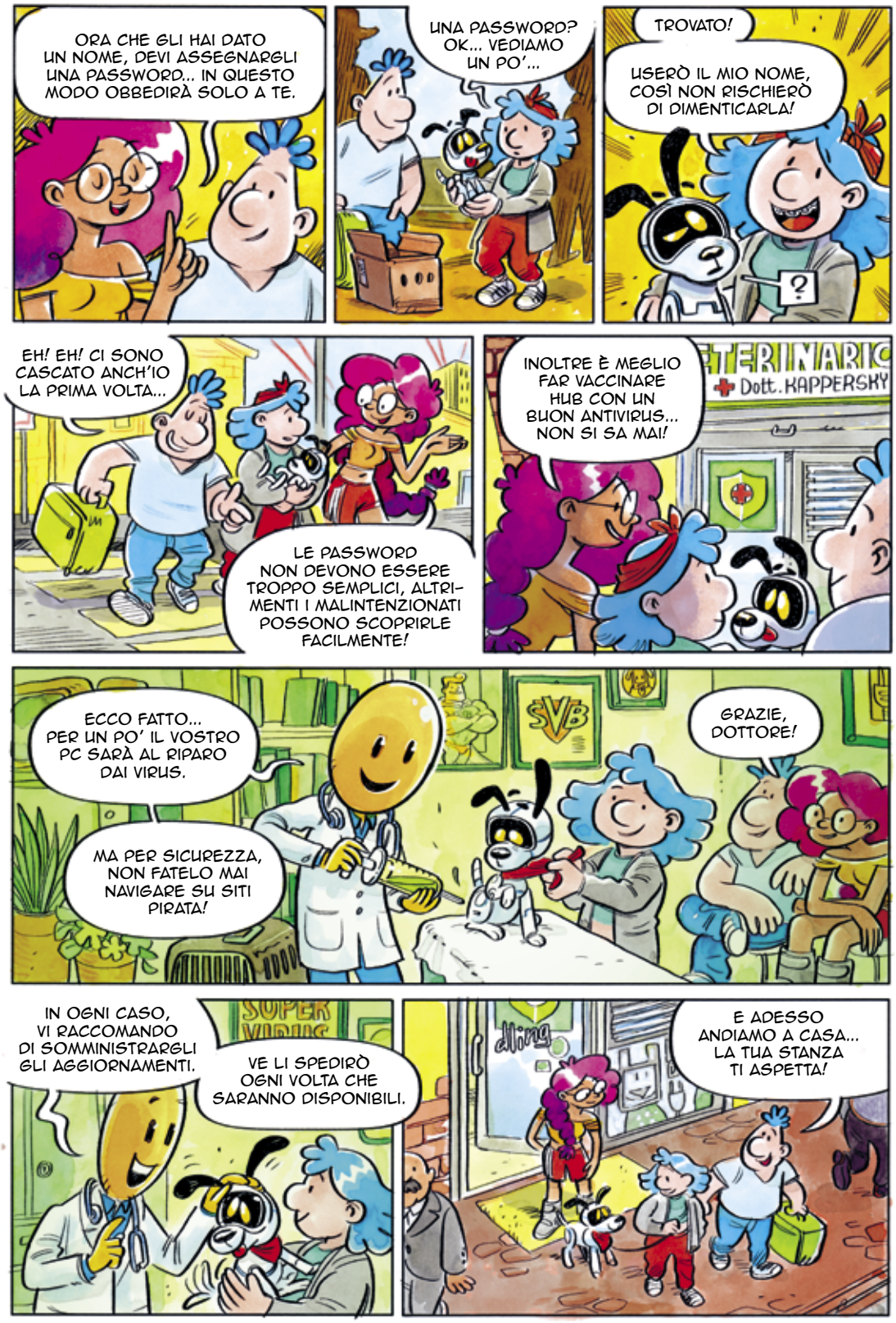
CYBER SECURITY: UNA CULTURA

DOMENICO LAFORENZA
Direttore dell'Istituto di Informatica e Telematica del Consiglio Nazionale delle Ricerche (CNR-IIT)

Il tema della sicurezza informatica (di cui la Cyber Security è parte) è di assoluta attualità ed è entrato ormai da tempo nella cronaca quotidiana. Ma non tutti siamo esperti e non sempre sappiamo come individuare le minacce e come comportarci nel caso di situazioni pericolose. A maggior ragione, se siamo educatori (genitori o insegnanti) abbiamo difficoltà a mettere in guardia i nostri ragazzi da *situazioni a rischio* e a insegnare loro come tenere *comportamenti saggi e corretti.*

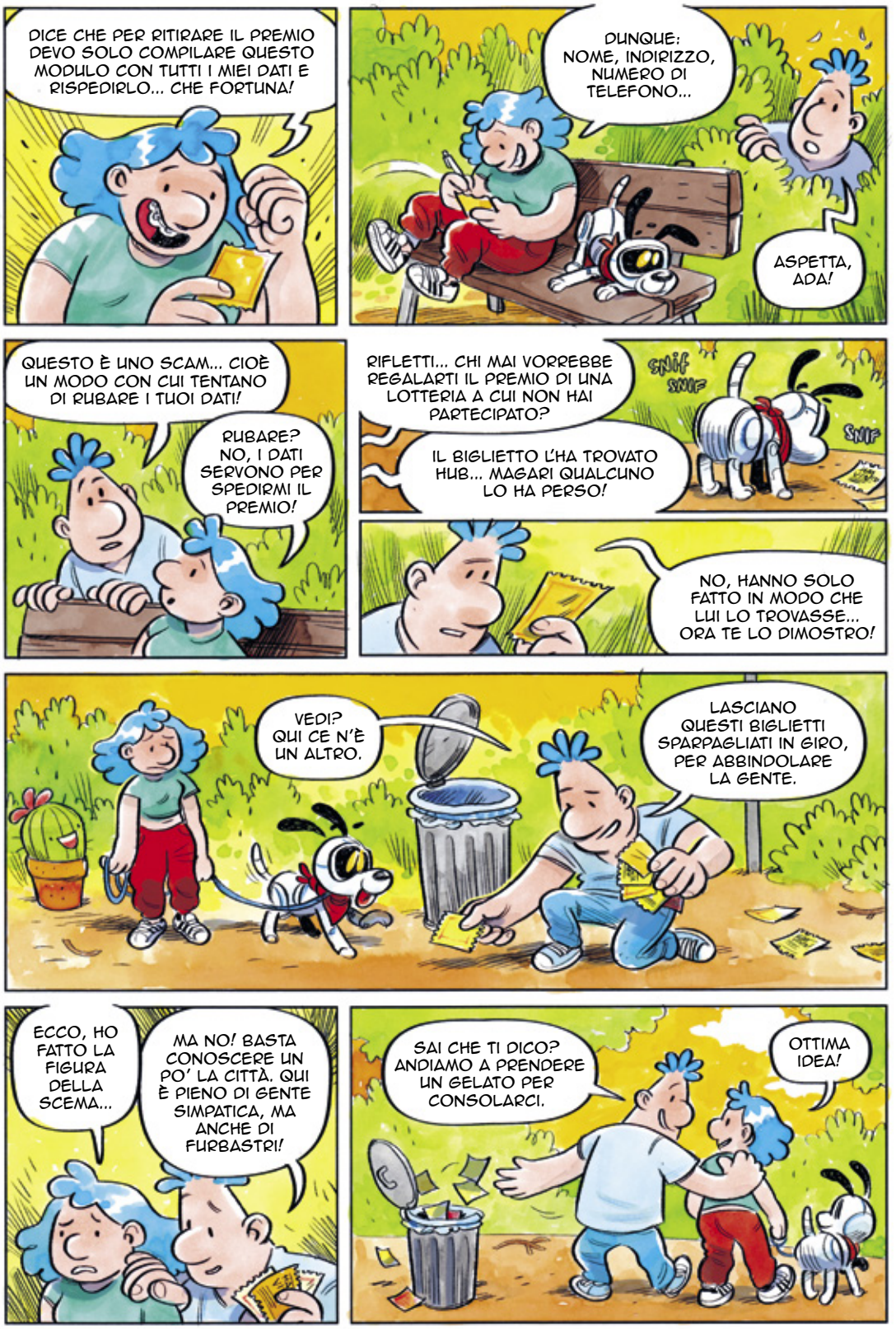
La Cyber Security è una delle maggiori sfide dei nostri tempi che riguarda i singoli, le imprese (grandi o piccole) e i governi di tutto il pianeta. Difendersi a tutti i livelli è complesso ma alcune misure possono essere adottate da chiunque. Quello che conta è conoscere i pericoli e sapersi muovere in Rete con consapevolezza. Si parla spesso di analfabetismo digitale, che bisogna combattere e superare in tutte le fasce di età. Registro .it è impegnato da anni nella divulgazione della cultura digitale, concentrando sempre più sforzi e risorse sulla Cyber Security anche mediante la creazione di un apposito laboratorio all'interno dell'Istituto di Informatica e Telematica del CNR. Più recentemente, nel 2018, è stato attivato un osservatorio per la Cyber Security a beneficio primario delle imprese e della Pubblica Amministrazione; inoltre, è stata ulteriormente ampliata l'offerta della Ludoteca del Registro .it, mediante la creazione di nuovi giochi e laboratori dedicati alla Cyber Security destinati principalmente ai bambini dagli 8 agli 11 anni. Ancora una volta, per rendere più efficace ed incisivo il nostro intervento, ricorriamo al linguaggio del fumetto, che ci consente di raccontare i temi della sicurezza in Rete a lettori di tutte le età.


Le AVVENTURE di
NABBO & LINDA
COME SI CHIAMA LA TUA CUGINETTA?
ADA! SI TRASFERISCE A INTERNETOPOLI PER QUESTIONI DI STUDIO.
VERRÀ AD ABITARE A CASA MIA.
"NABBOVALDO contro i PC ZOMBI"
di Giovanni Eccher e Gabriele Peddes
LE HO PRESO UN REGALO SU WWW.CUCCIOLIPUCCIOSI.IT... L'AIUTERÀ AD AMBIENTARSI!
OTTIMA IDEA!
NABBO! SONO QUI!
LEI È LINDA, LA MIA RAGAZZA!
CHE PIACERE! NABBO MI HA PARLATO MOLTO DI TE.
BENVENUTA!
QUESTO PC È PER TE... SO CHE AMI GLI ANIMALI!
WOF
WOFF!
GRAZIE! COM'È CARINO!
LO CHIAMERÒ HUB!


ORA CHE GLI HAI DATO UN NOME, DEVI ASSEGNARGLI UNA PASSWORD... IN QUESTO MODO OBBEDIRÀ SOLO A TE.
UNA PASSWORD? OK... VEDIAMO UN PO'...
TROVATO!
USERÒ IL MIO NOME, COSÌ NON RISCHIERÒ DI DIMENTICARLA!
?
EH! EH! CI SONO CASCATO ANCH'IO LA PRIMA VOLTA...
LE PASSWORD NON DEVONO ESSERE TROPPO SEMPLICI, ALTRIMENTI I MALINTENZIONATI POSSONO SCOPRIRLE FACILMENTE!
INOLTRE È MEGLIO FAR VACCINARE HUB CON UN BUON ANTIVIRUS... NON SI SA MAI!
Dott. KAPPERSKY
ECCO FATTO... PER UN PO' IL VOSTRO PC SARÀ AL RIPARO DAI VIRUS.
MA PER SICUREZZA, NON FATELO MAI NAVIGARE SU SITI PIRATA!
GRAZIE, DOTTORE!
IN OGNI CASO, VI RACCOMANDO DI SOMMINISTRARGLI GLI AGGIORNAMENTI.
VE LI SPEDIRÒ OGNI VOLTA CHE SARANNO DISPONIBILI.
E ADESSO ANDIAMO A CASA... LA TUA STANZA TI ASPETTA!

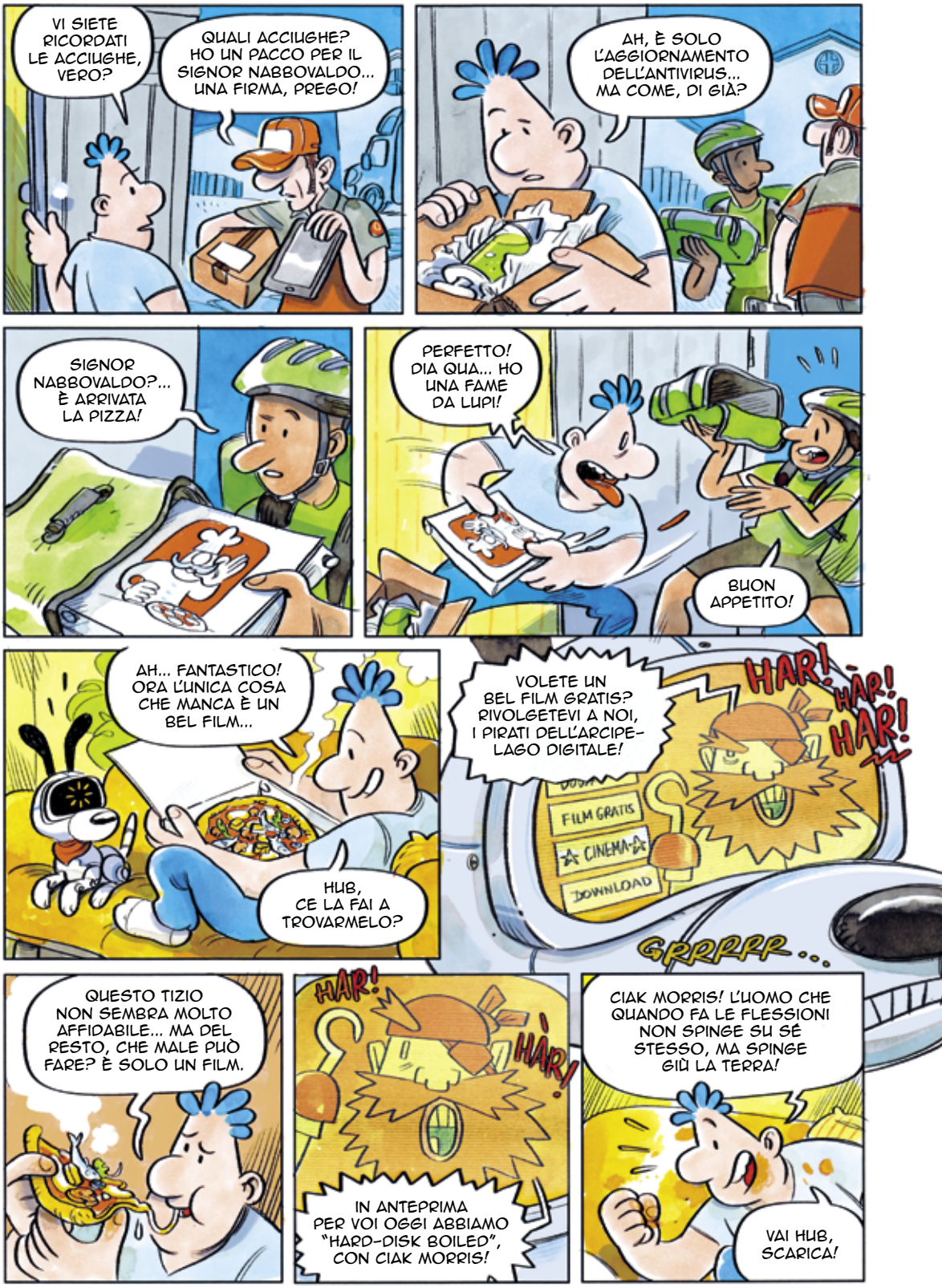

GUARDA COME MANGIA... DOVEVA ESSERE PROPRIO AFFAMATO!
ORA DOVRAI PRENDERTI CURA DI LUI, NUTRIRLO E COCCOLARLO.
HUB
E PORTARLO AL PARCO TUTTI I GIORNI! NON DIMENTICARE IL GUINZAGLIO.
BUONA PASSEGGIATA E MI RACCOMANDO, NON DARE RETTA AI TROLL!
CERTO! CI VEDIAMO DOPO!
LA MIA CUGINETTA È DAVVERO IN GAMBA, SCOMMETTO CHE SI AMBIENTERÀ IN FRETTA!
CERTO, MA SAI CHE INTERNETOPOLI È DIVERSA DALLE ALTRE CITTÀ...
CREDI CHE POTREBBE SUCCEDERLE QUALCOSA?
NON SI SA MAI. DATO CHE È NUOVA DEL POSTO, FORSE È MEGLIO CHE TU LA TENGA D'OCCHIO.
GIUSTO! MA LA SEGUIRÒ SENZA FARMI NOTARE... NON VOGLIO CHE ADA PENSI CHE NON MI FIDO DI LEI!
CHE POSTO MERAVIGLIOSO! POTREI PASSARE TUTTO IL GIORNO A GUARDARE QUESTA GENTE STRAMPALATA...

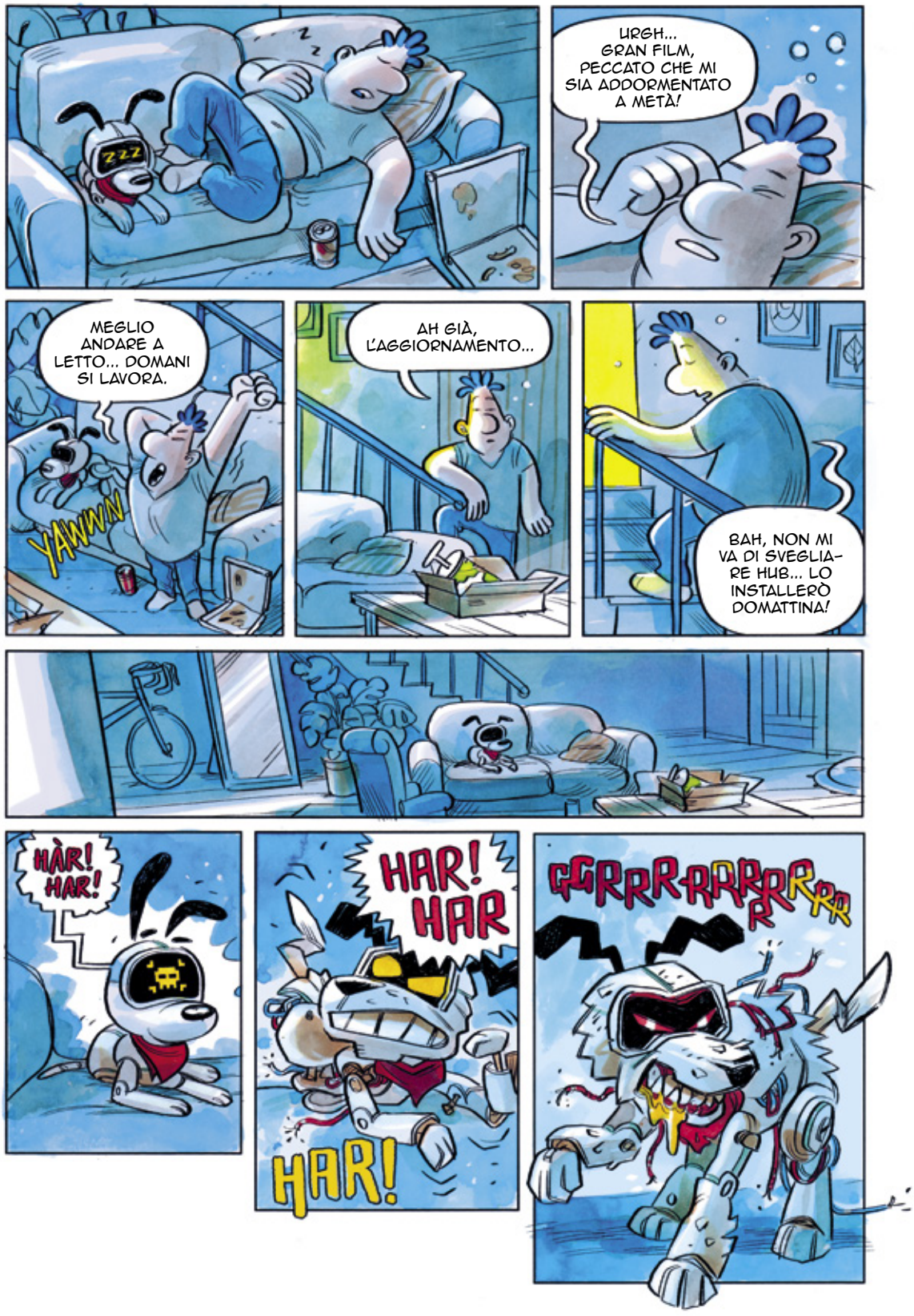

ECCOCI, QUESTA È L'AREA RISERVATA AI PC! ORA POSSO TOGLIERTI IL GUINZAGLIO.
SNIF
SNIF SNIF
MI RACCOMANDO, NON ATTACCARE BRIGA CON GLI ALTRI!
WOF!
GUARDA QUEI GATTINI! CHE TENERI!
BUONGIORNISSIMOOO
QUESTO PARLA! NON CI POSSO CREDERE!
OOOOOH LONG JOOOOHN SON
TELL ME MORE
OH, NO! DOV'È FINITO HUB?
OOOH
DON PIAN
HUB! VIENI QUI, BELLO!
CAVOLO... MI SONO DISTRATTA UN ATTIMO E L'HO GIÀ PERSO!
AH... ECCOTI QUI! COS'HAI TROVATO?
WOF!
SEMBRA UN BIGLIETTO DELLA LOTTERIA...
C'È SCRITTO CHE HO VINTO UNA BICICLETTA!


DICE CHE PER RITIRARE IL PREMIO DEVO SOLO COMPILARE QUESTO MODULO CON TUTTI I MIEI DATI E RISPEDIRLO... CHE FORTUNA!
DUNQUE: NOME, INDIRIZZO, NUMERO DI TELEFONO...
ASPETTA, ADA!
QUESTO È UNO SCAM... CIOÈ UN MODO CON CUI TENTANO DI RUBARE I TUOI DATI!
RUBARE? NO, I DATI SERVONO PER SPEDIRMI IL PREMIO!
RIFLETTI... CHI MAI VORREBBE REGALARTI IL PREMIO DI UNA LOTTERIA A CUI NON HAI PARTECIPATO?
IL BIGLIETTO L'HA TROVATO HUB... MAGARI QUALCUNO LO HA PERSO!
SNIF SNIF SNIF
NO, HANNO SOLO FATTO IN MODO CHE LUI LO TROVASSE... ORA TE LO DIMOSTRO!
VEDI? QUI CE N'È UN ALTRO.
LASCIANO QUESTI BIGLIETTI SPARPAGLIATI IN GIRO, PER ABBINDOLARE LA GENTE.
ECCO, HO FATTO LA FIGURA DELLA SCEMA...
MA NO! BASTA CONOSCERE UN PO' LA CITTÀ. QUI È PIENO DI GENTE SIMPATICA, MA ANCHE DI FURBASTRI!
SAI CHE TI DICO? ANDIAMO A PRENDERE UN GELATO PER CONSOLARCI.
OTTIMA IDEA!


PER ME UN CONO FRAGOLA E LIMONE...
Diploma
ASSOCIAZIONE GELATAI INTERNETOPOLI
COOKIES
PER ME PISTACCHIO E STRACCIATELLA!
CHE BEL PC AVETE! POSSO DARGLI UN BISCOTTINO?
COOKIES
UH.... NO, GRAZIE. HUB NON ACCETTA BISCOTTI DAGLI SCONOSCIUTI.
HO FATTO BENE, VERO? MI SEMBRA DI CAPIRE CHE IN QUESTA CITTÀ BISOGNA DIFFIDARE DELLE OFFERTE TROPPO GENTILI...
IN QUESTO CASO PUOI ACCETTARE... FREDDY È UN GELATAIO AUTORIZZATO!
HA ANCHE IL DIPLOMA APPESO AL MURO.
I BISCOTTINI, O COOKIES, NON SONO DI PER SÉ DANNOSI... DIPENDE SEMPRE DA CHI TE LI DÀ.
IN QUESTO CASO IL GELATAIO STA SOLO FACENDO AMICIZIA...
COSÌ, QUANDO TORNEREMO QUI, HUB LO RICONOSCERÀ.
WWW.GIO FREDDY GELATI SUPERFREDDI.IT
SONO PROPRIO UN DISASTRO... QUESTA CITTÀ È TROPPO COMPLICATA PER ME!
MA NO! BASTA IMPARARE A DISTINGUERE I MALINTENZIONATI.

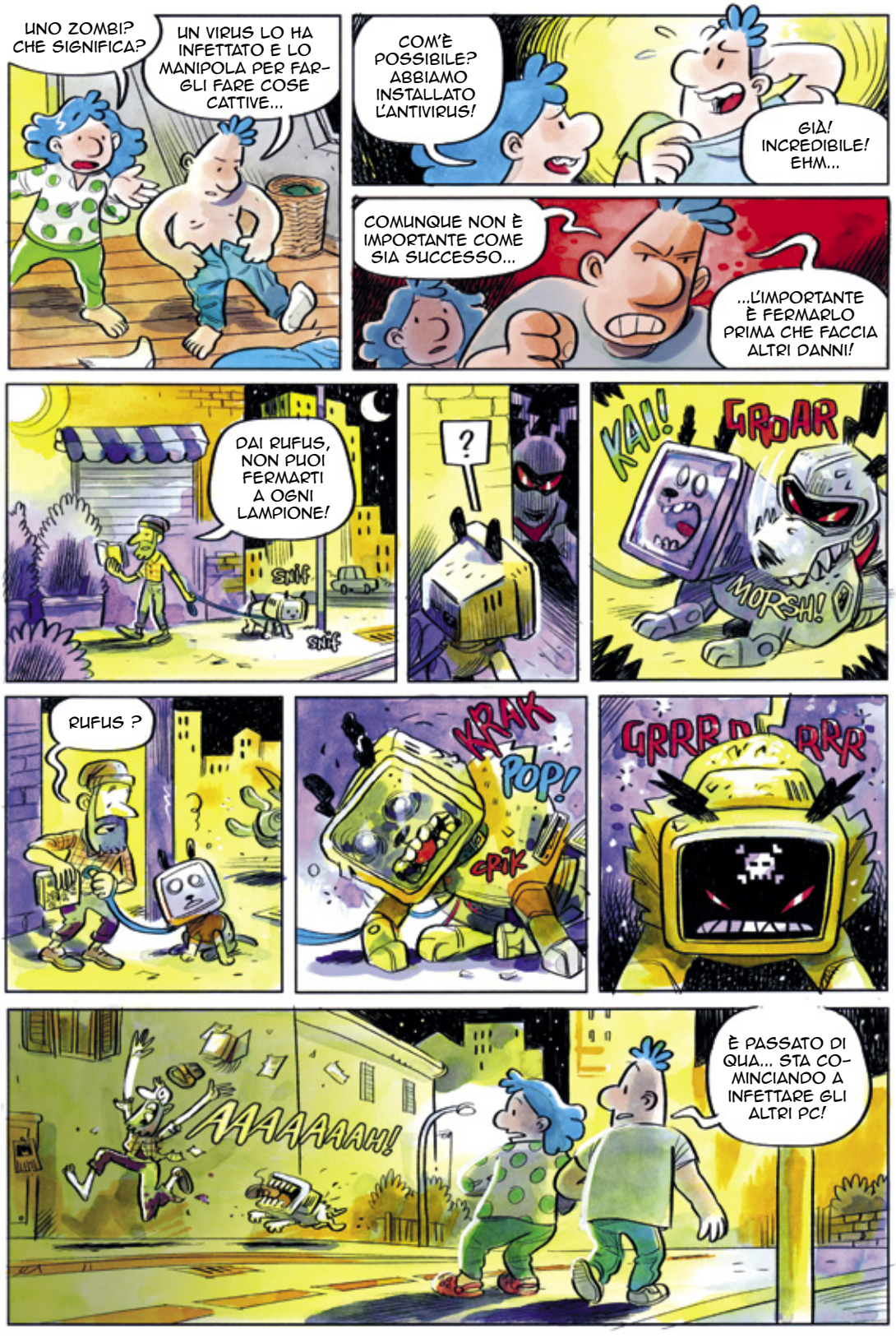

ECCOCI A CASA. SARAI STANCA, DOPO UNA GIORNATA COSÌ INTENSA!
PUOI DIRLO FORTE... MI SA CHE ANDRÒ A LETTO DI FILATA!
TU DORMIRAI QUI, HUB... CI VEDIAMO DOMATTINA!
WOF!
BUONANOTTE, NABBO... GRAZIE PER LA BELLA GIORNATA!
MA COME... NON CENI NEMMENO?
POVERETTA, È DAVVERO DISTRUTTA!
E ANCHE IO... MA NON IL MIO STOMACO!
GRROOO
OOOOOWL
EHI! POSSO ORDINARE UNA PIZZA! HUB MI AIUTERÀ...
QUI, BELLO! TROVAMI UNA PIZZERIA A DOMICILIO!
ECCO QUA! WWW.PIZZAPAZZAEXPRESS.IT... CONSEGNA GARANTITA ENTRO POCHI MINUTI!
€
BLING
BLONG
SUONANO ALLA PORTA... CHE VELOCITÀ!

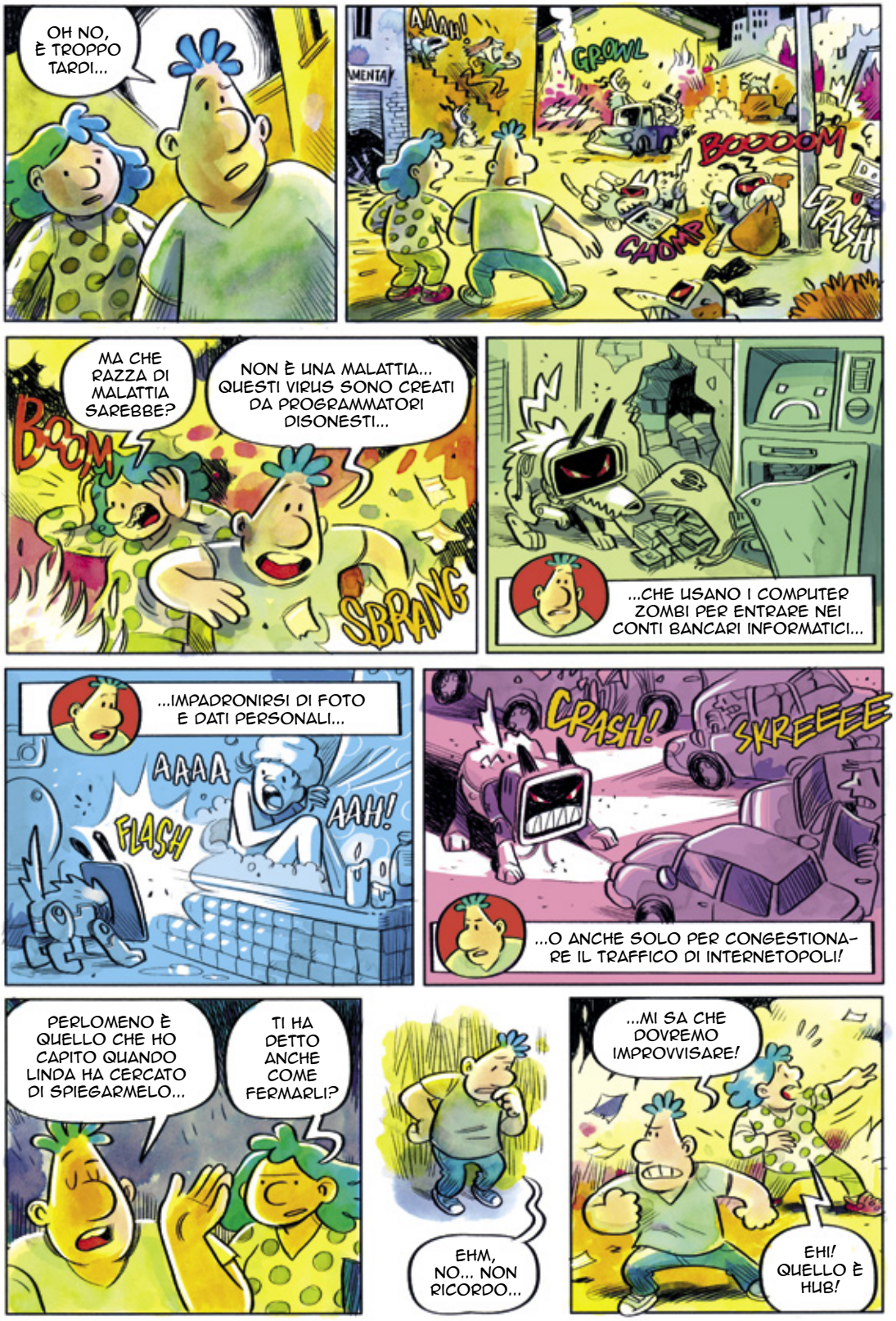

VI SIETE RICORDATI LE ACCIUGHE, VERO?
QUALI ACCIUGHE? HO UN PACCO PER IL SIGNOR NABBOVALDO... UNA FIRMA, PREGO!
AH, È SOLO L'AGGIORNAMENTO DELL'ANTIVIRUS... MA COME, DI GIÀ?
SIGNOR NABBOVALDO?... È ARRIVATA LA PIZZA!
PERFETTO! DIA QUA... HO UNA FAME DA LUPI!
BUON APPETITO!
AH... FANTASTICO! ORA L'UNICA COSA CHE MANCA È UN BEL FILM...
HUB, CE LA FAI A TROVARMELO?
VOLETE UN BEL FILM GRATIS? RIVOLGETEVI A NOI, I PIRATI DELL'ARCIPELAGO DIGITALE!
HAR! HAR! HAR!
FILM GRATIS
CINEMA
DOWNLOAD
GRRRRR...
QUESTO TIZIO NON SEMBRA MOLTO AFFIDABILE... MA DEL RESTO, CHE MALE PUÒ FARE? È SOLO UN FILM.
HAR!
HAR!
IN ANTEPRIMA PER VOI OGGI ABBIAMO "HARD-DISK BOILED", CON CIAK MORRIS!
CIAK MORRIS! L'UOMO CHE QUANDO FA LE FLESSIONI NON SPINGE SU SÉ STESSO, MA SPINGE GIÙ LA TERRA!
VAI HUB, SCARICA!

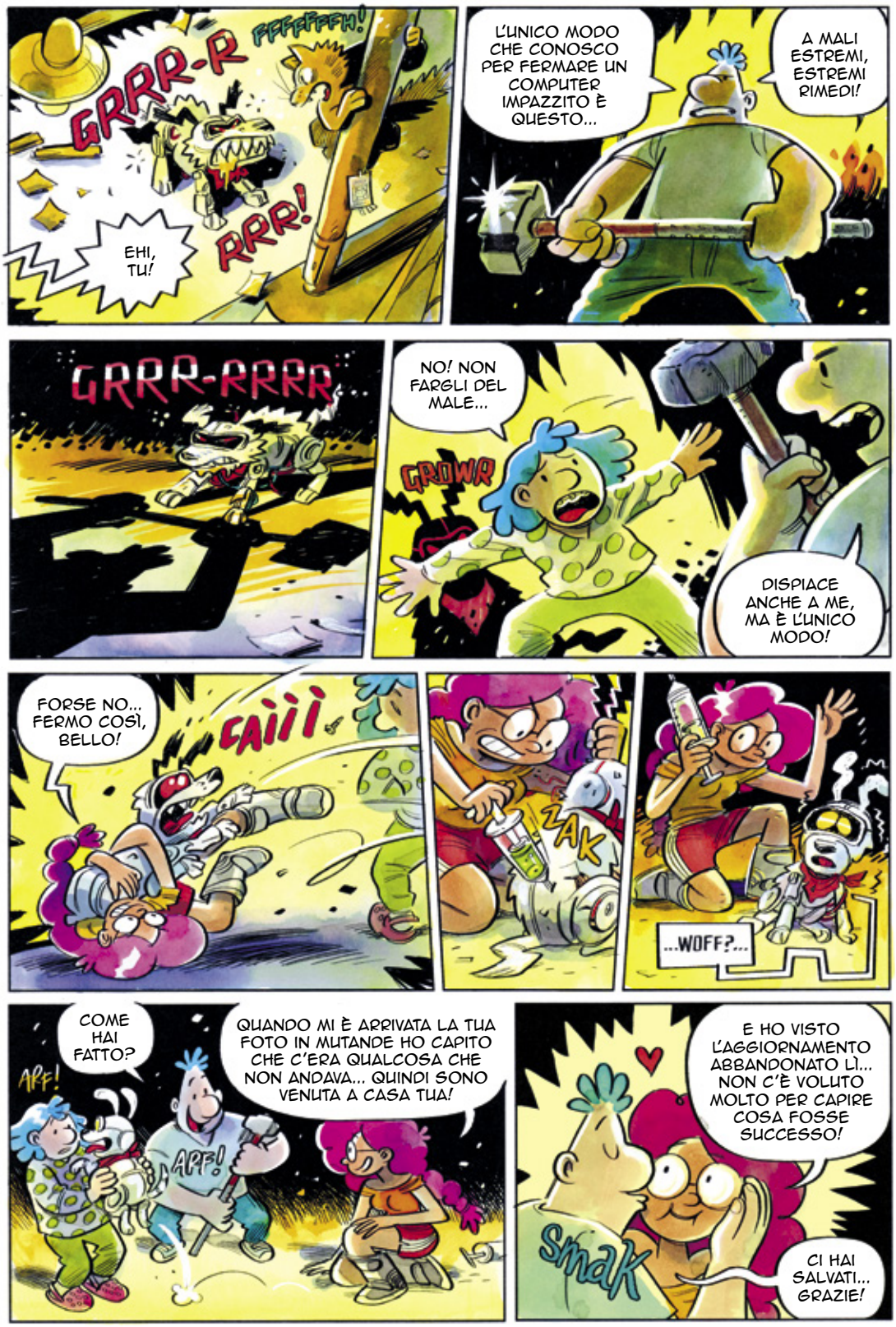

ZZZ
URGH... GRAN FILM, PECCATO CHE MI SIA ADDORMENTATO A METÀ!
MEGLIO ANDARE A LETTO... DOMANI SI LAVORA.
YAWWN
AH GIÀ, L'AGGIORNAMENTO...
BAH, NON MI VA DI SVEGLIARE HUB... LO INSTALLERÒ DOMATTINA!
HÀR! HAR!
HAR! HAR
HAR!
GGRRRRRRRRRRRR


AAAHHH... CHE STANCHEZZA...
E LA PIZZA MI È RIMASTA SULLO STOMACO!
GRAT GRAT
GROOOO
OOOOWL
UN MOMENTO... NON È IL MIO STOMACO A FARE QUESTO RUMORE!
È LA PORTA!
GRR
RR-RRRR
HUB? CHE TI SUCCEDE?
GR-R-ROOOOWR
FLASH
MI HAI SCATTATO UNA FOTO?
LA FOTO È STATA INVIATA CON SUCCESSO AI TUOI CONTATTI!
EHI! NON TI HO DETTO DI SPEDIRLA!
TORNA QUI!
PERBACCO! NON PENSAVO CHE IL MIO VICINO FOSSE UN ESIBIZIONISTA.
awful
what a shame
R-rated
AH AH!
AH! AH
AH! AH!
AH! AH! È PROPRIO UN NABBO! ORA LA INOLTRO A TUTTI I MIEI AMICI!
NON È DA LUI MANDARE FOTO DEL GENERE, MI SA CHE È SUCCESSO QUALCOSA...


FERMO!
GRR-RRR
...MMMH?
CHOMP
HUB... LASCIA STARE IL MIO DIARIO!
SBRÀN!
STRAAÀP!
SCANNING TEXT
GRRR-RR..RR
OH, NO! HA MEMORIZZATO IL MIO DIARIO SEGRETO E L'HA MANDATO A TUTTI I MIEI COMPAGNI!
MI È SFUGGITO! PRENDILO!
È UNA PAROLA!
UGH! È TROPPO VELOCE!
LA PROSSIMA VOLTA SCELGO UN PENTIUM 1...
È SCAPPATO! MA COSA GLI È PRESO?
TEMO CHE SIA DIVENTATO UN COMPUTER ZOMBI...


UNO ZOMBI? CHE SIGNIFICA?
UN VIRUS LO HA INFETTATO E LO MANIPOLA PER FARGLI FARE COSE CATTIVE...
COM'È POSSIBILE? ABBIAMO INSTALLATO L'ANTIVIRUS!
GIÀ! INCREDIBILE! EHM...
COMUNQUE NON È IMPORTANTE COME SIA SUCCESSO...
...L'IMPORTANTE È FERMARLO PRIMA CHE FACCIA ALTRI DANNI!
DAI RUFUS, NON PUOI FERMARTI A OGNI LAMPIONE!
SNIF
SNIF
?
KAI!
GROAR
MORSH!
RUFUS ?
KRAK
POP!
CRIK
GRRR
RRR
AAAAAAAAH!
È PASSATO DI QUA... STA COMINCIANDO A INFETTARE GLI ALTRI PC!


OH NO, È TROPPO TARDI...
AAAH!
MENTA
GROWL
BOOOOM
CHOMP
CRASH
MA CHE RAZZA DI MALATTIA SAREBBE?
NON È UNA MALATTIA... QUESTI VIRUS SONO CREATI DA PROGRAMMATORI DISONESTI...
BOOM
SBRANG
...CHE USANO I COMPUTER ZOMBI PER ENTRARE NEI CONTI BANCARI INFORMATICI...
...IMPADRONIRSI DI FOTO E DATI PERSONALI...
AAAA
AAH!
FLASH
CRASH!
SKREEEE
...O ANCHE SOLO PER CONGESTIONARE IL TRAFFICO DI INTERNETOPOLI!
PERLOMENO È QUELLO CHE HO CAPITO QUANDO LINDA HA CERCATO DI SPIEGARMELO...
TI HA DETTO ANCHE COME FERMARLI?
EHM, NO... NON RICORDO...
...MI SA CHE DOVREMO IMPROVVISARE!
EHI! QUELLO È HUB!


GRRR-R
FFFFFFFH!
RRR!
EHI, TU!
L'UNICO MODO CHE CONOSCO PER FERMARE UN COMPUTER IMPAZZITO È QUESTO...
A MALI ESTREMI, ESTREMI RIMEDI!
GRRR-RRRR
NO! NON FARGLI DEL MALE...
GROWR
DISPIACE ANCHE A ME, MA È L'UNICO MODO!
FORSE NO... FERMO COSÌ, BELLO!
CAIÌÌ
ZAK
...WOFF?...
COME HAI FATTO?
ARF!
ARF!
QUANDO MI È ARRIVATA LA TUA FOTO IN MUTANDE HO CAPITO CHE C'ERA QUALCOSA CHE NON ANDAVA... QUINDI SONO VENUTA A CASA TUA!
E HO VISTO L'AGGIORNAMENTO ABBANDONATO LÌ... NON C'È VOLUTO MOLTO PER CAPIRE COSA FOSSE SUCCESSO!
SMAK
CI HAI SALVATI... GRAZIE!


MA COME FACCIAMO PER TUTTI GLI ALTRI COMPUTER ZOMBI?
C'È UNA SOLA PERSONA IN GRADO DI RISOLVERE QUESTO PASTICCIO...
SUPER VIRUS BLOCKER!
OPLÀ! ECCOMI QUA.
SVB
AIUTACI, SVB... C'È UN'EPIDEMIA DI VIRUS ZOMBI!
LASCIATE FARE A ME... HO QUELLO CHE CI VUOLE!
SVB
GRAZIE, SVB!
GRAZIE A VOI, CITTADINI!
COM'È SEMPRE GENTILE, ANCHE NEL MOMENTO DEL PERICOLO...
BAH!
A CUCCIA, BELLI! TORNATE DAI VOSTRI PADRONI!
PSSS-ST


PER FORTUNA I DANNI SONO LIMITATI... TUTTO STA TORNANDO ALLA NORMALITÀ!
MA TU NABBO, PERCHÉ NON HAI SOMMINISTRATO SUBITO L'AGGIORNAMENTO A HUB?
BE', IO... ECCO... LO AVREI FATTO DOMATTINA!
È CHE HO SCARICATO UN FILM DA UN SITO PIRATA, E...
GRRRR
SAI CHE NON DOVRESTI FARLO. CI SONO MOLTE PIATTAFORME LEGALI DA CUI SI POSSONO VEDERE I FILM IN STREAMING!
SÌ, MA COSTANO, E POI...
VERGOGNA, NABBO! PAGARE PER VEDERE UN FILM È GIUSTO. COSA DIRESTI, SE TI RUBASSERO IL FRUTTO DEL TUO LAVORO?
PAZIENZA, TUTTO È BENE QUEL CHE FINISCE BENE!
PUOI PERDONARMI, ADA?
MA CERTO! PUÒ CAPITARE A TUTTI DI SBAGLIARE.
mpah mpah
OGGI MI HAI INSEGNATO TANTE COSE... E DOMANI È IL MIO PRIMO GIORNO DI SCUOLA!
GIUSTO! MEGLIO ANDARE A LETTO, O DOMATTINA NON SENTIREMO LA SVEGLIA!
AH AH AH
AH AH! AH AH AH AH!
?
IN OGNI CASO, STANOTTE POSSIAMO LASCIARE DORMIRE HUB IN GIARDINO?
DOPOTUTTO, FA ANCORA CALDO!
FINE

Perché raccontiamo **Internet** con i **fumetti**?
Uno sceneggiatore di punta del fumetto italiano
incontra gli **autori** di "Nabbo & Linda"
per capire come vedono la Rete.

Una via di mezzo. Domani

DIEGO CAJELLI

Per quanto il web si sia evoluto in modo opposto rispetto alle aspettative del suo creatore Tim Berners-Lee, e di tutte le persone dotate di buon senso, ormai la Rete c'è e ce la dobbiamo tenere. La questione è: ce la dobbiamo tenere così?
Direi proprio di no. Ecco perché è sempre più necessaria un'educazione al web, al pari dell'antica educazione civica che si insegnava a scuola nei secoli scorsi. L'educazione al web deve per forza partire dai più giovani, dai bambini e dai ragazzi, anche perché ormai gli adulti sono andati, ed è del tutto inutile perdere tempo con loro. A loro piace lo spam, non sono in grado di capire le differenze tra una fake news *e una notizia vera, adorano dover riformattare l'hard disk ogni due mesi perché cliccano su tutto in modo compulsivo. Le nuove generazioni non devono fare gli stessi errori delle precedenti, ecco perché la divulgazione della cultura informatica è così importante. Ecco perché il fumetto che avete tra le mani è importante, così come lo sono i suoi autori, Giovanni Eccher e Gabriele Peddes, che ho avuto il piacere di intervistare.*

C'è differenza di approccio nello scrivere un fumetto di intrattenimento puro e uno di divulgazione?

Giovanni mi risponde così:

La differenza più grossa è che nel fumetto di puro intrattenimento in genere prevale la forma, mentre in quello di divulgazione prevalgono i contenuti. Abbiamo cercato (non è un plurale maiestatis, parlo di tutti quelli che hanno collaborato al fumetto) di evitare di realizzare un libro di istruzioni a fumetti, o peggio ancora un'opera "educativa" in senso stretto, con i personaggi che spiegano cosa fare o non fare: sarebbe stato noiosissimo. Si tratta piuttosto di una storia divertente, almeno spero, che però contiene un certo numero di

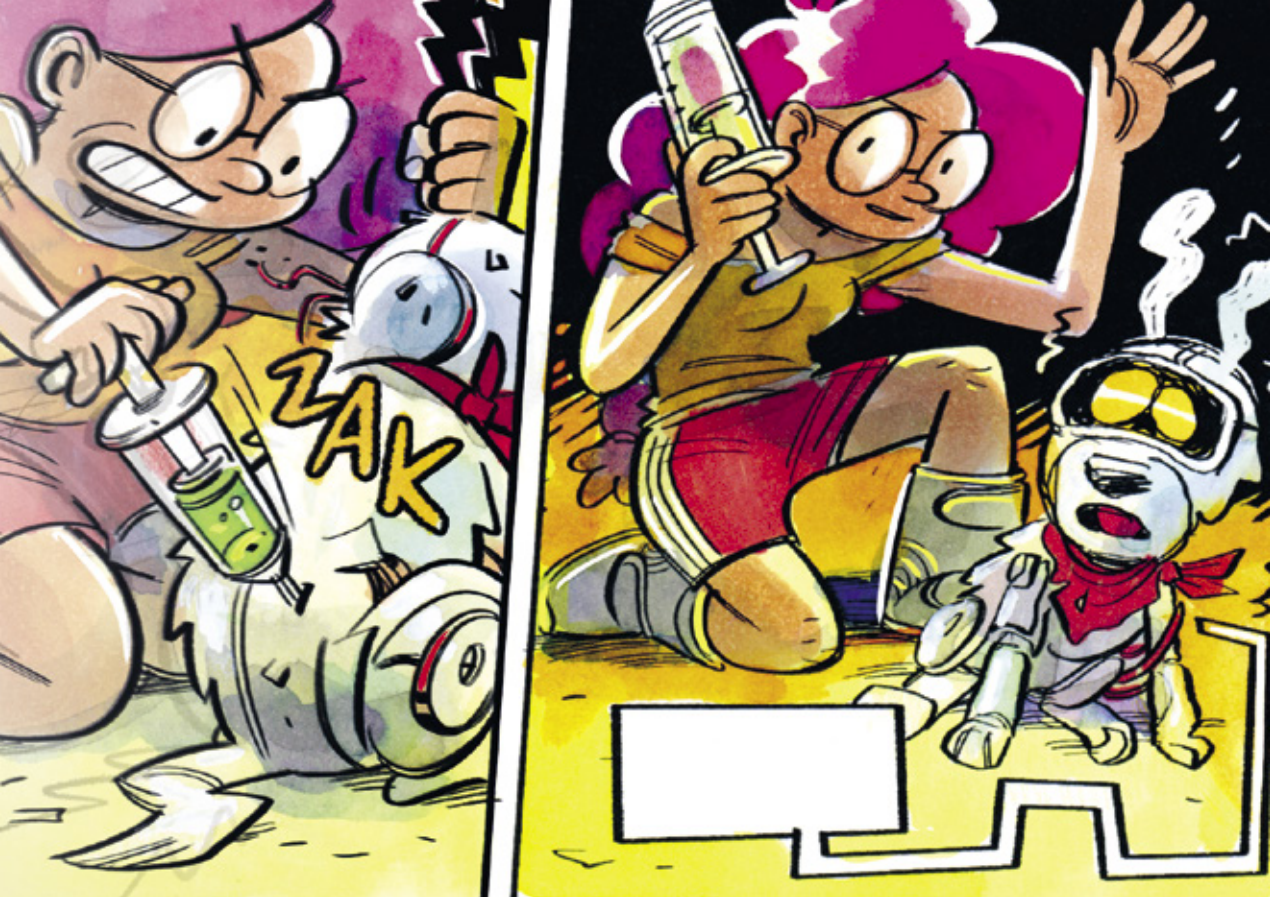
spunti di riflessione su cui chi vuole può informarsi e approfondire.

Nel fumetto mi ha colpito molto la rappresentazione grafica del web. Gabriele, come ci sei arrivato?

Sembra complicato, ma per fortuna raccontare con le immagini aiuta. Tutto l'immaginario della città come metafora del web nasce dall'app Internetopoli di Registro .it, assorbita e rielaborata dai ragazzi di prima media che avevano scritto il soggetto della storia *Nabbovaldo e le stagioni a Internetopoli*.
Con questo secondo episodio, l'universo narrativo di Internetopoli si è consolidato definitivamente, anche grazie a Giovanni. Le piazze sono luoghi *social* in cui accedere attraverso *login*, le proprietà private sono nomi a dominio che si proteggono tramite *password*, i messaggi sono inviati attraverso buste che spacchettano le frasi e così via. Il piccolo contributo visivo che avevo dato (e Giovanni ha rincarato la dose in questa storia) è stato, per esempio, quello di popolare la città di meme e personaggi assurdi che potrebbero essere appena usciti dai peggiori bar di *4chan* e *9gag*.

Sono una persona cattiva, vengo definito come un *web heretic*. Giovanni, questa domanda devo proprio fartela: Nabbo & Linda si rivolgono ai più giovani perché ormai gli adulti non li puoi più educare?

Si rivolgono ai più giovani perché sono quelli che hanno più dimestichezza con la Rete, essendoci praticamente nati in mezzo, ma sono anche (per mancanza di esperienza di vita) tra i soggetti meno consapevoli delle conseguenze che la rivoluzione digitale porta con sé. La grande familiarità con i *social network* a volte li porta a gesti estremamente ingenui, di cui vediamo quotidianamente le conseguenze, a volte tragiche e plateali (come i suicidi in conseguenza del



mobbing digitale) ma molto più spesso subdolamente invisibili. Per esempio, la svendita della propria privacy in cambio di un po' di bigiotteria digitale, o il supporto incondizionato agli interessi delle grandi multinazionali della comunicazione (si vedano le campagne degli *youtuber* contro la legislazione europea sul copyright).
Per quanto riguarda gli adulti, cioè quelli che non sono né giovani né vecchi, sono bocce perse: a mio avviso, se hanno capito l'antifona buon per loro, se non l'hanno capita si estingueranno darwinianamente e verranno sostituiti dai giovani, si spera presto.

Che rapporto hai con Internet?

Con Internet ho un rapporto abbastanza buono, nel senso che oramai credo di aver capito, grosso modo, cosa ci posso trovare e cosa no. Ha sicuramente cambiato in meglio il mio lavoro, nel senso che se ho bisogno di un'informazione storica o scientifica quasi accurata la posso trovare in pochi secondi, ed è un posto pieno di ottimi spunti narrativi.
Con i social network, invece, ho un rapporto conflittuale e me ne tengo lontano. Mi spiego: magari un giorno il nostro cervello si svilupperà abbastanza da riuscire a gestire flussi di informazione continui e massicci come quelli generati dai social, ma per ora ritengo che avere milioni di "amici" di cui nemmeno conosci il vero nome o il vero volto, con cui scambi prevalentemente faccine buffe, battutine e frasi sconnesse di pochi caratteri non sia particolarmente costruttivo.

E tu, Gabriele?

Lo utilizzo tantissimo come strumento di lavoro, passando dalla ricerca di immagini che possano ispirarmi per realizzare un nuovo disegno all'avere la possibilità di inviare e ricevere materiali

riguardo ai progetti in corso. Poi sono altrettanto spesso sul web per interagire con gli amici e passare il tempo libero! Negli ultimi anni, a dire il vero, ho smesso di essere un grande "navigatore", ma mi appoggio sempre di più alle piattaforme come Spotify per ascoltare la musica e Netflix per guardare i film, e, ovviamente, ai social network. Appena ho un attimo libero mi collego a Instagram per guardare gli ultimi lavori degli artisti che seguo, ogni tanto postando anche io qualche disegno sul mio profilo. E poi utilizzo un sacco YouTube, spesso come fosse una radio, ascoltando documentari, interviste e vlog e lasciando che i video correlati mi cullino mentre disegno.

Giovanni, hai mai avuto una "brutta avventura" con la Rete?

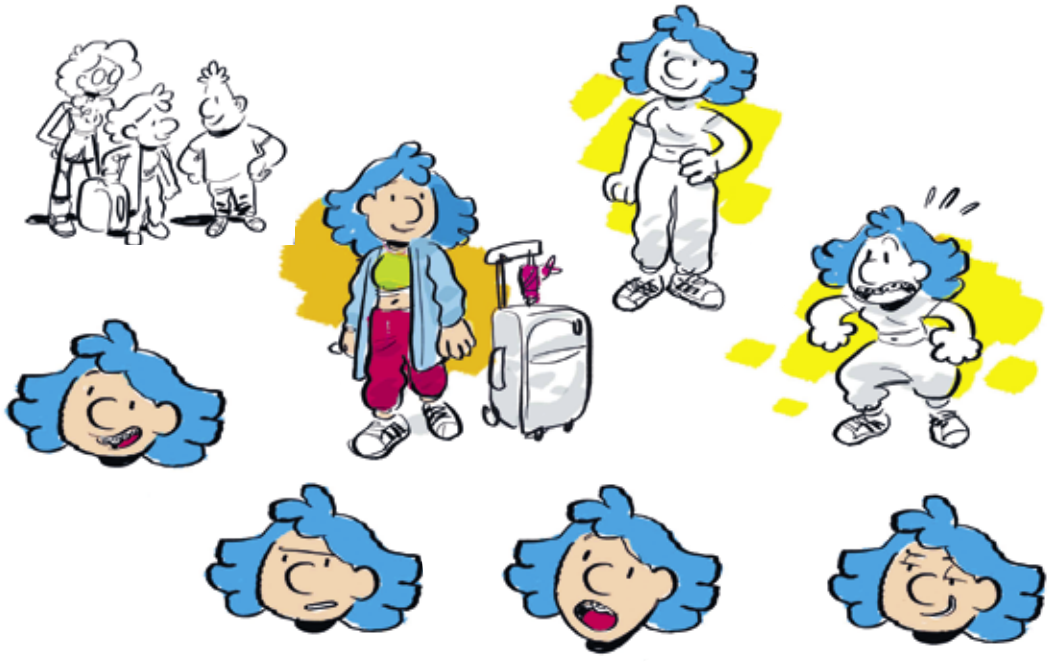
No, ma mi aspetto che prima o poi possa succedere. Non sono mai stato nemmeno rapinato per strada, però quando esco di casa lo metto in conto. È la vita, l'unica cosa che si può fare in proposito è mantenere un minimo di prudenza: se esco alle due di notte in zona Stazione Centrale a Milano in genere evito di sventolare biglietti da cento euro; se vado su Internet evito di cliccare su banner equivoci, anche se promettono di farmi diventare ricco o di ingrandire le mie naturali dotazioni anatomiche.

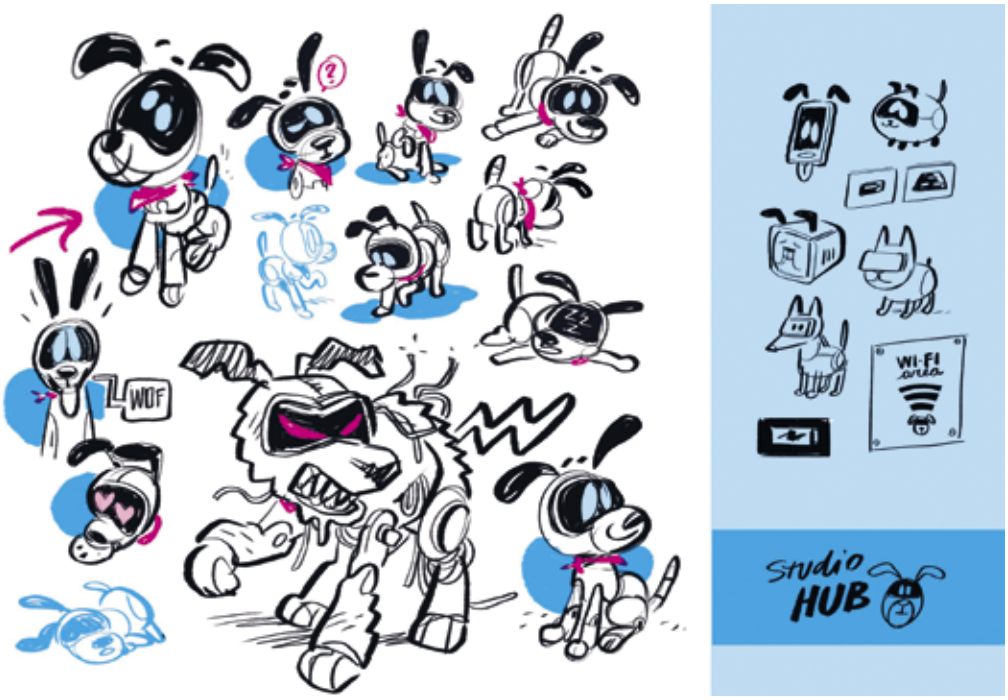
Perché sorridi, Gabriele?

Anche io come Nabbo qualche volta in passato per vedere un film di Ciak Morris sono stato in difficoltà a riconoscere quale finestra chiudere tra i cento pop-up che si aprono o quale tasto "play" spingere, ma per fortuna non ho mai avuto particolari disavventure con la Rete. Per esempio, non ho mai ricevuto fregature negli acquisti online e non ho mai subito attacchi di hacker, ma so che può succedere! Con qualche piccolo accorgimento spero di non avere disavventure da raccontarvi prossimamente.

Gabriele, come vedi il web di domani?

Bella domanda! Mi viene da pensare che dieci anni fa sarebbe stato impossibile prevedere come sarebbe stato il web oggi. C'è un'evoluzione talmente rapida





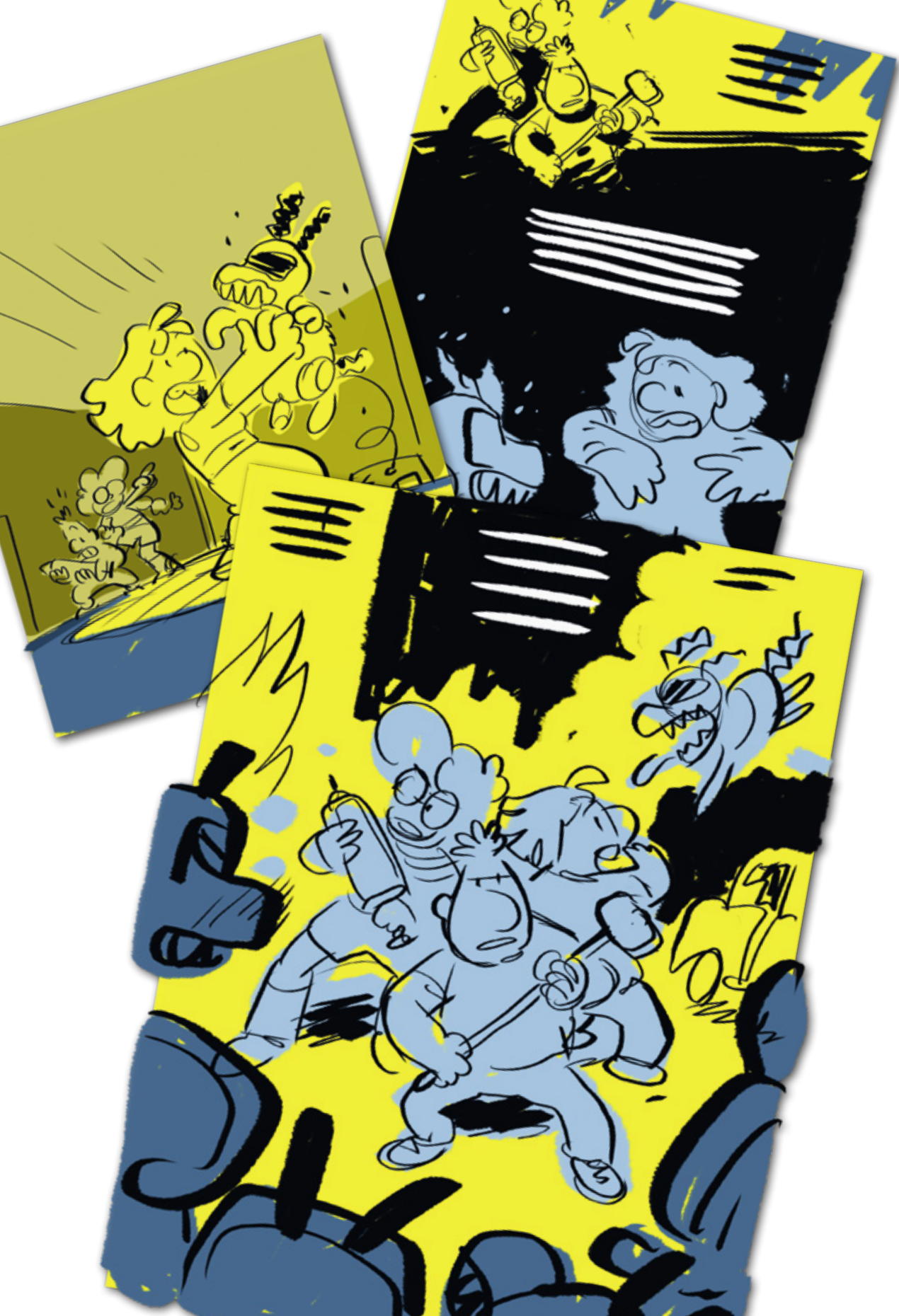
che sinceramente faccio fatica a immaginare come diventerà nel futuro, anche solo prossimo. Ci sono talmente tante direzioni in cui potrebbe andare... e sicuramente ne prenderà diverse. Per esempio, mi viene da pensare che il sistema che oggi vede l'informazione libera e i servizi gratuiti per tutti, in cambio della cessione di dati personali, si esaurirà. Il primo che troverà il modo per rendere il web sostenibile per i creatori di contenuti senza inondare gli utenti di pubblicità, rivoluzionerà il mondo. È solo un'idea... e in ogni modo, qualunque cosa accada, quello che spero è di trovare in futuro un web più costruttivo e positivo proprio perché gestito da chi è cresciuto ed è stato educato per renderlo tale!

E tu, Giovanni?

Che domandona difficile... soprattutto per un amante della privacy e anche un po' orso come me. Mi piacerebbe che fosse un posto in cui vai quando hai voglia, senza che nessuno ti obblighi, mettendoti in contatto con chi vuoi.

Ma per come si sta sviluppando adesso, temo che sarà più come avere tutto il mondo a fiatarti sul collo. Mi accontenterei di una via di mezzo.

Le vie di mezzo sono tra le più difficili da trovare sulla grande mappa della vita. Servono metodo, pazienza e grande conoscenza dei luoghi. Quindi bisogna essere preparati per trovare queste vie di mezzo.
Per ora il web ha trovato ed esplorato tutti i suoi eccessi, da quelli legati al marketing più aggressivo, all'azzeramento della privacy, al controllo dei flussi di voto, fino al fenomeno imbarazzante degli Influencer. *Non lo so se può esistere davvero una via di mezzo per la Rete, ma non dovete darmi retta perché io sono un musone pessimista.*
Detesto il mondo degli adulti, ma nutro grandissime speranze per le nuove generazioni, ecco perché un fumetto come Nabbovaldo, *può essere molto utile per trovare, un domani, questa famosa via di mezzo di cui parliamo. E mi auguro che, un "dopodomani", ci sia un social media manager che si ricordi di quello che ha letto su queste pagine quando era a scuola e che non ripeta gli stessi errori commessi nel passato.*

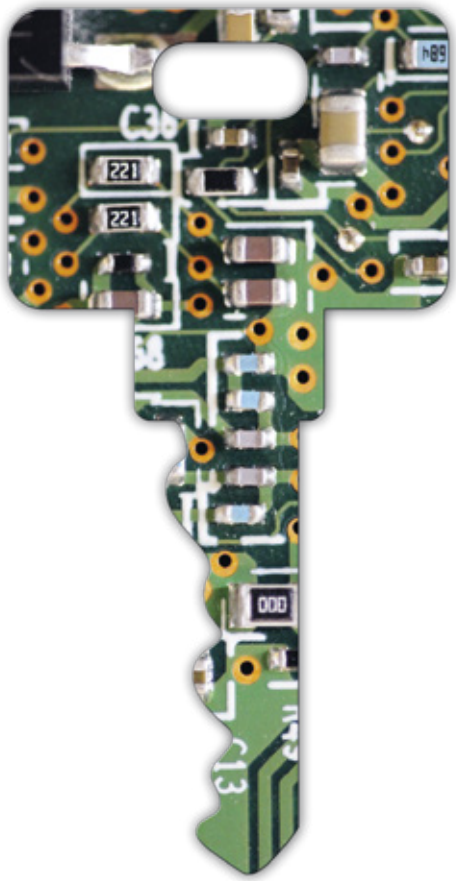


La **sicurezza informatica** è possibile?
Come difendersi nell'era
degli attacchi informatici e
dei ***data breach***.

Copiamo e cifriamo. Contro il declino dell'Impero

GIOVANNI ZICCARDI

Non è affatto semplice comprendere, oggi, il motivo per cui la sensazione più diffusa, quando si parla di tecnologie, di società dell'informazione e di *big data*, sia di *insicurezza*. La si percepisce sia nelle giovani generazioni che in quelle adulte quando si trascorre del tempo sui social network o si consulta il contenuto di una casella di posta elettronica, ma anche "girando" nei grandi archivi e leggendo i messaggini che transitano sui nostri smartphone. Un timore costante che qualcosa possa andare storto.
Eppure la Cyber Security – la disciplina che studia la sicurezza dei sistemi e dei dati – ha fatto passi veramente da gigante negli ultimi anni; a quanto pare, però, anche le minacce informatiche hanno avuto un'evoluzione che ormai non è facile da contenere.
Il primo problema sembra essere quello dei *big data*: enormi archivi che si rivelano sempre più difficili da proteggere. I *data breach* – gli attacchi ai sistemi che causano la esfiltrazione e fuoriuscita di dati – sono quotidiani e sembra quasi di assistere al declino dell'Impero Romano: quando, nel momento della sua massima espansione, Roma non riuscì più a controllare i suoi confini, iniziò a vedere all'orizzonte il crollo. Oggi i nostri dati viaggiano ovunque, sono presenti in decine di servizi, di dispositivi, di piattaforme. Ma tutti i servizi hanno subito, o stanno subendo, degli incidenti. I data breach colpiscono senza pietà banche, pubbliche amministrazioni, ospedali, università e partiti politici.
L'utente si sente disorientato e inerme di fronte a questa fuga di informazioni che può riguardare anche dati sensibili.
Al contempo, sembra che quotidianamente si verifichino truffe, attacchi a credenziali, frodi e reati informatici di ogni genere.
Come ci si può difendere, allora, in



maniera intelligente, anche al fine di non rinunciare a tutto il bene, alla libertà e agli aspetti positivi delle tecnologie, strumenti che senza dubbio sono ormai indispensabili per crescere?
Innanzitutto, occorrerebbe sempre tener presente che le moderne tecnologie tendono a "ingannare" l'utente facendolo sentire *sicuro* – si potrebbe dire "confidente" – nell'utilizzo di strumenti che, in realtà, non conosce bene. Uno smartphone, un tablet o un portatile sono oggi talmente semplici da usare – e con interfacce talmente intuitive – da far sì che nessuno legga più i manuali e inizi immediatamente a lavorare, con la convinzione di conoscere a fondo la macchina. In realtà, un approccio di questo tipo rivela diverse vulnerabilità quando il sistema non reagisce come ci aspetteremmo o quando siamo noi, per primi, a tenere comportamenti e azioni che mettono in pericolo la sicurezza dei nostri stessi dati.
Investire tempo in una cultura dell'informatica, in una conoscenza approfondita dei software e dei sistemi che usiamo quotidianamente, diventa la base per essere più sicuri e per evitare sorprese. Essere un po' hacker, insomma, e non fermarsi alla superficie, visto che nel nostro ambiente "conoscenza" significa "sicurezza".
Un secondo punto importante riguarda i comportamenti. Purtroppo, anche la tecnologia più sicura diventa inutile e vulnerabile se si sbagliano i comportamenti. Oggi le tecnologie che usiamo sono molto sicure, le più sicure mai prodotte: chi attacca cerca allora di convincerci a tenere comportamenti che mettano a rischio i sistemi e che aprano delle "porte". Si preferisce attaccare il nostro *cervello* piuttosto che le nostre macchine, cercando di convincerci a tenere un determinato comportamento. Questo è il motivo per cui quasi tutti i virus, le email di *phishing* e le trappole in Rete ci domandano di fare qualcosa: aprire un allegato, cliccare su un link, comunicare a qualcuno le nostre credenziali, inoltrare un messaggio. Ogni utente dovrebbe avere, in questi casi, un livello di paranoia molto alto (la paranoia, nell'ambito della sicurezza, va intesa come una virtù). "Paranoia" significa non fare ciò che sembra sospetto, fermarsi quando qualcosa stona, diffidare di qualsiasi richiesta.
Già dalla giovane età bisognerebbe essere in grado di individuare i *segnali di allarme* che possono rivelare la presenza di un tentativo di attacco informatico. Se si tratta di una email, i segnali di allarme possono essere che non sia attesa o annunciata, o che sia scritta in un italiano incerto, o che metta fretta all'utente, cercando di creare tensione per convincerci ad agire senza riflettere. Sono messaggi che prospettano qualcosa di negativo – una multa, un blocco del sistema, un furto di

credenziali – o, al contrario, qualcosa di positivo – la vincita di un premio, la possibilità di entrare in possesso di una somma di denaro – ma i toni sono appositamente scelti per metterci in agitazione, per convincerci ad agire in fretta, senza pensarci.
Mai come in questi anni la sicurezza informatica è strettamente legata al fermarsi a riflettere, alla necessità di pensare, ragionare e – speriamo – magari confrontarsi con esperti prima di prendere delle decisioni che possano mettere il sistema in pericolo.
Un altro aspetto spesso sottovalutato è che oggi gli attacchi possono essere *mirati* alla nostra persona, visto che i dati che ci riguardano sono spesso disponibili online. Gli attacchi mirati sono molto più pericolosi, perché il messaggio che ci perviene è appositamente creato per toccarci nel personale: si riferisce a qualcosa che è vero e, quindi, ci porta istintivamente a rispondere.
È semplice, oggi, preparare un attacco raccogliendo informazioni relative a una persona sui social network o sul suo sito. Siamo nell'era dell'esposizione dei propri dati personali – e quindi, secondo alcuni, della morte della privacy – e *profilare* un soggetto prima di attaccarlo diventa ogni giorno più semplice.
Uno dei metodi migliori per proteggersi è il *backup* costante dei dati. Si tratta di un rimedio semplice ma assolutamente fondamentale: significa avere sempre i propri dati in due o tre luoghi diversi così che, in caso di attacco a uno di questi luoghi, ci siano sempre dei dati disponibili da un'altra parte.
Insieme al backup, la cifratura dei dati ("crittografia") su tutti i nostri dispositivi – computer, smartphone, tablet, chiavette USB e dischi esterni, spazi sul *cloud* – è vista oggi come l'arma più efficace per difendersi, tanto da essere prevista esplicitamente anche dal recente Regolamento Europeo per la protezione dei dati.
Cultura e conoscenza, quindi, ma anche diffidenza (tanta), riflessione costante su ogni messaggio che riceviamo, protezione dai virus, backup e cifratura delle informazioni, sempre.
E accanto alle protezioni tecniche, valutare sempre ogni nostro comportamento, che costituisce sempre di più l'anello debole dell'intero sistema.

Ci aspettano al varco di ogni clic
su PC, Tablet e Smartphone.
Tipologie, comportamenti e provenienza
dei **pericoli online**.

Di malware in peggio: evitare si può

ANDREA SARACINO

I **malware**, contrazione di "MALicious softWARE", sono il mezzo più comune per attaccare un sistema informatico. I malware sono programmi che nascondono al loro interno istruzioni dannose per il dispositivo su cui vengono eseguiti e potenzialmente per i dispositivi collegati. I malware, infatti, possono colpire diversi tipi di dispositivi, dai computer agli smartphone e alle auto, oltre ai macchinari industriali interconnessi. Per capire in che modo possano essere dannosi, parleremo delle principali tipologie di malware esistenti e del loro comportamento.

Spyware: tipo di malware estremamente comune e dal comportamento molto subdolo. Gli spyware, infatti, non si manifestano all'utente e non hanno comportamenti che alterino le funzionalità del dispositivo. Tuttavia, raccolgono continuamente informazioni più o meno private che riguardano l'utente e il suo dispositivo, inviandole a un computer gestito dall'attaccante. A seconda dell'aggressività e delle debolezze che riesce a sfruttare, uno spyware può acquisire documenti privati dell'utente, liste di contatti email, abitudini dell'utente e configurazioni di sistema. Inoltre uno spyware può anche prendere il controllo della webcam (se presente), raccogliendo foto e video dell'utente, della tastiera e dello schermo. In questo modo, oltre ad ottenere i programmi e i siti web visitati dall'utente, è anche possibile ottenere username e password, che possono essere poi usati dall'attaccante per impersonare l'utente tramite email, sui social network o persino sui servizi di *e-banking*. Gli spyware sono molto presenti sia sui computer che sugli smartphone. Su questi ultimi, in particolare, possono avere accesso a un numero ancor maggiore di informazioni

private, come la lista dei contatti e il testo degli SMS, informazioni che gli attaccanti riescono a rivendere ad alto prezzo ad aziende interessate a fare pubblicità mirata.
Adware: letteralmente i malware della pubblicità (indesiderata). È molto facile esserne infettati navigando online, soprattutto su siti che offrono contenuti pirata. Una volta installati, questi malware modificano le impostazioni del browser, in modo da costringerlo a puntare sempre su siti commerciali. Aprono automaticamente nuove finestre (*pop up*) che tentano di vendere i prodotti più disparati, alcune delle quali propongono anche di scaricare software per rimuovere virus (altro modo tipico ma errato di riferirsi ai malware). Il software scaricato si rivela poi essere a sua volta un malware , afferente a una qualsiasi delle tipologie qui descritte. Su smartphone e tablet, gli adware risultano ancora più fastidiosi, poiché prendono il controllo della barra delle notifiche, bombardando l'utente di informazioni spazzatura e consumando rapidamente la batteria e il traffico di rete disponibile.
Bot: anche questo malware, come gli spyware, agisce in silenzio. Questi malware aprono una *backdoor* , una "porta sul retro" per l'attaccante, ossia un canale Internet tramite cui l'attaccante può inviare istruzioni. I computer infettati prendono il nome di "Zombi" o "Bot" (abbreviazione di Robot) e obbediscono all'attaccante, detto anche "Bot Master". I Bot Master puntano in genere a infettare più computer possibili, creando così delle Botnet, reti di computer infetti che eseguono a comando attacchi più complessi. Tramite i Bot, in genere i Bot Master inviano mail di spam (pubblicità non voluta) ad altri utenti, usando l'indirizzo di posta della vittima ignara, oppure aprono in continuazione connessioni a determinati siti web allo scopo di saturare di richieste il destinatario. Quest'ultimo attacco viene portato avanti in maniera coordinata da un'intera Botnet, in modo da generare abbastanza richieste da rendere irraggiungibile il sito vittima. Si parla in questo caso di "Denial of Service" (DoS). La cosa peggiore è che in questo modo l'attacco ha successo senza alcun rischio per l'attaccante, che si nasconde dietro i Bot, gli esecutori materiali.
Ransomware: tristemente noti negli ultimi anni, questi malware prendono il controllo del dispositivo infettato chiedendo all'utente di pagare un riscatto "ransom" per ripristinare le normali funzionalità. Una loro variante molto diffusa sui computer sono i *cryptolocker*, malware che una volta in esecuzione iniziano a crittografare tutti i file personali dell'utente (documenti, foto, fogli di calcolo, etc.), rendendoli di fatto inaccessibili. La restituzione dei file o della funzionalità del dispositivo è soggetta al pagamento di una somma in denaro da corrispondere in moneta virtuale, generalmente *Bitcoin*. I pagamenti effettuati in questa valuta possono infatti essere resi non tracciabili, proteggendo così l'attaccante. Questo malware è particolarmente insidioso poiché, soprattutto nel caso dei cryptolocker, non esiste alcun intervento che funzioni a posteriori: se non si paga il riscatto, i file sono persi per sempre. Inoltre, non vi è alcuna garanzia che a seguito del pagamento venga effettuata la restituzione dei file o del dispositivo. Questo accade soprattutto per i dispositivi mobili, dove piuttosto che cifrare i file, si preferisce bloccare l'accesso al dispositivo, mostrando

continuamente una schermata che chiede di pagare il riscatto e non consente l'accesso a nessun'altra funzionalità. In questo caso, fare il reset del dispositivo alle condizioni di fabbrica è l'unica soluzione efficace. Per i cryptolocker, invece, si può prevenire il danno con un backup periodico dei dati su un'altra unità di memoria, come un secondo hard disk o uno spazio su cloud.
I malware possono arrivare tramite diversi canali. Su smartphone e tablet il canale principale sono le App, ed è molto facile rimanere infettati se le App provengono da *marketplace* diversi da Google Play per Android e da Apple Store per iPhone. Per quanto riguarda i computer, i malware possono arrivare sempre sotto forma di applicazioni, mandando in esecuzione programmi non affidabili e non certificati, come ad esempio le applicazioni crackate. Queste ultime possono essere particolarmente pericolose in quanto possono comportarsi come Cavalli di Troia (*Trojan*). I Trojan sono infatti applicazioni che si comportano esattamente come si aspetta l'utente, eseguendo per esempio un videogioco, ma che in *background* eseguono anche istruzioni dannose senza che l'utente se ne accorga. Molti Spyware e Bot infettano i computer usando un Trojan.
Anche i file scaricati da Internet possono essere vettori di infezione. I malware si possono nascondere infatti anche dentro documenti o immagini che sfruttano le vulnerabilità dei programmi installati per portare avanti un attacco. Sono pericolosi anche i *plug-in* o le estensioni dei *browser*, che devono quindi essere aggiunti solo se necessari e dopo aver verificato l'identità del fornitore.
Altro canale praticato sono gli allegati delle email. Bisogna sempre diffidare di quelle che invitano ad aprire un allegato, quando il mittente non è noto, perché questo potrebbe eseguire un'applicazione malevola.
Un altro vettore di malware sono i sistemi operativi non aggiornati. Infatti, nuove vulnerabilità vengono scoperte ogni giorno e gli attaccanti possono sfruttarle per inserire via Internet dei malware nel dispositivo. Avere sempre il sistema operativo aggiornato minimizza la probabilità che l'attaccante riesca a trovare vulnerabilità utili ai suoi scopi.
Unendo questa accortezza a quelle sopracitate, secondo cui bisogna fare attenzione alla provenienza dei file che vengono scaricati e aperti, e aiutandosi magari con un programma antivirus, si rende più difficile il lavoro dell'attaccante e si riduce al minimo la possibilità di rimanere vittima di un attacco.

www.edizioni.cnr.it