Ludoteca

Registro.it

Ma siamo sicuri?
A scuola di Cybersecurity

Il primo manifesto per la sicurezza online
dedicato alle studentesse e agli studenti

LE 10 REGOLE PER NAVIGARE CONSAPEVOLI E SICURI

1

SCEGLI CON CURA.

Il primo passo è quello di adottare password alfanumeriche complesse. Quelle semplificate possono compromettere la sicurezza dei tuoi dispositivi informatici.

Spesso per pigrizia o per mancanza di tempo quando ci viene richiesta una password inseriamo una "stringa" facile da ricordare: il nome di un parente o del cane, la nostra data di nascita, la sequenza 12345…, la stessa parola "password". **Nord Pass** ha fatto una ricerca **pubblicata alla fine del 2021** che individua le password più frequenti usate in moltissimi Paesi, tra cui l'Italia. Un elenco che dovremmo consultare per verificare che le nostre password non siano in quell'elenco. È possibile anche **verificare la robustezza delle nostre password**, per esempio qui o qui o in siti simili. La facilità con cui le password semplici possono essere violate, attraverso attacchi molto facili da attuare e chiamati di "forza bruta", è spaventosa e, per evitare una piccola fatica iniziale, rischiamo di consegnare la nostra vita privata e, a volte, i nostri beni a qualche malintenzionato. Certo, si dirà, ma **come faccio a ricordare password complesse?** Scriverle sulla propria agenda o sui post-it non è certamente una bella idea. Potrebbe convenire affidarsi a un **gestore di password** che oggi troviamo spesso "nativo" sia sui computer che su tablet e cellulari. Il gestore di password (Single sign on) si "ricorda" per noi le password di accesso ai siti e alle app, le conserva cifrate e ce le fa usare se immettiamo una sola password per accedere al gestore, la cosiddetta **"master password"**. Il problema quindi si riduce a dover memorizzare una sola password, la master password del gestore delle password. Nel caso in cui non si disponga di un gestore di password disponibile nel sistema operativo del proprio dispositivo conviene scegliere con cura quello da utilizzare, eventualmente anche tra quelli a pagamento. Un'alternativa ai classici meccanismi di autenticazione basati sul login sono i **sistemi di riconoscimento biometrici**, che utilizzano parametri fisici (impronte digitali, retina, volto) per identificare in modo univoco l'utente. Un altro strumento molto utile è la **doppia autenticazione** che si basa sulla combinazione tra il classico inserimento di nome utente e password e una chiave di sicurezza, come il codice inserito nel sms di verifica che arriva al proprio smartphone.

APPROFONDISCI CON I VIDEO

- "Non è mai troppo web": Le password (Ludoteca del Registro .it)
- La password del wifi (The Jackal)
- Biometria (Giacomo Giorgi Cnr-Iit)

2

CUSTODISCI GELOSAMENTE.

Password e codici di accesso non vanno condivisi con nessuno. Ricordati che corri il rischio di diventare vittima di truffe online o di hackeraggio a causa di una banale distrazione.

Abbiamo scelto **password complicate**, in modo che siano abbastanza sicure. Siamo stati bravi, ma bisogna porre molta **attenzione nel custodirle**: condividerle con un amico o con la fidanzata o con un compagno non è mai una buona idea, soprattutto perché, pur fidandoci, non sappiamo con quale cura la custodirà a sua volta. Senza contare che in futuro potremmo non fidarci più di quelle persone e, in questo caso, dovremmo cambiare tutte le password che avevamo condiviso. Pensiamo ad esempio alle **password di accesso ai nostri profili social**: se cadono nelle mani sbagliate, possono farci dire online cose che non pensiamo e che non ci appartengono, creando a noi **danni per la nostra reputazione** o anche ad altre persone coinvolte, che magari vengono offese attraverso un nostro profilo, caduto nelle mani di una persona non più fidata. Bisogna anche evitare di appuntarle in chiaro sull'agenda del telefono o di tenere un bigliettino con le password nel portafoglio: se portafoglio o telefono cadessero in mano a un ladro tutti i nostri accessi, compresi probabilmente, quelli al conto in banca sarebbero in mano al ladro.
Attenzione anche ad effettuare il **login a applicazioni o siti critici** (per esempio la nostra banca) utilizzando wi-fi pubblici e dunque reti non protette: le credenziali potrebbero essere facilmente intercettate da un hacker.

APPROFONDISCI CON I VIDEO

- Social engineering (Ilaria Matteucci Cnr-Iit)
- Come navigare in sicurezza (Giorgia Bassi Cnr-Iit)

3

PENSA PRIMA, CONDIVIDI POI.

Prenditi il tuo tempo: prima di rilanciare un contenuto, prima di mettere un like o un cuore, prima di pubblicare un selfie o postare un video rifletti bene e poniti una domanda: ne vale davvero la pena?

Istintivamente, **"scrollando" i social** ci fermiamo su qualcosa che ci colpisce e la commentiamo immediatamente anche solo con una "faccina" o con un **commento esplicito**, come se il nostro intervento fosse visibile solo all'autore di quel contenuto, dimenticandoci che almeno tutta la sua cerchia di contatti potrà vederlo, come pure contatti nostri e, se abbiamo commentato per esempio negativamente il comportamento di un amico comune, quest'ultimo potrebbe rimanerci male e il commento incauto può rovinare una relazione.
Esistono anche altre ragioni per **evitare di rendere pubbliche alcune informazioni**: per esempio se siamo in vacanza e postiamo immagini di un posto esotico e lontano dichiarando apertamente che abbiamo chiuso casa per due settimane, stiamo automaticamente avvisando qualche ladro abile con la rete che ha campo libero per agire indisturbato in casa nostra…

APPROFONDISCI CON I VIDEO

- Quando devi scegliere che foto pubblicare (The Jackal)
- Penso Parlo Posto (Libro di Parole_Ostili)

4

FAI ATTENZIONE.

Ricorda che in rete e sui social tutto è pubblico, anche quello che può sembrare privato. Perché i contenuti online hanno una viralità difficilmente prevedibile. Quindi stai attento a ciò che decidi di condividere.

Spesso sentiamo parlare di **"diritto all'oblio"** riferito alla rete. Vuol dire che **la rete ha una memoria indelebile** e qualunque cosa pubblichiamo può essere ritrovata anche dopo molto tempo. La rimozione di contenuti pubblicati è praticamente impossibile perché anche se viene rimosso quel post o quella pagina web non è detto che non possa riapparire, ripubblicata da qualcuno che l'aveva scaricata e conservata nel suo computer. È questa la ragione per cui **dobbiamo stare attenti nel postare o pubblicare**: dobbiamo essere sicuri di non avere mai ripensamenti. Questo è tanto più vero se siamo ancora giovani, portati magari a condividere sui social qualche avventura anche strana. Tra qualche anno un possibile datore di lavoro, cercando nostre notizie online, potrebbe imbattersi in situazioni che ci riguardano e che ora potrebbero imbarazzarci e metterci in difficoltà, creandoci un **danno di "reputazione"**, come nella vita reale, e con ricadute concrete nella vita reale: quel datore di lavoro potrebbe decidere che non siamo adatti a ricoprire una certa posizione.
Bisogna anche prestare **attenzione all'impostazione dei nostri profili social**: a meno che non siamo un personaggio pubblico, conviene configurare un profilo privato, accessibile solo a persone autorizzate da noi. Questo vuol dire, come conseguenza immediata, che prima di concedere l'accesso al nostro profilo, dobbiamo verificare chi sia la persona o la pagina che ce lo sta richiedendo: è conosciuta? è affidabile?

APPROFONDISCI CON I VIDEO

- Diventare cittadini digitali I e II parte (Luca Bechelli P4I)
- "L'internet, l'io, l'oblio" (Valentina Amenta - Cnr-Iit)

5

USA LA TESTA, NON LA PANCIA.

Non rispondere in modo impulsivo. Parla, scrivi, chatta, ma con consapevolezza. Le parole hanno un peso. Scegli di interagire in modo tale da evitare di alimentare tutto questo.

"Prima pensa, poi parla, perché parole poco pensate portano pena" è un'espressione proverbiale, che alcuni fanno risalire all'antica Grecia. Nonostante l'età, **"la regola delle 10 P**" è ancora attuale, anche per la nostra vita in rete. Nelle interazioni online siamo abituati a tempi brevi, risposte immediate, che ci impediscono di riflettere prima di pubblicare definitivamente il nostro pensiero o l'immagine che vogliamo condividere. Ci sembra di non poterne fare a meno, importante ribattere in una conversazione, far sapere subito cosa stiamo facendo o dove siamo. Inoltre nello scrivere e commentare in rete manca la componente "fisica": non abbiamo davanti l'interlocutore e per lui è impossibile percepire le nostre intenzioni dalle espressioni del corpo o del viso o dalla inflessione della voce, come per noi è impossibile percepire l'effetto di quello che stiamo dicendo o mostrando. La stessa frase, pronunciata con tono diverso, può essere ironica o seria. Nel leggerla questo effetto si perde quasi completamente, se non per la presenza di qualche "faccina" esplicativa. Nei rapporti umani, l'interazione fisica in una conversazione è una componente importante, benché istintiva. Per questo è importante **riflettere sull'effetto che può avere su chi legge quello che stiamo per pubblicare**, per rispetto degli altri.
I pionieri della rete si erano posti il problema della correttezza da mantenere nella comunicazioni in rete definendo la **"netiquette"** (la combinazione di network+etiquette).

APPROFONDISCI CON I VIDEO

- Webinar Vera Gheno sulla comunicazione sui social media
- Il Manifesto di Parole_Ostili

6

NON CADERE NELLA RETE.

Perché in rete le fake news si moltiplicano su siti poco affidabili, presentati con video coinvolgenti e con titoli acchiappaclic, rilanciati spesso inconsapevolmente da profili di amici e conoscenti.

Oggi siamo bombardati dalle informazioni, ma dedichiamo a ciascuna di esse pochissimo tempo: **i tempi della rete sono sempre minimi**, ogni contenuto deve essere comunicato velocemente. Questa è la ragione per cui spesso ci fermiamo a leggere solo il titolo e non l'intera notizia, non ci prendiamo il tempo per riflettere, analizzarla con un po' di spirito critico e magari cercare altre fonti per confrontarla. In particolare, è buona norma **controllare la data dei testi, cercare sempre informazioni sull'autore e diffidare di quelli pieni di errori grammaticali**. Questo è il meccanismo con cui funzionano e si diffondono le bufale o **"fake news"**: i loro autori fanno affidamento sulla velocità e superficialità con cui accettiamo i contenuti che ci vengono proposti e magari li ripubblichiamo. Chi li riceve da noi, se ci conosce e si fida, automaticamente penserà che siano affidabili e, a sua volta, contribuirà a diffonderla. È come un'ondata, che **potremmo fermare dedicando un po' di tempo a verificare quello che ci viene proposto**. Un buon metodo è **selezionare**, sulla base della propria esperienze, un insieme di fonti che nel tempo si sono dimostrate affidabili e fare riferimento a quelle in caso di dubbio (e facciamoci sempre venire il dubbio!)

APPROFONDISCI CON I VIDEO

- Le Fake news (Marinella Petrocchi - Cnr-Iit)
- Social media: falsi profili e bot (Marinella Petrocchi -Cnr-Iit)

7

AIUTA CHI È PIÙ IN DIFFICOLTÀ A COMPRENDERE SOCIAL E RETE.

Diventa anche tu un influencer delle buone pratiche e spiega a tua mamma o a tuo papà, ai tuoi nonni e agli amici le opportunità di Internet, ma anche i rischi connessi.

Si parla spesso di **gap digitale** tra generazioni ed è innegabile che i ragazzi siano quasi sempre più esperti degli adulti nell'usare la rete. **Sarebbe auspicabile che gli adulti** non si chiudessero in un rifiuto ma **accettassero** per una volta **di essere discenti dei ragazzi** invece di insegnare loro. Un'occasione per imparare a sfruttare un mezzo che offre grande opportunità e magari rinsaldare un rapporto personale che vada al di la' di chi impara e di chi insegna.
Ci sono anche casi in cui la difficoltà non è dovuta a una scarsa dimestichezza con la rete ma a qualche problema o rischio che ci troviamo ad affrontare, indipendentemente dalla nostra età: esiste **il bullismo in rete, il sexting, lo stalking, il revenge porn**, eccetera, problemi che coinvolgono profondamente a volte incontrollatamente chi ne è vittima. Anche in questo caso, chi ne è consapevole e ne è capace, può offrire aiuto all'amico in difficoltà.

APPROFONDISCI CON I VIDEO

- "Non è mai troppo web" (Ludoteca del Registro .it)
- "Protocollo boomer" (The Jackal)

8

NON FIDARTI!

I tentativi di phishing e di truffe cibernetiche vengono talvolta messi a segno attraverso account di amici e parenti, spesso hackerati. Quindi anche i tuoi contatti più stretti, senza volerlo, diventano diffusori di malware. Fidarsi è bene, non fidarsi è meglio.

La fiducia sta alla base dei nostri rapporti: accettiamo quello che ci dice un amico perché di lui ci fidiamo. Tendiamo a estendere questo comportamento anche quando siamo in rete: se un messaggio o una email ci arriva da un mittente che conosciamo, ci fidiamo e lo accettiamo. Purtroppo in rete mascherarsi è molto più facile che nella realtà ed è quello che fanno molti truffatori: si "travestono" da un mittente che è tra i nostri contatti (un amico, la banca. l'assicurazione, l'associazione benefica) e carpiscono la nostra fiducia, inducendoci a dare loro informazioni che dovrebbero restare riservate: password, codici di accesso ecc. Si tratta di un vero e proprio **attacco hacker** che va sotto il nome di **attacco di ingegneria sociale** (social engineering). Gli **attacchi di phishing** sfruttano questo comportamento e inducono i destinatari di un messaggio malevolo a compiere un'azione imprudente. Questi messaggi possono arrivare via email (e allora si tratta proprio di phishing) o per messaggio e in questo caso si parla di **smishing** o tramite una telefonata e prende il nome di **vishing.** Riconoscere un messaggio falso a volte è abbastanza facile, perchè magari è scritto male, in un italiano scorretto e questo dovrebbe insospettirci. Controllare bene l'indirizzo del mittente di una email è una buona tecnica di difesa e anche passare il mouse o il dito sul link al quale ci suggeriscono di collegraci può rivelare il vero indirizzo di destinazione che possiamo riconoscere come falso. Il phishing (e i suoi "derivati") non è l'unico tipo di truffa basata sul social engineering. Spesso ci sono **siti che riproducono esattamente nell'aspetto un sito a noi noto** (p.es. quello della banca) ma ne sono una copia, che noi interpretiamo come vera e accettiamo di inserire i nostri dati e le nostre informazioni private, cadendo nella trappola. Questo attacco si chiama **spoofing** e per evitarlo spesso è sufficiente controllare che l'indirizzo del sito sia veramente identico a quello della nostra banca.

APPROFONDISCI CON I VIDEO

- Qual è la differenza tra virus, malware e spyware? (Fabio Martinelli Cnr-Iit)
- Lo spamming (Giacomo Giorgi Cnr-Iit)
- Social engineering (Ilaria Matteucci Cnr-Iit)

9

ALZA LA MANO, MAI LE MANI.

Chiedi aiuto a chi ne sa più di te se pensi di trovarti in una situazione di rischio a causa delle interazioni in rete. Hai a disposizione un indirizzo sempre presidiato: vai su Commissariatodips.it e mettiti in contatto con gli operatori della Polizia Postale e delle Comunicazioni.

La rete offre grandi opportunità ma presenta anche **zone di rischio**. Gli adulti sono meno consapevoli dei meccanismi che attivano i rischi ma probabilmente avrebbero gli strumenti per affrontarli, derivanti dall'esperienza. I ragazzi, invece, quasi sempre individuano la fonte di un possibile rischio ma non sempre hanno gli strumenti per gestire il pericolo a cui si trovano esposti, proprio a causa della giovane età. In entrambi i casi **è necessario un aiuto** e, in alcuni casi, è proficua una interazione, uno scambio tra chi capisce da dove viene il rischio e chi è in grado di affrontarlo da un punto di vista emotivo, sociale e pratico. Per questo, **in rete** (come nella vita reale) **è importante saper chiedere aiuto** e sapere a chi chiedere aiuto. Può essere un amico più esperto, un adulto se il pericolo riguarda un ragazzo o un giovane se chi è esposto è un adulto poco "smart". Nei casi più complicati, in cui ci si trova davanti a veri e propri reati (cyberbullismo, pedopornografia, revenge porn, stalking ecc.) è bene **rivolgersi alla polizia postale**, sia che siamo adulti sia che siamo ragazzi. Sul sito del Commissariato di Pubblica Sicurezza è possibile segnalare un possibile reato. Reagire direttamente, online o anche di persona, non è sempre una buona idea anche perchè non sempre sappiamo chi sta veramente interagendo con noi.

10

TIENITI AGGIORNATO SUI RISCHI CHE SI CORRONO QUANDO SI NAVIGA.

Cerca di cogliere i segnali che arrivano dagli esperti e impara ad essere prudente, a non fidarti ciecamente dei link condivisi e a ragionare prima di cliccare.

In rete tutto corre veloce, tutto cambia rapidamente, anche le tecniche di attacco e i tipi di truffe. Per stare al passo, bisogna **tenersi aggiornati** e lo si può fare proprio tramite la rete. Bisogna anche **tenere aggiornati i dispositivi, dal sistema operativo, alle applicazioni, agli anti virus** poichè spesso gli aggiornamenti contengono delle correzioni al codice (patch) che permettono di superare alcune vulnerabilità. È raccomandabile inoltre **selezionare le fonti affidabili** che, monitorate nel tempo, ci danno garanzia di essere credibili; possono essere siti di informazione, soprattutto quelli dedicati alla tecnologia e alla rete, le pagine di alcuni esperti, siano esse siti, blog, canali social ecc.,
siti di formazione autorevoli, su cui imparare le nozioni necessarie. **L'aggiornamento è la chiave di "sopravvivenza" in rete** ed è affidata per la maggior parte all'iniziativa personale: esistono alcune iniziative dedicate a diffondere la conoscenza della cybersecurity nelle scuole (come ad esempio la Ludoteca del Registro .it, promotrice di questo manifesto) e tra i cittadini, anche a cura di associazioni e organizzazioni no profit.

APPROFONDISCI CON I VIDEO

- Informarsi in rete (Sonia Montegiove, informatica, giornalista, divulgatrice)
- La Cybersecurity (Registro .it)