APRILE 2026
NUMERO 5

AttentiOnline Junior



BENVENUTI SU ATTENTIONLINE JUNIOR: IL TUO SCUDO DIGITALE!

Cari ragazzi, genitori e insegnanti,

Siamo felicissimi di presentarvi **Attentionline Junior**, la nuova sezione del nostro sito pensata appositamente per i giovani esploratori del web delle scuole elementari e medie!

Internet è come un grande parco giochi pieno di opportunità: puoi imparare cose nuove, divertirti con i giochi, chattare con gli amici e scoprire mondi fantastici. Ma proprio come in un parco reale, anche online è importante conoscere le regole di sicurezza per evitare piccoli e grandi pericoli.

Cosa troverai su Attentionline Junior?

Abbiamo creato uno spazio colorato e divertente dove imparare a navigare in sicurezza diventa un gioco! Troverai:

- **Rebus e giochi "trova le differenze"** con immagini sulla sicurezza online: perché imparare divertendosi è il modo migliore per ricordare!
- **Guide semplici e chiare** per creare password sicure che proteggano i tuoi account come un vero scudo.
- **Un glossario speciale** con tutte le parole della sicurezza spiegate in modo semplice.
- **Fumetti e storie** con protagonisti che affrontano le stesse situazioni che potresti incontrare tu.
- **Video tutorial** creati appositamente per la tua età.



Perché Attentionline Junior?

Abbiamo notato che sempre più giovani navigano in internet a età sempre più precoci. Smartphone, tablet e computer sono strumenti fantastici, ma è importante imparare a usarli in modo sicuro fin da subito. Il nostro obiettivo è rendere i ragazzi consapevoli e preparati, trasformandoli in veri "supereroi digitali"!
E ricorda: non sei mai troppo piccolo per essere attento e responsabile online!

Per genitori e insegnanti

Una sezione speciale sarà dedicata a voi adulti, con consigli pratici su come accompagnare i ragazzi nel mondo digitale, suggerimenti per il parental control e materiale didattico da utilizzare in classe o a casa.

Unisciti a noi in questa fantastica avventura digitale. **Attentionline Junior** è il posto dove la sicurezza online diventa un gioco da ragazzi!

CHE COSA E' L'INTELLIGENZA ARTIFICIALE?

Sara ha dieci anni e un pomeriggio, mentre fa i compiti, si trova bloccata su una domanda di storia. Prende il tablet e scrive su Google: "quando è caduto l'Impero romano d'Occidente". In meno di un secondo appaiono decine di siti, enciclopedie, pagine di Wikipedia, articoli di giornale. Google le mostra tutto quello che ha trovato sul web riguardo a quella frase, e lei sceglie il risultato che le sembra più affidabile. Problema risolto.

Il giorno dopo, invece, la sua insegnante fa vedere alla classe uno strumento nuovo: un chatbot con intelligenza artificiale. Sara digita la stessa domanda, ma questa volta invece di ricevere una lista di siti, riceve una risposta scritta direttamente, come se qualcuno gliel'avesse spiegata a voce. Quasi come se stesse parlando con qualcuno.

Sara si ferma a pensare: ma questi due strumenti non sono la stessa cosa? No, non lo sono. E capire la differenza è più importante di quanto sembri.

Google cerca, l'intelligenza artificiale risponde



Quando scrivi qualcosa su Google, il motore di ricerca fa una cosa sola, ma la fa molto bene: va a cercare in un archivio enorme, grande quanto quasi tutta la parte pubblica di internet, e ti porta i risultati che corrispondono meglio a quello che hai scritto. Non "pensa", non "capisce", non "elabora". Classifica e mostra. È come chiedere a un bibliotecario di cercare tutti i libri che parlano di un certo argomento: lui ti porta i libri, ma sei tu a doverli leggere e capire.

L'intelligenza artificiale funziona in modo completamente diverso. Non cerca pagine già scritte da qualcun altro, ma genera una risposta nuova, costruita nel momento in cui gliela chiedi. È come se invece del bibliotecario ci fosse un professore che ha letto milioni di libri, li ha studiati tutti, e ora è in grado di spiegarti le cose con parole sue, adattandosi a come gli fai le domande.

Ovviamente non c'è davvero nessun professore dentro al computer. Ma come funziona allora?

Come impara una macchina

Immagina di dover imparare a riconoscere i gatti. All'inizio non ne hai mai visto uno. Ti mostrano una foto e ti dicono: "Questo è un gatto." Poi un'altra: "Anche questo è un gatto." Poi una foto di un cane: "Questo non è un gatto." Dopo migliaia e migliaia di esempi, il tuo cervello ha capito le caratteristiche di un gatto: le orecchie appuntite, i baffi, la forma del muso. Adesso, anche se ti mostrano un gatto che non hai mai visto prima, riesci a riconoscerlo.

L'intelligenza artificiale impara più o meno nello stesso modo, solo che invece di guardare foto di gatti, ha "letto" una quantità incredibile di testi: libri, articoli, enciclopedie, conversazioni, siti web, dizionari, romanzi, manuali scientifici. Miliardi e miliardi di parole. Studiando tutti questi testi, ha imparato come le parole si collegano tra loro, come si costruiscono i ragionamenti, come si risponde a una domanda, come si racconta una storia.

Quando tu le scrivi qualcosa, lei non va a cercare quella cosa da nessuna parte. Costruisce la risposta basandosi su tutto quello che ha imparato. Proprio come farebbe un essere umano che ha studiato tanto.

La differenza che cambia tutto

Questa differenza, apparentemente tecnica, ha conseguenze pratiche molto importanti nella vita di tutti i giorni.

Con Google, puoi sempre cliccare sul sito e andare a controllare la fonte. Se la risposta è sbagliata o il sito non è affidabile, puoi accorgertene. Con l'intelligenza artificiale la risposta ti arriva già pronta, senza un link da controllare, senza una fonte che puoi verificare subito. Questo la rende molto comoda, ma anche un po' più insidiosa: devi fidarti di più, e questo richiede più attenzione.

C'è anche un'altra cosa importante da sapere: l'intelligenza artificiale può sbagliare. Non lo fa per cattiveria, ovviamente, ma perché i suoi "studi" hanno una data di fine, e dopo quella data non sa cosa è successo nel mondo. Inoltre, a volte può costruire una risposta che sembra perfetta ma che contiene un errore, esattamente come può fare uno studente che ha imparato una cosa in modo non del tutto corretto. Per questo motivo, quando usi questi strumenti per fare ricerche, è sempre bene verificare le informazioni importanti anche su altri siti o libri.

Non è magica, non è umana, ma è potente

Una cosa che spesso sorprende i ragazzi è che l'intelligenza artificiale non "capisce" le cose nel senso in cui le capiamo noi. Non prova curiosità, non si annoia, non è felice quando risolve un problema difficile. Elabora. Lo fa in modo straordinariamente sofisticato, così sofisticato che il risultato sembra quasi umano, ma sotto sotto è sempre e solo matematica e statistica applicata al linguaggio.

Questo non vuol dire che non sia utile, anzi. L'intelligenza artificiale può aiutarti a capire argomenti difficili spiegandoteli in modo diverso, può correggere i tuoi testi, può tradurre, può aiutarti a trovare idee quando sei bloccato. È uno strumento potente, come lo è un telescopio o un microscopio. Il punto è imparare a usarla nel modo giusto.

E il modo giusto inizia proprio da quello che ha capito Sara quel pomeriggio: non dare mai per scontato che la risposta di una macchina sia sempre corretta solo perché è scritta bene. Il pensiero critico, quello che ti fa chiedere "ma sarà vero?", è ancora e sempre il tuo superpotere più grande. Nessuna intelligenza artificiale potrà mai sostituirlo.

Lo sapevi?

Il nome "intelligenza artificiale" esiste da più di settant'anni. Lo usò per la prima volta uno scienziato americano di nome John McCarthy nel 1956, durante una conferenza universitaria. All'epoca i computer erano grandi come intere stanze e riuscivano a fare pochissime cose. McCarthy sognava macchine capaci di ragionare come gli esseri umani. Ci sono voluti decenni di ricerca, migliaia di scienziati in tutto il mondo e una quantità enorme di energia elettrica per arrivare agli strumenti che usiamo oggi.

Il nome "Google" invece viene da una parola matematica: "googol", che indica il numero 1 seguito da cento zeri. I suoi fondatori, due studenti universitari di nome Larry Page e Sergey Brin, lo scelsero nel 1998 per dare l'idea di una quantità immensa di informazioni. Fecero però un piccolo errore di ortografia quando registrarono il dominio, e "googol" diventò "Google". Quell'errore di battitura è oggi uno dei nomi più famosi del mondo.

Un'ultima curiosità: ogni giorno su Google vengono effettuate circa 8,5 miliardi di ricerche. Significa che mentre tu stai leggendo questa frase, in tutto il mondo qualcuno ha già cercato qualcosa su Google almeno un milione di volte.



Sei sempre in vetrina: la tua posizione è un segreto che vale oro

Emanuele ha tredici anni e ogni mattina, prima di uscire di casa, controlla il telefono. Posta una storia su Instagram con la scritta "finalmente venerdì!", poi apre Maps per vedere quanto ci vuole ad arrivare a scuola con la bici. Nel pomeriggio gioca a un gioco sul telefono che gli aveva chiesto, qualche settimana fa, di "accedere alla posizione" e lui aveva premuto "consenti" senza pensarci troppo. La sera, mentre guarda un video su YouTube, arriva una notifica da un'app meteo: "Pioggia prevista nella tua zona domani mattina."

Emanuele non se n'è mai accorto, ma durante quella giornata almeno sei applicazioni diverse sapevano esattamente dove si trovava. Non in modo approssimativo, non "in Italia" o "a Milano". Sapevano il nome della sua via, a quale isolato si trovava, a che ora era uscito di casa e a che ora era tornato.

Questo si chiama geolocalizzazione. Ed è una delle cose più importanti che devi imparare a gestire sul tuo telefono.

Come funziona: il tuo telefono sa sempre dove sei

Il tuo smartphone conosce la tua posizione grazie a tre sistemi che lavorano insieme, spesso senza che tu te ne accorga.

Il primo è il GPS, che sta per Global Positioning System. È una rete di satelliti che girano intorno alla Terra e che comunicano continuamente con il tuo telefono. Incrociando i segnali di almeno tre satelliti diversi, il telefono riesce a calcolare dove si trova con una precisione di pochi metri. È lo stesso sistema che usano le navi e gli aerei per navigare, solo che adesso ce l'abbiamo tutti in tasca.

Il secondo sistema usa le reti Wi-Fi. Ogni router Wi-Fi, quello di casa tua, quello del bar sotto casa, quello della scuola, ha un codice identificativo unico. Nel tempo, le grandi aziende tecnologiche hanno mappato la posizione di milioni di router in tutto il mondo. Quando il tuo telefono "vede" una rete Wi-Fi nei dintorni, anche se non ci sei connesso, può capire dove si trova incrociando quella informazione con la mappa che ha in memoria.



Il terzo sistema si basa sulle antenne della rete telefonica. Anche senza GPS e senza Wi-Fi, il tuo telefono è sempre in contatto con le antenne del gestore telefonico. Triangolando il segnale tra più antenne vicine, è possibile capire in quale zona ti trovi, anche se con meno precisione rispetto al GPS.

Questi tre sistemi insieme fanno sì che il tuo telefono sappia quasi sempre dove sei, in qualsiasi momento della giornata.

Perché le app vogliono sapere dove sei

Alcune app hanno bisogno della tua posizione per funzionare davvero. Google Maps senza geolocalizzazione sarebbe praticamente inutile. Un'app meteo ha senso solo se sa in quale città ti trovi. Il navigatore della macchina di papà non potrebbe guidarvi da nessuna parte senza sapere da dove partite.

Il problema nasce quando app che non ne avrebbero bisogno chiedono comunque l'accesso alla tua posizione. Un gioco di carte ha bisogno di sapere dove sei? No. Un'app per fare gli esercizi di matematica deve conoscere il tuo indirizzo? Assolutamente no. Un'app per suonare suoni divertenti ha qualcosa a che fare con la tua posizione? Nemmeno lontanamente.

Eppure queste app la chiedono lo stesso. E la ragione, quasi sempre, è che la tua posizione vale denaro. Sapere dove si trovano milioni di persone, a che ora, per quanto tempo, è un'informazione preziosissima per le aziende che fanno pubblicità. Sanno che ogni mattina passi davanti a una certa pizzeria, e ti manderanno la pubblicità di quella pizzeria proprio mentre ci passi davanti. Sanno che ogni sabato vai in palestra, e ti proporranno abbonamenti sportivi. La tua posizione racconta la tua vita, e c'è chi è disposto a pagare per saperlo.

I pericoli che non si vedono subito

Fin qui sembra quasi una questione tra adulti, qualcosa che riguarda la pubblicità e le grandi aziende. Ma i rischi legati alla geolocalizzazione per i ragazzi sono molto più concreti e molto più vicini di quanto sembri.

Il primo pericolo è rivelare dove abiti senza rendertene conto. Quando pubblichi una foto dal tuo giardino, dalla tua finestra o davanti al portone di casa, stai già dando molte informazioni sulla tua posizione. Ma se quella foto ha anche i dati di geolocalizzazione incorporati, chiunque la scarichi può sapere con precisione le coordinate esatte di casa tua. Molti telefoni, per impostazione predefinita, salvano questi dati nelle foto senza che l'utente lo sappia. Si chiamano dati EXIF e sono invisibili nell'immagine, ma sono lì.

Il secondo pericolo riguarda i tuoi spostamenti abituali. Se ogni mattina la tua posizione viene registrata dall'app X alle 8:15 in via Garibaldi e alle 8:35 davanti alla scuola media Manzoni, chiunque abbia accesso a quei dati conosce il tuo percorso quotidiano, i tuoi orari, le tue abitudini. Sa a che ora esci, quale strada fai, quando torni. Sono le stesse informazioni che un genitore attento non darebbe mai a uno

sconosciuto, eppure vengono condivise silenziosamente ogni giorno.

Il terzo pericolo riguarda i giochi online e i social. Alcuni giochi per smartphone mostrano su una mappa i giocatori vicini a te, proprio per spingerti a incontrarli. Funzionalità simili esistono su certi social network. L'idea sembra divertente, ma significa che persone che non conosci possono vedere in tempo reale dove ti trovi. E non sempre chi c'è dall'altra parte è davvero un coetaneo con buone intenzioni.

Il quarto pericolo è più sottile ma altrettanto importante: la geolocalizzazione continua scarica la batteria del telefono molto più velocemente e utilizza i dati della tua connessione. Non è un rischio per la sicurezza personale, ma è un buon motivo in più per tenere attiva la posizione solo quando serve davvero.

Come difendersi: tre regole che fanno la differenza

La prima regola è controllare i permessi delle app. Sia su iPhone che su Android puoi vedere, nelle impostazioni, quali app hanno accesso alla tua posizione. Troverai tre opzioni: "mai", "solo mentre uso l'app" e "sempre". Per quasi tutte le app la scelta giusta è "solo mentre uso l'app". L'opzione "sempre" va concessa solo a quelle che hanno davvero bisogno di sapere dove sei anche quando sono chiuse, come certe app di sicurezza familiare concordate con i genitori. A tutto il resto, "mai" o "solo mentre uso l'app" è più che sufficiente.

La seconda regola è disattivare la geolocalizzazione nelle foto. Nelle impostazioni della fotocamera del tuo telefono puoi disabilitare il salvataggio dei dati di posizione nelle immagini. È una piccola modifica che risolve in modo definitivo il problema dei dati EXIF. Una volta fatto, le tue foto non porteranno più con sé le coordinate di dove sono state scattate.

La terza regola è la più semplice e la più potente: quando non stai usando attivamente la navigazione o un'app che ha bisogno della posizione, tieni il GPS spento. Si accende in pochi secondi quando ti serve, e nel frattempo nessuna app può tracciarti.

Emanuele, alla fine di quella giornata, non sapeva di essere stato seguito da sei app diverse. Adesso lo sai tu. E sapere è sempre il primo passo per proteggere se stessi.

RINGRAZIAMENTI A DAVIDE MOROSINOTTO

In questo numero abbiamo una sorpresa davvero speciale per voi!

L'articolo che state per leggere non è scritto da una persona qualsiasi… ma da Davide Morosinotto, uno scrittore vero, di quelli che inventano storie avventurose, misteriose e piene di colpi di scena!

Forse qualcuno di voi ha già sentito il suo nome: Davide ha scritto tanti libri per ragazzi letti in tutto il mondo, e uno dei più famosi è Il rinomato catalogo Walker & Dawn.
Ma non solo: si occupa anche di temi importanti per chi cresce oggi, come internet e i social.

Infatti ha scritto anche Cyberbulli al tappeto, un libro che spiega come difendersi dal cyberbullismo. E sapete una cosa? Scrive anche per Focus Junior!

Quando gli abbiamo chiesto di darci una mano per AttentiOnline Junior, ha trovato il tempo (anche se è sempre super impegnato!) per scrivere un articolo proprio per voi: un vero regalo!

Quello che leggerete tra poco è importante, perché parla di qualcosa che può capitare a tutti: il bullismo e il cyberbullismo. Ma non lo fa per spaventare… lo fa per aiutarvi a capire, a difendervi e a non sentirvi mai soli. Quindi… pronti? Si sale sul ring! Buona lettura!



Immaginati di salire su un ring. Proprio uno di quelli dove si combatte, arti marziali o boxe o wrestling. Probabilmente non ne hai mai visto uno davvero, ma immagina di salirci. Immagina anche di avere addosso dei vestiti da combattimento, guantoni, pantaloncini eccetera. Perché… ebbene sì… sta per cominciare un incontro!

È facile che ti stia venendo un po' di tremarella, giusto? Combattere fa paura, e l'idea di prendersi un pugno non piace a nessuno.

Soprattutto perché, beh, tu hai un punto debole: soffri tantissimo il solletico al fianco sinistro. Se solo qualcuno prova a sfiorarti lì a sinistra, ti butti a terra e cominci a ridere e non puoi controllarti.

Purtroppo, qualcuno ti ha disegnato una freccia che indica proprio il fianco sinistro. Accidenti. Combattere così sarà proprio difficile!

È arrivato il momento in cui l'arbitro chiama sul ring il tuo avversario. Che è un… minuscolo, tenerissimo, dolcissimo micetto. Ecco che la paura scompare, giusto? Un micetto non ti preoccupa di sicuro. Però al momento in cui suona il gong, il micetto si trasforma, e diventa una gigantesca tigre! Questo fa molta, molta paura.

E adesso immagina che però l'arbitro ti permetta di chiamare sul ring chi vuoi ad aiutarti. Per esempio tre tuoi amici, per farti coraggio, e una veterinaria che ha un bel fucile a sonnifero per addormentare la tigre…

Okay, l'ho tirata anche troppo per le lunghe, mi fermo qui. Ma che tu ci creda o no, fino a questo momento, ti stavo parlando di cyberbullismo. E di come difendersi. Perché alla fine, il cyberbullismo (e il bullismo) assomiglia proprio molto a un combattimento. Un combattimento in cui magari ti trascinano controvoglia, ma quando vieni attaccata o attaccato, beh, devi difenderti. E come si fa?

Il primo modo è, ovviamente, non rivelare al tuo avversario i tuoi punti deboli, le cose che possono essere sfruttate contro di te per "farti male": per esempio i dati sensibili, dove abiti, in che scuola vai, il tuo numero di telefono, eccetera. Sono tutte informazioni che potrebbero essere usate contro di te, e più le proteggi e più ti senti al sicuro.

Il secondo modo è diventare più forte di chi sta cercando di attaccarti. Per esempio, chiedendo aiuto a qualcuno (la veterinaria del mio esempio) che possa mettersi al tuo fianco. Come i tuoi genitori, degli amici, un insegnante. I bulli, e i cyberbulli, sono bravissimi a farti credere di essere delle tigri, ma se vedono che sai difenderti spesso scappano e diventano dei… micetti.

Quindi, non devi averne paura. E tieni sempre alta la guardia!

TROVA I PERICOLI – IL PHISHING: "Hai vinto un milione di euro!"

Martina ha undici anni e quel pomeriggio stava usando il tablet di sua mamma per guardare un video di cucina, perché aveva deciso che avrebbe preparato i pancake da sola per la prima volta. Ma mentre cercava la ricetta, le arrivò una notifica. Era un messaggio, con un mittente che non riconosceva, e la scritta era in grassetto, tutta maiuscola: "CONGRATULAZIONI! Hai vinto un milione di euro. Clicca qui entro 24 ore per riscuotere il premio."

Martina rimase ferma a fissare lo schermo. Un milione di euro. Sua mamma aveva il tablet, quindi forse era sua mamma ad aver vinto. Oppure no, magari erano lei. Rimase lì a pensarci, con il dito già pronto sul link, e poi si fermò. Qualcosa non tornava. Ma cosa esattamente?

Quando è troppo bello per essere vero, quasi sempre non è vero

La prima cosa che non tornava era la più semplice: Martina non aveva partecipato a nessun concorso. Non si vince un milione di euro senza aver fatto niente, senza essersi iscritti da nessuna parte, senza aver comprato un biglietto. Eppure quel messaggio diceva che aveva vinto. Come è possibile vincere qualcosa a cui non hai mai partecipato?

Non è possibile. E questa è la prima regola d'oro per riconoscere una truffa online: se ti arriva un messaggio che ti dice che hai vinto qualcosa e tu non ricordi di aver partecipato a nessun concorso, quel messaggio è falso. Punto.

I truffatori lo sanno che la maggior parte delle persone non ha partecipato a nulla. Ma lo sanno anche che la parola "vinto" e la parola "milione" mettono in moto qualcosa nel cervello che fa smettere di ragionare bene. Ci si emoziona, ci si agita, e in quel momento di confusione si clicca su quel link senza pensarci.

Questo tipo di truffa si chiama phishing, una parola inglese che si pronuncia "fishing" e che significa letteralmente "pesca". I truffatori lanciano l'amo — il messaggio falso — e aspettano che qualcuno abbocchi. L'amo può essere un milione di euro, ma anche un pacco in consegna che non esiste, un account bloccato da sbloccare subito, una bolletta non pagata, un regalo da ritirare. Cambia l'esca, ma il meccanismo è sempre lo stesso.

Il link è la trappola!

La seconda cosa che non tornava a Martina era quel "clicca qui". In quasi tutte le truffe online c'è un link su cui cliccare. Perché? Perché cliccando su quel link succedono cose diverse a seconda di come è costruita la truffa.

Alcune volte il link porta a una pagina che sembra uguale a un sito famoso — la pagina della banca, di Amazon, di un ente pubblico — ma in realtà è una copia falsa costruita per ingannare. Se inserisci i tuoi dati lì dentro, nome, cognome, numero di carta, password, li stai consegnando direttamente al truffatore.

Altre volte il link scarica automaticamente un programma nel dispositivo, senza che tu te ne accorga, che poi ruba informazioni o blocca il telefono o il computer. Questi programmi si chiamano malware, un'altra parola inglese che unisce "malicious" (malvagio) e "software" (programma).

Altre volte ancora, la pagina che si apre chiede di "verificare la tua identità" inserendo un codice che ricevi via SMS. Quel codice, in realtà, è quello che la tua banca o un'altra app manda per autorizzare un'operazione importante. Se lo inserisci nella pagina falsa, stai autorizzando qualcosa che non hai deciso tu.

Tutto comincia sempre da quel link. Non cliccare su link che arrivano da mittenti sconosciuti è una delle abitudini più utili che puoi costruire online. Costa zero fatica e salva da un sacco di guai.

Come si riconosce un messaggio falso

Martina, nel dubbio, chiamò sua mamma. E sua mamma le insegnò a guardare alcune cose specifiche, quelle che i truffatori quasi sempre sbagliano o trascurano.

La prima è il mittente. L'indirizzo email o il numero da cui arriva il messaggio quasi mai corrisponde a quello reale dell'azienda o dell'ente che il truffatore finge di essere. Se un messaggio dice di venire dalla tua banca ma l'indirizzo è qualcosa come "premi2026@serviziomail.net", non viene da nessuna banca. Le aziende vere usano indirizzi ufficiali, riconoscibili, con il loro nome nel dominio.

La seconda è la fretta. I messaggi truffaldini quasi sempre cercano di metterti sotto pressione con scadenze brevissime: "entro 24 ore", "solo oggi", "sbrigati o perdi il premio". Questo non è un caso. La fretta è nemica del ragionamento. Se hai solo un'ora per decidere, non hai tempo di chiedere a un adulto, di fare una ricerca, di pensarci su. I truffatori lo sanno benissimo e ci contano.

La terza sono gli errori. Molti messaggi di phishing contengono errori grammaticali, parole storpiate, frasi che sembrano tradotte male da un'altra lingua. Non tutti, però: alcuni sono scritti molto bene. Quindi gli errori possono essere un segnale, ma la loro assenza non significa che il messaggio sia autentico.

La quarta è la richiesta di dati personali. Nessuna azienda seria, nessuna banca, nessun ente pubblico chiede mai password, codici PIN, numeri di carta di credito o dati personali via email o via messaggio. Mai. Se qualcuno li chiede, è una truffa, qualunque cosa dica e qualunque aspetto abbia il messaggio.

Cosa fare quando arriva un messaggio strano

Martina non cliccò. Chiamò sua mamma, le mostrò il messaggio, e insieme decisero di cancellarlo. Fine della storia, senza danni.

Questa è esattamente la cosa giusta da fare: non cliccare, non rispondere, non inserire nessun dato, e parlarne con un adulto di cui ti fidi. Se il messaggio è arrivato sul dispositivo di un genitore, dirglielo è già un gesto importante. Se è arrivato sul tuo telefono o tablet, mostrarlo a un adulto è la mossa più intelligente che tu possa fare.

C'è anche una cosa da non fare, che in pochi sanno: non rispondere mai al messaggio per chiedere chi è o per dire che è una truffa. Rispondere conferma al truffatore che quel numero o quell'indirizzo email è attivo e usato da una persona reale. E questo, per chi fa phishing, è già un'informazione preziosa.

Il milione di euro di Martina non esisteva. Ma la sua capacità di fermarsi un secondo prima di cliccare? Quella

Lo sapevi?

La parola "phishing" nacque intorno al 1996, quando alcuni truffatori informatici americani cominciarono a inviare messaggi falsi cercando di rubare password agli utenti dei primi servizi di posta elettronica. È un gioco di parole con "fishing", che in inglese significa pescare: si lancia l'amo e si aspetta che qualcuno abbocchi.

La prima grande truffa via email della storia si chiamava "la truffa nigeriana": arrivava un messaggio da un fantomatico principe straniero che chiedeva aiuto per spostare una fortuna, promettendo in cambio una percentuale enorme. Milioni di persone ci cascarono. Quella truffa esiste ancora oggi, riadattata in mille versioni diverse. Oggi gli esperti di sicurezza informatica stimano che ogni giorno vengano inviati nel mondo circa tre miliardi di email di phishing. Tre miliardi, ogni giorno.

GIOCHIAMO

CACCIA ALLE SILLABE

In ogni riga c'è una parola con una sillaba mancante. Leggi la definizione, capisci che parola è, poi scrivi la/e sillaba/e mancante/i nella casella vuota. Alla fine, leggi tutte le sillabe scoperte nell'ordine delle righe: formeranno una frase segreta sulla sicurezza online!

PASSWORD E SICUREZZA DEGLI ACCOUNT

#	SILLABA	PAROLA	DEFINIZIONE
1	_ _ _	___NA	*La mamma di tuo papà o di tua mamma*
2	_ _ _	VO___NO	*Quello che fanno gli uccelli e gli aerei quando si alzano nell'aria*
3	_ _ _	ME___A	*La valutazione scolastica calcolata sommando tutti i voti e dividendoli*
4	_ _ _	MA___	*La grande distesa d'acqua salata dove si va a nuotare d'estate*
5	_ _ _	___GENDA	*Il libretto dove si scrivono gli impegni e gli appuntamenti*
6	_ _ _	___POLA	*Piccolo frutto primaverile*
7	_ _ _	___GO	*Il condimento rosso e saporito che si mette sulla pasta*
8	_ _ _	BUO___	*Il contrario di cattivo!*

FRASE SEGRETA

Riscrivi le sillabe trovate nel gioco sopra:

_ _

PRIVACY E DATI PERSONALI

#	SILLABA	PAROLA	DEFINIZIONE
1	_ _ _	___OSTANTE	*parola che si usa quando succede qualcosa anche se c'è una difficoltà o qualcosa che potrebbe impedirlo.*
2	_ _ _	PA___TO	*La parte superiore interna della bocca, tra le gengive e la gola*
3	_ _ _	___RE	*Scendere veloci sulla neve con gli sci ai piedi*
4	_ _ _	FIO___	*La parte colorata e profumata della pianta, che attira le api*
5	_ _ _	___DO	*Il cubo con i puntini da uno a sei che si lancia nei giochi da tavolo*
6	_ _ _	MAT___NA	*Le prime ore del giorno, subito dopo essersi svegliati*
7	_ _ _	___VERNO	*La stagione più fredda dell'anno, quella della neve e del ghiaccio*
8	_ _ _	A___LE	*Veloce e scattante: chi si muove con molta facilità e precisione*
9	_ _ _	___BOT	*Una macchina automatica programmata per svolgere compiti al posto nostro*

FRASE SEGRETA

Riscrivi le sillabe trovate nel gioco sopra:

_ _

GIOCHIAMO

PHISHING E TRUFFE ONLINE

#	SILLABA	PAROLA	DEFINIZIONE
1	_ _ _	___TESA	*La sensazione di chi aspetta qualcosa con ansia e impazienza*
2	_ _ _	IN___SA	*Si dice di un'emozione molto forte, come la paura o la gioia*
3	_ _ _	___PO	*Il piccolo animale grigio che vive nei buchi e ama il formaggio*
4	_ _ _	GU___	*I problemi grossi che ti mettono nei pasticci*
5	_ _ _	___TIERE	*un'attività lavorativa, solitamente di natura manuale o tecnica*
6	_ _ _	___GIO	*Una persona molto esperta e piena di esperienza e conoscenza*
7	_ _ _	MA___	*I tre re che, secondo la tradizione, portarono i doni a Gesù Bambino*
8	_ _ _	___CO	*Il grande uccello rapace dalla vista acutissima e dal volo potente*
9	_ _ _	MU___CA	*L'arte dei suoni: si ascolta, si canta e si suona con gli strumenti*

FRASE SEGRETA

Riscrivi le sillabe trovate nel gioco sopra:

_ _

CYBERBULLISMO

#	SILLABA	PAROLA	DEFINIZIONE
1	_ _ _	___TITA	*Una gara sportiva tra due squadre o due giocatori*
2	_ _ _	FARFAL___	*L'insetto colorato con le grandi ali che vola di fiore in fiore*
3	_ _ _	___INTERRATO	*Il piano di un palazzo che si trova mezzo sotto il livello della strada*
4	_ _ _	___ZZO	*La cifra in euro che devi pagare per comprare qualcosa al negozio*
5	_ _ _	___SIGLIO	*Un suggerimento utile che qualcuno ti dà per aiutarti a scegliere*
6	_ _ _	___O	*Il numero che viene subito prima del due*
7	_ _ _	___LIANTE	*Un velivolo leggero senza motore che vola grazie alle correnti d'aria*
8	_ _ _	MO___O	*un foglio (di carta o anche digitale) con degli spazi da compilare scrivendo informazioni*
9	_ _ _	TRAMON___	*Il momento della sera in cui il sole scende e il cielo si tinge di rosso*

FRASE SEGRETA

Riscrivi le sillabe trovate nel gioco sopra:

_ _

PROTEGGI I NONNI DAI PERICOLI DEL WEB

1. WHATSAPP: ATTENTI AI FALSI NIPOTI

Se ricevi un messaggio da numero sconosciuto tipo "Nonna, sono io, ho cambiato numero", NON rispondere subito. Chiama tu al vecchio numero del nipote per verificare. I truffatori copiano foto profilo e nomi!

2. EMAIL SOSPETTE: MAI CLICCARE SUI LINK

Se arriva un'email dalla banca, dalla posta, dall'INPS con scritto "clicca qui urgente": NON cliccare mai! Le banche vere non mandano email con link. Cancella subito.

3. FACEBOOK: NON ACCETTARE SCONOSCIUTI

Se qualcuno che non conosci ti manda richiesta d'amicizia, anche se ha foto bella e profilo gentile: rifiuta. I truffatori creano profili falsi per studiare le tue abitudini.

4. LE VINCITE ONLINE NON ESISTONO

"Hai vinto un iPhone!", "Sei il visitatore numero 1000!": sono TUTTE truffe. Non cliccare, non compilare moduli, non dare dati personali. Chiudi la pagina.

5. SHOPPING ONLINE: SOLO SITI CONOSCIUTI

Compra solo su Amazon, eBay, siti di negozi veri che conosci. Se trovi offerte incredibili su siti mai sentiti: è truffa. Il prezzo troppo basso è sempre sospetto.

6. MAI DARE CODICI AL TELEFONO O PER MESSAGGIO

Se qualcuno (anche dicendo di essere della banca) ti chiede codici SMS, PIN, password: riattacca! Le banche NON chiamano mai per chiedere questi dati.

7. VIDEO E FOTO: OCCHIO ALLE BUFALE

Prima di condividere video "incredibili" o notizie "shock", chiedi a noi se sono vere. Il 90% delle cose che girano su WhatsApp sono false o vecchie di anni.

8. COMPUTER LENTO? NON CHIAMARE NUMERI A CASO

Se compare un messaggio "il tuo PC è infetto, chiama questo numero": è una truffa! Chiama noi o un tecnico che conosci di persona, mai numeri trovati online.

9. DONAZIONI ONLINE: SOLO ORGANIZZAZIONI VERIFICATE

Se vuoi fare beneficenza online, usa solo siti ufficiali di associazioni conosciute (Croce Rossa, Telethon, ecc). Mai mandare soldi a privati o raccolte fondi sconosciute.

10. PAGAMENTI ONLINE: CARTA PREPAGATA O PAYPAL

Se proprio devi comprare online, usa una carta prepagata con pochi soldi sopra, mai la carta principale. Se ti truffano, perdono solo quei pochi euro.

PROTEGGI I NONNI DAI PERICOLI DEL MONDO REALE

1. LA POLIZIA NON CHIEDE MAI SOLDI

Se qualcuno telefona dicendo "Sono il maresciallo, suo nipote ha avuto un incidente, servono soldi subito": è FALSO. Riattacca e chiama tu il 112 vero.

2. NON APRIRE LA PORTA AGLI SCONOSCIUTI

Tecnici del gas, controllori, postini che non aspetti: prima guarda dallo spioncino, poi chiedi documenti attraverso la porta CHIUSA, poi chiamaci per verificare.

3. AL BANCOMAT VAI SEMPRE DA SOLO

Se qualcuno ti "aiuta" al bancomat, ti sta probabilmente spiando il PIN. Rifiuta ogni aiuto, anche se sembrano gentili. Se serve aiuto, chiama la banca.



4. NESSUNO VIENE A CASA PER RITIRARE SOLDI

INPS, Agenzia delle Entrate, Comune, Banca: NON mandano MAI persone a casa a prendere soldi, gioielli o carte. Se viene qualcuno: porta chiusa e chiama 112.

5. CONTRATTI ALLA PORTA: MAI FIRMARE

Luce, gas, telefono, assicurazioni: mai firmare nulla con persone che suonano alla porta. Anche se insistono. Di' "devo parlarne con mio figlio" e chiudi.

6. IL TRUCCO DEL "SOLDO FALSO"

Al mercato o nei negozi, se qualcuno ti fa vedere una banconota dicendo "questa è falsa, me la cambi?": è una truffa per scambiare i soldi. Rifiuta sempre.

7. FALSE BENEFICENZE PER STRADA

Persone con pettorine che chiedono donazioni per disabili, bambini, animali: molte sono truffe. Dona solo a organizzazioni che conosci, non per strada a sconosciuti.

8. ATTENZIONE ALLE DISTRAZIONI

Una persona ti chiede l'ora, un'altra "ti è caduto qualcosa": mentre sei distratto, un complice ti ruba portafoglio. In gruppo: diffidate sempre.

9. FARMACI PORTA A PORTA: SEMPRE FALSI

Nessuno può vendere medicine per strada o porta a porta. Sono sempre prodotti inutili o pericolosi. Medicine solo in farmacia, con ricetta.

10. AL TELEFONO: NESSUNA INFORMAZIONE PERSONALE

Non dire mai: se sei solo in casa, dove tieni i soldi, quali carte hai, quando torni da un viaggio. Queste cose non servono a nessuno onesto.

Glossario di Cybersecurity per Bambini

Antivirus: Un programma speciale che protegge il tuo computer dai virus, come un "dottore" per il computer.

Avatar: L'immagine o il personaggio che usi per rappresentarti online nei giochi o sui social media.

Bug: Un errore o un problema in un programma del computer. Come quando un giocattolo non funziona bene.

Browser: Il programma che usi per visitare i siti web, come Chrome, Firefox o Safari.

Cyberbullismo: Quando qualcuno usa internet per essere cattivo o ferire i sentimenti di un'altra persona.

Chat: Una conversazione online con altre persone tramite messaggi di testo.

Crittografia: Un modo per trasformare messaggi in codici segreti così solo le persone giuste possono leggerli.

Download: Quando prendi un file da internet e lo salvi sul tuo computer o tablet.

Dati personali: Informazioni su di te, come il tuo nome, indirizzo o età, che dovrebbero rimanere private.

Firewall: Un programma che funziona come un guardiano, controllando chi può entrare nel tuo computer da internet.

Hacker: Una persona che usa il computer per entrare nei sistemi di altre persone. Alcuni hacker sono buoni e aiutano a trovare problemi di sicurezza, altri sono cattivi.

Internet: La grande rete che collega computer in tutto il mondo, permettendoci di condividere informazioni.

Link: È un collegamento che ti porta da una pagina web a un'altra. Può essere una parola, un'immagine o un pulsante su cui puoi cliccare. Quando lo premi, vieni "trasportato" in un altro sito, documento o contenuto online.

Password: Una parola o un codice segreto che usi per accedere ai tuoi account, come la chiave della tua casa digitale.

Phishing: Un trucco in cui qualcuno finge di essere una persona o un'azienda di cui ti fidi per rubare le tue informazioni.

Privacy: Il diritto di mantenere le tue informazioni personali al sicuro e decidere chi può vederle.

Social Media: Siti web e app come Instagram o TikTok dove le persone condividono foto, video e messaggi.

Spam: Messaggi o email indesiderati, spesso pubblicità, che possono contenere virus o truffe.

Virus: Un programma dannoso che può danneggiare il tuo computer o rubare informazioni, come un "raffreddore" per il computer.

Wi-Fi: Il sistema che permette ai dispositivi di connettersi a internet senza fili.

Partecipa al mondo di Attentionline Junior!

Hai idee per rendere il web più sicuro per i giovani navigatori? Sei un insegnante con suggerimenti per attività in classe? O forse sei un ragazzo con domande sulla sicurezza online? La tua opinione è importante!

Scrivici a junior@attentionline.it - insieme possiamo creare un internet più sicuro e divertente per tutti!